L'Odyssée de Whally

Les chroniques numériques de Whaller

Whaller blog

Sommaire

Introduction

« L'Odyssée numérique de Whally » vous offre une plongée dans le monde fascinant de la souverai neté numérique et de la cybersécurité. C'est une invitation à explorer les différentes facettes de la transformation numérique et de comprendre ses impacts sur différents secteurs d'activité. Nous partageons avec vous, à travers ces pages, les expériences et les enseignements tirés de l'année 2023, année riche en évolution technologique et en défis de sécurité numérique.

« L'Odyssée numérique de Whally » est conçu pour vous accompagner partout, devenant ainsi une source d'inspiration et d'information constante dans un monde digital en perpétuelle mutation. Alors que nous laissons derrière nous une année de transformations majeures, nous observons comment des technologies telles que la blockchain, l'intelligence artificielle et les plateformes collaboratives comme Whaller ont non seulement façonné les modes de travail, mais ont également joué un rôle crucial dans la protection des données et la gestion de la souveraineté numérique.

« L'Odyssée numérique de Whally » met un accent particulier sur l'importance de la souveraineté numérique dans un monde où les données sont devenues un actif précieux. Il examine comment des outils comme Whaller peuvent aider les organisations à renforcer leur sécurité, à améliorer la collabo ration et à innover dans la manière de travailler à distance.

En ces temps de digitalisation accélérée, impulsée par des circonstances mondiales sans précédent, nous avons cherché à répondre à vos questions et à vous offrir des solutions pratiques pour naviguer avec succès dans l'univers numérique. Ce Blog Book est un guide essentiel pour quiconque souhaite comprendre et s'adapter aux changements rapides dans le domaine de la technologie et de la cyber sécurité.

Nous vous invitons à rejoindre cette aventure passionnante et à participer à la prochaine édition de « L'Odyssée numérique de Whally » en partageant vos expériences et vos idées avec nous, en nous écrivant à l'adresse mail suivante : marcom@whaller.fr

Bienvenue dans le monde de Whaller, où l'innovation numérique rencontre la souveraineté et la sécu rité !

L'équipe Whaller

L’histoire de Whaller

Crée en 2013 par Thomas Fauré, Whaller est une plateforme française de réseaux sociaux et collabo-ratifs sécurisés. Pendant 5 ans, Whaller a été une filiale du groupe Bolloré. En juin 2018, nous avons pris notre indépendance. Nous nous efforçons de faire émerger des solutions souveraines et indé-pendantes pour proposer des leaders forts face aux GAFAM et BATX.

En quelques chiffres :

- + 20 collaborateurs,
- 1 000 000 utilisateurs,
- + 200 clients,
- + 10 expériences,
- 1 déploiement par jour.

A propos de Whaller

La cybersécurité à l'ère de l'hyperconnexion

Une vision proactive

Dans l'ère numérique où nous naviguons, la cybersécurité est devenue un sujet de premier plan, touchant aussi bien les entreprises que les individus. En tant que directeur de la Cybersécurité chez Whaller, il me parait essentiel d'être dans une posture de veille permanente , afin d'une part, d'identifier les nouveaux modes opératoires des attaquants, mais aussi de faire évoluer nos dispositifs de protection

La cybersécurité n'est plus un sujet confiné aux départements IT ; elle est désormais omniprésente, impactant chaque aspect de notre vie digitale. Les menaces évoluent rapidement, exploitant les failles dans nos systèmes et nos comportements. Face à cela, notre réponse ne peut être que dynamique et adaptative. Les entreprises, quelle que soit leur taille, doivent adopter une posture proactive, intégrant la cybersécurité dès la conception de leurs produits et services. Cela va au-delà de la simple mise en place de solutions technologiques ; il s'agit d'une démarche globale impliquant tous les niveaux de l'organisation. Cependant, elle conduit aussi à l'humilité car en dépit des meilleurs efforts, le système sûr à 100% n'existe pas.

Dès lors que nous utilisons des services numériques, nous devons être vigilants. Les cyberattaques les plus courantes ciblent, souvent par facilité, l'utilisateur final, exploitant des lacunes dans la sensibilisation ou la négligence. Elles peuvent se déclencher autant dans le monde numérique que dans le monde physique (attaque par Quishing). L'acculturation à l'hygiène numérique est donc essentielle et doit être permanente.

Enfin, l'aspect collaboratif de la lutte contre les cybermenaces est crucial. Le partage d'informations sur les menaces sur les modes opératoires des attaquants, les bonnes pratiques s'avère être indispensable afin de rendre les attaques plus couteuses. Les cybercriminels ne se privent pas de partager de l'information sur leurs victimes, il est donc évident qu'il doit en être de même du côté de la défense.

En somme, une cybersécurité efficace nécessite une vigilance constante et une adaptation rapide aux nouvelles menaces. Chez Whaller, la cybersécurité fait partie de notre ADN et ne souffre aucune discussion dans la mise en œuvre des bonnes pratiques.

Cyril Bras
Directeur cybersécurité
Whaller & VP Hexatrust

Décrypter la cybersécurité

Cybersécurité

Cyril Bras, directeur de la Cybersécurité au sein de Whaller, nous décrypte la cybersécurité.

Qu'est-ce la Cyber Resilience ?

La résilience, ce sont toutes les mesures qui vont me permettre de mieux faire face à une situation anormale. Par exemple, je suis victime d'une inondation, j'ai un étage, je monte tous mes meubles à l'étage et quand l'inondation est finie, je peux redescendre mes meubles. La Cyber Resilience, ça va être la même chose mais du point de vue numérique, c'est "qu'est-ce que je fais en amont ?", "Quelles mesures je prends pour me prémunir d'une cyberattaque ?

Par exemple, je vais faire des sauvegardes et je vais m'assurer que ces sauvegardes ont fonctionné. Je vais avoir un inventaire de mon parc, je sais quel serveur, quelles ressources, quel logiciel j'utilise. Je vais avoir tout un ensemble de mesures organisationnelles en place pour que le jour où un incident survient, je ne sois pas à la recherche d'informations pour recréer mon infrastructure ou redémarrer mon service à minima pour, à terme, revenir à une utilisation nominale.

Qu'est-ce qu'un « Firewall » ?

Un "Firewall" ou "Pare-feu" en français, c'est un équipement en réseau physique. Mais maintenant on se rend compte qu'un pare-feu, ça peut être aussi un logiciel qui vise à protéger la ressource informatique des accès malintentionnés. Je vais avoir ne serait-ce que moi, ma maison, j'ai mon ordinateur et bien je vais avoir un pare-feu qui va être installé dessus pour empêcher que des gens s'introduisent dans ma machine et aussi pour limiter ce que ma machine envoie par l'extérieur.

Dans une entreprise, je vais avoir un pare-feu en entrée, en coupure, entre la connexion Internet et mes serveurs. Sur ce pare-feu, je vais écrire des règles qui vont dire par exemple que j'autorise les personnes de l'extérieur à venir consulter mon site web. En revanche, les personnes de l'extérieur ne peuvent pas aller sur un autre serveur. De la même façon, le pare feu va aussi embarquer des mesures de sécurité. Par exemple, il peut y avoir un antivirus à l'intérieur, il peut faire de l'analyse de trafic Internet. Ce qui fait que mes utilisateurs dans mon entreprise, lorsqu'ils vont vouloir sortir sur Internet, toutes leurs requêtes vont être analysées par le pare feu qui va oui ou non, les laisser sortir en fonction des mesures de sécurité qui auront été définies.

Qu'est-ce qu'un antivirus ?

L'antivirus, c'est un logiciel que l'on va installer sur un serveur, sur un poste de travail ou même sur un pare-feu afin de détecter des codes malveillants. Les codes malveillants, qu'est-ce que c'est ? Ce sont des programmes informatiques qui ont une finalité malveillante d'exfiltrer de l'information, de chiffrer de la donnée pour me réclamer une rançon derrière, ou bien tout simplement de la détruire ou même de détruire physiquement du matériel. Un antivirus à l'heure actuelle, il n'y a aucun équipement qui ne devrait se trouver sans antivirus. Il n'y a pas de système qui n'a pas de menaces vis-à-vis des codes malveillants.

Que ce soit un ordinateur Windows, que ce soit un Mac, que ce soit un Linux, peu importe, tous ces systèmes-là sont infectés par des virus. Il y avait une légende urbaine d'ailleurs, qui consistait à penser que les systèmes Mac n'étaient pas concernés par les virus, qu'il y en avait très peu. Il se trouve que c'est vraiment totalement faux puisque l'année passée il y a eu plus de code malveillant développé pour les Mac que pour Windows. Donc c'est vraiment une belle illustration.

Un antivirus, ça ne peut pas être gratuit parce qu'encore une fois, "si c'est gratuit, c'est vous le produit". Il suffit de regarder dans la presse où l'on se rend compte qu'il y a eu déjà des cas où les données ont été revendues derrière. Il y a vraiment une nécessité d'être mis à jour fréquemment. Fréquemment c'est-à-dire plusieurs fois par jour, une fois par heure, etc. Une version gratuite, au mieux on aura une mise à jour par jour, donc ça sera très largement insuffisant pour avoir une idée du volume que ça représente ces codes malveillants. Tous les jours, on a plusieurs millions de nouveaux virus qui sont créés et petit à petit, l'antivirus est capable de les détecter car ce sont des virus déjà connus et tous les jours il reste 3000 nouveaux virus totalement inconnus. C'est vraiment important d'avoir quelque chose qui va être capable d'éliminer tous ces virus et de souscrire un abonnement auprès d'un fournisseur.

En termes de choix, tout dépend si on a à cœur la souveraineté ou pas. Il y a des opérateurs européens, des opérateurs américains et des opérateurs russes. Tout dépend à qui on souhaite accorder sa confiance sur la détection de codes malveillants.

Qu'est-ce qu'une plateforme MISP ?
MISP c'est un logiciel qui permet de partager des IOC. Les IOC sont des indices de compromission, des artéfacts techniques qui correspondent à des tentatives d'intrusion, à des attaques avérées, mais des marqueurs, c'est-à-dire que si je les analyse, si je les reprends dans un autre environnement, si je les trouve chez moi. Ça veut dire que potentiellement, mes serveurs, mes ressources ont été attaqués et peut-être ont été compromis.

Chez Whaller, nous avons décidé de déployer ce type de plateforme pour accumuler de l'informations parce que nous avons des serveurs qui sont attaqués tous les jours et nous avons des signatures d'attaques qui sont intéressantes, de cumuler pour nous pour pouvoir savoir qui nous veut du mal. Nous avons décidé de les partager avec nos clients et nos partenaires afin de les aider en leur donnant ces éléments-là.

Si vous les retrouvez chez vous, peut-être potentiellement vous avez été attaqué et ça serait bien de chercher à savoir si c'est vrai ou pas.

Qu'est-ce qu'un « pentest » ?

L'objectif de ces tests d'intrusion, c'est de rechercher les vulnérabilités sur un système. Nous définissons un périmètre que nous voulons tester, par exemple, les serveurs de l'entreprise. Nous allons tout d'abord effectuer une recherche sur les services exposés sur Internet. Une fois que nous avons énuméré tous ces services-là, nous les avons identifiés.

Nous allons utiliser des outils qui vont spécifiquement tester ces services pour savoir s'ils sont à jour, si j'ai mis des mots de passe robustes, s'il n'y a pas des erreurs de configuration, "est ce que je n'ai pas laissé la configuration par défaut" ?

Donc trouver un point d'entrée sur ces services-là.

Le pentest, ça peut être aussi de l'intrusion physique. C'est-à-dire que si je me rends compte que par Internet je ne peux pas accéder à une ressource, elle est bien protégée, il y a un pare-feu, il y a des règles qui font que c'est compliqué d'y arriver. Je vais voir si par l'environnement physique, je ne peux pas m'introduire sur ce serveur. Pour cela c'est soit je m'introduis physiquement dans les locaux de la structure où l'on fait le pentest, j'essaye d'aller sur le serveur, brancher une clé USB, brancher un implant informatique qui va me donner un accès à distance ou bien m'appuyer sur la vulnérabilité humaine en jetant des clés USB devant l'entrée de l'entreprise afin de voir qui va prendre ces clés USB les range sur son ordinateur pour me donner accès au système d'information.

Qu'est-ce que représente la qualification SecNumCloud ?

La qualification SecNumCloud a été créée il y a quelques années par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) afin d'obliger les fournisseurs de services cloud à respecter un certain nombre de mesures de sécurité afin de garantir à leurs clients un usage en confiance de leurs technologies et des services qu'ils proposent.

SecNumCloud, c'est aussi la garantie que les données sont hébergées en France. C'est une des obligations à respecter, les serveurs doivent être en France et ne pas être soumis à des lois extraterritoriales.

Qu'est-ce que le RGPD ?

Le Règlement Général de Protection des Données (RGPD), c'est un règlement européen qui a été mis au point en 2016 par la Commission européenne, qui a demandé aux États membres de le transposer dans leurs législations nationales et avec une entrée en vigueur prévue le 25 mai 2018.

Concrètement, à quoi ça correspond ? L'idée, c'est de protéger les données des citoyens européens, quel que soit l'endroit où ces données sont localisées. Si elles sont sur un serveur en France ou un serveur aux Etats-Unis, le RGPP va s'appliquer.

De quoi parle le RGPD ? Il aborde deux critères. Le premier, c'est que la sécurité doit être là par conception, c'est-à-dire que lorsque je mets en place une solution, elle doit embarquer des mesures de sécurité, elle doit être à l'état de l'art. Je ne peux pas me permettre d'avoir des serveurs pas à jour, d'avoir des mots de passe triviaux, etc.

Le second élément, c'est de garantir la confidentialité par défaut. C'est le nerf de la guerre. C'est de faire en sorte que ces données-là, elles ne soient pas librement accessibles auprès de n'importe qui, n'importe quel internaute.

Le RGPD, va également demander le consentement des citoyens. C'est-à-dire que lorsque je donne des données me concernant, on doit me demander mon avis, on doit me dire ce qu'on va en faire. Ce n'est pas un libre accès à mes données et un usage sans mesure.

L'autre élément aussi, c'est qu'il y a eu un changement entre temps, quand ce RGPD est arrivé, en France, nous avions la loi informatique et liberté qui cadrait déjà ce que nous pouvions faire avec les données personnelles. Le RGPD est venu un peu modifier le rôle de la Commission nationale de l'informatique (CNIL) et des libertés qui est l'organe en charge de l'application du RGPD en France et qui est passé d'un organe qui va s'assurer que c'était à peu près bon, à maintenant nous vous faisons confiance. Vous avez de votre côté vous désignez une personne qui va être le délégué à la protection des données, qui va avoir la charge de référencer tous les traitements de données qui sont dans l'entreprise.

Le jour où un incident survient, c'est lui qui va servir d'interlocuteur avec la CNIL pour expliquer ce qui s'est passé et quelles données ont été affectées. Est-ce que ces données étaient bien correctement enregistrées dans son registre de traitement ?

Qu'est-ce qu'un VPN ?

Le VPN – Virtual Private Network, c'est une technologie qui, en anglais, signifie un réseau privé virtuel et qui a pour objectif de créer un tunnel entre un poste client, un ou plusieurs postes client, et un nœud de communication, en général le serveur à un serveur de l'entreprise.

L'idée de tunnel VPN c'est que lorsque je le lance, toute ma navigation, tout ce que je vais faire va être cachée vis-à-vis d'Internet va être envoyée dans ce tunnel qui est un tunnel chiffré et toutes les données seront véhiculées de façon transparente vers le point de sortie.

L'autre avantage aussi du VPN, c'est que le poste client se retrouve dans la même situation que s'il était physiquement dans les locaux de l'entreprise. De ce fait, toutes les mesures de sécurité qui sont mises en œuvre au quotidien pour protéger l'accès aux ressources, l'accès à Internet, le collaborateur qui se retrouve en situation de nomadisme va bénéficier des mêmes avantages, des mêmes protections.

Que valent nos données personnelles ?

Cybersécurité

Il est aujourd'hui pratiquement impossible d'éviter de divulguer au moins certaines de vos données personnelles. Chaque fois que vous visitez un site web, utilisez les médias sociaux, acceptez les conditions générales, vous inscrivez à un formulaire ou approuvez les cookies, vos données sont collectées.

Pour posséder ces données, les entreprises du numérique sont prêtes à payer afin d'obtenir un avantage concurrentiel en offrant un niveau de personnalisation de leurs produits et de leurs services comme cela n'a jamais été vu auparavant. Par exemple, l'algorithme de Spotify vous propose des artistes et des listes de lecture en fonction de votre âge, de votre sexe, de votre localisation et de votre historique d'écoute. Pour y parvenir, l'application s'est appuyée sur les données personnelles de l'internaute. Autre exemple : il est dans l'intérêt d'Amazon de nous encourager à parcourir son site, même si nous n'achetons rien. L'historique des éléments consultés, les mots-clés utilisés ou le temps passé sur une page, peuvent tous être monétisés.

Aussi, sources de profits potentiels, les données personnelles sont surnommées le nouvel or blanc. En 2020, on estime qu'une personne type a créé 1,7 mégaoctets de données chaque seconde de chaque jour.

Mais qu'appelle-t-on nos « données personnelles », qui les exploite et comment sont-elles évaluées, autant de questions auxquelles nous allons tenter de répondre.

Qu'est-ce qu'une donnée personnelle ?

Les données personnelles sont « toute information permettant d'identifier directement ou indirectement une personne physique » selon la Commission Nationale de l'Informatique et des Libertés. Elles peuvent être divisées en quatre catégories :

Données personnelles : elles concernent les informations personnellement identifiables, telles que le numéro de sécurité sociale et le sexe, votre adresse IP, les cookies du navigateur web et les identifiants de l'appareil (que votre ordinateur portable et votre appareil mobile possèdent) ;
Données d'engagement : ces données concernent la manière dont les consommateurs interagissent avec le site web d'une entreprise, les applications mobiles, les messages texte, les pages de médias sociaux, les e-mails, les publicités payantes ;
Données comportementales : cette catégorie fait référence aux détails transactionnels tels que les historiques d'achat, les informations sur l'utilisation du produit (par exemple, les actions répétées) et les données qualitatives (par exemple, les informations sur les mouvements de la souris).
Données attitudinales : ces dernières mesurent la satisfaction du consommateur, les critères d'achat, la désirabilité du produit, etc.

Comment nos données personnelles sont-elles utilisées ?

La manière dont vos données sont utilisées et valorisées dépend du profil et des objectifs de ceux qui les utilisent. Nous pouvons distinguer quatre types de grands utilisateurs : les GAFAM et les plateformes, les entreprises, les services publics et les organisations malhonnêtes.

Les GAFAM (Google, Apple, Facebook, Amazon et Microsoft) et les plateformes (comme Twitter, LinkedIn ou YouTube), qui offrent aux utilisateurs un endroit pour créer leur propre contenu, utilisent les données comme monnaie d'échange pour soutenir leurs ventes publicitaires. Parce que leurs services sont utilisés par des centaines de millions d'utilisateurs chaque jour, ils génèrent des milliards de dollars de revenus annuels en les exploitant, en les vendant (via un data broker) ou en les échangeant contre d'autres données.

Les entreprises sont, elles, prêtes à investir des milliards dans la publicité, car les données collectées permettent de garantir que le bon message touchera le bon public au bon moment. Ainsi, elles peuvent cibler et ajuster très finement leurs produits, leurs services et leurs communications pour assurer un haut retour sur investissement.

Les services publics ne sont pas en reste, qui, eux aussi analysent les données connectées pour améliorer la qualité de leurs missions.

Enfin, les organisations malhonnêtes (ou criminelles) volent des données personnelles pour diverses raisons (chantage, usurpation d'identité, extorsion), mais la plus courante consiste à vendre ces informations à quiconque est prêt à payer. Ces acheteurs sont souvent d'autres organisations criminelles, des courtiers en données, et même des gouvernements étrangers. Parce que le vol est facile, peu cher et sans conséquence, ceux qui les font peuvent souvent vendre les données volées à un prix nettement inférieur à celui d'une plateforme ou d'un courtier en données.

Combien valent les données personnelles pour les entreprises ?

Actuellement, il n'existe aucune formule reconnue mondialement pour identifier la valeur de nos informations personnelles. Néanmoins, des études montrent que la valeur dépend d'abord du sexe et de l'âge. Par exemple : les entreprises sont prêtes à dépenser plus pour acquérir les données des hommes plutôt que celles des femmes ou bien les entreprises sont prêtes à payer plus pour les données des 18-24 ans que pour celles des 25-34 ans. En outre, les informations d'évolution majeures dans la vie d'une personne, comme se fiancer, devenir parent, déménager, acheter une voiture, sont parmi les données les plus chères car elles entraînent des changements dans les habitudes d'achat.

D'une manière générale, il ressort de toutes les études que les données personnelles de base sur un individu (par exemple, l'âge, le sexe et le lieu) ne valent que 0,0005 € par personne (c'est-à-dire 0,50 € pour mille personnes). Les informations financières sur un individu (tels que l'historique des paiements récents ou les détails de santé) sont légèrement plus précieuses.
Dans le cas de Facebook, la valeur moyenne des données d'un utilisateur actif pour Facebook est d'environ moins de 2 euros par mois. Par ailleurs, les revenus publicitaires de Google sont un bon indicateur de la valeur des données personnelles. En 2020, chaque utilisateur a généré environ 26 euros.

Néanmoins, il existe une autre estimation de la valeur des données personnelles. Selon les données d'une enquête de CouponBirds, un site web d'informations états-unien sur les coupons et les consommateurs, l'acheteur américain moyen serait prêt à vendre ses données personnelles pour 1 452,25 $. En ventilant les données par État, il est apparu que les habitants du Colorado demanderaient 2 800 $ contre 623 $ pour les habitants du Tennessee. In fine, il reste une question en suspens : quel que soit l'État, est-ce le juste prix ? Comme nous l'avons vu plus haut, il est impossible de répondre à cette question, les données de certaines personnes valant plus que d'autres.

Une autre manière de tente de connaître la valeur des données a été de poser la question aux internautes, combien faudrait-il payer une personne pour qu'elle cesse d'utiliser Google. La réponse est 17 500 dollars par an, et plus de 500 dollars par an pour l'amener à désactiver son compte Facebook.

Il faut se souvenir d'un dicton à propos du monde numérique : « Si vous ne payez pas le produit, alors vous êtes le produit ». La conséquence est que de nombreux services que nous utilisons « gratuitement » sur le web gagnent de leur argent en fournissant des données personnelles aux annonceurs. Cela veut donc bien dire que vos données sont disponibles, qu'elles ont de la valeur et qu'elles sont probablement plus précieuses que vous ne le pensez.

Afin d'en avoir le cœur net, le Financial Times a programmé une calculatrice interactive qui aide à calculer la valeur des données personnelles d'un individu. Elle propose de recueillir pour faire son calcul des informations comme les données personnelles (âge, sexe, etc.), antécédents familiaux, état de santé, achats en ligne, ainsi que son goût pour des activités. Cependant, elle n'englobe pas de très nombreux détails que les spécialistes du marketing recueillent pour profiler les individus.

Alors, combien valent vos données personnelles ? Faites le test.

Shikitega, le code malveillant furtif qui cible les systèmes Linux

Cybersécurité

Si pendant de nombreuses années, les défenseurs du système d'exploitation Linux se louaient de l'absence relative de codes malveillants a ectant ce système, tout ceci a commencé à voler en éclat dans le dernier trimestre de 2021. Cependant cette légende perdurant encore de nos jours, la proportion de code malveillants Linux est peut-être sous-estimée aussi en raison du faible taux d'équipement de ces serveurs en solutions antivirales.

En septembre 2022, un groupe de chercheur en Cybersécurité de chez AT&T découvre un nouveau code malveillant furtif ciblant explicitement les systèmes Linux, il fut nommé Shikitega. Ce code utilise des vulnérabilités pour se propager sur les systèmes notamment les CVE-2021-4034 et CVE-2021-3493 ; on remarque alors des vulnérabilités datant de 2021 ! Comme l'a récemment évoqué l'ANSSI dans son panorama de la Cybermenace de 2022, bon nombre d'incidents observés par l'agence ont pour origine l'exploitation de vulnérabilités anciennes, connues et corrigées.

Il n'y a donc rien d'étonnant à ce qu'un code malveillant utilise de vieilles failles. Pourquoi alors rédiger un article sur ce code malveillant ? Et bien tout simplement pour partager des éléments qui ont permis à la direction Cyber de Whaller de détecter comment un attaquant a essayé de déployer ce code sur certains de nos serveurs.

Grâce aux éléments mis à disposition par le CERT-FR, il est possible d'écrire des règles de détection lors de l'analyse des journaux d'activité. En partant du bulletin CERTFR-2021-ALE-022 qui traitait des vulnérabilités CVE-2021-45046 et 45105 concernant LOG4J, il est possible de rechercher certains motifs contenus dans les URL et les User-agent : ${jndi: ainsi que $%7Bjndi:

Comment fonctionne le code malveillant Shikitega ?

La première alerte a été activée par une tentative d'exploitation de vulnérabilité Log4J.

Nous retrouvons dans le user-agent le pattern communiqué par le CERT-FR ${jndi:

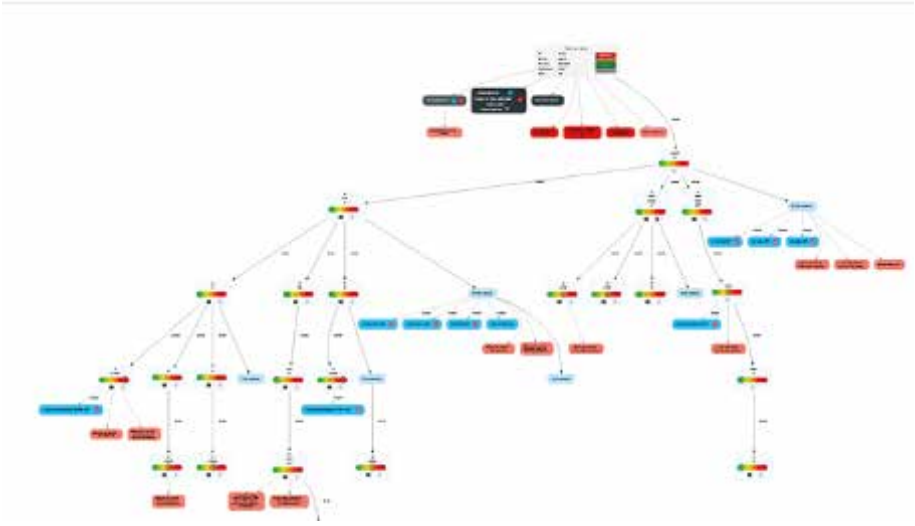
Continuons nos investigations du code malveillant, le user-agent contient une chaine encodée en base64 voyons quelles informations l'on obtient en la décodant.

Il s'agit donc de l'exécution de la commande wget qui permet le téléchargement d'une ressource. La vulnérabilité Log4J est résumée par le CERT-FR par :
« *Cette vulnérabilité permet à un attaquant de provoquer une exécution de code arbitraire à distance s'il a la capacité de soumettre une donnée à une application qui utilise la bibliothèque log4j pour journaliser l'évènement. Cette attaque peut être réalisée sans être authentifié, par exemple en tirant parti d'une page d'authentification qui journalise les erreurs d'authentification.* »
Le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR)

Ainsi, ce code exécuté sur un serveur vulnérable permettra le téléchargement du fichier pwer, son exécution, puis sa suppression. L'analyse du fichier montre qu'il s'agit d'un exécutable.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	7F	45	4C	46	01	01	01	02	03	01	54	80	04	08	34	34	▮ELF▯▯▯ ▯▯T▮▯▯44
00000010	20	0D	0A	01	01	80	04	08	80	04	08	F2	04	90	20	07	. . ▯▯▮▯▯ ▮▯▯č▯ .▯
00000020	10	DB	DD	D9	74	24	F4	BD	90	40	08	AD	5A	29	C9	66	▯ÛÝÙt$ôM ▯@ -Z)Éf
00000030	B9	21	01	31	6A	1A	83	C2	04	03	6A	86	A2	FD	C7	AD	¹!▯ 1j▯ ▮Â▯▯ j▮¢ýÇ-
00000040	7A	67	45	D7	12	BA	20	9E	04	AC	E2	D3	A2	2D	95	93	zgE×▯ º. ▮▯ -âÓ¢-▮▮
00000050	72	E4	B2	34	15	9C	41	E5	87	39	D2	D6	33	AF	69	06	rä²4▯ ▮Åå▮9ÒÖ3¯i▯
00000060	CF	46	E0	39	57	B8	D1	CA	87	95	46	0D	0A	20	E7	93	ÏFà9W¸ÑÊ▮▮F. . ç▮
00000070	F9	3F	D8	2F	97	CF	20	BC	0E	5E	37	3A	EA	BE	D4	D2	ù?Ø/▮Ï ¼▯ ^7:ê¾ÔÒ
00000080	61	D0	7E	02	4D	19	48	62	9E	13	D7	10	CF	AF	7A	A4	aÐ~ ▯M▯Hb▮▯ ×▯ Ï¯z¤
00000090	20	23	EC	2A	5E	BB	D5	92	C3	5E	0D	0A	20	ED	25	C1	#ì*^»Õ'Ã^ ▯▯ í%Á

L'exécution en environnement bac à sable sur JoeSandbox montre une multitude d'itérations avec de nombreux programme téléchargés et exécutés.



A l'issu de ces itérations, la machine est compromise par Shikitega.

En guise de conclusion, avoir des systèmes à jour et regarder régulièrement ses logs sont des étapes indispensables pour se prémunir de tout code malveillant.

La gestion des risques cyber dans les entreprises

Cybersécurité

Les entreprises dépendent de plus en plus des technologies numériques dans l'exercice de leurs missions. Qu'il s'agisse des directions commerciale, financière, industrielle ou des ressources humaines, tous leurs services ont été digitalisés. L'objectif est de maximiser la vélocité, l'agilité, l'effi - cité et la rentabilité de ces derniers.

Néanmoins, si pour l'écrasante majorité des décideurs la digitalisation est une priorité, à mesure que celle-ci s'accroit, les cyberattaques se développent concomitamment. En effet, les hackers utilisent des technologies de plus en plus sophistiquées pour mener à bien leurs attaques mais s'appuient aussi sur des failles béantes dans les systèmes.

Afin de vous aider à identifier les risques cyber – c'est-à-dire à diminuer autant que faire se peut vos vulnérabilités – nous avons dressé la liste des 10 menaces les plus courantes auxquelles vous êtes exposés.

1. Rançongiciels et logiciels malveillants

Le rançongiciel, ou ransomware, consiste en l'introduction sur le système d'information de la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange de la clef de déchiffrement. Le paiement de la rançon ne garantit en aucune manière l'obtention de la clef. L'impact d'une telle attaque affecte la productivité de l'entreprise, les temps d'arrêt du système, le coût de la reconstruction des systèmes et du remplacement du matériel.

Pour s'en prémunir, il convient de sauvegarder le patrimoine informationnel régulièrement et de contrôler que les sauvegardes fonctionnent. Le déploiement d'un antivirus sur l'intégralité des machines (postes utilisateurs, serveurs smartphones…) permettra également de détecter plus facilement les logiciels malveillants.

2. Attaques de terminaux

En plaçant leurs ressources dans le cloud et en autorisant leurs collaborateurs de plus en plus souvent à utiliser des postes de travail à distance, les entreprises ont augmenté leur exposition à des risques cyber.

Le défi est, là, de savoir comment sécuriser au mieux ces systèmes hors site et ces appareils distants. Plusieurs approches sont possibles, concernant l'informatique en nuage, l'application du concept Zero Trust force la mise en œuvre de dispositif d'authentification forte et globalement d'augmenter les preuves à fournir pour obtenir un accès à la ressource. Ce concept s'applique également pour le nomadisme numérique et va exiger que l'utilisateur garantisse son identité mais également que son poste informatique ne présente pas de risque pour s'introduire sur le réseau de l'entreprise.

3. Hameçonnage ou phishing

L'hameçonnage, ou phishing, des e-mails professionnels restent la cyberattaque low-tech la plus utilisée par les cybercriminels pour accéder aux réseaux d'entreprises. Les e-mails d'hameçonnage ressemblent à des e-mails quotidiens normaux provenant d'entreprises et de personnes de confiance. En cliquant sur des liens malveillants, la victime arrivera sur des « vraies-fausses » pages lui demandant généralement de « mettre à jour » ou de « confirmer vos informations suite à un incident technique », notamment des coordonnées internes (codes personnels, identifiants, etc.).

La sensibilisation des collaborateurs permettra de limiter les chances de succès, l'attaque par hameçonnage se situant sur le volet sémantique elle est difficile à détecter par des logiciels. Des mesures techniques telles que le chiffrement ou la signature électronique des e-mails permettent aussi de limiter les risques.

4. Attaques par la chaîne d'approvisionnement

Une attaque par la chaîne d'approvisionnement, ou par la chaîne logistique, se produit lorsqu'un cybercriminel cible les fournisseurs d'une entreprise plutôt que l'entreprise elle-même. Il se sert du tier comme d'un cheval de Troie. Ces attaques sont donc plus difficiles à détecter et à empêcher si vos fournisseurs n'appliquent pas des politiques strictes de cybersécurité et n'utilisent pas des outils performants.

Il est donc indispensable de vous assurer que vos fournisseurs ont mis en place de mesures de cybersécurité suffisantes. Il est possible d'encadrer ces mesures à l'aide d'un plan d'assurance sécurité (PAS).

5. Attaques d'apprentissage automatique et d'intelligence artificielle

Alors que l'apprentissage automatique (Machine Learning, ML) et l'intelligence artificielle (IA) sont utilisés par les entreprises, ils sont également utilisés par les cybercriminels pour lancer des attaques. Avec ces outils, les cybercriminels peuvent élaborer des attaques sophistiquées sans pour autant disposer de compétences élevées.

L'application des règles d'hygiène numérique (application des correctifs, acculturation à la cybersécurité des collaborateurs, faire des sauvegardes…) sont toujours la parade élémentaire à déployer pour mieux gérer les risques cyber.

6. Attaques IoT

L'utilisation de l'Internet des objets (IoT) augmente chaque jour. L'IoT comprend tout, des ordinateurs portables aux tablettes, en passant par les routeurs, les webcams, les appareils électroménagers, les montres intelligentes, les appareils médicaux ou les automobiles. Plus d'appareils connectés signifient plus de risques cyber. Une fois contrôlés par des hackers, les appareils IoT peuvent être utilisés pour surcharger les réseaux, exploiter des données sensibles ou verrouiller des équipements essentiels à des fins financières.

L'utilisation de l'Internet des objets (IoT) augmente chaque jour. L'IoT représente de nombreux composants électroniques comme par exemple les caméras de vidéoprotection, des capteurs connectés tels les appareils électroménagers, les montres intelligentes, les appareils médicaux ou les automobiles. Plus d'appareils connectés signifient une augmentation des risques cyber.

Une fois contrôlés par des hackers, les appareils IoT peuvent être utilisés pour surcharger les réseaux, exploiter des données sensibles ou verrouiller des équipements essentiels à des fins financières.

En 2016, le malware Mirai avait compromis plusieurs milliers de caméra à travers le monde et réalisé une attaque qui avait failli faire s'écrouler Internet. Certains appareils ne disposent pas de niveau de sécurité suffisant, il faut alors s'assurer que ces derniers ne sont pas exposés directement sur Internet mais aussi d'appliquer les correctifs et autres mises à jour disponibles.

7. Gestion inadéquate des correctifs

Le but d'un correctif, ou patch, est d'éliminer une vulnérabilité dans un programme logiciel. Lorsque des vulnérabilités sont détectées, les éditeurs publient des correctifs pour remédier aux risques cyber liés à leurs systèmes d'exploitation et logiciels. Les correctifs sont donc essentiels à la sécurité de l'entreprise.

Pourtant, les correctifs sont largement ignorés à la fois par les utilisateurs et les services informatique. Quelle que soit la raison, de nombreuses technologies restent non corrigées, laissant les entreprises et leurs données vulnérables même aux menaces de cybersécurité les plus élémentaires.

8. L'injection de code

Les sites Internet collectent des données sensibles au travers de formulaires. Ces derniers, lorsqu'ils sont mal protégés, peuvent permettre à un attaquant d'injecter des requêtes malveillantes. Lorsque cela fonctionne l'attaquant peut alors accéder aux contenus de bases de données mais également modifier voire piéger des sites Internet.

L'application des principes de l'OWASP permet de limiter ces risques ; complétés par des tests d'intrusion, il est possible de détecter les faiblesses éventuelles de sites web.

9. Cryptojacking

Les cybercriminels vont rechercher de la puissance de calcul pour miner de la monnaie virtuelle. Pour cela, ils vont soit cibler des utilisateurs individuels ou compromettre des serveurs en s'appuyant sur des vulnérabilités non corrigées. L'impact sur les performances pourra être significatif et la facture de consommation électrique en hausse.

Pour s'en prémunir là aussi l'application des correctifs de sécurité est un bon point de départ. En le complétant avec de la supervision, il sera alors possible de détecter les consommations de ressources inhabituelles.

10. Une grave pénurie de professionnels de la cybersécurité

Dernière faiblesse : l'insuffisance d'experts en cybersécurité pour faire face aux cyber attaques croissantes. Il convient donc de se mobiliser pour recruter ces experts, non seulement en les chassant, mais également en acceptant de les payer à la hauteur des enjeux fondamentaux qu'ils représentent. Il est également nécessaire de proposer des cursus de formation pour les étudiants mais aussi pour favoriser la reconversion professionnelle vers cette thématique. Se soucier des dix points évoqués est un bon point de départ. Néanmoins, il conviendra de la compléter par une analyse de risques cyber mais aussi de se préparer à faire face à une cyberattaque.

Le site de l'ANSSI ainsi que les conseils de notre Directeur cybersécurité, Cyril Bras, vous seront utiles pour être en sécurité sur Internet.

Comment évaluer de façon simple le niveau de cybersécurité d'une solution ?

Cybersécurité

En tant que client, il est parfois difficil de se faire une idée sur le niveau réel de mise en œuvre de la Cybersécurité dans une solution logicielle. Comment aller au-delà des présentations commerciales tout en restant dans des opérations non intrusives ? C'est ce que vous propose cet article.

Le cadre légal concernant les atteintes à la cybersécurité

Avant de rentrer dans le vif du sujet, un petit rappel sur le cadre légal. La législation française est très précise sur les atteintes aux systèmes de traitement automatisé de données (STAD). Le code pénal précise plusieurs points :

- **323-1** Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de 3 ans d'emprisonnement et 100 000 € d'amende
- **323-2** Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de 5 ans d'emprisonnement et de 150 000 € d'amende
- **323-3** Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de 5 ans d'emprisonnement et de 150 000 € d'amende
- **323-7** La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

Il est donc hors de propos de tester le niveau de cybersécurité des plateformes en recherchant des vulnérabilités ou des failles présentes, c'est tout simplement illégal !

Si vous souhaitez approfondir le volet juridique concernant la Cybersécurité, nous vous conseillons la lecture du Code de la Cybersécurité aux éditions Dalloz.

Quels outils pour évaluer le niveau de cybersécurité d'une solution ?

Comme nous venons de le voir, il est n'est pas question d'aller scanner un site internet, mais de simplement naviguer et analyser les informations ainsi recueillies. En effet, plusieurs éléments permettent de déterminer si des mesures relevant des bonnes pratiques de développement sont mises en œuvre. Nous allons pour cela nous appuyer sur différents outils en ligne gratuits. L'avantage d'une telle approche, outre le fait qu'elle n'est pas intrusive, permet de reproduire et de comparer facilement différentes solutions.

> 💡 Retrouvez les 10 bonnes pratiques pour naviguer en sécurité sur internet.

Mozilla Observatory

Ce site attribue une note comprise entre A+ et F, F étant la pire en fonction de différents éléments présents lors de la navigation. Seront évaluées par exemple la protection des cookies, l'implémentation de CSP ou encore de https. Il s'agit donc d'évaluer la mise en œuvre de mesures préventives. Tous les sites Web commencent avec un score de base de 100 et reçoivent des pénalités ou des bonus à partir de là. Le score minimum est 0, mais il n'y a pas de score maximum.

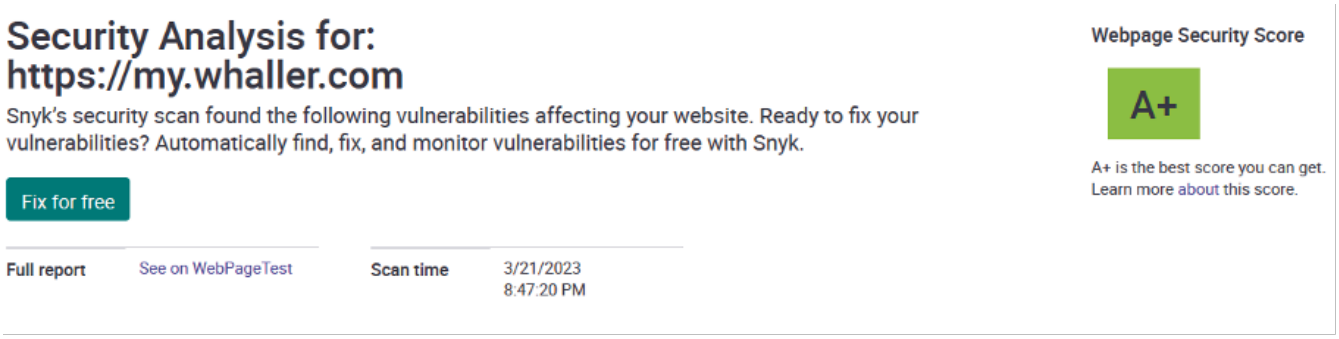
- Résultat du test de la plateforme collaborative Whaller

SNYK

Ce site attribue lui aussi une note comprise entre A+ et F. Celui-ci va notamment s'assurer que les librairies Javascript utilisées ne présentent pas de vulnérabilités connues. Il teste également que les en-têtes comportent bien les éléments suivants :

- strict-transport-security
- x-content-type-options
- x-frame-options
- content-security-policy
- x-xss-protection

- Résultat du test de la plateforme Whaller



Immuniweb

Ce site comme les précédents va tester la bonne implémentation des bonnes pratiques de cybersécurité mais va également s'assurer de la conformité aux exigences du RGPD.

- Résultat du test de la plateforme collaborative Whaller

Ces différents outils permettent de se faire une opinion sur les bonnes pratiques de Cybersécurité mises en œuvre de façon autonome et reproductible. Elle facilite la comparaison en toute transparence des offres disponibles sur le marché.

La Cybersécurité, il y a ceux qui en parle et ceux qui la mettent en œuvre.

Comment détecter une tentative d'escroquerie par mail ?

Cybersécurité

Toutes les entreprises, quelle que soit leur taille, subissent des cyberattaques. En revanche, les petites et moyennes entreprises (PME) sont parfois moins armées pour se défendre. Or les cyberattaques peuvent être très coûteuses pour celles-ci, allant même jusqu'à provoquer leur faillite.

C'est à l'aune de ce constat que nous souhaitons attirer votre attention sur les tentatives d'escroquerie qui pèsent sur les messageries professionnelles. Elles sont des vecteurs d'attaques privilégiées, car assez simples à mettre en œuvre pour le cybercriminel, tout en permettant d'obtenir des accès avancés dans l'entreprise.

Quelles sont les méthodes les plus courantes ? Comment détecter des tentatives d'escroquerie ? Que faire en cas de cyberattaque ? Voici une liste de 7 méthodes d'attaque par courriel utilisées par les cybercriminels. Elles appartiennent pour la plupart à l'ingénierie sociale.

L'hameçonnage

L'hameçonnage – phishing – est l'attaque la plus répandue d'après le rapport annuel sur l'état de la menace dressé par l'European Union Agency for Cybersecurity (ENISA). Il se produit lorsque des hackers créent un courriel conçu pour donner l'impression qu'il provient d'une entreprise réputée ou d'une personne de confiance. Le courriel contient des liens ou des pièces jointes malveillants qui, lorsqu'on clique dessus ou on les télécharge, conduisent la victime à fournir des informations confidentielles (numéros de cartes bancaires, identifiant de connexion…). Ces informations seront ensuite revendues ou utilisées par le cybercriminel.

Comment fonctionne l'hameçonnage ?

Pour donner l'impression qu'un courriel illicite est légitime, les fraudeurs utilisent souvent les couleurs de la marque et le logo de l'entreprise qu'ils usurpent. Les liens contenus dans l'email mèneront ensuite à des sites web de phishing qui tenteront également de se faire passer pour une entreprise connue.

Quel en est le risque ?

La tentative d'escroquerie par hameçonnage va permettre à l'attaquant d'obtenir par exemple un accès au compte informatique d'un utilisateur victime. En effet, le site web de phishing est conçu pour vous inciter à révéler vos informations d'identification pour les services bancaires, les emails ou simplement le poste de travail. Il va être une copie conforme du site original de la structure visée. Après une attaque de phishing réussie, l'entreprise est alors accessible aux hackers, comme si vous leur aviez donné les clés de votre maison.

Comment réduire le risque lié à une tentative d'hameçonnage ?

Un certain nombre d'indicateurs permettent de déjouer un grand nombre de ces attaques. Il faut être attentif à plusieurs éléments :

- L'expéditeur est-il connu ? Est-ce bien son adresse de messagerie ?
- L'expéditeur est-il un collaborateur de l'entreprise ?
- L'objet du message est-il en lien avec les activités connues de l'expéditeur ?
- La date et l'heure d'expédition du message.
- Est-ce qu'il y a une forme de pression psychologique dans le corps du message ?

En complément, équiper son poste informatique d'un antivirus analysant l'activité de messagerie et de navigation sera un bon complément. Il convient également de ne pas répondre au message reçu.

💡 Si vous avez cliqué sur le lien ou ouvert une pièce jointe malveillante :

👉 Conservez le courriel original.
👉 Lancez une analyse antivirale de votre poste.
👉 Changez vos identifiants de messagerie, si vous avez communiqué des données bancaires, contactez votre banque.
👉 Déposez plainte auprès de la gendarmerie ou la police.

> 📽 Apprenez à détecter une menace informatique avec notre Directeur cybersécurité, Cyril Bras.

Le harponnage

Le harponnage ou spear-phishing fonctionne comme le phishing mais cible une personne ou une entreprise en particulier.

Comment fonctionne la tentative d'escroquerie par harponnage ?

Alors que les attaques de phishing envoient des emails en grand nombre dans l'espoir d'obtenir une « prise », le spear-phishing cible une personne en particulier. Le cybercriminel a au préalable collecté des informations sur sa cible afin de créer une sollicitation qui va lui paraître la plus légitime possible.

Quel en est le risque ?

S'adressant par son nom et l'intitulé de son poste au destinataire de l'email, le cybercriminel augmente ses chances de succès. En effet, sa cible, mise en confiance, tombe dans le piège qui lui est tendu en cliquant sur le lien présent ou en ouvrant l'éventuelle pièce jointe.

Comment réduire le risque lié à une tentative d'harponnage ?

En appliquant les mêmes mesures que pour l'hameçonnage classique.

L'usurpation d'emails

L'usurpation d'email est une forme plus sophistiquée de tentative d'escroquerie par phishing où l'adresse email à partir de laquelle l'email est envoyé semble être une adresse légitime associée à l'entreprise dont l'identité est usurpée.

Comment fonctionne l'usurpation d'emails ?

Chaque email a un en-tête qui est composé de lignes de texte invisibles dans l'email. Celles-ci permettent à votre messagerie de savoir, notamment, de qui provient l'email.

À l'aide de techniques sophistiquées, il est possible de modifier l'en-tête d'un email frauduleux pour donner l'impression qu'il provient d'une adresse légitime.

Quel en est le risque ?

Étant donné que l'adresse « de provenance » dans l'email semble provenir d'un compte authentique, l'attaque a beaucoup plus de chances de réussir. Les attaques d'usurpation d'identité peuvent alors contenir des rançongiciels, des virus ou exiger des paiements de la part des salariés. Par exemple, croyant l'email authentique car signé par leur président, des collaborateurs d'une direction financière vont procéder au paiement en ligne d'un faux fournisseur. On parle alors de Business e-mail compromiss (BEC).

Comment réduire le risque lié à l'usurpation d'emails ?

Il est essentiel de bien lire le champ expéditeur au complet. En effet dans ce type d'attaque, l'adresse réelle de l'attaquant apparaitra après celle de l'expéditeur usurpé. Il convient également de mettre en place au sein de l'entreprise des mécanismes de validation interne ne permettant pas la réalisation d'actions sensibles par courriel.

💡 Si vous avez cliqué sur le lien ou ouvert une pièce jointe :

👉 Conservez le courriel original.
👉 Lancez une analyse antivirale de votre poste.
👉 Changez vos identifiants de messagerie, si vous avez communiqué des données bancaires, contactez votre banque.
👉 Déposez plainte auprès de la gendarmerie ou la police.

> 🔎 Décryptez une tentative de fraude au président avec un cas concret à l'encontre de notre président, Thomas Fauré.

Détournement de fil de discussion par email

Il s'agit d'une forme plus élaborée d'ingénierie sociale où un cybercriminel s'infiltre dans un serveur de messagerie et intercepte une conversation en cours. Cette tentative d'escroquerie peut faire suite à une campagne d'hameçonnage ayant permis à l'attaquant de récupérer les identifiants d'accès à un compte mail. Il va alors récupérer l'intégralité des échanges présents sur le serveur et la liste des destinataires. Il va alors utiliser ces échanges depuis une autre adresse de messagerie pour reprendre le contact. Vous pensez que vous communiquez avec la personne avec qui vous avez communiqué, mais vous communiquez en fait, maintenant, avec un hacker.

Comment fonctionne le détournement de fil de discussion par email ?

Ces attaques sont bien souvent la suite d'une campagne d'hameçonnage réussie ou peuvent aussi se produire lorsqu'un serveur de messagerie n'est pas à jour de ses correctifs de sécurité.

Quel en est le risque ?

Parce que l'attaque s'appuie sur une conversation en cours, son taux de réussite peut être extrêmement élevé. Les risques sont multiples, l'attaquant peut obtenir des informations sensibles ou des données personnelles contenues dans les courriels mais il peut également vous inviter à ouvrir une pièce jointe piégée afin de prendre le contrôle de votre ordinateur.

Comment réduire le risque lié au détournement de fil de discussion par email ?

La signature électronique des messages permet de déjouer plus facilement ces attaques. Les clients de messagerie proposent aujourd'hui d'ajouter des signatures électroniques au format OpenPGP.

Il arrive que les échanges repris soient anciens (dépendant de la date de piratage initial de la messagerie de l'expéditeur), cet indice doit être un point de vigilance. Dans le doute, contacter l'expéditeur par un autre canal (téléphone) peut être une solution.

Déni de service et attaques DDoS par email

Une attaque en déni de service ou en déni de service distribué (DDoS pour Distributed Denial of Service en anglais) vise à envoyer des quantités massives d'emails à un serveur de messagerie afin de l'empêcher de fonctionner normalement, empêchant ainsi les emails légitimes de passer.

Comment fonctionne le déni de service par email ?

Il existe plusieurs manières de réaliser une attaque en déni de service : activer un botnet pour bombarder un serveur de messagerie avec des emails, ou bien envoyer un torrent d'emails avec d'énormes pièces jointes de fichiers texte au format zip. Le serveur recevant le fichier le décompressera pour rechercher les logiciels malveillants, ce qui ralentira fortement les capacités du serveur.

Quel en est le risque ?

Le but d'une attaque DDoS est d'empêcher le serveur de messagerie de l'entreprise de fonctionner normalement en raison d'une surcharge, empêchant ainsi les salariés de se servir de leur messagerie. Ce type d'attaque peut conduire à un arrêt du serveur ciblé nécessitant une lourde opération de maintenance pour le redémarrer.

Comment se protéger d'une tentative de DDoS ?

Il est possible de souscrire à des offres de protection anti-DDOS proposées par les fournisseurs d'accès Internet pour protéger le serveur de messagerie. Un élément à prendre en considération lorsque vous souscrivez à une offre d'hébergement ou de messagerie.

Usurpation d'identité ou email spoofing

Le spoofing, ou usurpation d'identité, se produit lorsqu'un hacker utilise votre adresse de messagerie pour envoyer des courriels à partir de son propre serveur de messagerie.

Comment fonctionne l'usurpation d'identité ?

En s'appuyant sur une erreur de configuration au niveau du nom de domaine e : masociete.fr.

Si dans votre configuration du Domain Name Service (DNS) vous n'avez pas donné la liste des serveurs légitimes pour envoyer des courriels, vous vous exposez alors à ce type d'attaque. Il sera alors possible pour l'attaquant d'envoyer des courriels de pierre.dupont@masociete.fr, il sera alors très difficile de détecter le pot aux roses.

Quel en est le risque ?

Bien que l'attaque ne vise pas votre entreprise, elle peut avoir des effets dévastateurs sur la réputation de celle-ci, les cybercriminels se servent de vos noms de domaine pour mener à bien leurs entreprises criminelles

Comment se protéger d'une tentative d'escroquerie par usurpation d'identité ?

Identifier clairement la liste des serveurs de messagerie légitimes en les déclarant dans le champ Sender Permitted From (SPF) de votre domaine. L'activation des champs DomainKeys Identified Mail (DKIM) et Domain Message Authentication Reporting & Conformance (DMARC) permettront également au destinataire de vérifier grâce à des signatures électroniques que le serveur utilisé est bien légitime. Là encore, ce sont des éléments à exiger auprès de vos offreurs de solution de messagerie.

Prise de contrôle d'une messagerie

Il s'agit de l'une des attaques les plus dangereuses. La prise de contrôle d'une messagerie donne au hacker un accès direct à un compte de messagerie authentique dans l'entreprise. Cela lui permet d'envoyer des emails frauduleux qui ne sont plus détectables.

Comment fonctionne la prise de contrôle d'une messagerie ?

Dès qu'un pirate dispose de vos identifiants de connexion, il peut envoyer et recevoir des emails directement depuis votre compte. Pour y parvenir, il peut utiliser les sites web de phishing vous demandant de vous connecter avec votre adresse email ou bien le vol d'un téléphone portable ou d'un PC non sécurisé.

Quel en est le risque ?

Étant donné que les emails proviennent d'un compte d'entreprise, tous les contrôles de sécurité internes sont contournés. Les destinataires sont alors floués. La seule méthode dont ces derniers disposent pour le détecter est de détecter un comportement « anormal » du compte de messagerie ou des demandes soudaines d'informations sensibles telles que des mots de passe ou des coordonnées bancaires.

Comment réduire le risque lié à la prise de contrôle d'une messagerie ?

L'activation de l'authentification à facteurs multiples (MFA) permet de complexifier l'attaque. En effet bien que disposant de vos noms d'utilisateur et de mot de passe, l'attaquant ne pourra pas fournir le code temporaire de validation. Attention toutefois certains cybercriminels utilisent la ruse et suivant les informations dont ils disposent pourraient vous contacter en se faisant passer pour le service informatique pour vous demander ce code par téléphone par exemple.

Assurer la Cyber Résilience dans un monde numérique incertain

Cybersécurité

La Cyber Résilience des entreprises est désormais mise à l'épreuve comme jamais elle ne l'a été auparavant. Aussi, pour y parvenir, il convient de tirer des enseignements des évènements les plus récents afin de préparer l'avenir.

Le numérique, un outil de déstabilisation

Le 23 février 2022, la veille de l'invasion russe de l'Ukraine, les systèmes informatiques de plusieurs ministères, organismes gouvernementaux et banques ukrainiens ont été la cible de cyberattaques. Depuis, l'OTAN a déclaré qu'une cyberattaque contre l'un de ses membres déclencherait l'article 5 de la Charte de l'OTAN, permettant à celle-ci de riposter avec tous les moyens disponibles. Depuis un an, les cyberattaques augmentent à mesure que le conflit s'intensifie. Comme nous le voyons, le numérique joue un rôle important, sinon décisif, dans le conflit Ukraine-Russie.

Ainsi, pandémies, guerres, compétition économique globale et questions climatiques bouleversent l'ordre géopolitique mondial apparu après la chute du mur du Berlin en 1989. En conséquence de quoi, pour les entreprises, l'accès aux marchés et les chaînes d'approvisionnement étant fortement perturbés, ce sont autant de nouveaux défis vitaux à relever.

Un risque majeur pour l'infrastructure informatique des entreprises

Rappelons-nous qu'avant la crise du Covid, il était déjà difficile pour de nombreuses entreprises de suivre le rythme des changements technologiques. Depuis la pandémie, le défi n'a fait que s'accélérer : l'avenir du travail et de la vie en règle générale sera plus numérique que nous ne l'avions imaginé. Cela signifie que toutes les organisations – entreprises ou administrations – dépendant des datas, des outils numériques et de l'automatisation des tâches sont touchées.

En effet, des vulnérabilités dans n'importe quel domaine comme le commerce, le suivi clients, les ressources humaines, les finances, peuvent affecter la capacité d'une entreprise à survivre et à continuer d'être profitable. Une entreprise doit donc intégrer la Cyber Résilience dans tous les aspects de son organisation, de la production de ses biens ou de ses services en passant par ses infrastructures les plus critiques, notamment son système d'information.

En effet, les capacités technologiques jouent un rôle déterminant dans le renforcement de la résilience. La raison fondamentale est que plus aucune entreprise ou une organisation ne peut aujourd'hui se passer du numérique. Leur dépendance vis-à-vis de ces technologies augmente chaque jour. Aussi, leur maîtrise est essentielle à la survie des entreprises. Elle est même, pour l'écrasante majorité des dirigeants, à la lumière de la crise du Covid, un enjeu crucial, c'est-à-dire vital.

> 💡 En savoir plus : Managing the Cyber Risks of Remote Work.

La cybersécurité clé de voûte de la Cyber Résilience

Dans ce cadre, un dispositif numérique opérationnel ne se contentera pas d'assurer la production et l'accès aux marchés des biens ou des services, la productivité de la main-d'œuvre et la génération de profits à court et moyen termes.

Pour véritablement y parvenir, la direction des systèmes d'information (DSI) responsable du numérique devra surtout se conformer à la stratégie de cybersécurité définie par la direction générale ou la direction Cybersécurité. Pour ce faire : les étapes clés, les acteurs, la combinaison des moyens humains et financiers seront définis dans la Politique de Sécurité des Systèmes d'Information (PSSI) de la structure.

Car c'est bien elle, la cybersécurité, qui est désormais la clé de voûte de la résilience. Sans elle, tout l'édifice s'effondrera ; avec elle, la résilience pourra être menée à bien. La cybersécurité est un peu comme le contrôle technique automobile. C'est elle qui va définir les mesures de sécurité à mettre en œuvre, les seuils d'usure ou d'obsolescence au-delà desquels la sécurité n'est plus assurée, charge ensuite aux garagistes de s'y conformer. Qui accepterai que le contrôle technique de son véhicule soit effectué par le garagiste ou le loueur de voiture ? C'est pour cette raison que le contrôle de conformité, la définition des règles de sécurité numérique ne doit pas être réalisé par les services informatiques mais par une instance extérieure rattachée au plus haut niveau.

Voilà la raison qui oblige les dirigeants d'entreprises et d'organisations à tout mettre en œuvre pour assurer leur Cyber Résilience dans un monde numérique incertain : investir dans un système d'information robuste et fiable pour assurer la continuité des activités, établir des plans de continuité des activités en veillant à ce qu'ils soient régulièrement mis à jour et testés, et former leurs collaborateurs à propos des risques et des meilleures pratiques en matière de sécurité afin de minimiser les vulnérabilités.

> 💡 En savoir plus : Adoptez un système de communication et de collaboration en parallèle de votre système SI pour assurer votre Cyber Résilience.

Enfin, les dirigeants pourront faire leur ce vieil adage latin recommandant la préparation au combat, « Si vis pacem, para bellum » – Si tu veux la paix, prépare la guerre – qui, s'il avait été pensé pour les Etats, s'appliquent désormais aux entreprises et aux organisations tant les menaces cyber s'apparentent à des faits d'armes.

LinkedIn suite des attaques

Cybersécurité

Depuis plusieurs semaines, de nombreux utilisateurs du réseau social LinkedIn ont été victimes du piratage de leur compte [1]. Ces derniers se sont trouvés expulsés et ne pouvaient alors plus accéder à leur compte. Si certains se sont vus réclamer une rançon, il semble à présent que les attaquants passent à une seconde phase, la collecte d'informations personnelles.

La plupart des utilisateurs souhaitent retrouver l'accès à leur compte piraté et entreprennent des signalements auprès de LinkedIn. Le réseau social indique sur cette page https://www.linkedin.com/help/linkedin/answer/a1342692, les modalités pour justifier son identité. C'est alors que les attaquants entrent en scène.

L'analyse du contenu du message

Ces derniers vont envoyer un courriel usurpant l'identité de LinkedIn et reprenant les conditions évoquées dans le lien cités supra. Ce message propose d'envoyer via un lien sécurisé une copie d'un document d'identité.

Premier élément suspect, le lien sécurisé de transfert hébergé chez 10tix.me, cela ressemble fort à du hameçonnage d'autant que ce service semble inconnu, pire la page web donne une erreur Json

L'analyse des en-têtes

Continuons à investiguer en regardant les en-têtes du courriel.

Etrange, il y a une erreur spf [2] (un champ qui permet de limiter l'usurpation d'adresse mail), le courriel provenant de linkedin_fr@cs.linkedin.com n'est pas passé par un serveur déclaré dans le champ spf de LinkedIn (rntac72.rnmk.com). Le message est accepté car les paramètres définis sur le domaine linkedin.com sont permissifs et demandent à laisser passer les échecs mechanism '~all' matched

Rnmk.com est affilié à Oracle

Source Abuseipdb.com

Autant s'il s'agissait d'un serveur appartenant à Microsoft [3] le doute aurait été permis mais Oracle…

```
v=spf1 ip4:129.152.44.123 ip4:129.152.44.124 ip4:129.152.44.125 ip4:129.152.44.115 include:linkedin.com ~all
```

Source mxtoolbox.com

L'adresse ne fait pas partie des serveurs autorisés !

Les attaquants exploitent une faiblesse de configuration sur le sous-domaine cs.linkedin.com pour émettre des courriels frauduleux rendant la détection très difficile pour le commun des mortels.

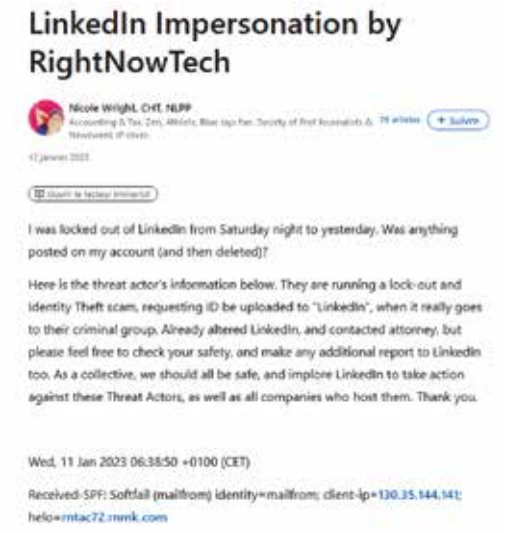
Globalement c'est l'ensemble des mécanismes de protection qui semblent inexistants, le champ OpenDMARC est lui aussi très permissif…

OpenDMARC; dmarc=fail (p=reject dis=none) header.from=cs.linkedin.com

Source mxtoolbox.com

Et pourquoi ne pas le signaler à LinkedIn ?

Si l'on recherche un petit peu sur le net on trouve cet article datant de janvier 2023 et évoquant déjà le problème…



LinkedIn Impersonation by RightNowTech

Nicole Wright, CHT, NLPP

I was locked out of LinkedIn from Saturday night to yesterday. Was anything posted on my account (and then deleted)?

Here is the threat actor's information below. They are running a lock-out and identity Theft scam, requesting ID be uploaded to "LinkedIn", when it really goes to their criminal group. Already altered LinkedIn, and contacted attorney, but please feel free to check your safety, and make any additional report to LinkedIn too. As a collective, we should all be safe, and implore LinkedIn to take action against these Threat Actors, as well as all companies who host them. Thank you.

Wed, 11 Jan 2023 06:38:50 +0100 (CET)

Received-SPF: Softfail (mailfrom) identity=mailfrom; client-ip=130.35.144.141;

https://www.linkedin.com/pulse/linkedin-impersonation-rightnowtech-nicole-wright-cht-nlpp/

Pour conclure

Le phishing et l'ingénierie sociale sont des vecteurs d'attaque redoutables surtout s'ils sont combinés à des configurations permissives.

Pour déceler ces messages il faut apprendre à les reconnaitre en s'appuyant par exemple sur les recommandations du site cybermalveillance.

Dans le cas présent, le lien présent dans le message sans connexion avec LinkedIn doit mettre la puce à l'oreille. Le second élément est visible dans l'en-tête des messages pour peu que l'on aille les regarder. La présence du terme Softfail est un indicateur qui doit alerter sur la légitimité du message. Malheureusement, il est encore très fréquent d'observer des noms de domaines qui ne sont pas suffisamment protégés et qui n'utilisent pas correctement le triptyque SPF/DMARC/DKIM.

Cyril Bras

Directeur Cybersécurité chez Whaller

[1] https://www.tomsguide.fr/linkedin-attaque-massivement-par-des-pirates-votre-compte-est-en-danger/

[2] Sender Permitted From https://www.proofpoint.com/fr/blog/user-protection/what-spf-sender-policy-framework

[3] https://www.lesechos.fr/tech-medias/hightech/-quatre-ans-apres-son-mega-rachat-par-microsoft-linkedin-poursuit-sa-croissance-fulgurante-1208075quatre-ans-apres-son-mega-rachat-par-microsoft-linkedin-poursuit-sa-croissance-fulgurante-1208075

La qualification SecNumCloud : un pas de géant vers la sécurité des données en ligne

Cybersécurité

La sécurité des données en ligne est plus cruciale que jamais à l'ère numérique, et les autorités gouvernementales françaises prennent des mesures significatives pour renforcer cette sécurité. L'une de ces mesures est la qualification SecNumCloud, une norme de sécurité rigoureuse destinée à protéger les informations sensibles stockées dans le cloud. Dans cet article, nous explorerons ce qu'est la qualification SecNumCloud, pourquoi elle est importante pour les fournisseurs de services cloud tels que Whaller, et son impact sur la sécurité des données en France.

Qu'est-ce que la qualification SecNumCloud ?

La qualification SecNumCloud est une certification de sécurité mise en place par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en France. Contrairement à une simple certification, elle représente une évaluation approfondie de la sécurité d'un service cloud, plutôt qu'une simple validation de conformité. Elle garantit que les données stockées dans le cloud sont protégées contre une gamme de menaces potentielles.

À qui est-elle destinée ?

La qualification SecNumCloud s'adresse principalement aux fournisseurs de services cloud, qu'ils soient des entreprises privées ou des organismes publics. Elle vise à évaluer et à certifier la conformité des solutions de cloud computing aux normes de sécurité définies par l'ANSSI.

Qui est concerné par la qualification SecNumCloud ?

En fin de compte, la qualification SecNumCloud bénéficie à un large éventail de parties prenantes, notamment :

- **Les fournisseurs de services cloud :** Les prestataires de services cloud qui cherchent à obtenir la qualification SecNumCloud doivent se conformer à des normes strictes de sécurité des données. Cela signifie qu'ils doivent mettre en œuvre des mesures de sécurité avancées pour protéger les données de leurs clients.
- **Les clients utilisant le cloud** : Les entreprises, les organisations gouvernementales et d'autres entités qui utilisent des services cloud peuvent être assurées que leurs données sont hébergées sur des plateformes répondant aux normes de sécurité les plus élevées.
- **L'ANSSI :** En renforçant la sécurité des données dans le cloud, l'ANSSI contribue à protéger les intérêts nationaux et à réduire les risques de cyberattaques et de fuites de données.

Pourquoi la qualification SecNumCloud est-elle importante ?

La qualification SecNumCloud revêt une importance cruciale pour plusieurs raisons :

- **Protection des données sensibles :** Elle garantit que les données sensibles stockées dans le cloud sont sécurisées contre les menaces potentielles telles que le piratage informatique, les fuites de données et les accès non autorisés.
- **Renforcement de la confiance :** Elle renforce la confiance des clients et des utilisateurs dans les services cloud, en leur assurant que leurs informations sont entre de bonnes mains.
- **Normes de sécurité élevées :** Elle élève les normes de sécurité dans l'ensemble de l'industrie du cloud computing, encourageant ainsi les fournisseurs à améliorer leurs pratiques de sécurité.

- **Protection des intérêts nationaux :** Elle contribue à protéger les informations sensibles et les infrastructures nationales contre les cybermenaces, ce qui revêt une importance stratégique. Elle permet aussi de garantir une immunité aux lois extraterritoriales qui peuvent parfois s'appliquer lorsque l'on s'appuie sur un fournisseur non qualifié.

Le rôle crucial de l'ANSSI

L'ANSSI joue un rôle central dans la mise en place et l'application de la qualification SecNumCloud. Elle établit les exigences de sécurité et vérifie la conformité des prestataires de services cloud. Grâce à son expertise, l'ANSSI assure un au niveau de sécurité numérique en France.

Pourquoi la qualification SecNumCloud est importante pour Whaller

Whaller, en tant que fournisseur de services cloud (SaaS), attache une grande importance à la qualification SecNumCloud. Cette qualification garantit que les données de ses utilisateurs, qu'elles soient personnelles, professionnelles ou gouvernementales, bénéficient d'un niveau de sécurité de premier ordre et une immunité aux lois extraterritoriales.

Whaller s'appuie ensuite sur un prestataire qualifié (OVHcloud) pour la partie infrastructure (IaaS). Ainsi les clients de Whaller ont la garantie que leurs données sont correctement hébergées à chaque étape.

Whaller est également en cours de qualification SecNumCloud.

La Version 3.2 et son importance

La dernière version de la qualification SecNumCloud, la 3.2, a été fortement encouragée par Guillaume Poupard, l'ancien directeur général de l'ANSSI. Elle introduit un élément essentiel : l'indépendance vis-à-vis des lois extraterritoriales. Cette mise à jour vise à garantir que les données stockées en France ne sont pas soumises à des lois étrangères potentiellement conflictuelles avec la protection des données personnelles. En adoptant la version 3.2, Whaller et d'autres fournisseurs de services cloud français s'engagent à protéger la souveraineté des données et la confidentialité de leurs clients.

Conclusion

La qualification SecNumCloud joue un rôle crucial dans la garantie de la sécurité des données stockées dans le cloud en France. Pour Whaller, elle représente un engagement envers la sécurité et la protection de la confidentialité des données de ses utilisateurs. Grâce à l'ANSSI, la qualification SecNumCloud est un élément essentiel pour la protection des données sensibles en ligne, ainsi que pour l'indépendance juridique des données stockées sur des serveurs français.

> 📖 En savoir plus : Cybersécurité.

Les voitures connectées : passoires numériques et quête de confidentialité

Cybersécurité

Dans l'ère numérique actuelle, l'intégration de technologies de pointe dans nos vies quotidiennes est devenue monnaie courante. Nos smartphones, montres et maisons sont connectés, mais rien ne l'est autant que nos véhicules. Les voitures connectées, avec leurs systèmes avancés d'info-divertissement, de navigation et de télématique, ont radicalement transformé notre expérience de conduite. Cependant, cette révolution technologique s'accompagne de préoccupations majeures concernant la sécurité informatique et la confidentialité des données.

Les voitures connectées : des passoires numériques ?

Les voitures connectées sont devenues des ordinateurs roulants. Grâce à des systèmes sophistiqués d'infodivertissement, de navigation et de connectivité, elles offrent un large éventail de services et de fonctionnalités. Cependant, ces avantages s'accompagnent d'une vulnérabilité significative. Les chercheurs en sécurité ont démontré à maintes reprises que les voitures connectées peuvent être des passoires numériques, exposant les conducteurs à des risques majeurs.

L'une des principales vulnérabilités réside dans le manque de sécurité des systèmes informatiques embarqués. De nombreux constructeurs automobiles n'ont pas accordé la priorité à la sécurisation de ces systèmes, ce qui signifie que les pirates informatiques peuvent exploiter des failles pour prendre le contrôle des véhicules à distance. Les conséquences potentielles sont effrayantes, allant de la désactivation de fonctions de sécurité à la manipulation de la direction et de la vitesse.

En outre, les voitures connectées sont exposées à des menaces de sécurité informatique courantes, telles que les attaques par déni de service (DDoS) et les intrusions dans les réseaux Wi-Fi générés par la voiture. L'interconnexion de divers composants des véhicules rend les attaques plus sophistiquées possibles. Un exemple concret est l'attaque Spectre, qui a démontré comment un pirate informatique peut accéder à des données sensibles stockées dans le système de divertissement d'une voiture.

Cependant, ce n'est pas seulement la sécurité qui est en jeu. Les voitures connectées sont également des mines de données personnelles, collectant une quantité considérable d'informations sur les conducteurs et les passagers. Les constructeurs automobiles, pour diverses raisons, s'adonnent à une collecte de données massive, alimentée par des capteurs intégrés, des systèmes de navigation GPS et des connexions cellulaires. Ces données incluent des informations sur les habitudes de conduite, les destinations, les préférences personnelles et plus encore.

Voici quelques exemples :

1. Attaque à distance sur une Tesla Model S (2016) : Des chercheurs en sécurité ont démontré comment ils pouvaient prendre le contrôle d'une Tesla Model S à distance en exploitant une vulnérabilité dans le logiciel de la voiture. Ils ont pu verrouiller et déverrouiller les portes, activer les freins, et même éteindre la voiture.

2. Vulnérabilité dans le système d'infodivertissement Uconnect de Jeep (2015) : En 2015, des chercheurs en sécurité ont révélé une vulnérabilité dans le système Uconnect de Jeep qui permettait aux pirates de prendre le contrôle à distance du véhicule. Ils pouvaient couper le moteur, désactiver les freins, contrôler la radio, et même prendre le contrôle du volant.

3. Piratage de Tesla par des chercheurs chinois (2021) : Des chercheurs en sécurité chinois ont montré comment ils pouvaient pirater à distance une Tesla Model S en utilisant des vulnérabilités de sécurité. Ils ont réussi à accéder aux caméras, aux écrans tactiles et à d'autres systèmes de la voiture.

4. Attaque sur les véhicules BMW, Mercedes-Benz et Audi (2020) : Des chercheurs ont révélé des vulnérabilités dans les clés de communication sans fil utilisées par de nombreuses voitures connectées de ces marques. Cela aurait pu permettre à des attaquants de cloner des clés et de voler des voitures.

5. Vulnérabilités de l'application mobile de Nissan (2016) : Des chercheurs ont découvert que l'application mobile NissanConnect, utilisée pour interagir avec certaines voitures Nissan, était vulnérable aux attaques. Cela aurait pu permettre aux pirates d'accéder aux données des utilisateurs et de prendre le contrôle de certaines fonctions de la voiture.

Ces exemples illustrent les défis de sécurité auxquels sont confrontées les voitures connectées. Les constructeurs automobiles et les chercheurs en sécurité travaillent continuellement pour identifier et corriger ces vulnérabilités, mais il est essentiel que les propriétaires de voitures connectées prennent également des mesures pour sécuriser leurs véhicules, comme garder les logiciels à jour et éviter de télécharger des applications non sécurisées.

L'Exploitation des données par les constructeurs

Pour les constructeurs automobiles, les données représentent une mine d'or. Ils peuvent les utiliser de diverses manières, notamment pour améliorer leurs produits, personnaliser les services, et même créer de nouvelles sources de revenus. Les données peuvent être exploitées pour optimiser la maintenance des véhicules, fournir des mises à jour logicielles à distance et offrir des fonctionnalités de connectivité avancée.

Cependant, il y a une ligne fine entre l'utilisation légitime des données pour améliorer les services et l'exploitation excessive de la vie privée des conducteurs. Les constructeurs automobiles peuvent être tentés de monétiser ces données en les vendant à des tiers, comme les annonceurs ou les compagnies d'assurance. Cela soulève des préoccupations légitimes concernant la confidentialité et la sécurité des données personnelles.

Luc Julia chez Renault : un nouveau chapitre pour les données connectées

L'arrivée de Luc Julia, l'un des cerveaux derrière Siri d'Apple, chez Renault en tant que Chief Scientific Officer, soulève des questions sur l'exploitation des données personnelles dans l'industrie automobile. Julia est un expert en intelligence artificielle et en apprentissage automatique, des domaines qui ont un potentiel énorme pour l'analyse des données collectées par les voitures connectées.

Renault, comme de nombreux autres constructeurs, cherchera probablement à tirer parti des compétences de Julia pour optimiser l'utilisation des données des véhicules connectés. Cependant, il sera essentiel pour Renault et d'autres entreprises du secteur de l'automobile de garantir que les données des conducteurs sont protégées de manière appropriée, et que la transparence et le consentement des utilisateurs sont respectés.

Solutions pour améliorer la sécurité numérique et la confidentialité

Face à ces défis, des solutions doivent être envisagées pour améliorer la sécurité numérique des voitures connectées et protéger la confidentialité des données des conducteurs.

Voici quelques pistes à explorer :

- **Sécurisation des systèmes embarqués :** Les constructeurs automobiles doivent investir davantage dans la sécurisation des systèmes informatiques embarqués, en utilisant des méthodes de chiffrement et des mises à jour logicielles fréquentes pour corriger les vulnérabilités.
- **Règlementation renforcée :** Les gouvernements doivent élaborer des réglementations plus strictes en matière de cybersécurité pour l'industrie automobile, exigeant des normes minimales de sécurité et la divulgation des pratiques de collecte de données.
- **Contrôle des données :** Les conducteurs doivent avoir un contrôle plus granulaire sur les données collectées par leurs véhicules, avec la possibilité de consentir ou de refuser leur utilisation pour des finalités spécifiques.
- **Transparence et responsabilité :** Les constructeurs automobiles doivent être transparents quant à leur utilisation des données, et responsables en cas de violations de données ou d'abus.
- **Technologie de sécurité :** Les conducteurs devraient être encouragés à utiliser des solutions de sécurité telles que des pares-feux pour leurs voitures connectées, en plus d'outils de gestion de la confidentialité.

La sécurité informatique et la confidentialité des données dans le secteur des voitures connectées sont des défis cruciaux pour l'industrie et les législateurs. La protection de la vie privée des conducteurs tout en permettant aux constructeurs d'innover et de fournir des services de qualité est un équilibre délicat à atteindre. L'arrivée de spécialistes de l'intelligence artificielle tels que Luc Julia dans des entreprises automobiles comme Renault promet des avancées significatives dans l'utilisation des données des véhicules connectés. Cependant, cela souligne également l'importance de garantir que ces données sont utilisées de manière éthique et sécurisée, dans le respect de la vie privée des utilisateurs

L'avenir des voitures connectées est prometteur, avec des avancées technologiques qui pourraient rendre nos routes plus sûres et nos expériences de conduite plus agréables. Cependant, il est impératif que les constructeurs automobiles, les régulateurs et les consommateurs collaborent pour s'assurer que la sécurité numérique et la confidentialité des données sont au cœur de cette transformation. La route vers des voitures connectées plus sûres et plus respectueuses de la vie privée est en cours, mais elle exige une vigilance constante et des efforts collectifs pour atteindre cet objectif.

En fin de compte, les voitures connectées doivent offrir une expérience de conduite enrichissante sans compromettre la sécurité numérique ni violer la vie privée des conducteurs. La clé de cette réussite réside dans l'adoption de pratiques exemplaires de sécurité, une réglementation appropriée et une sensibilisation continue des consommateurs. Il est temps de façonner un avenir où la technologie des voitures connectées peut véritablement servir l'humanité, tout en respectant ses droits fondamentaux à la sécurité et à la confidentialité.

Cybermoi/s 2023 : Whaller souscrit à la CharteCyber de Cybermalveillance.gouv.fr

Cybersécurité

Pendant le mois de la cybersécurité « Cybermoi/s » , de nombreuses entités se sont engagées à promouvoir un cadre de cybersécurité responsable et vertueux en signant la CharteCyber. Les premiers signataires visent à démontrer l'importance de la cybersécurité au sein de leurs organisations, en respectant ces engagements. Ils souhaitent également sensibiliser leur écosystème et encourager d'autres organisations à suivre leur exemple.

Selon Jérôme Notin, Directeur Général de Cybermalveillance.gouv.fr, « À travers cette charte, nous avons souhaité envoyer un signal fort pour que la cybersécurité soit reconnue comme un enjeu sociétal. Les organisations s'engagent à mettre en place des mesures de sensibilisation et de protection cyber de premier niveau, tant sur les aspects techniques qu'humains. »

La ChartеCyber Les organisations signataires de la ChartеCyber s'engagent à :

1. Prioriser la cybersécurité en fonction des risques pesant sur leur activité.
2. Désigner un « référent cybersécurité » chargé de promouvoir ce sujet en interne.
3. Sensibiliser l'ensemble de leurs collaborateurs aux risques cyber et aux enjeux pour l'organisation.
4. Former leurs collaborateurs aux bonnes pratiques et aux réflexes de cybersécurité, et à veiller à leur application.
5. Anticiper les cyberattaques en élaborant des plans de secours adaptés et les tester régulièrement.
6. Évaluer fréquemment le niveau d'exposition aux risques cyber de leurs systèmes d'information.
7. Faire appel, si nécessaire, à des fournisseurs et prestataires de cybersécurité compétents, certifiés par des labels ou certifications.
8. Promouvoir les enjeux de la cybersécurité et les bonnes pratiques auprès de toutes leurs parties prenantes (clients, administrés, fournisseurs, partenaires) pour évoluer dans un environnement numérique de confiance.

Une évidence pour Whaller

L'importance de la cybersécurité réside dans plusieurs aspects cruciaux :

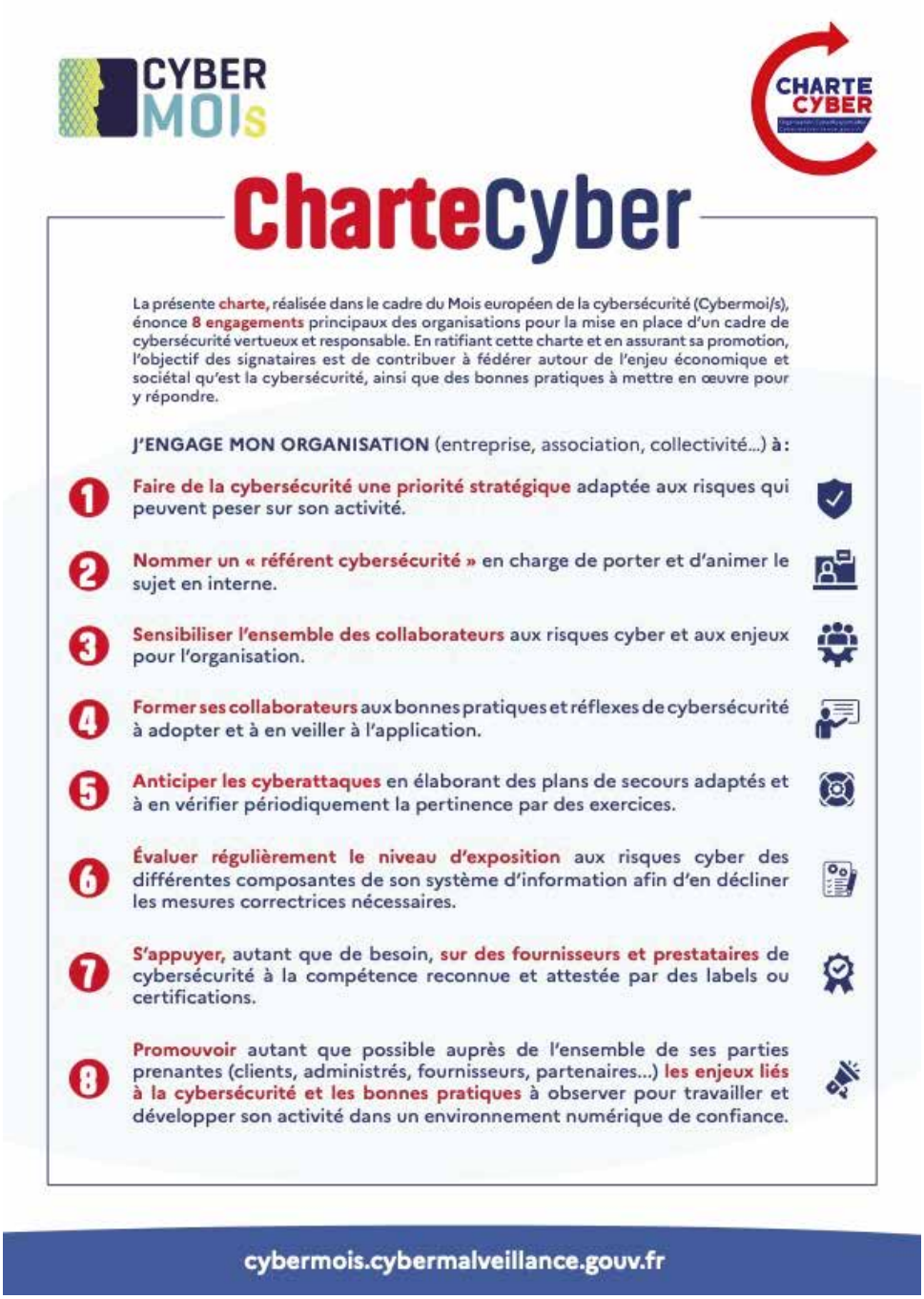
1. **Protection des données utilisateurs :** Whaller est une plateforme sociale qui traite et stocke potentiellement des données sensibles de ses utilisateurs. La cybersécurité est essentielle pour garantir la protection de ces données contre les menaces de piratage et de vol.
2. **Maintien de la confiance des clients :** Les utilisateurs de Whaller s'attendent à ce que leurs informations personnelles et leurs communications soient sécurisées. En maintenant un haut niveau de sécurité, Whaller renforce la confiance de ses clients et utilisateurs.
3. **Conformité aux règlements :** De nombreuses réglementations, telles que le Règlement général sur la protection des données (RGPD), exigent que les entreprises protègent adéquatement les données de leurs utilisateurs.
4. **Protection de la réputation :** Les violations de données et les atteintes à la cybersécurité peuvent entraîner une perte de réputation majeure pour une entreprise. Une solide cybersécurité permet d'éviter ces situations préjudiciables.
5. **Continuité des opérations :** Les attaques informatiques peuvent perturber les opérations d'une entreprise. La cybersécurité aide à garantir la continuité des services, ce qui est essentiel pour des plateformes comme Whaller.
6. **Innovation et développement :** En investissant dans la cybersécurité (qualification SecNumCloud en cours), Whaller peut continuer à innover et à développer de nouvelles fonctionnalités sans craindre les vulnérabilités potentielles.

Whaller intègre déjà le module « Assistance Cyber en ligne » de Cybermalveillance.gouv.fr dans Whaller.

Rejoignez la ChartеCyber

Si vous souhaitez que votre organisation s'engage dans cette démarche de responsa-bilité cyber, nous vous invitons à adopter la ChartеCyber et à partager votre engagement avec toutes vos parties pre-nantes.

Que vous soyez une entre-prise, une collectivité ou une association, et que vous cher-chiez à renforcer la cybersé-curité de votre système infor-matique, Cybermalveillance.-gouv.fr peut vous mettre en relation avec des profession-nels de la cybersécurité label-lisés ExpertCyber, spécialisés dans la sécurisation des sys-tèmes d'information profes-sionnels.



Comprendre les cyber wargames : Le défi ludique du hacking

Cybersécurité

Les experts en cybersécurité sont constamment mis au défi de repousser les limites de leur savoir-faire pour contrer les menaces en constante évolution. L'un des moyens les plus fascinants et éducatifs pour renforcer ces compétences est le cyber wargame. Ces jeux de hacking simulés offrent une plateforme unique pour mettre à l'épreuve les compétences en sécurité informatique, apprendre de nouvelles techniques et relever des défis stimulants.

Qu'est-ce qu'un « cyber wargame » ?

Un cyber wargame est un jeu informatique qui simule des scénarios de sécurité réalistes où les participants doivent utiliser leurs compétences en hacking éthique pour résoudre des défis spécifiques. Ces jeux peuvent varier en complexité, allant des énigmes relativement simples aux scénarios de sécurité réseau sophistiqués. Les participants sont souvent confrontés à des problèmes tels que la recherche de vulnérabilités, l'exploitation de failles, la détection d'intrusions, et bien plus encore. Les cyber wargames permettent aux professionnels de la cybersécurité de s'entraîner dans un environnement contrôlé et sans risque.

Comment fonctionnent-ils ?

Les cyber wargames sont généralement hébergés sur des plateformes en ligne dédiées. Les participants se voient attribuer un scénario et doivent résoudre un ensemble de défis pour progresser. Ces défis sont conçus pour imiter des situations réelles que les professionnels de la cybersécurité pourraient rencontrer. Les participants utilisent leurs compétences techniques pour analyser les systèmes, identifier les failles, développer des exploits et protéger les actifs numériques.

Pourquoi sont-ils importants pour la cybersécurité ?

1. **Apprentissage pratique :** Les cyber wargames offrent un apprentissage pratique qui complète la théorie. Les participants peuvent mettre en pratique leurs compétences en temps réel, ce qui renforce leur compréhension de la cybersécurité.
2. **Détection de vulnérabilités :** Les wargames permettent aux professionnels de la cybersécurité de rechercher et de comprendre les vulnérabilités et les failles de sécurité. Cela les aide à anticiper les attaques potentielles.
3. **Amélioration des compétences :** Les participants développent constamment leurs compétences, car les cyber wargames évoluent pour refléter les dernières menaces et techniques de hacking.
4. **Préparation aux situations réelles :** Les wargames préparent les professionnels de la cybersécurité à réagir efficacement en cas d'incident de sécurité réel. Ils acquièrent de l'expérience dans la gestion de crises.
5. **Innovation :** Les wargames favorisent l'innovation en encourageant les participants à penser de manière créative pour résoudre des problèmes complexes.

Les cyber wargames, tels que ceux organisés par TEHTRIS, jouent un rôle crucial dans la formation et le perfectionnement des experts de la cybersécurité. Ils offrent une expérience pratique et stimulante qui permet de rester en phase avec les menaces numériques en constante évolution. Les wargames sont bien plus qu'un simple jeu, ce sont des outils éducatifs et de formation, essentiels pour ceux qui défendent les systèmes informatiques du monde entier. Ils incarnent la fusion passionnante du hacking éthique, de l'apprentissage continu et de la cybersécurité moderne.

Internet en toute sécurité : protégez-vous avant qu'il ne soit trop tard

Cybersécurité

Internet est un vaste univers regorgeant d'opportunités et d'informations précieuses, mais il comporte également des risques pour ceux qui ne prennent pas leur sécurité numérique au sérieux. Dans cet article, nous expliquerons pourquoi il est essentiel pour les utilisateurs ordinaires d'Internet de comprendre les bases de la sécurité numérique et d'adopter de bonnes pratiques. Nous illustrerons notre propos avec des exemples concrets pour vous aider à prendre conscience que la sécurité numérique est une priorité, car les menaces ne concernent pas seulement les autres.

Pourquoi la Sécurité Numérique est cruciale pour tous

Imaginez Internet comme une grande ville virtuelle. Dans cette ville, vous partagez des informations personnelles, effectuez des transactions financières, échangez des messages avec des amis, et bien plus encore. Tout comme dans une grande ville, il existe des risques.

1. **Protection des informations personnelles :** Si vous ne protégez pas vos informations personnelles, des cybercriminels peuvent les voler. Par exemple, votre identité pourrait être usurpée, et vous pourriez être victime de fraudes financières.
2. **Cyberharcèlement :** Les réseaux sociaux peuvent être un lieu de harcèlement en ligne. Des inconnus peuvent vous envoyer des messages haineux, ce qui peut avoir un impact sérieux sur votre bien-être émotionnel.
3. **Virus et malwares :** Naviguer sur des sites web douteux ou télécharger des fichiers suspects peut infecter votre ordinateur avec des virus ou des malwares. Cela peut endommager vos données ou votre matériel.
4. **Vol d'identité :** Lorsque vous partagez des informations sensibles, comme des numéros de carte de crédit, sans protection, vous courez le risque de devenir une victime de vol d'identité.

Comment vous protéger

- **Mots de passe solides :** Utilisez des mots de passe uniques et complexes pour vos comptes en ligne. Ne réutilisez pas les mêmes mots de passe pour tous vos comptes.
- **Mises à jour régulières :** Assurez-vous que votre système d'exploitation et vos logiciels sont à jour. Les mises à jour contiennent souvent des correctifs de sécurité essentiels.
- **Ne cliquez pas sur des liens suspects :** Si vous recevez un e-mail ou un message inattendu avec des liens, ne les cliquez pas. Les escrocs utilisent souvent de fausses pages web pour voler des informations.
- **Sensibilisation :** Apprenez à reconnaître les signaux d'alarme. Si une offre semble trop belle pour être vraie, c'est peut-être le cas. Soyez prudent lorsque vous partagez des informations personnelles en ligne.
- **Utilisez une protection antivirus :** Investissez dans un bon logiciel antivirus pour protéger votre ordinateur contre les menaces en ligne.

La sécurité numérique est essentielle pour tous les utili-sateurs d'Internet, car les me-naces peuvent toucher n'im-porte qui. Si vous adoptez de bonnes pratiques et suivez des mesures de sécurité de base, vous serez mieux proté-gé contre les cybercriminels et les conséquences potentielles de l'absence de sécurité numérique. Prenez les devants pour sécuriser vos données et votre bien-être en ligne. Ne laissez pas les me-naces numériques devenir votre réalité.

Passer du hameçonnage au moissonnage

Cybersécurité

Le phénomène du hameçonnage (ou « phishing » en anglais) connu également sous le nom de phishing, permet à un pirate informatique de s'emparer d'identifiants de connexion, de données personnelles ou encore de données bancaires. C'est une attaque qui est redoutable lorsqu'elle est bien menée. Elle est fréquemment utilisée en amont des attaques par rançongiciel par exemple.

Le moissonnage (ou « harvesting » en anglais) quant à lui, fait souvent référence à la collecte automatisée de grandes quantités d'informations, généralement à des fins malveillantes.

L'exemple du jour montre à quel point les pirates sont ingénieux et réactifs.

Etape 1 : Réception d'un courriel se faisant passer pour le service informatique

De : DSI <remboursements@etudiant.univ>
Pour : [redacted]
Sujet : [EXT] Problème technique
Date : 23 Oct 2023 06:03:26 +0100
Identifiant du message : [redacted]
Return-Path : <remboursements@etudiant.univ>
Received : [redacted] Mon, 23 Oct 2023 05:03:35 +0000

Remboursement 20/10/2023

Bonjour,

Cette procédure concerne les étudiants ayant déjà été inscrits et se réinscrivant pour l'année en cours.
Suite à un prélèvement bancaires injustifié de notre part, votre carte a été débité par erreur.
Conformément à la loi la banque doit vous rembourser immédiatement la somme engagée en vertu de l'article L133-18 du Code Monétaire et Financier.
Nous vous invitons à mettre à jour vos données bancaires pour pouvoir créditer votre compte, *Cliquez-ici*

Cordialement,
L'équipe de la DSI Direction des Systèmes d'Information
Assistance aux étudiants

Il s'agit d'un courriel émis à l'aide d'un compte piraté d'une université. Le courriel semble cohérent néanmoins, il y a des fautes d'orthographe.

Etape 2 : Collecte du numéro étudiant et clic sur le lien

La page reprend l'aspect d'un formulaire d'une université, le lien d'aide pointe vers la page officielle d'aide de l'application. En revanche l'adresse de la page n'a aucun lien :

https://frremb.web.app/identification.html?xml_id=/fr_FR/Login?ID=972911073

Nous ne sommes donc pas sur le site officiel.

Là encore des fautes sur la page peuvent être un indice complémentaire.

Etape 3 : Collecte des données bancaires

Désormais l'attaquant souhaite obtenir vos moyens de paiement. Vous pensez être protégés par les dispositifs mis en place par les banques type 3DSecure… il n'en n'est rien, l'attaquant a tout prévu.

Etape 4 : Validation 3DSecure et débit sur la carte

Désormais l'attaquant dispose des informations de votre carte et peut donc procéder à des achats sur Internet qui normalement seront bloqués par la protection 3DSecure sauf si vous donnez le code de sécurité…

Comment l'attaquant réussi-t-il à envoyer un SMS à la victime ou à faire afficher une notification via l'application de la banque ? En réalité, l'attaquant ne connait pas le numéro de téléphone de la victime ; la banque oui et le numéro est associé à votre carte ou à votre appli mobile. L'attaquant va donc procéder à un achat en ligne dès qu'il dispose du numéro de carte. Cet achat va entrainer la procédure 3DSecure qui passe soit par votre appli mobile, soit par SMS. Vous validez la transaction ou communiquez le code reçu par SMS, l'attaquant peut alors valider son achat en ligne.

Étape 5 : Exploitation des informations.

Une fois que l'attaquant a réussi à collecter les informations, il peut les exploiter de diverses manières : ventes sur le darkweb, transactions frauduleuses, usurpation d'identité, ou lancement d'autres attaques ciblées en utilisant les informations collectées.

Étape 6 : Comment se protéger ?

1. Ne jamais cliquer sur les liens dans les mails dès lors qu'il s'agit d'argent ou de problème informatique
2. Regarder l'adresse de l'expéditeur et s'il y a un lien avec la signature du mail (dans notre exemple le courriel provient d'un compte remboursement mais dans le contenu il est fait état de la DSI)
3. Passez la souris au-dessus du lien dans le message pour révéler l'adresse. (Dans notre exemple le lien ne pointe pas vers une ressource l'université).
4. Ne communiquez jamais vos coordonnées bancaires si vous n'êtes pas en train de réaliser un achat. Les remboursements sont rarement réalisés par carte bancaire.
5. Ne communiquez jamais les codes de validation reçu par SMS ou sur vos applications mobiles. Dans les applications regardez toujours le détail de la transaction pour le ver le pot aux roses. Utilisez un gestionnaire de mots de passe pour éviter de saisir vos identifiants sur des sites web malveillants.
6. Activez la double authentification (2FA) chaque fois que cela est possible, ce qui ajoute une couche de sécurité supplémentaire même si vos identifiants sont compromis.
7. Soyez sceptique vis-à-vis des demandes urgentes ou des menaces dans les courriels, car les attaquants utilisent souvent des tactiques d'intimidation.
8. Gardez vos logiciels à jour, y compris votre système d'exploitation, votre navigateur et les plugins, car cela réduit les vulnérabilités potentielles.
9. Éduquez-vous et formez-vous régulièrement sur les dernières techniques du hameçonnage et les tendances en matière de sécurité.

Il est essentiel de se rappeler que, bien que la technologie soit un élément crucial pour se défendre contre le hameçonnage, la sensibilisation et l'éducation sont tout aussi importantes pour prévenir de telles attaques.

> 📖 En savoir plus : Cybersécurité

Jeux vidéo et cybersécurité : naviguer en sécurité dans l'arène numérique

Cybersécurité

Dans l'arène des jeux vidéo, chaque joueur est un héros, traversant des mondes épiques, formant des alliances légendaires et remportant des victoires historiques. Cependant, chaque héros fait face à des ennemis et dans le monde numérique, ces adversaires prennent la forme de menaces en matière de cybersécurité.

Des ennemis cachés dans l'ombre

Le monde du jeu en ligne est vaste et, malheureusement, il n'est pas exempt de menaces. En plus des dangers déjà largement reconnus tels que le swatting (l'action d'envoyer des forces de l'ordre à l'adresse d'un joueur en feignant une situation d'urgence), le doxing (la divulgation non autorisée de données personnelles) et le cyberharcèlement, d'autres menaces, plus sournoises, continuent de surgir :

Swatting : quand le jeu tourne au cauchemar

Le swatting est une menace effrayante qui a malheureusement fait son chemin dans le monde du jeu en ligne. Imaginons un instant que vous soyez plongé dans une partie de jeu, seulement pour être soudainement interrompu par l'arrivée inattendue de la police ou d'une équipe d'intervention d'urgence à votre porte. C'est exactement ce que subissent les victimes de swatting. En exploitant des informations personnelles, certains individus malveillants signalent de fausses urgences aux forces de l'ordre, provoquant des interventions chez des joueurs innocents. Les résultats peuvent être traumatisants, voire mortels.

Doxing : la divulgation d'informations privées

Le doxing est une autre menace qui plane sur la communauté des joueurs. Il s'agit de la révélation d'informations personnelles, telles que l'adresse, le numéro de téléphone ou les informations de contact, d'un joueur. Cette exposition volontaire ou involontaire, met en danger la sécurité physique et numérique des joueurs. Les conséquences peuvent aller du harcèlement en ligne à des actes malveillants dans la vie réelle.

Cyberharcèlement : un combat permanent

Le cyberharcèlement touche un grand nombre de joueurs et il peut prendre diverses formes, notamment les menaces, les insultes, le harcèlement en ligne, et plus encore. Le cyberharcèlement peut avoir un impact dévastateur sur la santé mentale des victimes et les contraindre à quitter leur passion pour les jeux vidéo.

Pédocriminalité : l'exploitation des innocents

La pédocriminalité dans l'univers du jeu en ligne est une réalité alarmante. De nombreux prédateurs utilisent ces plateformes pour entrer en contact avec des jeunes joueurs innocents. En se faisant passer pour des amis ou des camarades, ces individus malintentionnés essaient d'établir une relation de confiance avec leurs cibles afin de les manipuler ou les exploiter. Les parents et les tuteurs doivent être vigilants et éduquer les jeunes sur les dangers potentiels, et les encourager à signaler tout comportement suspect.

Apologie du terrorisme : le jeu en tant que vecteur d'idéologies

L'apologie du terrorisme est une menace croissante dans le monde du jeu en ligne.

Des groupes extrémistes exploitent la popularité et la portée des plateformes de jeux pour diffuser leurs idéologies haineuses et recruter de nouveaux membres. En utilisant les moyens de communication intégrés à ces jeux, ils peuvent toucher un large public, souvent jeune et impressionnable. Il est essentiel que les plateformes de jeux mettent en place des mécanismes de surveillance et de signalement pour combattre ces activités.

Hameçonnage : l'illusion des récompenses

L'hameçonnage, ou phishing, est une technique de fraude courante dans le monde numérique. Dans l'univers des jeux en ligne, les joueurs reçoivent souvent des messages les incitant à cliquer sur des liens pour obtenir des récompenses ou des avantages dans le jeu. Cependant, ces liens peuvent être malveillants, ayant pour but de voler des données personnelles ou financières. Les joueurs doivent toujours être prudents avant de cliquer sur des liens ou de partager des informations.

IoT (Internet des Objets) : l'ère des appareils connectés vulnérables

Avec l'essor de l'Internet des Objets (IoT), de plus en plus d'appareils sont connectés, y compris dans le monde du jeu. Consoles, écouteurs, claviers, souris, et d'autres périphériques peuvent être la cible de cyberattaques. Ces attaques peuvent compromettre la sécurité des informations personnelles des joueurs ou même prendre le contrôle de leurs appareils. Il est crucial de mettre à jour régulièrement les logiciels et de veiller à la sécurité de tous les appareils connectés.

Un guide dans cette quête : COMCyberGEND

Face à ces risques grandissants dans l'univers du gaming, le COMCyberGEND (Commandement de la Gendarmerie dans le Cyberespace) s'est imposé comme une force majeure pour la protection des joueurs. Spécialisé dans la lutte contre la cybercriminalité, ce commandement de la Gendarmerie Nationale française œuvre activement pour traquer et arrêter les criminels en ligne, y compris ceux qui ciblent les gamers.

Dans cette mission, le COMCyberGEND ne se limite pas à des interventions réactives. Il collabore activement avec les acteurs du secteur du jeu vidéo pour sensibiliser les joueurs aux risques en matière de sécurité informatique, et encourage vivement la signalisation des incidents. Cette approche est vitale pour combattre le cyberharcèlement et le doxing.

Ce travail collaboratif s'étend jusqu'à inclure des experts du secteur privé. Notamment, deux collaborateurs de Whaller, membres éminents de la réserve citoyenne du ComCyberGend, apportent leur expertise en participant activement au groupe de réflexion « Communication et rayonnement du ComCyberGend », consacré à la sécurité numérique des gamers. Leur contribution souligne l'importance de la sensibilisation et de la prévention dans ce domaine souvent négligé.

Le Commandement de la Gen-darmerie dans le Cyberespace est un exemple remarquable d'engagement pour la sécurité numérique dans un domaine souvent négligé. Grâce à leurs efforts, de nombreux joueurs peuvent continuer à explorer des mondes virtuels en toute sécurité.

Les joueurs doivent rester conscients des risques poten-tiels en matière de sécurité informatique et prendre des mesures pour protéger leurs informations personnelles. En cas d'incident, la collaboration avec des organisations telles que le COMCyberGEND est essentielle pour lutter contre ces menaces.

Bien que les jeux vidéo peuvent offrir d'innombrables heures de divertissement, il est crucial de veiller à ce que cette passion ne se trans-forme pas en cauchemar numérique. Les initiatives de groupes comme le COMCy-berGEND sont essentielles pour garantir un univers de jeu aussi sécurisé qu'amusant.

> 📖 Découvrez plus sur la Cybersécurité et comment vous protéger.

Formation et sensibilisation à la cybersécurité : un enjeu capital

Cybersécurité

À l'ère du tout numérique, la cybersécurité s'impose comme un pilier essentiel de l'écosystème informatique. L'éducation et la sensibilisation à la cybersécurité ne sont plus de simples options, mais des nécessités impératives pour les individus et les entreprises. Cet article se propose d'explorer les enjeux de la cybersécurité, soulignant l'importance cruciale de la formation et de la prise de conscience, tout en mettant en lumière le rôle stratégique des digital workplaces telles que Whaller dans cet écosystème.

L'importance de la sensibilisation

La première ligne de défense contre les cybermenaces n'est autre que l'utilisateur lui-même. Une sensibilisation adéquate permet non seulement d'identifier les menaces potentielles, mais aussi d'adopter les bonnes pratiques pour les contrer. La formation de sensibilisation à la sécurité informatique devient ainsi un outil précieux pour protéger les informations sensibles et préserver la réputation des entreprises. Elle est le fondement sur lequel repose la sécurité des données et des systèmes d'information.

La formation à la cybersécurité

L'éducation en matière de cybersécurité ne doit pas se limiter à de simples directives, mais plutôt évoluer vers une formation continue qui s'adapte aux menaces sans cesse renouvelées. Smart Formation, en collaboration avec des plateformes comme Whaller, offre des programmes de formation dynamiques qui non seulement élèvent le niveau de connaissance des employés, mais les engagent également à être vigilants et proactifs.

Le rôle de Whaller

Dans la sensibilisation à la cybersécurité, Whaller se distingue comme une digital workplace qui va au-delà de la simple fourniture d'outils collaboratifs. Elle intègre la sensibilisation à la cybersécurité dans son ADN, offrant un environnement sécurisé où la formation devient partie intégrante de l'expérience utilisateur. En partenariat avec Smart Formation, Whaller se positionne à l'avant-garde de la lutte contre l'illettrisme numérique, armant les utilisateurs des connaissances nécessaires pour naviguer en toute sécurité dans le cyberespace.

Notre action avec Pif Le Mag

L'initiative récente avec Pif Le Mag illustre parfaitement l'engagement de Whaller envers la sensibilisation des jeunes générations. En unissant leurs forces, Whaller et Pif Le Mag s'attaquent à la racine du problème en éduquant les « petits explorateurs du numérique » à l'hygiène numérique. Ces efforts préventifs sont essentiels pour instaurer une culture de la cybersécurité dès le plus jeune âge.

La sensibilisation et la formation à la cybersécurité ne sont pas de simples mesures de précaution, mais des composantes essentielles de la stratégie globale de toute entreprise. Des plateformes comme Whaller, en collaboration avec des entités de formation telles que Smart Formation, jouent un rôle pivot en façonnant un environnement numérique où sécurité et éducation vont de pair. Alors que le paysage des cybermenaces évolue, notre résilience collective dépendra de notre capacité à rester informés, éduqués et préparés.

Numérique souverain

Forger l’Indépendance de la France dans l’ère du digital

À l'ère du tout numérique, la question de la souveraineté numérique s'impose avec acuité, révélant ses enjeux cruciaux pour la sécurité et l'autonomie de la France. En ma qualité de Président et fondateur de Whaller, j'ai pu observer de près les défis et opportunités que le numérique présente pour notre souveraineté nationale.

La souveraineté numérique transcende la simple protection des données. Elle incarne une prise de contrôle sur nos infrastructures numériques, essentielle pour notre avenir économique et social. Face à la prédominance des géants technologiques non européens, tels que les GAFAM, notre dépendance actuelle nous confronte à des vulnérabilités majeures.

Il est temps pour l'Europe de se réveiller et de contrer cette forme de colonisation numérique. Nous devons nous orienter vers des solutions technologiques européennes et renforcer notre législation pour sauvegarder nos intérêts stratégiques. L'émergence d'un cloud souverain marque une première étape décisive, mais il ne s'agit là que du commencement d'une longue marche vers l'autonomie.

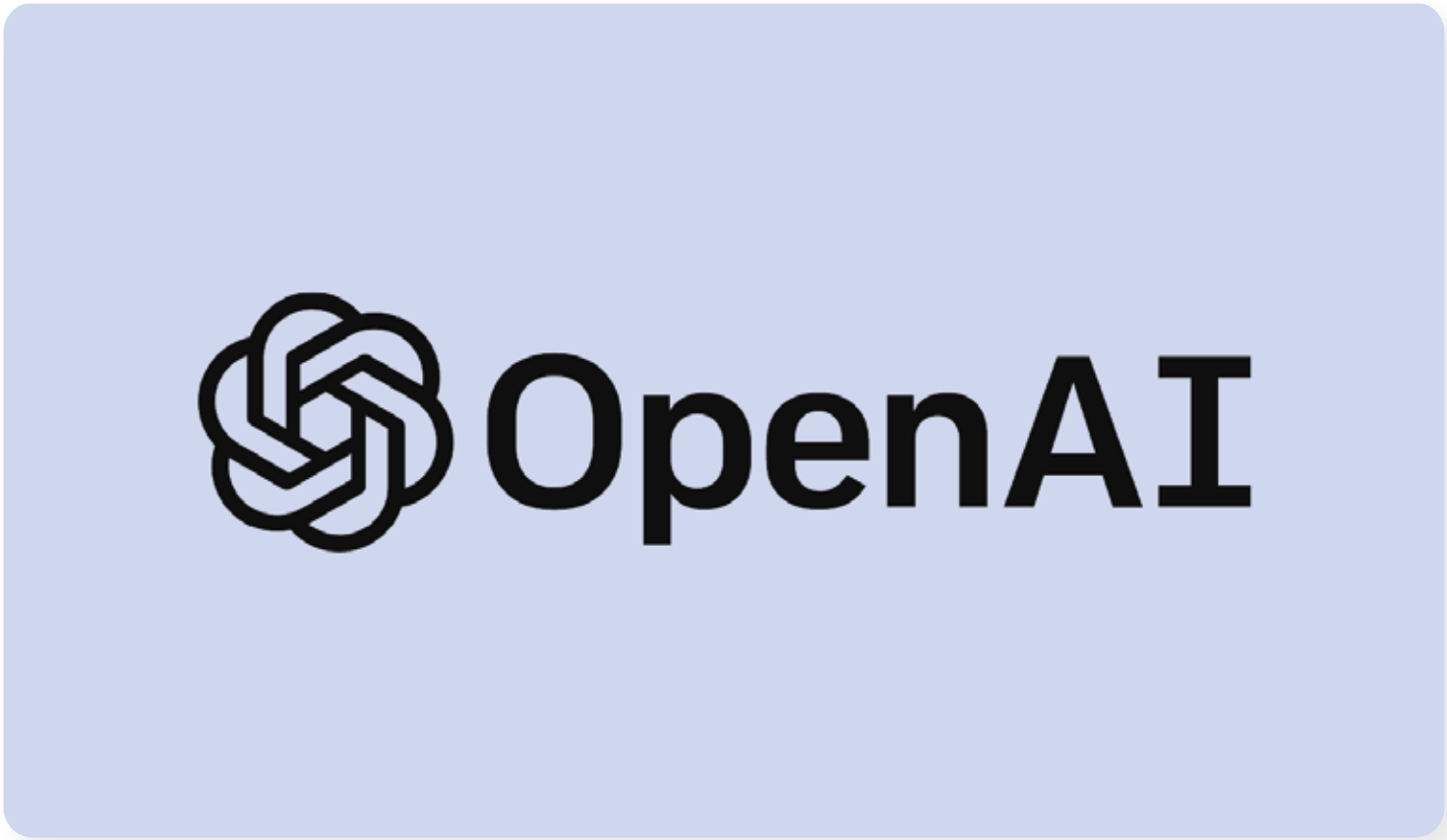
La crise sanitaire de la Covid-19 a mis en exergue notre dépendance critique envers l'extérieur pour des ressources essentielles, un constat qui doit nous alerter également sur le front numérique. L'urgence est à l'action pour bâtir une Europe numérique forte et autonome.

Enfin, j'appelle à une prise de conscience collective. La souveraineté numérique n'est pas seulement l'affaire des gouvernements et des entreprises, mais de tous les citoyens. En nous informant et en soutenant les initiatives locales, nous pouvons tous contribuer à cette souveraineté tant nécessaire.

Thomas Fauré
Président & fondateur de Whaller

L'IA Chat GPT : une évolution ou une révolution ?

Souveraineté numérique



C'était la fin de l'année 2022. Nous voulions écrire sur une IA – intelligence artificielle – qui faisait beaucoup parler d'elle, Chat GPT (pour Generative Pre-Trained Transformer). Or, il se trouve que les célébrations du centenaire de la mort de l'écrivain Marcel Proust s'achevaient – l'un des auteurs préférés, soit dit en passant, du ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique, Bruno Le Maire.

Nous avons donc demandé au robot conversationnel Chat GPT de le faire en lui posant la question suivante « Merci de m'écrire un texte à la manière de Marcel Proust sur les forces de l'intelligence artificielle ». Et voici sa réponse :

« Dans un monde où les progrès de l'intelligence artificielle sont de plus en plus spectaculaires, il est difficile de ne pas être fasciné par les forces qui la sous-tendent. Depuis l'aube de l'humanité, nous avons toujours été attirés par l'idée de créer des êtres plus intelligents que nous, capables de résoudre les problèmes complexes qui nous dépassent. Et aujourd'hui, grâce aux progrès de la technologie, nous sommes enfin en mesure de réaliser cet ancien rêve […] »

Etonnant ! Même si on est encore loin de la beauté du style de Proust, il y a un tout petit air de l'auteur de La Recherche du temps perdu. Mais alors est-ce à dire que Chat GPT signe la fin de l'écriture humaine ? Car, le fait est là : ce chatbot, enrichi par l'intelligence artificielle, a franchi un seuil. Il peut non seulement répondre de manière experte à vos questions, mais aussi générer des idées, écrire des histoires, donner des conseils de vie, composer des poèmes « à la manière de » et coder des programmes informatiques.

Après avoir suscité beaucoup d'enthousiasme, est venu le temps des interrogations : Chat GPT est-il une évolution ou bien une révolution qui verra l'IA servir les êtres humains puis, peut-être, les dominer ? Essayons d'y voir clair en regardant ce que permet cette nouvelle application et les questions qu'elle soulève.

Comment fonctionne l'algorithme ?

Chat GPT, développé par la fondation américaine OpenAI, dont Elon Musk est un fondateur, construit ses modèles de génération de texte en utilisant des algorithmes d'apprentissage automatique. Cela lui permet de traiter d'immenses quantités de données textuelles que sont les livres, les articles de presse, les pages Wikipedia et les millions de sites Web. Certains pensent même que Chat GPT a indexé l'entièreté du web…

Optimisé pour engager la conversation, Chat GPT peut répondre aux questions et être utile en tant qu'assistant d'écriture. Il fait un travail très acceptable, voir solide et sophistiqué, en rédigeant du texte et peut même proposer des idées en apparence « originales » et ce, dans toutes les langues. Il peut également créer du code informatique sur commande. La conséquence est qu'il peut faire gagner un temps fou dans la réalisation de toutes sortes de projets intellectuels, commerciaux, artistiques, etc. Les entreprises vont pouvoir produire plus de documents écrits, plus rapidement. Dans le domaine informatique, un bon programmeur peut désormais légitimement faire ce qui, il n'y a pas si longtemps, était le travail de plusieurs codeurs. Quant aux personnes qui n'ont jamais programmé, elles pourront bientôt créer également du code exploitable.

Ainsi, en arrivons-nous à un autre impact majeur : la possibilité d'un travail hybride homme-machine.

Parce que les hommes et les femmes peuvent désormais guider l'IA de Chat GPT et corriger ses erreurs. La conséquence est que les experts seront en mesure de combler les lacunes de la capacité de l'IA, même si l'IA devient plus utile à l'expert.

Mais parallèlement, Chat GPT peut créer pour chaque utilisateur sa propre IA personnalisée qui prédit ce dont il a besoin, y répond personnellement et se souvient de toutes ses interactions. Ce n'est pas de la science-fiction. C'est désormais la réalité. Comme le dit une figure de la Silicon Valley « Chat GPT ressemble à un être humain. C'est comme un être humain, sauf qu'il possède toutes les connaissances du monde ».

Les limites de Chat GPT

Toutefois, malgré les premiers enthousiasmes que font naître Chat GPT, celle-ci est porteuse de plusieurs faiblesses qui ne sont pas sans provoquer des risques.

Un utilisateur intègre peut faire rédiger par Chat GPT une note de synthèse à partir de document que lui-même a choisi. Ensuite, il pourra lui-même contrôler la pertinence du texte. En revanche, sans vérification, l'outil risque de faire des erreurs importantes, puisque le sens lui en est étranger.

Des étudiants pourront être tentés de faire écrire leurs devoirs à leur place, comme des professionnels peu scrupuleux, des articles, y compris scientifiques. L'outil peut, en effet, ajouter des listes de références bibliographiques. Quant aux « fakes news », il peut en générer autant que l'on veut.

Quant aux entreprises, les premières qui s'empareront de Chat GPT pourraient bénéficier d'un avantage concurrentiel important, tant ce dernier est puissant, rapide et agile.

Comme nous le voyons, nous avons avec Chat GPT un outil, certes sophistiqué, capable de disserter sur tous les sujets, mais indifférent à la vérité ou à la crédibilité de ses propos.

Par ailleurs, nous ne sommes encore qu'au début de l'ère de l'IA. Nous effleurons encore la surface de ce qu'elle va nous apporter de bien ou de contestable. Et personne ne sait vraiment où celle-ci nous emmène. Dans tous les cas, il convient donc d'être prudent et d'interroger Chat GPT, comme les autres IA, afin de n'être pas surpris de leurs évolutions qui pourraient se transformer en révolution.

En effet, si Chat GPT est désormais la plus connue des IA conversationnelle, Google, Microsoft, Meta et IBM travaillent aussi au lancement de Chats rivaux. La concurrence va être rude.

Quant à nous, nous lui avons posé une dernière question pour terminer cette chronique, « Faut-il défendre la souveraineté numérique ? », dont voici la réponse :

« Il est important de défendre la souveraineté numérique pour plusieurs raisons :

- La souveraineté numérique concerne la capacité d'un pays à contrôler et à gérer son infrastructure

numérique, y compris ses réseaux de communication, ses systèmes de stockage de données et ses plateformes en ligne. Elle est essentielle pour assurer la sécurité et la stabilité de cette infrastructure.

- La souveraineté numérique permet également de protéger la vie privée et les données personnelles des citoyens d'un pays. Elle garantit que ces données ne sont pas utilisées à des fins commerciales ou politiques sans le consentement des personnes concernées.

- Enfin, la souveraineté numérique est importante pour permettre à un pays de développer son économie numérique et de maintenir sa compétitivité sur le plan international. Elle est essentielle pour encourager l'innovation et l'entrepreneuriat dans le domaine de la technologie et de l'économie numérique.

En résumé, la souveraineté numérique est un enjeu crucial pour les pays du monde entier, et il est important de la défendre pour assurer la sécurité, la vie privée et la prospérité économique à l'ère numérique. »

Que dire, si ce n'est que, là, Chat GPT, nous a convaincu…

Comment se prémunir du vol de l'attention à l'ère numérique ?

Souveraineté numérique

Nos contemporains le disent : ils sont distraits par leurs téléphones, leurs emails, les réseaux sociaux et les écrans d'une manière générale. Il est grand temps de l'admettre : le numérique vole notre attention. Il nous coupe de nos proches, de nos amis et de nos collègues de travail. Pensons un instant à la dernière fois que nous sommes allés au restaurant : combien de personnes étaient en train de regarder leurs téléphones mobiles et non pas en train de parler avec leurs interlocuteurs ? Un nombre important, quand ce ne sont pas tout simplement les enfants, parfois très jeunes, qui regardent des tablettes et ne parlent pas à leurs parents. Ainsi, devenus dépendants à la technologie, cette situation a des conséquences importantes sur nos vies. Il est temps de retrouver ce temps perdu.

Les conséquences des réseaux sociaux

Tout est documenté. Les preuves sont là. Les entreprises du numérique, à commencer par les GAFAM, travaillent délibérément à voler notre attention. C'est ce que l'on nomme l' « économie de l'attention ». Le journaliste français, Bruno Patino, a publié un livre au titre éloquent à ce sujet, La civilisation du poisson rouge, petit traité sur le marché de l'attention (Le Livre de poche, 2019).

En effet, Google a mesuré la durée d'attention moyenne de la génération des millénaires (ceux qui sont nés avec un portable dans la main). Elle est de neuf secondes, contre huit secondes pour un poisson rouge. Et Bruno Patino montre que ce n'est pas le fruit du hasard, mais le modèle économique des GAFAM qui se sont appuyés sur les études comportementales des joueurs de casinos.

Face aux bandits manchots, ces derniers ne cessent jamais de remettre des pièces dans la machine, car celle-ci les fait gagner à échéance régulière. En effet, elles ont été programmées avec un mécanisme de récompense aléatoire pensé pour rendre accro les joueurs. C'est ce mécanisme que l'on retrouve sur les fils d'infos de Facebook ou les vidéos d'Instagram : seulement une info ou une vidéo sur dix intéresse l'internaute, mais cela suffit à le tenir en haleine des heures, et ainsi à en faire un prisonnier en lui volant son attention.

Difficulté à se concentrer

La conséquence est que notre capacité à nous concentrer diminue, ce qui provoque des conséquences en cascade : solliciter en permanence, nous travaillons moins bien, nous sommes moins disponibles aux autres et les performances de notre mémoire baisse.

Lorsque nous recevons un message, la plupart d'entre-nous ressentent le besoin de répondre immédiatement. Quant aux notifications, nous les regardons sans attendre.

Par ailleurs, il est prouvé que la simple présence d'un smartphone sur une table réduit notre capacité de mémoire et celle de raisonner. Sa vision provoque une sorte de stimuli dans notre cerveau qui se met à attendre que nous ouvrions notre smartphone.

Chez les plus jeunes, l'hyper-connectivité est la source d'une anxiété forte qui provoque des symptômes de dépression.

Last but not least, de nombreuses études montrent que la consultation de son téléphone avant de se coucher réduit la qualité de notre sommeil. Les messages, les images et les vidéos nous hantent.

Dégradation de la qualité de nos échanges

Parallèlement à la captation de notre attention, lorsque nous envoyons des e-mails, des SMS ou lorsque nous conversons en ligne, sur WhatsApp par exemple, nous sommes plus susceptibles de mal interpréter ce que les autres disent.

Nous pensons que nous comprenons bien nos interlocuteurs, or ce n'est pas le cas, comme nous avons souvent pu le constater. Combien de fois avons-nous été la cause ou la victime d'un malentendu ? Souvent, car cela arrive régulièrement.

Ainsi, l'utilisation accrue de la technologie entrave nos manières de communiquer avec les autres. Nous altérons notre capacité à bien nous exprimer et à nous faire comprendre. Quant aux signaux physiques émis par les autres – le fameux body-language -, il s'efface avec le numérique, y compris en visio-conférence. Et ce ne sont pas les émoticônes ou l'usage répété de trois petits points en fin de phrase qui permettent d'augmenter la qualité et la clarté de nos échanges via le numérique. Au contraire, ils illustrent l'appauvrissement que nous constatons de la qualité de nos relations.

Comment regagner notre temps perdu ?

Si nous voulons récupérer notre temps, notre attention et notre énergie pour les choses que nous jugeons importantes, nous devons commencer par examiner notre relation avec nos téléphones. Ce sont les plus grands « voleurs d'attention » du moment, c'est-à-dire du temps perdu pour nous.

En effet, il en va de notre santé mentale, de notre indépendance d'esprit, de notre liberté, tant chez les adultes que chez les enfants.

Tout comme un voleur, les voleurs de temps sont sournois, secrets et prennent ce qui a de la valeur pour nous sans que nous le sachions. Il convient maintenant de se protéger. Pour ça, nous vous proposons 5 mesures. Elles demandent de la volonté et de la discipline. Mais c'est le prix à payer pour retrouver son discernement et son indépendance.

Faire attention à son temps d'écran

Cela revient à éteindre son smartphone et tous les écrans multimédias, de les mettre dans une autre pièce. Il faut aussi créer des limites efficaces – un « mur de Chine » ! – entre son travail et sa vie personnelle lorsque vous les utilisez et ne les utilisez pas.

C'est peut-être la meilleure façon de commencer à devenir plus productif, plus heureux et plus connecté aux gens qui vous entourent, à commencer par sa famille et ses amis.

Il existe dans chaque smartphone une fonctionnalité qui permet de savoir le temps que l'on a passé sur ce dernier. La consulter sera utile, la vérité sortant aussi des chiffres.

Se désintoxiquer des médias sociaux

Éteignez simplement votre téléphone pendant quelques heures et remplacez le temps que vous auriez passé devant l'écran par des activités alternatives qui peuvent s'avérer plus enrichissantes : aller au musée, lire, écouter de la musique ou cuisiner.

Parallèlement, désactivez les fonctionnalités qui vous signalent la réception d'un message ou d'une notification. Vous ne serez plus tenté de vous précipiter pour savoir ce qui se passe.

Définir des moments d'utilisation des médias sociaux

Plutôt que de faire défiler votre écran pendant un nombre d'heures incontrôlé, gagnez du temps en allouant certains moments de la journée où vous pourrez utiliser les médias sociaux à votre guise.

Regardez des vidéos plus longues ou lisez des messages plus longs

En faisant cela, vous serez en mesure de persévérer lorsque vous vous engagez avec un contenu qui prend plus de temps à assimiler. Regardez un film ou lisez un livre, vous retrouverez, outre la maîtrise de votre concentration, des sensations dont vous avez probablement oublié les bienfaits.

Enfin, en conclusion, sachez que vous n'êtes pas seul ; que tous vos amis, que tous les parents, que tous les salariés, sont dans le même cas que vous. Aussi, on peut imaginer que bientôt, éteindre son téléphone en arrivant chez autrui reviendra, comme ce fut le cas au temps du Far West, à déposer son arme au vestiaire – mais que cette analogie soit bien comprise comme une image naturellement !

Internet des objets : quels risques pour nos données personnelles ?

Souveraineté numérique

L'ère numérique dans laquelle nous vivons a créé un monde hyper-connecté. Chaque jour, de gigantesques quantités de données personnelles sont ajoutées à Internet et partagées via des appareils connectés. Ainsi, on estime que d'ici 2030, chaque personne aura en moyenne une vingtaine d'appareils connectés – ce qu'on appelle l'Internet des objets (IdO). Ce dernier comprend les ordinateurs portables, les smartphones, les montres, les compteurs d'électricité ou de gaz, les enceintes « intelligentes », etc.

Mais à mesure que le nombre d'appareils connectés croit – estimé à 200 milliards d'ici 2030 -, le nombre de points de vulnérabilité croit aussi. Résultat : l'expansion des cyberattaques portant atteintes à la vie privée augmentent également. Il est donc légitime de se poser la question : que deviennent nos données personnelles ?

Quelles données pour quel objet connecté ?

Qu'une information seule soit connue n'est pas le fond de problème. La difficulté dans l'Internet des objets est que celle-ci soit croisée avec d'autres. Elle peut alors révéler mon état personnel, comme le fait que je sois malade, addictif à certains produits ou passions, présent ou absent d'un lieu, etc. Il y a là une intrusion caractérisée dans ma vie privée qui me rend vulnérable. Et ce, que mes données personnelles soient utilisées à mon insu en raison d'une zone grise réglementaire – id. « Qui ne dit mot, consent » – ou bien qu'elles étaient délibérément volées pour être utilisées, revendues, échangées.

En effet, on peut alors faire pression sur moi, se faire passer pour moi, profiter de mes habitudes pour me voler, etc. La liste est longue des usages malveillants.

Prenons plusieurs exemples, en apparence anodin : les robots aspirateurs. Ils n'aspirent pas que de la poussière ! Pour être efficaces, ils engrangent toutes les informations utiles (plan, surface, agencement des pièces) à l'aide de capteurs, de caméras et de micros. Il se pose donc ensuite l'usage de toutes ces informations relatives à la vie privée de l'utilisateur. Les mêmes questions se posent pour les voitures. Elles sont désormais toutes connectées, secrétant elles-aussi des cohortes de données confidentielles comme les destinations, les trajets et leurs fréquences.

Ainsi, les critiques les plus vives à l'égard de l'Internet des objets concernent le droit à maintenir secrets certains aspects de la vie privée et à contrôler leur divulgation : la collecte et l'utilisation des données personnelles sont bien le nœud du problème.

Les enjeux de l'Internet des objets

L'avenir de la vie privée et de la cybersécurité sont donc au premier plan des préoccupations concernant la numérisation des données personnelles. Contrôler à quoi servent les données, qui peut y accéder et comment elles sont conservées sont autant de sujets désormais traités par les législations étatiques ou bien les unions politique et économique comme l'Union européenne.

Trois types de défis apparaissent :

- Le premier défi concerne la nature des données personnelles. La vie privée pourra être considérée comme un droit dans certains Etats, alors qu'elle pourra l'être comme une marchandise ou même un luxe dans d'autres (on pense aux dictatures).

Demain, plusieurs cadres juridiques encadrant la confidentialité et la protection des données cohabiteront dans le monde comme c'est déjà le cas aujourd'hui. Par exemple, si aux Etats-Unis les données personnelles sont considérées comme une marchandise ayant une valeur, ce n'est pas le cas dans l'Union européenne. Celle-ci a édicté le règlement général sur la protection des données (RGPD) qui encadre le traitement des données personnelles sur le territoire des Etats membres de l'UE.

- Le deuxième défi concerne les entreprises : la fonction même de l'Internet des objets est de capter des données personnelles. Il revient donc aux fabricants de penser, dès la conception de ces derniers, une connectivité respectueuse de la vie privée. C'est une question d'éthique.

Parallèlement, les constructeurs doivent s'atteler au défi de la cybersécurité. Pour y parvenir, celle-ci doit être pensée globalement, à l'échelle de l'organisation, et non plus comme un simple aspect technique. C'est ce qu'on appelle « Security and Privacy by design ». La sécurité et la protection de la vie privée doivent être intégrées dès la conception des objets connectés en les rendant les plus robustes possibles.

- Le troisième défi concerne la confiance numérique des utilisateurs. Il existe de nombreux cas d'entreprises violant la vie privée des consommateurs, tandis que d'autres ne parviennent pas à se protéger contre les cyberattaques. Cela alimente la méfiance des consommateurs envers les entreprises. Aussi, les entreprises doivent être plus transparentes et afficher la conformité et l'adaptabilité de leurs produits connectés à l'évolution des cadres réglementaires.

Protéger ses données personnelles

Afin de s'armer face aux risques de violation de la vie privée, il existe plusieurs solutions numériques :

- **L'anonymisation des données personnelles :** c'est un traitement qui consiste à utiliser des techniques de manière à rendre impossible, en pratique, toute identification de sa personne par quelques moyens que ce soit et de manière irréversible ;
- **L'authentification continue :** elle peut remplacer l'utilisation actuelle des noms d'utilisateur, des mots de passe et des codes PIN ;
- **L'utilisation d'algorithmes d'IA pour détecter et contrer la désinformation :** par exemple, l'IA pourra être exploitée sur les plateformes de médias sociaux et les sites d'actualités pour détecter les fausses nouvelles et les données non-fiables, puis avertir les utilisateurs afin d'empêcher leur diffusion ;
- **L'utilisation de la technologie de la blockchain pour vérifier l'authenticité des données :** lorsque les entreprises créent un nouveau contenu, elles peuvent s'en servir comme preuve de l'origine du contenu ;

- **Services d'alibi authentifiés :** il s'agit d'appareils portables et de stockage pour authentifier sa localisation. Cela aide les gens à « enregistrer » leurs moments personnels et publics et leur fournir ainsi des alibis authentifiés si cela s'avère nécessaire. Par exemple, pour démystifier un faux contenu ou des accusations injustifiées. Cela peut être une solution particulièrement utile pour les politiciens et les célébrités, dont la réputation est souvent menacée par la nature de leurs profils publics. Remarquons que, déjà, des chauffeurs de taxis filment en permanence, grâce à des petites caméras numériques embarquées, leurs déplacements afin de disposer de preuves en cas d'accidents.

Les utilisateurs doivent s'engager

Il ne faut pas laisser aux Etats et aux entreprises le sujet de la défense de la vie privée face aux objets connectés. L'histoire récente nous a montré que nos données sont officiellement exploitées, notamment par les GAFAM qui ne s'en cachent pas.

Le cas de la messagerie Whatsapp est emblématique. À plusieurs reprises, en niant avoir été piratée, elle a estimé ne pas avoir à se plier aux obligations du règlement européen de protection des données personnelles (RGPD). Par ailleurs, après avoir annoncé la modification de ses conditions d'utilisation, elle a perdu des dizaines de millions d'utilisateurs au profit de ses concurrents Signal et Telegram. La raison en était que l'application de messagerie partagerait certaines données avec sa maison mère, Facebook. Voilà un exemple de réaction salutaire des internautes s'engageant pour la défense de leurs données personnelles.

L'engagement des internautes pour leur cybersécurité est appelé la « confiance répartie ». L'exemple le plus parlant est la monnaie cryptée, le bitcoin. Son mécanisme de confiance est basé sur un système où le registre des transactions est réparti entre plusieurs nœuds du réseau. Le bitcoin prouve ainsi l'inutilité d'un tiers de confiance, en l'occurrence une banque.

L'internet des objets est en train de bâtir un nouveau continent, la Terra data, la « Terre des données ». Il convient donc, pour que celle-ci soit habitable, que tous ces acteurs, les fabricants comme les utilisateurs, travaillent ensemble pour une utilisation des données personnelles responsable et respectueuse de la vie privée. Il s'agit, ni plus ni moins, que de préserver nos libertés fondamentales.

La liberté d'expression sur les réseaux sociaux

Souveraineté numérique

La liberté d'expression est l'un des principaux droits humains fondamentaux, inscrit dans plusieurs traités internationaux relatifs aux droits humains. Ce droit s'applique à la fois hors ligne et en ligne. C'est la raison pour laquelle il a figuré en bonne place sur l'agenda diplomatique ces dernières années. Que ce soit au Conseil des droits de l'homme des Nations unies ou au Conseil de l'Europe.

En effet, dans quelle mesure les plateformes numériques sont-elles et doivent-elles être liées par la liberté d'expression même s'il s'agit d'entreprises privées ? Cette question est au cœur de la question de la modération des contenus.

Protection de notre liberté d'expression

Plusieurs instruments internationaux garantissent le droit à la liberté d'opinion et d'expression sans ingérence, ainsi que le droit de rechercher, de recevoir et de répandre des informations et des idées par le biais de tout média ou de toute frontière, notamment :

- Article 19 de la Déclaration universelle des droits de l'homme (UNHR, 1948) ;
- Article 19 du Pacte international relatif aux droits civils et politiques (PIDCP, 1966) ;
- Article 10 de la Convention européenne des droits de l'homme (CEDH, 1950) ;
- Article 13 de la Convention américaine des droits de l'homme (CADH, 1969).

Lorsqu'il s'agit d'appliquer la liberté d'expression à l'environnement en ligne, le principal instrument est la résolution du Conseil des droits de l'homme des Nations Unies sur la protection de la liberté d'expression sur Internet (2012), qui stipule que « les mêmes droits que les personnes ont hors ligne doivent également être protégés en ligne, en particulier la liberté d'expression, qui s'applique sans considération de frontières et par tout média de son choix ».

Les limites de cette liberté

Indépendamment du rôle fondamental joué par la liberté d'expression dans une société démocratique, ce droit n'est pas absolu et peut faire l'objet de limitations sous certaines conditions. Selon le droit international des droits de l'homme, une restriction à la liberté d'expression doit répondre, cumulativement, aux exigences de légalité, de légitimité, de nécessité et de proportionnalité.

Ainsi, chacun des traités évoqués ci-dessus présente une liste d'objectifs légitimes pouvant justifier une restriction à la liberté d'expression dans son propre système.

Par exemple, le PIDCP et la CADH établissent comme buts légitimes : le respect des droits ou de la réputation d'autrui, la protection de la sécurité nationale et de l'ordre public et la protection de la santé et de la morale publiques.

La CEDH présente une liste plus large, puisqu'elle inclut la prévention de la divulgation d'informations confidentielles et le maintien de l'autorité et de l'impartialité du pouvoir judiciaire comme objectifs légitimes supplémentaires susceptibles de justifier une restriction à la liberté d'expression dans le système européen de droits humains.

Naturellement, l'un des principaux problèmes est que les limitations sont ouvertes à de nombreuses interprétations différentes des normes et, en fin de compte, à des implémentations différentes.

Comment contrôler la liberté d'expression ?

Internet, et les médias sociaux en particulier, sont devenus la principale plateforme d'échange d'informations et d'idées dans le monde. Chaque jour, une énorme quantité de contenu est publiée et partagée sur les réseaux sociaux, sur lesquels plus de 4,7 milliards d'utilisateurs sont enregistrés.

En raison de ce flux toujours croissant, les médias sociaux développent des systèmes de modération de contenus afin de contrôler ce que les utilisateurs publient en ligne.

Ces systèmes, humains ou le fait d'intelligences artificielles, peuvent supprimer, signaler ou limiter la portée d'un contenu particulier ou même suspendre ou bloquer les comptes des utilisateurs. Par conséquent, ils risquent d'entraver de manière illégale l'exercice de la liberté d'expression telle qu'elle est garantie par les traités ou les conventions comme nous l'avons vu. C'est déjà ce qui est arrivé dans de nombreux pays. Les autorités gouvernementales, y compris dans des démocraties, ont surveillé les contenus, puis restreint l'accès à certains d'entre-eux. Cela s'appelle la censure.

Dans certains cas, les gouvernements vont jusqu'à fermer l'accès à Internet pour des régions ou même pour tout le pays.

Comment limiter légalement ce droit ?

Il existe un large éventail de justifications, y compris à l'occasion de l'organisation de manifestations, d'élections ou d'examens publics passés à l'université par exemple.

En 2019, dans diverses régions de l'Inde, l'accès à Internet a été interrompu de nombreuses fois en raison de manifestations contre la loi sur la citoyenneté.

En Iran, Internet a été fermé en raison de manifestations contre les réductions des subventions aux carburants qui ont fait grimper les prix pour les consommateurs.

Au Bangladesh, en République démocratique du Congo et au Gabon, l'accès a été suspendu pendant les élections.

En Éthiopie, Internet a été coupé afin de lutter contre la tricherie lors des examens finaux des écoles secondaires nationales.

Les limites de l'intelligence artificielle

C'est l'intelligence artificielle (IA) utilisée pour modérer le contenu en ligne qui présente le plus de risque, en particulier lorsqu'il s'agit de contenu controversé. La raison en est que les algorithmes d'IA n'ont pas la capacité d'évaluer le contexte, de repérer l'ironie ou de mener l'analyse complète qui est nécessaire pour identifier un contenu posant un problème.

Pour cette raison, les systèmes de modération de contenu qui s'appuient fortement ou exclusivement sur des outils d'IA sont plus susceptibles de bloquer ou de restreindre le contenu par défaut. Dans ce cas, ils peuvent violer le droit des utilisateurs de rechercher, recevoir et partager des idées et des informations. C'est ce qu'a souligné le Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression.

Par exemple, l'outil d'IA d'Instagram, DeepText, a identifié le mot « mexicain » comme une insulte. Cette confusion est née parce que le mot « mexicain » était souvent associé au mot « illégal », probablement à cause de commentaires malveillants trouvés sur Internet.

Ainsi, la modération de contenu en ligne implique un processus complexe, dans lequel le contexte du contenu publié sur les réseaux sociaux doit pouvoir être pris en compte. Pour cette raison, les outils d'IA utilisés pour la modération de contenu en ligne doivent être conçus et utilisés de manière à respecter le droit des utilisateurs à la liberté d'expression.

Les traités internationaux sur les droits de l'homme créent des obligations juridiques pour les États souverains, mais n'imposent pas directement d'obligations aux entreprises privées, telles que les entreprises de médias sociaux.

C'est la raison pour laquelle il faut être vigilant et se battre pour renforcer le droit à la liberté d'expression en ligne afin de ne pas laisser les réseaux sociaux décider seuls.

Et les sujets sont nombreux : la surveillance étatique des communications ; la protection des droits des citoyens lors des élections ; les discours de haine en ligne ; l'utilisation du cryptage et de l'anonymat ; le rôle du secteur privé et des fournisseurs d'accès numérique ; etc.

Ainsi, sauvegarder la liberté d'expression sur les réseaux sociaux est un enjeu politique, économique et social, comme la liberté de la presse en son temps. Ni plus, ni moins.

Les traités internationaux sur les droits de l'homme créent des obligations juridiques pour les États souverains, mais n'imposent pas directement d'obligations aux entreprises privées, telles que les entreprises de médias sociaux.

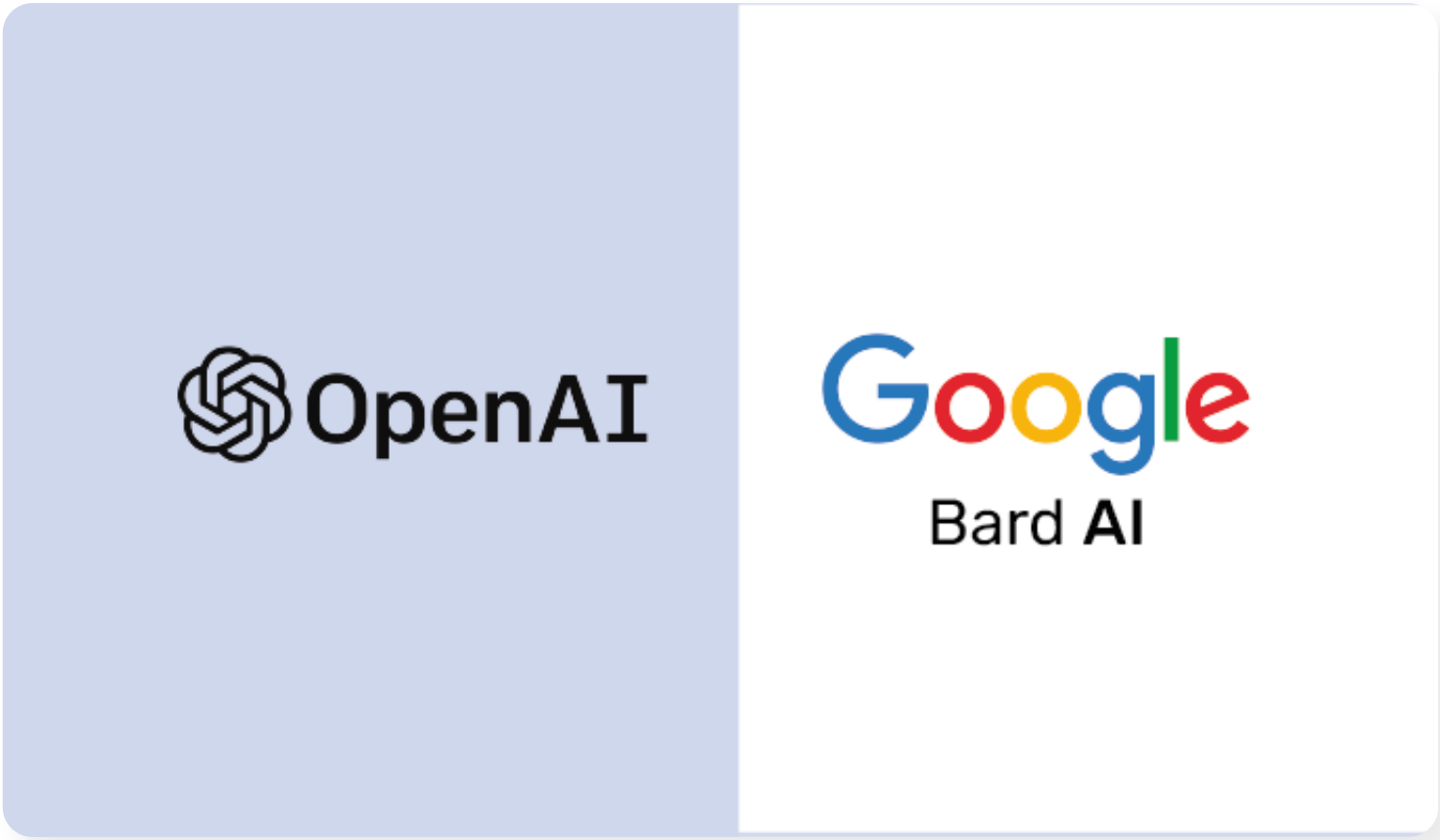
C'est la raison pour laquelle il faut être vigilant et se battre pour renforcer le droit à la liberté d'expression en ligne afin de ne pas laisser les réseaux sociaux décider seuls.

Et les sujets sont nombreux : la surveillance étatique des communications ; la protection des droits des citoyens lors des élections ; les discours de haine en ligne ; l'utilisation du cryptage et de l'anonymat ; le rôle du secteur privé et des fournisseurs d'accès numérique ; etc.

Ainsi, sauvegarder la liberté d'expression sur les réseaux sociaux est un enjeu politique, économique et social, comme la liberté de la presse en son temps. Ni plus, ni moins.

Tout savoir sur Google Bard, le prochain concurrent du ChatGPT

Souveraineté numérique



Google Bard est un nouvel outil de chatbot. Conçu à l'aide d'intelligences artificielles (IA) par Google, il est encore en phase de tests. Dressons la carte d'identité de cet outil qui a pris le nom du « poète et chanteur chez les Celtes », et explorons ses différences avec son illustre concurrent, ChatGPT développé par OpenAI.

Qu'est-ce que Google Bard ?

Google Bard est en développement depuis plusieurs années. Construit sur l'architecture de réseau neuronal Transformer de Google, il est conçu pour simuler des conversations avec un humain. Il utilise une combinaison de traitement du langage naturel et d'apprentissage automatique. Il est pensé pour augmenter les propres outils de recherche de Google (comme Bing de Microsoft utilise maintenant ChatGPT).

Les différences entre Google Bard et ChatGPT

Bien que les deux chatbots aient des capacités similaires et soient conçus pour imiter la conversation humaine, ils ne sont pas pensés de la même façon. L'une des principales différences entre ChatGPT et Bard réside dans les données d'entraînement utilisées pour créer chaque modèle.

Le modèle de ChatGPT est formé sur une quantité massive de données accessibles au public provenant d'Internet, y compris des livres, des articles et des sites Web. Ces données de formation permettent à ChatGPT de comprendre les nuances du langage humain et de générer des réponses à la fois précises et contextuellement pertinentes. Néanmoins, ces données sont limitées puisqu'elles n'ont pas été mises à jour depuis septembre 2021.

Bard a été formé sur un ensemble de données moins important que ChatGPT. En revanche, en tant que produit Google, il pourra intégrer les données mises à jour en temps réel grâce au moteur de recherche Google Search mais aussi les services de Google Maps et Google Assistant. Il offrira donc des réponses plus précises et pertinentes à certaines requêtes, en phase avec l'actualité.

Fondé sur la technologie LaMDA (Language Model for Dialogue Applications) de Google, Bard est conçu pour comprendre et générer le langage d'une manière plus proche de la façon dont les humains communiquent. Cela signifie que Bard est capable de répondre à des requêtes complexes et de fournir des réponses plus nuancées que ChatGPT. Cela donne à Google un avantage significatif en termes de qualité et de quantité de données qu'il peut utiliser pour répondre aux demandes.

Enfin, il existe des différences dans la manière dont OpenAI et Google abordent le développement et le déploiement de leurs chatbots. OpenAI est une organisation axée sur la recherche qui s'engage à faire progresser l'état de la technologie de l'IA et à la rendre accessible au plus grand nombre. A contrario, Google est une grande entreprise technologique qui propose une gamme de produits et de services, et se concentre sur la création de valeur pour ses clients et ses actionnaires.

Dans l'ensemble, bien que ChatGPT et Bard soient des chatbots très sophistiqués capables de fournir une assistance et des informations précieuses aux utilisateurs, ils diffèrent de plusieurs manières comme nous l'avons vu – que ce soit leurs données de formation, les cas d'utilisation prévus, la complexité et l'approche du développement

et du déploiement. Alors que la technologie de l'IA continue d'évoluer, il sera intéressant de voir comment ces deux chatbots continuent de se développer et de se concurrencer sur le marché.

Quand Google Bard sera-t-il disponible ?

A l'heure où nous publions cet article, Google Bard n'est disponible que pour des bêta-testeurs. Quant à son ouverture au grand public, aucune date n'a été communiquée. Cependant, dans son discours prononcé il y a quelques semaines à l'occasion du lancement de Google Bard, le PDG de Google, Sundar Pichai, a affirmé qu'il serait bientôt utilisé pour améliorer la recherche sur Google.

Notons qu'à l'occasion de cette présentation, Google Bard a connu un démarrage difficile. En effet, lors de sa démonstration en avant-première, Google Bard s'est trompé en répondant à une question sur les récentes découvertes du télescope spatial James-Webb. Il a affirmé qu'il avait été le premier à prendre une photo d'une exoplanète en dehors de notre système solaire. Or, c'était faux. Dans la foulée, le cours de l'action Google a chuté de 7 points à la bourse.

Les enjeux de souveraineté numérique au sein de l'Éducation nationale

Souveraineté numérique

L'Éducation nationale représente, en 2022, 1,2 million d'enseignants et encadrants pour 12,7 millions d'élèves et apprentis. Elle produit des quantités gigantesques de données numériques liées aux informations personnelles des élèves. Une grande variété de données personnelles sont ainsi collectées, stockées et font l'objet de traitements par une multitude d'acteurs : écoles et établissements scolaires, services académiques, collectivités territoriales, partenaires privés fournissant des ressources pédagogiques et services numériques.

Qu'en est-il de la souveraineté numérique au sein de l'Éducation nationale ? Quelles sont les mesures prises par le gouvernement pour garantir la protection des données numériques ? Quels sont les enjeux techniques pour les établissements scolaires ?

Quelles instances pour assurer la souveraineté numérique ?

En 2014, le ministère de l'Éducation a créé la direction du numérique pour l'éducation (DNE). Quelques années plus tard, son deuxième titulaire fut recruté par Amazon, ce qui fit désordre.

Face aux enjeux posés par la transformation numérique qui ne cessaient de croître, le ministère de l'Éducation nationale créa en 2019, une instance indépendante, le Comité d'éthique pour les données d'éducation. Ce dernier a pour mission de conduire et développer la réflexion sur les aspects éthiques associés à l'utilisation des données d'éducation, afin de garantir un juste équilibre entre valorisation et protection des données personnelles.

À propos de la souveraineté numérique, le comité appelle à « définir une stratégie nationale et portée par l'Europe concernant le développement de produits numériques d'éducation ». Il s'agit ainsi de proposer une « offre gratuite d'outils de téléenseignement de bonne qualité ». Inversement, il recommande le fait d' « identifier au niveau national les offres dont le fonctionnement peut poser à moyen ou long termes des problèmes éthiques liés aux données ».

Comme nous le voyons, la prise de conscience est longue à se mettre en place. Nous sommes en 2019, alors que la question de la souveraineté numérique est à l'agenda politique depuis de longues années déjà. À ce stade, ce comité émet de simples vœux qui n'engagent en rien le ministère de l'Éducation nationale.

Les enjeux liés à la pandémie

Pendant le confinement, les professeurs et leurs élèves ont utilisé massivement les outils d'enseignement à distance. Dans le peloton de tête, on trouve les plateformes numériques étrangères Microsoft – qui propose, en France, gratuitement et sans contrepartie, une partie de son offre logicielle et matérielle à de nombreux établissements scolaires – et Google avec Google Classroom, Workspace for Éducation, etc.

Cette situation agaça la direction du numérique pour l'éducation. « On ne rigole pas avec les données personnelles des élèves, considérées comme sensibles » déclara son directeur Audran Le Baron. Il fallait donc proposer autre chose.

En mai 2021, la Commission nationale de l'informatique et des libertés (CNIL) a rendu un avis, non-coercitif, déconseillant aux établissements de l'enseignement supérieur d'utiliser des « suites collaboratives états-uniennes pour l'éducation ».

La raison ? Que les données soient stockées sur le sol américain ou en Europe, en vertu de la législation des Etats-Unis, les GAFAM pouvaient les récupérer et les exploiter. La CNIL envoyait donc un message d'alerte bienvenue par les acteurs français.

> 💡 Découvrez comment Whaller a répondu aux besoins des établissements scolaires pendant la crise sanitaire avec la suite bureautique Whaller 365.

apps.education.fr, la plateforme éducative souveraine

Afin d'offrir une alternative aux outils des GAFAM, la direction numérique pour l'éducation passa aux actes en développant Apps.education.fr. C'est une plateforme libre, souveraine, compatible avec le règlement général sur la protection des données (RGPD).

Elle propose les outils essentiels du quotidien à l'ensemble des agents de l'Éducation nationale : Peertube, alternative libre à YouTube (Google), le service de partage de documents Nextcloud, comparable à Google Drive et One Drive (Microsoft), ou encore la solution de visioconférence Classe virtuelle, l'équivalent de Zoom, Meets ou Teams côté éducation.

Néanmoins, il reste une difficulté à l'adoption de la plateforme : les collectivités locales sont libres, puisque ce sont elles qui paient, d'équiper les établissements en matériels et en logiciels. Il n'est donc pas possible d'imposer une solution nationale. La DNE ne peut que prescrire sa plateforme. Aussi, compte tenu de la puissance des outils des GAFAM, que les enseignants utilisent personnellement et depuis longtemps, on peut facilement penser qu'il faudra du temps pour qu'ils adoptent la plateforme apps.education.fr.

Des mesures fortes pour les données personnelles des établissements

À la fin de l'année 2022, le ministère de l'Éducation nationale a publié une « doctrine technique du numérique dans l'éducation ». Elle constitue le cadre de référence pour les services numériques éducatifs. Elle recense des bonnes pratiques, tantôt incitatives, tantôt obligatoires, ainsi que des rappels sur la conformité au RGPD.

Parallèlement, la DNE va lancer un programme de sensibilisation des enseignants et des personnels administratifs au numérique et notamment à la protection des données personnelles.

Mais la grande nouvelle est que, simultanément, le ministère de l'Éducation nationale « a demandé d'arrêter tout déploiement ou extension [dans les classes] de cette solution [Microsoft Office 365] ainsi que celle de Google, qui seraient contraires au RGPD ». Le hic est que le ministère ne donne pas d'échéance.

L'annonce du bannissement des GAFAM de l'Éducation nationale est historique. Elle montre la prise de conscience des équipes de la rue de Grenelle. Elle respecte, d'une part, le cadre du RGPD, et d'autre part, la stratégie cloud au centre que le gouvernement a mis en place en 2021 avec la Direction interministérielle du numérique (DINUM). Cette stratégie a pour objectif de stopper l'usage et le déploiement de projets utilisant des suites américaines non conformes (notamment Microsoft et Google).

Que faire maintenant ? Que proposer aux enseignants et aux élèves qui soit opérationnel et performant ? Un collectif s'est monté. Il s'appelle le collectif Fab 8. Il est composé de 7 acteurs français de la Digital Workplace : Jalios, Jamespot, Netframe, Twake, Wimi, Talkspirit et Whaller.

En effet, Fab 8 propose une alternative crédible et puis-sante aux GAFAM tout en res-pectant la souveraineté numérique de l'Éducation nationale. Elle offre une solu-tion technologique qui reflète nos valeurs et permet de garder la maîtrise du choix de la société dans laquelle nous voulons vivre. N'est-ce pas l'essentiel ?

Il appartient désormais à l'Éducation nationale de la tester pour s'en emparer.

Fausses nouvelles : comment interpréter les fake news ?

Souveraineté numérique

Internet et les réseaux sociaux ont transformé l'information. Celle-ci est disponible partout, tout le temps, avec, comme source potentielle, chaque utilisateur. L'information n'est donc plus le privilège des médias, des agences et des journalistes. C'est dans ce nouvel environnement informationnel que les fake news ou infox sont apparues et se sont multipliées. C'est-à-dire des nouvelles qualifiées de fausses informations ou d'informations fallacieuses dont le but est de manipuler ou de tromper le public.

La conséquence de l'explosion des fake news, ou récits alternatifs, est que la vérité apparaît désormais comme une notion relative, les faits étant tout le temps et partout remis en cause. On parle alors de « post-vérité ».

Qu'est-ce que la vérité ?

Habituellement la vérité est ce qu'un individu pense être la réalité. Il formalise ses idées à travers le langage qui donne alors des caractéristiques et des limites à sa conception du monde.

Cette brève définition peut nous aider à saisir d'emblée la complexité de la vérité. Tout homme pourra donc penser être vrai ce qu'il a entendu, vu ou lu dans sa langue. Il suffira d'un bref dialogue entre deux personnes étant nées dans des pays différents, aux coutumes différentes pour s'apercevoir de la difficulté de rendre absolue une vérité. C'est-à-dire d'affirmer qu'une idée peut être vraie en tout lieu et en tout temps.

Ce problème correspond à une vision classique de la logique. Depuis Aristote, en Europe, nous pensons le plus souvent la vérité en deux termes distincts : ou bien une proposition est vraie, ou bien elle est fausse. La science moderne, qui a conduit à d'immenses avancées depuis le XVIème siècle s'est également fondée sur ce principe. Et l'émergence des sociétés démocratiques, depuis le XIXème, repose aussi sur l'idée qu'une société meilleure est possible en la fondant sur des faits considérés objectifs (comme les niveaux de revenus, les diplômes, etc).

Les événements politiques favorisent la diffusion des fausses informations

C'est ce modèle, à la fois philosophique et scientifique du monde moderne, que les phénomènes politiques majeurs des dernières années, l'élection de Trump, le Brexit, la guerre en Ukraine ont remis en cause.

Ils partagent les traits communs d'avoir vu débattre, ou s'affronter, des acteurs qualifiés, comme des journalistes scientifiques ou des universitaires reconnus, et des individus sans qualifications particulières. Cependant, ces derniers ont su s'appuyer sur une rhétorique efficace accordant plus d'importance aux émotions de leurs partisans qu'aux faits établies par la science, les faits et les chiffres.

De la même manière, dans le cadre de la guerre en Ukraine, les comptes officiels des belligérants se livrent à une véritable guerre de l'information. Ils essayent de capter l'attention du public, en déployant simultanément des récits opposés des mêmes événements en passant à la fois par les comptes twitter du ministère de la Défense comme ceux des soldats sur le terrain ou des influenceurs. Ainsi, pour lutter contre la propagation de fausses informations, le secrétariat général de la Défense et de la Sécurité nationale s'est doté d'un nouveau service depuis 2021 : VIGINUM. Ce service, technique et opérationnel, est en charge de la protection contre les ingérences numériques étrangères.

Parallèlement, l'émergence récente des logiciels de deepfake (hypertrucage) qui permettent à tout un chacun de créer des fausses vidéos ayant l'esthétique et les voix de vraies personnes, a provoqué un autre basculement. Si les faits et les données chiffrés sont considérés comme pouvant être relatifs, désormais les images et les vidéos ne sont plus des preuves

factuelles décisives.
En réaction aux fausses informations, les journaux, en France et dans le monde, ont lancé de nouvelles rubriques dont l'objectif est de vérifier les informations publiées en ligne et sur les réseaux sociaux.

Le rôle des réseaux sociaux dans la désinformation

Comme nous le constatons, l'avènement des réseaux sociaux et d'internet a drastiquement changé la puissance des organes d'informations traditionnelles. La « vérité » d'un compte Twitter ayant des millions de followers devient tout aussi puissante que celle, par exemple, des quotidiens Le Figaro ou Le Monde. Or, si les seconds sont des sources considérées comme fiables, la première est celle d'un citoyen, parfois anonyme, dont nous ignorons les motivations et les connaissances réelles.

Ainsi, de manière simple et brutale, les réseaux sociaux ont offert la possibilité de propager des informations vérifiables, ou non, à une vitesse sans précèdent. Il est donc devenu possible de créer publiquement, même sans preuve, à l'aide de quelques centaines de mots, des récits alternatifs. C'est ce nouvel état de fait dans le discours public qui a mené à parler de post-vérité.

En effet, la multiplication des informations peut donner, d'une part, le sentiment qu'il est impossible de discerner le vrai du faux. Et d'autre part, le sentiment que toute personne a la légitimité de s'exprimer sur tous les sujets. Ce qui revient à nier qu'une personne ayant du savoir est plus à même de parler sur ce qu'elle connaît qu'une autre. L'idée de post-vérité est donc dangereuse. Elle marque une rupture entre les citoyens d'un pays qui ne s'accordent plus sur la reconnaissance de la valeur du travail effectué en amont.

Paradoxalement, la violence dans les débats à propos des informations vs. fausses informations signifie pourtant que nous croyons à l'idée de vérité. Quand sur un plateau de télévision, nous mettons face à face des opposants politiques c'est que nous pensons que l'un doit avoir tort et l'autre raison. La confrontation apparaît nécessaire pour savoir lequel est le plus proche de la vérité. Ainsi, l'idée de vérité est plus vivante que jamais.

Face à la crise de la légitimité de la parole, afin de savoir « qui dit vrai ? » dans tout débat, nous pouvons être des spectateurs actifs. Pour cela, nous pouvons nous poser les questions suivantes qui nous permettront de discerner : qui parle ? Le discours de la personne est-il fondé ? A-t-elle eu accès à des faits spécifiques connus ou inconnus ? Ses sources semblent-elles solides ou pas ? S'appuie-t-elle sur la raison ou sur l'émotion ?

Par ailleurs, l'arrivée en force de l'intelligence artificiel, comme ChatGPT, va nous obliger à sourcer de plus en plus l'information. Il va devenir de plus en plus essentiel de s'assurer que ce que nous lisons, ce que nous voyons et ce que nous entendons, est fiable.

La vérité n'est donc pas morte, elle attend simplement que l'on y prête plus attention.

Le numérique, est-ce de l'industrie ?

Souveraineté numérique

Anaïs Voy-Gillis, Docteure en géographie mention géopolitique, Directrice associée de June Partners, cabinet spécialisé dans la transformation des entreprises en situation complexe est venu échanger sa vision du numérique.

Le numérique, est-ce de l'industrie ?

De mon point de vue, nous pouvons dire que le numérique est une industrie. À la fois le numérique est un élément qui peut être déclencheur de certaines révolutions industrielles, il a induit des changements techniques et sociétaux. On a eu dans les années 70, au moment du début de la 3e révolution industrielle, la révolution liée aux technologies de l'information et de la communication, des progrès techniques avec l'essor des découvertes sur certains composants clés du numérique de l'industrie. On pense par exemple aux microprocesseurs chez Intel, qui ont été des accélérateurs des transformations et des transformations notamment dans l'industrie. On parle de 3ème révolution industrielle, de 4ème révolution industrielle certains ont parlé de 5ème révolution industrielle. Mais dans les composants de la 3ème et la 4ème révolution industrielle, nous sommes sur des accélérations des procédés industriels liés à des évolutions techniques qui sont liées au numérique. Le numérique est très lié à l'industrie de ce point de vue-là.

Le numérique peut également être considéré comme une industrie, si on considère la définition de l'industrie, comme l'aspect d'avoir des choses très « processé », la capacité de gérer de la masse, d'un point de vue « donnée ». La 3ème chose c'est que le numérique repose sur des choses extrêmement tangibles, des infrastructures physiques pour communiquer, des objets qui sont le support des logiciels de la couche « soft ». Il n'y aurait pas de numérique sans ordinateur sans câble sous-marin et ces objets sont des résultants de l'industrie et des différentes révolutions industrielles.

Notre souveraineté numérique passe-t-elle par la ré-industrialisation ? Par la re-localisation ?

La réponse est « Oui » et « Non ». Oui dans le sens où derrière la notion de souveraineté il y a la notion de ce qu'on maîtrise sur notre territoire, c'est-à-dire notre faculté à ne pas dépendre d'un autre, qui peut être une entreprise. Lorsque l'on regarde la taille de certaines entreprises aujourd'hui, on voit qu'elles sont capables de rivaliser avec certaines nations mais cela peut être une nation, un groupe d'individus, il y a plein de choses qu'on peut considérer, il y a cette notion d'indépendance derrière la souveraineté.

Si on se dit être souverain sur le plan du numérique, c'est à la fois maîtriser la couche de « hard » et la couche de « soft ». C'est-à-dire, c'est comment est-ce que l'on produit une grande partie du « hard » sur le territoire français. Comment est-ce que l'on a des ordinateurs, des microprocesseurs, tous les composants que l'on va retrouver dans les outils de communication sur le territoire français. Comment est-ce que l'on maîtrise les infrastructures physiques nécessaires au numérique avec des acteurs français ?

Ensuite, nous avons toutes les couches « soft », logiciel, algorithme qui pour avoir une souveraineté doit être française.

L'enjeu pour être sur cette souveraineté, à travers la ré-industrialisation c'est de décider ce que l'on veut re-localiser, reproduire en France pour être sur un fonctionnement de dépendance choisi et non pas subi. D'autre part, c'est lorsque dans un certain nombre de domaines, que l'on ne perçoit pas forcément et qui sont peut-être moins liés à la ré-industrialisation, si on considère que la partie « soft » est peut-être moins vue comme une activité industrielle, si on ne la maîtrise pas sur le territoire français, alors on aura une ré-industrialisation partielle et je pense que dans tous les domaines nous avons pris du retard par rapport à certains grands acteurs américains ou asiatiques.

De quelle manière, une plateforme collaborative devrait-elle selon vous contribuer aux performances des organisations ?

Les plateformes collaboratives sont des outils clés pour travailler ensemble au sein d'une entreprise. Nous nous en servons pour travailler en tant que cabinet de conseil, au sein de nos équipes afin d'échanger ensemble et travailler simultanément sur un document. Nous l'utilisons également avec nos clients et les équipes clients, ce qui nous permet d'avancer ensemble et de travailler sur ces projets de transformation qui sont parfois assez lourds.

Il y a également un enjeu derrière les outils que l'on choisit, qui est l'enjeu d'avoir des outils qui garantissent la sécurité des données, la confidentialité des échanges et qui peuvent prémunir éventuellement de certains risques légaux. Avoir des outils français ou européens est un plus pour ces questions de confidentialité de sécurité.

Quelle est l'importance de la commande publique dans le développement d'un écosystème économique et industriel ?

Je considère qu'il y a 4 piliers dans la demande :

- **Le « B to C »**: On va essayer de faire en sorte que les consommateurs consomment un peu plus de produits français et permettre de structurer les écosystèmes.
- **Le B to B :** Comment les acteurs industriels vont s'approvisionner auprès d'autres acteurs industriels français donc provision France,
- **L'export**,
- **La commande publique** : La commande publique a un rôle structurant même si elle n'est pas suffisante pour accompagner certains développements, c'est-à-dire elle va garantir des volumes et donc permettre le développement aussi des activités. Là où la commande publique peut jouer un rôle notamment dans le domaine du numérique, nous avons beaucoup d'acteurs français qui sont situés à différents points de la chaîne de valeur, qui sont très performants dans ce qu'ils proposent. Le problème c'est qu'ils n'ont pas la capacité pour un certain nombre d'avoir autant de cas d'usage que des mastodontes américains ou d'autres nationalités.

La commande publique peut jouer son rôle, parce qu'elle peut donner des cas d'usage à ses acteurs pour leur per-mettre de montrer qu'ils savent faire et encourager aussi les acteurs privés de choisir ces solutions et donc de soutenir l'écosystème.

Quelle est la question que personne ne vous a jamais posée et que vous attendez déses-pérément que l'on vous pose ?

Peut-être que ce que j'aime-rais, c'est que l'on arrive tous collectivement à se dire que c'est incroyablement dur. Que tous les jours on a des raisons de désespérer de se dire que l'on n'y arrivera pas, que les choses ne vont pas dans le bon sens et que collective-ment on reste positif en se disant que chaque jour on fournit un effort, mais que chaque jour on peut contri-buer à transformer le monde pour le rendre meilleur et en tout cas plus soutenable

Qu’est-ce que la souveraineté numérique ?

Souveraineté numérique

Aux Etats-Unis, les GAFAM (Google, Apple, Facebook, Amazon et Microsoft) et en Chine les BATX (Baidu, Alibaba, Tencent et Xiaomi) dominent l’internet mondial sur lequel ils exercent une profonde influence. La dépendance des utilisateurs, qu’ils soient des particuliers, des organisations privées, publiques ou des Etats, ne cessent d’augmenter. Cet état de fait d’une « monoculture » des outils numériques soulève des enjeux stratégiques, économiques, politiques et éthiques, notamment à propos de l’utilisation des données personnelles fournies par les utilisateurs. C’est là que prend place le concept de souveraineté numérique : il vise à redonner l’indépendance numérique et le contrôle des données aux gouvernements, aux entreprises et aux particuliers.

Qu'est-ce que la souveraineté numérique ?

Selon la définition du dictionnaire Larousse pour la langue française un État souverain est un État indépendant, « reconnu dans ses frontières par la communauté internationale » et qui exerce « un pouvoir d'administration et de juridiction » sur sa population.

Néanmoins, dans l'univers numérique, cette notion n'est pas aussi claire. Si la souveraineté numérique renvoie généralement au fait qu'un État (gouvernement) ou une organisation doit établir son autorité pour exercer ses pouvoirs dans le cyberespace, elle englobe aussi des questions plus concrètes, telles que la dépendance technologique ou le contrôle des données personnelles des utilisateurs.

En effet, le mouvement défendant la souveraineté numérique vise à reconquérir une part du pouvoir exercé au sein d'un espace numérique. Aux débuts d'Internet, ses promoteurs cherchaient à développer un pouvoir affranchi des gouvernements. Publiée en 1996, « La Déclaration d'indépendance du cyberespace » est un texte célèbre rédigé à Davos, en Suisse, par John Perry Barlow, écrivain et militant politique libertaire. Elle précise que les gouvernements n'ont aucune autorité dans cet écosystème.

Or, la souveraineté des gouvernements a été très rapidement remise en cause par le développement du numérique. Ce dernier ignorant les frontières et les lois, il permet aux acteurs influents du web d'établir leurs propres règles, voire d'être considérés comme des « nations entièrement numérisées ». En témoigne la nomination par le Danemark, en 2017, d'un ambassadeur auprès des GAFAM.

En France, l'expression a été introduite dans le domaine public dans les années 2000 par Pierre Bellanger, président de la radio Skyrock, puis définie quelques années plus tard dans un essai intitulé La Souveraineté numérique. Depuis, le terme a été repris par des personnalités politiques. En 2013, l'affaire Snowden (la révélation d'écoutes massives par la NSA, Agence nationale de la sécurité, un organisme gouvernemental du département de la Défense des États-Unis) a mis en lumière les risques liés à la gouvernance des espaces numériques. Puis, en 2015, le scandale Cambridge Analytica impliquant Facebook, a mis en lumière l'utilisation frauduleuse des données personnelles des utilisateurs par des sociétés privées.

L'indépendance numérique est une notion désormais bien ancrée. Elle se traduit par des décisions concrètes prises au niveau de l'Union européenne. Elle a pour objectif de développer des solutions cloud souveraines (comme OVHcloud) et des moteurs de recherche locaux (comme la société française Qwant). Ces initiatives incitent ainsi les entreprises européennes à rechercher leur indépendance vis-à-vis des GAFAM au profit de solutions nationales ou européennes. Cela s'applique à l'utilisation des données sensibles par les entreprises. Et c'est là que réside la question fondamentale de la souveraineté numérique d'un point de vue organisationnel.

Les enjeux de la souveraineté numérique

On peut distinguer deux enjeux majeurs : l'un stratégique et l'autre éthique.

Alors que la pandémie de Covid a encore accru la dépendance des entreprises vis-à-vis des solutions cloud transnationales opérées par des acteurs américains, celles-ci doivent plus que jamais développer leur autonomie numérique afin de maîtriser leurs données (les leurs et celles de leurs clients). En effet, ces acteurs majeurs du web sont soumis à des réglementations qui peuvent aller à l'encontre des intérêts stratégiques des organisations qui les utilisent.

Par exemple, les GAFAM doivent respecter des règles d'extraterritorialité, comme le Cloud Act. Ce dernier autorise le gouvernement américain à accéder aux données hébergées par des entreprises nationales, même si leurs serveurs sont situés en dehors des États-Unis ! En conséquence de quoi, la confidentialité de ces données n'est en aucun cas garantie. Considérant que 92% des données produites en Occident sont hébergées aux USA (étude du cabinet Oliver Wyman, 2020), ces lois menacent les intérêts commerciaux européens.

Un autre exemple est l'audition récente du président de l'application Tiktok par le Congrès américain. Il a dû prouver qu'il était indépendant du pouvoir chinois (ce qui pourrait être savoureux, mais montre par l'absurde que le gouvernement américain joue sur tous les tableaux).

Par ailleurs, la question ne concerne pas seulement les règles d'extraterritorialité, elle interroge aussi les individus, en mettant l'accent sur la préservation du droit à la vie privée. En effet, dès que les organisations collectent des données, elles ont la possibilité de les revendre à des annonceurs ou à des institutions politiques. Ce fut le cas dans le scandale évoqué plus haut de Cambridge Analytica où les données personnelles des électeurs ont été utilisées pour influencer les intentions de vote. C'est aussi le cas lorsque les données confiées aux opérateurs sont sensibles, notamment les coordonnées bancaires, les informations de santé, les données financières, etc.

Pourquoi les entreprises devraient-elles prioriser la souveraineté de leurs données ?

Tout d'abord, pour protéger leurs données. Cela est particulièrement vrai pour les entreprises traitant des données sensibles, dans des secteurs tels que la défense, la santé, la sécurité, la banque et l'assurance, l'industrie, etc. Cependant, toutes les données personnelles sont en danger si elles sont volées, altérées ou détournées. Aujourd'hui, nous le savons, il n'y a absolument aucun moyen de garantir la confidentialité des données lorsqu'elles sont hébergées par les géants de la Tech. À l'inverse, les données en Europe sont protégées par les lois continentales, notamment le Règlement général sur la protection des données (RGPD) de l'Union européenne.

Deuxièmement, pour fournir des assurances aux utilisateurs. Les Français sont parfaitement conscients des enjeux liés au traitement de leurs données. Dans toutes les études d'opinion, ils souhaitent désormais que leurs données personnelles soient stockées par des acteurs européens. Ils se disent même prêts à renoncer à un service numérique s'ils ont un doute sur l'utilisation et le stockage de leurs données.

Troisièmement, réduire la dépendance vis-à-vis des solutions étrangères et les changements qui en résultent. En retour, le choix de travailler avec des acteurs locaux offre des avantages tels que la proximité, l'écoute, la réactivité et la sécurité.

En conclusion, l'Union européenne, avec 512 millions de citoyens-internautes éduqués et dotés d'un haut pouvoir d'achat, est le premier marché économique mondial, vital pour les GAFAM. Quand l'Union européenne édicte des standards, ils sont souvent repris largement par le reste du monde, excepté la Chine et le Japon, et dans une moindre mesure les Etats-Unis. Néanmoins, bientôt, le Digital Services Act et le Digital Markets Act, renforceront la protection des Européens. Quant à la Chine, gardons en mémoire qu'elle a purement et simplement banni les GAFAM de son espace.

Mais il n'est pas trop tard pour que les Européens récupèrent leur souveraineté numérique. Nous ne sommes pas David contre Goliath. C'est affaire de volonté et de convictions. Mais il n'y a « point de milieu » à la souveraineté comme l'écrivait Jean-Jacques Rousseau. Elle est ou elle n'est pas. A l'Europe d'agir désormais souverainement. Pour ça, elle peut compter sur le soutien total des entrepreneurs européens.

Les enjeux de souveraineté numérique au sein des entreprises

Souveraineté numérique

La souveraineté numérique est devenue une question stratégique pour les entreprises. Elle concerne la capacité d'une entreprise (ou d'un pays) à contrôler son propre environnement numérique, c'est-à-dire ses données, ses infrastructures et ses logiciels.

Examinons les principaux enjeux de la souveraineté numérique pour les entreprises et les raisons pour lesquelles celle-ci est désormais une question cruciale pour leurs directions générales.

Contrôler ses données

Les données sont souvent décrites comme « l'or blanc » ou le « nouveau pétrole » de l'économie numérique. En effet, les entreprises produisent et collectent une immense quantité de données qui peuvent être utilisées pour améliorer les produits et services, comprendre et satisfaire les clients, et prendre des décisions stratégiques.

Cependant, l'écrasante majorité de ces données sont stockées et traitées par des fournisseurs de services cloud dont la plupart sont basés hors de France et d'Europe. Ainsi, les trois leaders mondiaux du cloud, Amazon, Microsoft et Google qui captent environ les deux tiers du chiffre d'affaires mondial, sont américains. Cela soulève naturellement plusieurs questions : qui contrôle réellement ces données ? Qu'en est-il de leur sécurité ? Et quid de leur confidentialité malgré les engagements de ces fournisseurs : quelle loi s'applique, celle des Etats-Unis ou celle de la France ?

Evaluer sa dépendance technologique

Un autre enjeu clé de la souveraineté est la dépendance à l'égard des fournisseurs de technologie étrangers. En effet, de nombreuses entreprises dépendent de logiciels et de matériel informatique produits à l'étranger. Cette situation crée des vulnérabilités : l'entreprise peut se trouver dans une situation difficile si le fournisseur décide de changer ses termes et conditions, d'augmenter ses prix ou de cesser de fournir ses services.

Il faut aussi ajouter les risques liés aux taux de change. Les fluctuations des taux de change peuvent augmenter le coût des technologies étrangères, ce qui peut avoir un impact sur les marges de l'entreprise.

Par ailleurs, la guerre en Ukraine et les sanctions qui ont été votées par les Américains et les Européens contre la Russie ont bloqué l'accessibilité à des services numériques russes. Cela rappelle les risques politiques et réglementaires. Les politiques étrangères, les tensions internationales, les embargos ou les sanctions peuvent affecter la capacité de l'entreprise à utiliser ou à accéder à la technologie étrangère.

D'autres risques sont liés à l'intégration et à l'interopérabilité. Les technologies étrangères peuvent ne pas s'intégrer facilement avec les systèmes existants ou peuvent ne pas être compatibles avec d'autres technologies utilisées par l'entreprise, ce qui peut conduire à une baisse de la qualité des services proposés, à des pertes de temps pour rendre compatible ce qui ne l'est pas vraiment et in fine à une augmentation des coûts.

Evaluer sa cybersécurité

La cybersécurité est un autre aspect important de la souveraineté numérique. Les entreprises doivent être en mesure de se protéger contre les cyberattaques qui peuvent compromettre la confidentialité, l'intégrité et la disponibilité de leurs systèmes d'information et de leurs données.

Elles doivent pour cela mener une analyse de risque afin d'identifier les sources de menaces qui peuvent être internes ou externes à l'entreprise. Cette analyse permettra ainsi de dresser la liste des risques et ainsi prendre les mesures adéquates pour se protéger.

Qu'en est-il si les données de l'entreprise sont hébergées à l'extérieur ? Comment peut-elle s'assurer que ses fournisseurs sont eux-mêmes protégés ? Est-ce qu'elle sera informée par ces derniers si leurs systèmes d'information étaient corrompus ? Voilà autant de points à encadrer en s'appuyant sur un plan d'assurance sécurité (PAS) dans lequel d'une part l'entreprise fixe ses objectifs de sécurité et d'autre part le prestataire va expliciter ce qu'il fait pour y répondre. La perte ou le vol de données, comme le feu, peuvent entraîner la disparition d'une entreprise.

Assurer ses compétences et son innovation

Pour être véritablement souveraines sur le plan numérique, les entreprises doivent également disposer des compétences et des capacités nécessaires en interne. C'est-à-dire maîtriser les savoir-faire technologiques dont elles ont besoin pour innover et créer.

Cela nécessite qu'elles investissent dans le recrutement de collaborateurs ad hoc et dans la formation afin d'être capable d'assurer à la fois l'interface avec leurs fournisseurs de services numériques ainsi que la maîtrise de leurs programmes de recherche et développement. Il en va là de leur indépendance et de leur futur.

Maîtrise la législation et la réglementation

La souveraineté numérique amène les entreprises à se confronter à un environnement réglementaire complexe. En effet, lors de l'utilisation d'un service, d'un logiciel opéré par une société étrangère, il est probable que les lois du pays d'origine s'appliquent au produit et contraigne la société à une collaboration avec les autorités (Services de renseignement par exemple). Autre difficulté, se conformer à une multitude de lois et de règlements relatifs à la protection des données, à la cybersécurité, à la concurrence, etc. Par exemple, le RGPD s'impose à toute entreprise européenne ou non qui manipule des données personnelles de citoyens européens.

Cela peut être particulièrement délicat lorsque les entreprises opèrent à l'échelle internationale et ont à se conformer à des législations étrangères. Elles doivent alors être solidement conseillées pour bien comprendre le sens et l'esprit des lois, la jurisprudence et surtout les risques auxquels elles s'exposent.

Comment minimiser ces risques

Pour y parvenir, les entreprises doivent avoir une bonne compréhension de leur dépendance à l'égard des technologies étrangères et mettre en place des stratégies robustes pour gérer les risques que nous avons vu.

Cela peut emprunter les voies de la diversification de leurs fournisseurs, l'investissement dans la sécurité et la confor-mité, et la mise en place de plans de continuité d'activité pour faire face à des interrup-tions de service.

Néanmoins, dans un environ-nement numérique de plus en plus mondialisé et inter-connecté, la souveraineté numérique est devenue un enjeu aussi crucial pour les entreprises que ceux de l'innovation, de la conquête de parts de marché ou du recru-tement des meilleurs collabo-rateurs.

Pour y parvenir, elle exige une vigilance particulière et constante pour assurer la sécurité, l'innovation et le contrôle de leurs données. Elle demande surtout aux diri-geants du discernement, de l'indépendance d'esprit et de la capacité à s'affranchir des modes et des pressions, notamment des actionnaires.

Quelles sont les opportunités et les menaces sur le plan numérique en France ?

Souveraineté numérique

Nicolas Malbec, Capitaine de vaisseau de réserve, dirigeant également les programmes de cyber-défense au sein de l'École Hexagone, est venu nous présenter son projet de création d'entreprise « Fidelilium » et sa conception de la souveraineté numérique.

Quel est votre parcours ?

Attiré à la fois par la mer, l'informatique et le service du pays par une carrière militaire, j'ai rejoint l'école navale à l'issue de mes études et j'ai eu une carrière qui m'a permis d'alterner des postes de commandement à la mer et dans le numérique.

À la mer, j'ai pu participer à de nombreuses opérations sous tous types de bâtiments et j'ai notamment eu l'honneur de commander la frégate Nîvose. Dans les technologies de l'information, ce qui est bien dans la Marine, c'est que nous sommes formés tout au long de notre carrière. J'ai pu passer un master en réseaux de télécommunications, j'ai pu suivre un titre d'expert SSI de l'ANSSI à l'ANSSI. Cela m'a permis d'être en charge de l'entraînement cyberdéfense de la flotte, d'être responsable de la sécurité des systèmes d'information (RSI) pour l'ensemble de la Marine et d'être directeur de la transformation numérique au sein de la Marine avec un focus très important sur la donnée, la politique de la donnée, la création d'un centre de service de la donnée et d'un centre d'intelligence artificielle maritime. Plus récemment, j'ai été en charge de la planification des opérations dans le cyberespace au sein du commandement de la cyberdéfense (COMCYBER).

Pouvez-vous nous présenter « Fidelilium » ?

Le nom de la société est « Fidelilium », c'est un clin d'œil à la ville de Versailles avec « lilium » le Lys, puisque la société aura son siège social dans cette ville. Dans une démarche d'apporter de la confiance dans le numérique, vous retrouvez aussi « fidé » de « fidélise » donc l'ensemble « Fidelilium » ça doit incarner cette excellence dans la confiance numérique.

La mission de Fidelilium est de libérer et de sécuriser la vie numérique. Cela veut dire apporter de la confiance là où nous avons tendance à perdre confiance. Et probablement aussi apporter de la cohérence dans un monde numérique qui se complexifie. L'objet sera d'apporter du conseil stratégique, du conseil en cybersécurité, du conseil en transformation numérique et de manière plus générale, en souveraineté numérique. Le tout en allant chercher les standards d'excellence de l'ANSSI comme celui de prestataire en accompagnement de conseil en sécurité des systèmes d'information.

La cible prioritaire pour Fidelilium, ce sont les opérateurs d'importance vitale, les opérateurs de services essentiels et d'une manière générale, les grandes entreprises ou les entreprises qui ont de grands besoins en cybersécurité, qui ont besoin de protéger leurs actifs numériques.

Comment expliquez-vous la montée en puissance du thème de la souveraineté numérique ?

Je pense que nous arrivons à un moment de l'histoire du numérique où nous nous posons certaines questions. Nous avions un grand élan enthousiaste quand les solutions numériques sont apparues.

Nous sommes souvent allés au plus pratique, au moins cher, au plus diffusé, sans forcément se poser beaucoup de questions sur comment ça marchait, sur qui se cachait derrière telle ou telle solution…

Aujourd'hui, sans que nous ne nous en rendions compte, nous nous reposons sur ces solutions numériques. L'enthousiasme initial doit être un peu modéré. Il est plus que temps de se poser les vraies questions, c'est-à-dire quels sont les États qui sont derrière les solutions numériques que j'emploie ? Quelles sont leurs lois et éventuellement leurs applications extraterritoriales qui s'appliquent ? Comment est stocké ma donnée ? Que fait précisément tel logiciel qui est installé sur mon système d'information critique ?

Je pense que cette notion de souveraineté numérique allait arriver à un moment où nous sommes tellement dépendants des solutions numériques, que nous nous posons des questions. Est-ce que je maîtrise vraiment mon destin numérique ? Est-ce que je sais ce que je fais avec ces outils ?

Quelle est votre propre conception de la souveraineté numérique ?

La souveraineté numérique est aujourd'hui théorique, nous voulons nous réapproprier les choses, maîtriser ces systèmes d'information. C'est un concept que l'on épouse volontiers, en tout cas sur le plan théorique. Les vrais pratiquants de la souveraineté numérique, se rendent compte que ce n'est pas quelque chose de facile à réaliser.

Nous nous retrouvons dans la situation où nous avons laissé dériver une situation où des compétiteurs ont pu faire des investissements massifs dans les solutions numériques depuis les années 70, ont su développer des formations, des centres de recherche d'excellence, ont su imposer leurs standards et su développer toute une industrie du numérique. Aujourd'hui, pour avoir la maîtrise de nos systèmes d'information, il va falloir beaucoup travailler pour rattraper notre retard.

La cybersécurité est-elle une composante majeure de la souveraineté numérique ?

Effectivement, la cybersécurité, si nous rappelons ses 3 piliers qui sont : la confidentialité, l'intégrité et la disponibilité, un maillon essentiel de la souveraineté numérique. Par exemple, si nous nous situons au niveau d'un État, la confidentialité des informations dans le domaine militaire, est quelque chose d'essentiel. Si nous nous plaçons au niveau d'une centrale nucléaire, d'une entreprise de transport ou d'un système bancaire, l'intégrité des données, c'est juste vital. Pour chacun d'entre nous et pour l'ensemble des acteurs économiques et étatiques, la disponibilité des services numériques est quelque chose d'essentiel parce que sans cela, la vie s'arrête. Nous sommes dépendants de ces systèmes. Maîtriser ces trois piliers : la confidentialité, l'intégrité et la disponibilité, c'est essentiel en matière de souveraineté numérique.

Je dirais qu'en la matière, la France possède un atout non négligeable, car elle a su conserver une filière d'excellence en mathématiques permettant d'avoir une maîtrise des outils cryptographiques. Ainsi la cryptographie va participer à la confidentialité à l'intégrité et d'une certaine mesure, la disponibilité des systèmes.

Quelles sont les caractéristiques des milieux numérique et maritime ?

Le milieu maritime comme le milieu numérique, ont déjà la caractéristique de vivre complètement sur l'innovation. Au début de l'humanité, il n'y avait ni bateau, ni ordinateur et d'innovation en innovation, nous avons pu créer des systèmes aussi complexes que des sous-marins nucléaires, lanceurs d'engins ou des ordinateurs quantiques. Deux domaines portés par l'innovation, après deux domaines qui ont connu leur âge d'or sur la liberté de navigation.

Ce sont vraiment des domaines où ce sont les flux que nous considérons et nous pouvons aller naviguer, au gré du vent et au gré des envies. Cet âge d'or est malheureusement révolu dans le milieu maritime où il y a une appropriation de la mer, des zones économiques exclusives qui s'agrandissent et des enjeux géopolitiques très marqués, comme nous pouvons le voir en mer de Chine par exemple, des enjeux économiques liés aux hydrocarbures enfouis sous les mers. Dans le domaine numérique, c'est un peu la même chose, nous pouvons voir des Etats qui se retranchent derrière leur propre Internet. Nous avons le cri de firewall en Chine qui a la capacité d'isoler son réseau. Nous avons le runet en Russie, etc.

Chacun essaie d'avoir la maîtrise de son environnement numérique et je pense que c'est très lié à la montée en puissance du champ cognitif dans le cyberespace. Aujourd'hui, il y a des enjeux d'influence énorme, notamment via les réseaux sociaux. L'étincelle qui nous y a fait penser enfin qui nous a fait découvrir la puissance de ces réseaux sociaux c'était le printemps arabe. Mais depuis, nous voyons bien que nous allons de crise en crise et à chaque fois, la dimension numérique, la dimension cognitive dans le cyberespace a toujours un rôle clé.

Quelles sont les opportunités et menaces sur le plan numérique en France ?

En matière d'opportunités, elles sont nombreuses puisque nous sommes dans le domaine du numérique sur des technologies qui évoluent et qui changent presque tous les quatre ou cinq ans. Ce que nous voyons arriver de façon massive, c'est la robotique humanoïde, ce sont les technologies du numérique dans l'espace, c'est l'intelligence artificielle et là je pense que dans ces trois domaines, par exemple, la France a de réels atouts. Par exemple, sur la robotique humanoïde, nous sommes à un moment de l'histoire où toutes les technologies existent. Maintenant, il va falloir trouver l'intégrateur de génie qui va donner satisfaction au marché. Pourquoi pas une entreprise française ?

En matière de menaces, la principale est de ne pas suffisamment former notre jeunesse à ces enjeux numériques. Il faut dès le collège et le lycée présenter les filières scientifiques comme des filières d'excellence, créer des centres de recherche qui soient compétitifs. En tout cas, si nous ne le faisons pas c'est sûr que d'autres pays dans le monde le feront en investissant massivement dans l'éducation aux sciences de l'informatique et du numérique.

Qu'attendez-vous d'une plateforme collaborative ?

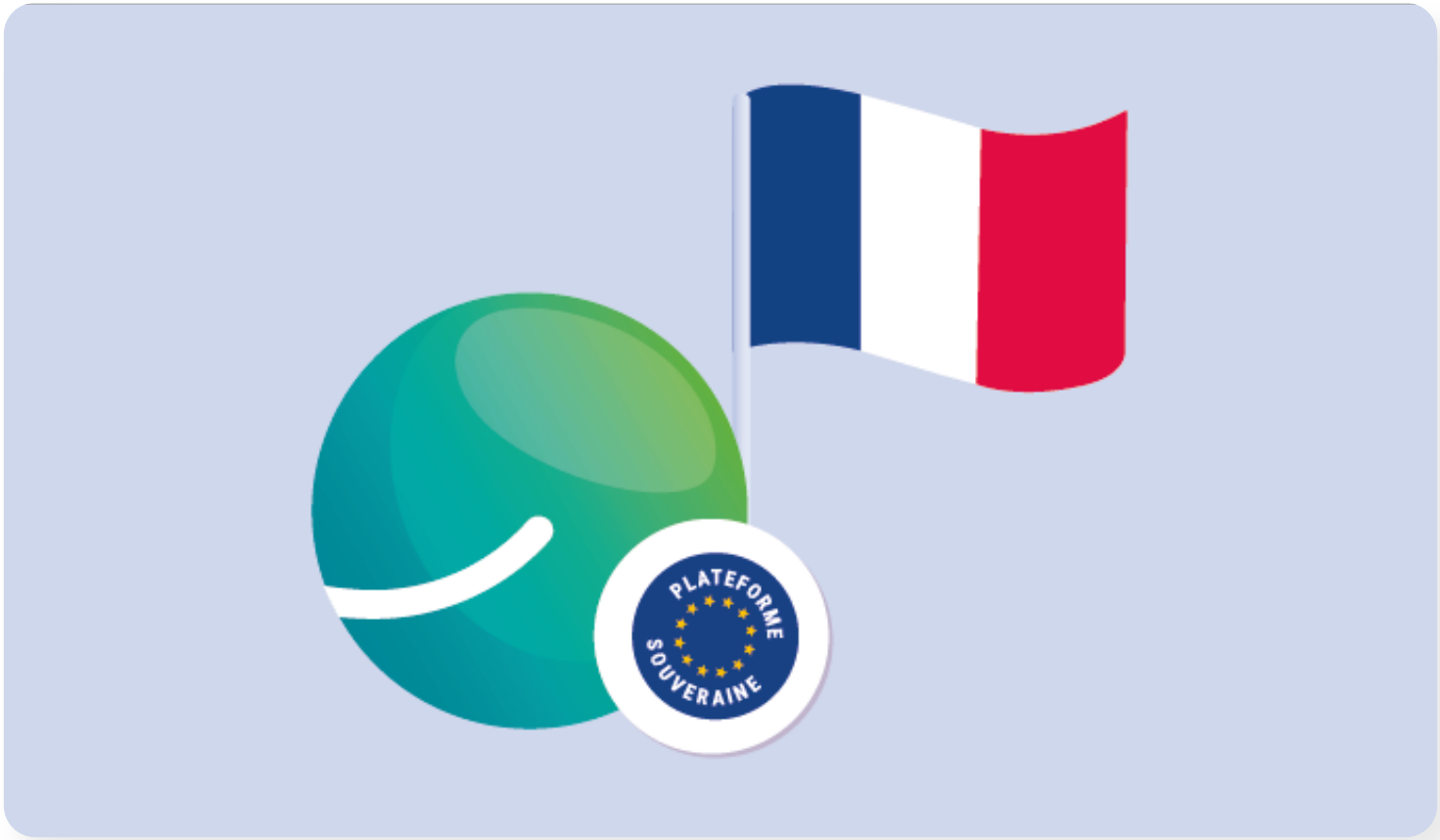
La première chose que j'en attends, c'est de pouvoir collaborer, c'est-à-dire une diffusion très large de la solution. Il faut que cette solution soit portable, c'est-à-dire qu'elle soit un peu indépendante du support du device, que nous puissions vraiment l'utiliser en toutes circonstances. Il faut aussi qu'elle soit compatible, il faut quand même pouvoir collaborer avec la personne qui aurait une autre solution. C'est vraiment ma principale attente d'une plateforme collaborative.

Un auteur, une œuvre, une phrase qui vous inspirent ?

Dans ces temps où je me lance dans une nouvelle aventure entrepreneuriale, il y a une phrase que j'aime beaucoup qui est du père Laval, qui était un bâtisseur de cathédrales et d'églises dans les îles éloignées de Polynésie française aux Gambier, qui tout seul a construit des édifices extraordinaires en ayant peu de moyens. Sa phrase c'était « le premier geste du bâtisseur, c'est de se retrousser les manches ». Je pense qu'en matière de souveraineté numérique, au-delà des beaux discours, retroussons-nous les manches et je suis persuadé que nous arriverons à accomplir de très belles choses.

Réinventer la collaboration : mettre en place une Digital Workplace souveraine

Souveraineté numérique



Dans un monde numérique en constante évolution, la mise en place d'une Digital Workplace efficace est devenue essentielle pour les entreprises cherchant à stimuler la collaboration, à renforcer la sécurité numérique et à se conformer aux réglementations en vigueur.

Dans cet article approfondi, nous plongerons dans le processus de mise en place d'une digital workplace tout en soulignant les défis auxquels les entreprises sont confrontées lorsqu'elles envisagent de passer d'outils américains bien établis à des solutions souveraines françaises, telles que Whaller, avec une attention particulière portée au changement et à la transformation.

La Quête de la Digital Workplace idéale

L'ère de la digital workplace offre un éventail de possibilités pour les entreprises, allant des géants américains bien connus tels que Microsoft 365 et Slack aux alternatives françaises souveraines comme Whaller, Talkspirit, Jalios ou encore Wimi. Alors que de plus en plus d'entreprises reconnaissent les avantages de la souveraineté numérique et de la conformité aux réglementations françaises et européennes, le passage à une solution souveraine n'est pas sans ses défis.

Les défis du changement

Le premier obstacle majeur auquel sont confrontées les entreprises est le défi du changement. Les outils américains tels que Microsoft 365 sont devenus omniprésents au sein des organisations, ce qui les rend familiers et confortables pour les employés. Passer à une solution souveraine française peut susciter de la résistance au sein de l'entreprise, car les employés doivent s'adapter à de nouvelles interfaces et à de nouvelles méthodes de travail. Le changement, en particulier lorsqu'il s'agit de technologies, nécessite une gestion experte. Les entreprises doivent mettre en place une stratégie de « change management » solide pour accompagner la transition vers une digital workplace souveraine. Cela implique de communiquer efficacement les avantages de la nouvelle solution, d'offrir une formation adaptée aux employés et de créer une culture qui favorise l'adoption de la nouvelle plateforme.

La Transformation Numérique à l'œuvre

Au-delà du changement, la mise en place d'une digital workplace souveraine est une composante clé de la transformation numérique d'une entreprise. C'est l'occasion de repenser les processus, d'encourager la collaboration et de renforcer la sécurité des données. Les solutions souveraines françaises, telles que Whaller, offrent des fonctionnalités avancées tout en garantissant que les données restent sous contrôle et en conformité avec les réglementations françaises et européennes.

Whaller : Une solution de référence

Parmi les alternatives françaises, Whaller se distingue par son engagement envers la souveraineté numérique et la confidentialité des données. Cette plateforme offre un environnement sûr et clos, appelé « sphère », où les utilisateurs peuvent collaborer en toute confiance. Elle propose une personnalisation avancée et une interface moderne pour stimuler l'adoption.

De plus, il est important de noter que Whaller est actuellement en cours de qualification SecNumCloud, une certification de sécurité numérique reconnue en France. Cette démarche démontre l'engagement de Whaller envers la sécurité des données de ses utilisateurs et renforce sa position en tant que solution souveraine de confiance.

Les limites des solutions américaines

Lorsque nous examinons les solutions américaines bien établies telles que Microsoft 365, Slack et Google

Workspace, il est important de noter certaines limites.
Ces plateformes opèrent souvent avec des serveurs situés aux États-Unis, ce qui soulève des questions quant à la localisation des données et à leur conformité aux réglementations européennes, notamment la RGPD. Pour les entreprises qui traitent des données sensibles, cela peut constituer une source de préoccupation majeure.

Ces solutions opèrent conformément au Patriot Act et au Cloud Act, ce qui signifie que les données peuvent être soumises à des demandes d'accès gouvernementales américaines sans notification préalable. Pour les entreprises françaises et européennes, cela représente un risque pour la confidentialité et la souveraineté de leurs données.

L'émergence de la Souveraineté Numérique

La souveraineté numérique est devenue une priorité pour de nombreuses entreprises qui cherchent à protéger leurs données et à assurer leur conformité réglementaire. Les solutions souveraines françaises, telles que Whaller, offrent un contrôle accru sur les données, garantissant que les informations restent en France et sous le contrôle des entreprises utilisatrices. Cette approche est cruciale pour la protection des données sensibles et la préservation de la confidentialité.

Le rôle clé du Change Management

La transition vers une digital workplace souveraine ne peut être réalisée avec succès sans une gestion experte du changement. Les entreprises doivent investir dans la formation des employés, la sensibilisation aux avantages de la nouvelle plateforme et la création d'une culture qui favorise l'adoption de la souveraineté numérique. Le « change management » est l'élément clé qui permet de surmonter les résistances au changement et de garantir le succès de la transformation

Réinventer la collaboration en toute souveraineté

La mise en place d'une digital workplace souveraine est un investissement dans l'avenir de votre entreprise. Si le passage de solutions américaines à des alternatives françaises peut être un défi, il offre également l'opportunité de renforcer la souveraineté numérique, de favoriser la conformité réglementaire et de réinventer la collaboration au sein de l'entreprise.

Le changement est inévitable, mais avec une gestion experte et une vision claire, il peut être transformateur. Alors, plongez dans l'ère de la souveraineté numérique avec une digital workplace française telle que Whaller et réinventez la collaboration au sein de votre entreprise, en toute sécurité et conformité.

Techno-logique ou techno-labyrinthe ?

Le parcours de la transformation numérique

Dans cet édito, je souhaite aborder la transformation numérique en m'interrogeant sur la neutralité de la technologie et son impact sur nos sociétés. La transformation numérique, avec des outils comme Whaller et les digital workplaces, façonne profondément nos modes de vie et de travail.

La technologie, souvent considérée comme neutre, n'est en réalité ni bonne ni mauvaise en elle-même. Elle reflète plutôt les intentions et les utilisations de ceux qui la développent et la réglementent. Comme le soulignait Tim Cook, c'est un miroir de nos ambitions et intentions. Pourtant, comme l'a démontré le penseur Jacques Ellul, la technologie possède une ambivalence intrinsèque, produisant des effets indépendants de ses usages. Elle n'est donc pas neutre.

Cette perspective soulève des questions essentielles lorsqu'on considère la mise en place de digital workplaces et l'intégration de plateformes comme Whaller. Ces espaces de travail numériques doivent être conçus avec une compréhension profonde de leurs impacts potentiels - non seulement sur l'efficacité et la productivité, mais aussi sur les aspects politiques, économiques, sociaux, organisationnels, culturels et écologiques.

La transformation numérique offre des possibilités immenses pour améliorer la collaboration, la communication et la gestion des données. Cependant, elle doit être abordée avec prudence et responsabilité. Les digital workplaces comme Whaller offrent des opportunités uniques pour renforcer la souveraineté numérique et la protection des données, mais elles nécessitent une réflexion approfondie sur leurs effets à long terme.

En conclusion, alors que nous naviguons dans cette ère de transformation numérique, il est impératif de reconnaître l'ambivalence de la technologie et d'agir avec clarté et responsabilité. Les digital workplaces ne sont pas seulement des outils de productivité, mais des instruments qui façonnent notre avenir. C'est dans cette optique que nous devons les concevoir et les utiliser.

Grégory Saccomani
Directeur Marketing et Communication
Whaller

La technologie est-elle neutre ?

Transformation numérique

Les technologies impactent nos sociétés. Les avantages qu'elles apportent sont nombreux : elles améliorent la santé, la qualité de vie, la diffusion de l'information, tout en augmentant l'efficacité et la productivité. Cependant, chaque innovation technique a des impacts de nature politique, économique, sociale, organisationnelle, culturelle et écologique. Quant à ses conséquences, elles peuvent être plus ou moins importantes et ressenties sur des horizons parfois lointains.

Alors qu'elle façonne nos sociétés et nos modes de vie depuis des décennies, la technologie peut-elle être considérée comme neutre ?

Plusieurs personnalités du monde de la technologie défendent la neutralité inhérente de la technologie. Parmi celles-ci, Tim Berners-Lee, le créateur du World Wide Web, considère que les avantages de la technologie sont bons ou mauvais selon son utilisation. Développer une technologie peut être bénéfique si ses processus de création sont strictement axés sur les besoins des utilisateurs. Il explique que les technologies de l'information et de la communication doivent être comprises comme des instruments à usages multiples plutôt que comme des « entités actives » influençant la société.

C'est aussi ce que pense Tim Cook, directeur général d'Apple, qui a déclaré que « Nous savons que la technologie n'est ni bonne ni mauvaise en soi ; c'est ce que nous en faisons ». Pour lui, elle est un miroir qui reflète les ambitions et les intentions de ceux qui l'utilisent, de ceux qui la construisent et de ceux qui la réglementent. La déclaration de Tim Cook évoque la célèbre première loi de la technologie de l'historien américain Melvin Kranzberg (1917-1995) : « La technologie n'est ni bonne ni mauvaise ; elle n'est pas non plus neutre ». Remarquons que le dirigeant d'Apple s'est arrêté avant la dernière partie – fondamentale en l'occurrence – qui pose le postulat que la technologie n'est pas neutre.

Cependant, des penseurs de l'éthique de la technologie contredisent ces affirmations du « ni-ni ». Dès le milieu du XXe siècle, le penseur français Jacques Ellul a démontré dans ses travaux, grâce au concept d' « ambivalence de la technologie », que la technologie elle-même a des effets indépendamment de ses usages. Il écrit que « La technologie n'est ni bonne, ni mauvaise, ni neutre. » Il nous invite donc à considérer les conséquences de chaque avancée technologique avec clarté et prudence. De la même manière qu'avec un couteau on peut peler une pomme ou tuer son voisin, il est moralement erroné, par exemple, de séparer les usages criminels de l'intelligence artificielle de ceux visant à guérir le cancer.

Par ailleurs, Jacques Ellul nous fait prendre conscience des difficultés à appréhender les effets de la technologie. Il divise ces effets en trois catégories : intentionnels, prévisibles et imprévisibles. Comme l'a montré la reconnaissance faciale en France, certains impacts sont difficilement prévisibles – par exemple, elle offre des opportunités de fraudes en cas de piratage. Mais, au-delà de la question de la prédiction, Jacques Ellul soutient que plus un domaine technologique progresse, « plus la relation entre ce qui est « bon » et « mauvais » devient inextricable, plus le choix est impossible, et plus la situation est tendue, c'est-à-dire moins nous pouvons échapper aux effets ambivalents du système. »

Fort de ces constats, dire que la technologie est neutre apparaît donc comme un leurre. Alors, que faire ? Faut-il se résigner à la complexité du problème et son insolubilité ?

Jacques Ellul nous propose de faire appel à la retenue afin de répondre à ce constat : « Tout bonheur humain se paie, et il faut toujours se demander quel prix on paiera. ».

En effet, face aux effets nocifs échappant à tout contrôle durable, il faut faire preuve de prudence et de responsabilité dans le développement et l'utilisation des nouvelles technologies. Nous devons prendre conscience des défis et des limites de la technologie et s'interroger sur la nécessité de mettre en place une réglementation appropriée pour protéger les individus.

C'est ce que semble penser Tim Cook qui a déclaré que « Ceux d'entre nous qui créent la technologie et établissent les règles qui la régissent ont une profonde responsabilité envers les personnes que nous servons. Assumons cette responsabilité. » Sa déclaration faisait écho aux actions que les leaders de l'industrie, les GAFAM notamment, ont commencé à mettre en place, comme les comités d'éthique ou « cours suprêmes », pour identifier les principes et les valeurs auxquels ils adhèrent et délimiter le périmètre de leurs responsabilités.

Notons que la question de la régulation de l'innovation technologique est désormais au cœur du développement fulgurant de l'intelligence artificielle. C'est ce que le créateur de ChatGPT, Sam Atman, pense. Selon lui, des IA « potentiellement terrifiantes […] vecteurs de destruction de l'humanité » vont arriver. « La société a besoin de temps pour s'adapter à quelque chose d'aussi massif » ajoute-t-il. Sa mise en garde a été suivie par celle d'Elon Musk et de centaines d'experts mondiaux qui ont récemment signé un appel à une pause de six mois dans la recherche sur les IA en évoquant « des risques majeurs pour l'humanité ». Ils demandent un moratoire jusqu'à la mise en place de systèmes de surveillance des systèmes d'IA et des autorités réglementaires dédiées afin de permettre de distinguer le réel de l'artificiel. Sans quoi il y aura des « perturbations économiques et politiques dramatiques (en particulier pour la démocratie) que l'IA provoquera ».

Ces appels démontrent ainsi que la technologie est bien tout sauf neutre.

La place des nouvelles technologies dans l'optimisation de notre quotidien

Transformation numérique

C'est un dimanche après-midi. Vous êtes assis sur votre canapé, un verre à la main et discutez paisiblement avec un ami. Tout semble aller pour le mieux quand, soudain, la montre à votre poignet se met à vibrer. Une notification vous informe que votre taux de sucre dans le sang est supérieur à votre moyenne habituelle. Huit minutes de marche supplémentaires sont nécessaires. Une légère angoisse monte. Comment vais-je rattraper cela ?

Si nous reprenons l'exemple de la montre, il semble légitime de faire de l'exercice, d'avoir un corps sain. Mais est-ce que cette angoisse, qui n'aurait pas existé sans la technologie, était bien nécessaire ? N'aurait-il pas mieux fallu pouvoir pleinement profiter de cette après-midi entre amis sans angoisse ?

Ainsi il parait légitime de s'interroger sur le sens que peut avoir le fait d'améliorer sans cesse nos outils. Pour ce faire nous allons d'abord réfléchir à ce qu'est l'optimisation avant de revenir sur le tournant analytique des vingt dernières années.

L'optimisation, une idée d'ordre économique

Pour le dictionnaire Larousse, optimiser signifie : « Donner à quelque chose, à une machine, à une entreprise, etc., le rendement optimal en créant les conditions les plus favorables ou en en tirant le meilleur parti possible. »

Ce qui frappe dans cette définition, ce sont les deux premiers exemples qui nous sont donnés : la machine et l'entreprise. L'optimisation est avant tout liée à un perfectionnement du rendement. C'est-à-dire qu'on optimise un produit de départ pour en avoir un meilleur. L'idée est de gagner plus d'argent en vendant un meilleur produit. Seulement qu'est-ce qu'un meilleur produit ? Tout repose sur la performance. La capacité du produit à effectuer sa mission de la manière la plus rapide, la plus conforme et donc la plus optimale.

L'optimisation d'un produit de masse oblige néanmoins la considération suivante : est-ce que tous les individus ont les mêmes critères pour juger cette performance ? Un sportif de haut niveau aux Etats-Unis n'aura pas la même attente que celle d'un joggeur de l'Ouest parisien. Or tous deux utilisent la même montre connectée.

C'est la raison pour laquelle de plus en plus de marques ont développé des produits que l'on peut personnaliser. Tout le monde dispose de la même machine, mais à partir d'un programme originel nous pouvons modifier sa manière d'interagir avec nous.

Mais si la personnalisation d'une montre connectée semble une bonne chose, que penser de la personnalisation des réseaux sociaux. Du fait que plus nous adhérons à un mode de pensée plus les réseaux nous amènent à penser de cette même manière ? Dans ce cas-là, l'optimisation et la personnalisation semblent être plutôt négatifs.

Pour y réfléchir, il semble nécessaire de se demander : comment en sommes-nous arrivés là ?

Le développement d'Internet et l'émergence de nouveaux métiers

L'optimisation est un processus global dans une société de consommation où l'objectif est de vendre toujours plus et toujours mieux. Néanmoins, il semble que le développement du « Big Data » a conduit à une précision toujours plus puissante quant aux goûts et aux attentes des utilisateurs de tous types de produits. Ainsi, comprendre le lien entre internet et l'optimisation peut permettre de mieux saisir cette caractéristique du monde moderne.

En effet, le développement d'internet a conduit au stockage d'une immense base de données.

Elle provient de toutes les interactions effectuées en ligne. Voilà pourquoi depuis une vingtaine d'années un nouveau métier à vue le jour : « Data Analyst » (analyste data). Ceux-ci ont pour mission dans les entreprises de lier des données entre elles pour arriver à faire des bilans. Leur rôle est de modéliser les statistiques en tableaux de chiffres. Et ces modèles sont désormais réputés auprès des directions pour leur précision et leur apport stratégique.

Cependant, la précision d'un tableau et l'optimisation d'un produit ne veut pas dire que la vie de l'utilisateur est réellement améliorée. C'est l'un des problèmes fondamentaux de cette logique. Les critères de l'optimisation sont avant tout quantitatifs, analytique et économiques. Ils paraissent mettre de côté une dimension plus simple, plus humaine.

Nous ne sommes pas seulement attachés aux outils et aux objets pour leur efficacité mais aussi pour leur beauté par exemple. Conserver un vieux livre usé n'est pas optimal puisqu'il n'est pas certain qu'il survive à une prochaine lecture intensive. Mais nous pouvons aimer les souvenirs que nous avons de cet objet. Ce sont ces dimensions symboliques qui échappent à la logique du marché.

Cette dernière considération à propos d'une qualité immatérielle et inquantifiable, va de pair avec le mouvement de la personnalisation au sein de l'optimisation. Sans doute le prochain tournant analytique sera de prendre en compte ses désirs chez chaque personne et de parvenir à aller au-delà. On peut imaginer que des entreprises importantes chercheront à créer de plus en plus d'objets adaptés aux besoins de chaque individu dans une démarche de personnalisation extrême – comme, c'est déjà le cas du sur-mesure dans la couture. Ce nouvel enjeu suivrait la logique d'une société dans laquelle l'individu est considéré comme autonome et singulier. Optimiser deviendrait alors synonyme d'adapter.

10 Conseils pour une transition réussie vers une collaboration virtuelle en entreprise

Transformation numérique

De nos jours, la collaboration virtuelle est devenue la norme incontournable. La pandémie de COVID-19 a incontestablement accéléré cette tendance, forçant de nombreuses entreprises à s'adapter rapidement à un environnement de travail en ligne. Cependant, réussir dans cette nouvelle ère de travail nécessite bien plus que de simples réunions Zoom et des échanges d'e-mails. Il faut une plateforme de collaboration solide et des pratiques efficaces pour tirer le meilleur parti de cette transition.

L'importance de la Collaboration Virtuelle

La collaboration virtuelle transcende les frontières géographiques et permet aux entreprises de recruter des talents du monde entier, d'optimiser les coûts et de maintenir une continuité des opérations, même en cas de perturbations majeures. Cependant, pour réussir dans ce nouvel environnement, il est essentiel de choisir les bons outils et d'adopter des méthodes de travail appropriées.

1. Choisissez la bonne plateforme de collaboration

La première étape cruciale pour une collaboration virtuelle réussie est de sélectionner la plateforme adaptée à vos besoins. Parmi les options disponibles, Whaller se distingue en offrant des fonctionnalités de communication sécurisées et une interface conviviale. Il est impératif de vous assurer que la plateforme que vous choisissez répond spécifiquement aux exigences de votre entreprise.

La polyvalence de Whaller

Whaller brille par sa polyvalence, permettant à une variété d'entreprises, des petites startups aux grandes entreprises, de personnaliser leurs espaces de travail virtuels en fonction de leurs besoins uniques. Sa sécurité de pointe et son interface intuitive en font une option attrayante pour les entreprises de toutes tailles.

2. Établissez des objectifs clairs

Avant d'entamer la transition vers la collaboration virtuelle, prenez le temps de définir des objectifs clairs pour votre équipe. Qu'espérez-vous accomplir grâce à cette transition ? Des objectifs bien définis servent de boussole pour maintenir tout le monde sur la même longueur d'onde.

Alignement des Objectifs

L'alignement des objectifs est essentiel pour garantir que chaque membre de l'équipe comprend la vision globale de l'entreprise et travaille vers des résultats cohérents. Des objectifs spécifiques, mesurables, atteignables, pertinents et limités dans le temps (SMART) offrent une orientation claire.

3. Formation et sensibilisation

Assurez-vous que tous les membres de votre équipe sont formés à l'utilisation de la plateforme de collaboration virtuelle choisie. Organisez des sessions de formation pour garantir que chacun maîtrise les outils à sa disposition.

Investir dans la Formation

Investir dans la formation est un investissement dans la productivité future. Plus votre équipe est à l'aise avec la technologie et les pratiques de travail virtuelles, plus elle peut tirer parti de ces outils pour atteindre ses objectifs.

4. Créez un espace de travail structuré

Exploitez les fonctionnalités de votre plateforme, telles que les « sphères » proposées par Whaller, pour créer des espaces de travail structurés, adaptés à différents projets ou équipes. Cette organisation contribue à maintenir l'ordre et facilite la navigation.

L'Efficacité de la Structuratio

La structuration de l'espace de travail réduit la confusion, permet une meilleure gestion de l'information et favorise la collaboration ciblée. Les équipes peuvent ainsi se concentrer sur leurs tâches spécifiques sans être submergées par des informations superflues.

5. Encouragez une communication transparente

La communication transparente est essentielle dans un environnement de travail virtuel. Encouragez activement les membres de l'équipe à partager des mises à jour régulières et à poser des questions pour éliminer toute confusion.

La Communication comme Colle Sociale

Dans un contexte virtuel, la communication ne se limite pas aux tâches professionnelles, elle joue également un rôle crucial dans le maintien des liens sociaux au sein de l'équipe. Les conversations informelles peuvent contribuer à renforcer la cohésion et à prévenir l'isolement.

6. Utilisez les fonctionnalités collaboratives

Whaller propose une gamme complète de fonctionnalités collaboratives, telles que le partage de fichiers, la co-création de documents, les vidéoconférences, les discussions en groupe et les sondages. Exploitez ces outils pour améliorer la productivité de votre équipe.

La Puissance de la Collaboration en Ligne

Les outils de collaboration en ligne ne se limitent pas à la communication. Ils permettent également le partage instantané de documents et la collaboration en temps réel, ce qui peut considérablement accélérer la réalisation des projets.

7. Établissez des réunions régulières

Planifiez des réunions virtuelles régulières pour maintenir un contact humain essentiel avec votre équipe. Servez-vous des fonctionnalités de rappel et d'invitation pour garantir la participation de tous.

Le Contact Humain Virtuel

Même dans un environnement virtuel, les réunions restent un moyen crucial de discuter des progrès, de résoudre les problèmes et de favoriser la collaboration. Les rappels et invitations automatisés assurent que personne n'est laissé de côté.

8. Respectez la vie privée et la sécurité

Assurez-vous que la vie privée et la sécurité des données occupent une place centrale. Whaller offre des options de sécurité avancées pour protéger les informations sensibles, ce qui en fait un choix judicieux pour les entreprises soucieuses de la sécurité.

La Sécurité des Données

La protection des données est essentielle, que ce soit pour les informations confidentielles de l'entreprise ou les données personnelles des employés. Whaller propose des mécanismes de sécurité robustes pour garantir une collaboration en ligne en toute confiance.

9. Encouragez la flexibilité

L'un des avantages clés de la collaboration virtuelle est la flexibilité. Encouragez votre équipe à tirer parti de cette flexibilité pour améliorer l'équilibre entre vie professionnelle et vie personnelle, favorisant ainsi le bien-être de tous.

L'Équilibre Travail-Vie Personnelle

La collaboration virtuelle permet aux employés de mieux gérer leur temps, ce qui peut contribuer à réduire le stress lié au travail et à améliorer la satisfaction globale au travail.

10. Évaluez et Adaptez en Continu

Enfin, n'oubliez pas d'évaluer régulièrement votre transition vers la collaboration virtuelle. Soyez prêt à apporter des ajustements en fonction des retours d'expérience de votre équipe, car l'adaptabilité est la clé du succès continu.

L'Importance de l'Adaptation

Le paysage de la collaboration virtuelle évolue constamment, avec de nouvelles technologies et de nouvelles pratiques qui émergent. Restez à l'affût des tendances et soyez prêt à ajuster votre approche en conséquence. L'apprentissage continu est essentiel pour prospérer dans cet environnement en constante évolution.

En conclusion, la transition vers une collaboration virtuelle réussie en entreprise repose sur la sélection d'une plateforme appropriée, des objectifs clairs et une communication efficace. Whaller offre un ensemble d'outils puissants pour faciliter cette transition. En suivant ces 10 conseils, votre équipe peut maximiser les avantages de la collaboration virtuelle et prospérer dans l'environnement de travail moderne.

N'attendez plus pour faire de votre entreprise un modèle de collaboration virtuelle efficace grâce à Whaller !

> 📽️ Découvrez le retour d'expérience de l'APEC.

> 📖 En savoir plus : Transformation Numérique.

Comment OVHcloud tire parti de Whaller pour dynamiser sa communication

Transformation numérique

OVHcloud est une entreprise française leader européen du cloud. Ils fournissent à leurs clients des solutions de cloud public, de cloud privé, de serveurs dédiés, de VPS. Ils font également de l'hébergement web, de la téléphonie et tout cela pour leurs clients dans 140 pays à travers le globe. Ils comptent aujourd'hui plus de 1,6 million de clients. Parmi ses clients se trouvent aussi des startups. C'est dans ce cadre-là qu'OVHcloud, depuis 2015, accompagne les startups dans le développement de leur infrastructure serveurs et les aide à basculer dans le cloud. C'est dans ce contexte-là qu'ils ont également créé un programme de mentoring qui leur permet de mettre en relation leurs startups avec des experts métiers OVHcloud.

Comment avez-vous connu Whaller ?

Whaller est client OVHcloud depuis plusieurs années déjà, je connaissais à titre personnel un peu la solution, mais c'est vraiment il y a trois ans, en 2020 que nous avons décidé de basculer sur cette plateforme parce que le marketplace OVHcloud qui est un autre programme de l'entreprise au même titre que le Startup Program, le programme Open Trusted Cloud aussi ou le Partner Program.

Le programme marketplace utilisait déjà la solution, ce qui nous a vraiment aidé à basculer sur cette plateforme. D'autant plus que Whaller partage les mêmes valeurs que nous au niveau de la souveraineté des données, au niveau de la protection des données. Il faut également savoir que Whaller est dans une démarche de certification SecNumCloud. Tous les éléments sont rassemblés pour que nous puissions travailler main dans la main ensemble.

Pourquoi le choix de Whaller ?

Le mentoring est un projet bien spécifique. Notre but c'est réellement d'aider des startups sur un challenge particulier, sur une problématique qu'elles auraient dans le développement de de leur activité avec un mentor OVHcloud sur une expertise métier. À ce titre, nous cherchions vraiment une plateforme qui pourrait nous faire gagner du temps, une plateforme tout-en-un qui pourrait automatiser certaines fonctions comme la description des mentors, le matchmaking entre mentor et startup, la communication auprès de notre communauté de mentoring en sachant que nous utilisons depuis trois ans déjà Whaller mais plus pour l'animation de notre communauté Startup.

Quelles étaient vos attentes de l'outil ?

Globalement, nous avions besoin d'une plateforme sur laquelle nous pouvons réellement communiquer avec nos membres sur le projet spécifique de mentoring. Nous avions aussi besoin donc de créer des groupes par expertise, par domaine d'activité. Pour cette troisième session de mentoring, nous avons eu de 36 mentors et ces 36 mentors se regroupent en dix grands domaines d'expertises tels que la communication, le marketing et j'en passe.

Le but c'était vraiment d'avoir une plateforme qui nous permettrait de dissocier facilement les mentors pour que les startups puissent facilement trouver et postuler au mentoring avec le mentor qu'ils auraient choisi.

Quels usages faites-vous de Whaller ?

Nous utilisons Whaller pour deux usages bien spécifiques : le premier, c'est l'animation de notre communauté au quotidien. Il faut savoir qu'au sein du Startup Program OVHcloud, nous donnons de la visibilité à nos startups lors de nos événements, lors d'appels à projets aussi, nous travaillons avec beaucoup d'autres structures d'accompagnement startup. Le but c'est réellement de faire en sorte qu'elles soient au courant de toutes nos actualités qui peuvent leur servir.

Ça c'est très important pour nous, l'aspect animation de la communauté.

D'autre part, nous utilisons aussi Whaller depuis peu, depuis l'année dernière sur le programme de mentoring et qui est un programme différent et qui est plus limité dans le temps.

Quelles fonctionnalités vous sont utiles ?

Nous avons pas mal travaillé avec Cléa Ancelly, Directrice de l'expérience client chez Whaller et qui nous avait déjà accompagnés au design de la plateforme et du projet de mentoring sur Whaller pour notre communauté. Notre principale problématique, c'était de bien dissocier l'accompagnement et l'animation de notre réseau de startup au quotidien du projet de mentoring.

Pour cela, nous avons tout d'abord créé des familles de sphères, deux familles de sphères : une liée à l'accompagnement des startups et l'animation de nos startups au quotidien et une autre dédiée au mentoring. Cela a permis aux startups de bien identifier les deux canaux de communication qui sont différents.

Une de nos volontés, c'était vraiment de bien mettre en avant les mentors et leur expertise pour que les startups puissent facilement les identifier. Pour cela, nous avons rajouté des champs spécifiques personnalisés aux mentors sur leur mini profil. Cela a vraiment permis aux startups d'en savoir plus sur la description de leurs mentors et de pouvoir postuler en fonction.

Pour ce projet, nous avons décidé de mettre en place des sphères ouvertes pour permettre aux startups de facilement accéder aux sphères sans invitation. Mais nous pouvions être confronté à une problématique qui était celle de ne pas bien dissocier donc qui était qui ? C'est-à-dire les mentors d'un côté et les startups.

Pour ce faire, nous avons décidé d'attribuer un rôle spécifique, un rôle aux mentors et un rôle de gestionnaire mentoring qui m'était attribué. Ça a vraiment permis donc aux startups de facilement identifier qui était qui dans ce projet de mentoring. Par ailleurs, la mise en place du rôle nous a permis de facilement filtrer les mentors et les startups dans le moteur de recherche, ce qui nous a fait gagner en efficacité.

Comment Whaller contribue à votre organisation ?

Au-delà de l'animation de notre communauté. Whaller est un outil très efficace pour fidéliser aussi ses clients, ses membres. Parce qu'une fois que l'année Startup Program est terminée, nos membres restent actifs sur la plateforme, ce qui nous permet de continuer à échanger avec eux, d'être toujours en contact avec nos membres alumni. En plus de l'aspect de fidélisation des membres et de structuration de la communauté.

Ce qui est vraiment intéressant avec Whaller c'est la flexibilité de la plateforme qui permet justement de s'adapter à différents projets que nous voulons mettre en place et que nous pourrions mettre en place à l'avenir.

En quelques mots qu'est-ce qui distingue Whaller ?

Ce qui distingue Whaller, je vais résumer ça en trois points :

- Le premier point, c'est **la souveraineté de la solution**. D'autant plus que Whaller est hébergé chez OVHcloud.
- Le deuxième point, c'est **l'accompagnement et la proximité de l'accompagnement** qui nous permet réellement de gagner du temps dans la mise en place du projet et dans l'adoption de la solution par les membres.
- Le troisième point c'est le fait que **les clients de Whaller peuvent eux-mêmes participer à l'amélioration continue de la plateforme** en suggérant des modifications qui seront prises en compte dans leur roadmap.

Les 5 meilleures pratiques pour optimiser la collaboration virtuelle

Transformation numérique

La collaboration virtuelle est au cœur de la manière dont les entreprises fonctionnent aujourd'hui. Que votre équipe soit répartie à travers le monde ou que vous cherchiez simplement à faciliter le travail à distance, les outils de collaboration en ligne comme Whaller offrent des solutions puissantes. Dans cet article, nous vous guiderons à travers les meilleures pratiques pour améliorer l'efficacité de votre collaboration virtuelle.

1. Créez des espaces de travail dédiés

La première étape pour optimiser la collaboration virtuelle avec Whaller est de créer des espaces de travail dédiés. Ces espaces servent de hubs centraux où les membres de l'équipe peuvent se réunir, discuter, partager des documents et collaborer en temps réel. Chaque espace est conçu pour un projet spécifique ou une équipe, ce qui permet une organisation claire et la gestion de plusieurs initiatives sans confusion.

Pourquoi c'est important ?
La création d'espaces de travail dédiés aide à :

- **Centraliser les informations :** Toutes les discussions, documents et tâches liées à un projet ou une équipe sont accessibles au même endroit, éliminant la recherche fastidieuse d'informations dispersées.
- **Faciliter la gestion :** Les responsables de projet peuvent surveiller les progrès, assigner des tâches et organiser les ressources plus efficacement.
- **Réduire la clutter :** En évitant les fils de discussions éparpillés et les e-mails chaotiques, la collaboration devient plus fluide.

2. Utilisez les fonctionnalités de messagerie instantanée

La messagerie instantanée est l'épine dorsale de la collaboration virtuelle efficace. Whaller offre des fonctionnalités de chat en temps réel qui permettent aux membres de l'équipe de communiquer instantanément, qu'ils se trouvent à quelques pas ou à des milliers de kilomètres les uns des autres. Cette communication fluide encourage la spontanéité et la réactivité.

Pourquoi c'est important ?
L'utilisation de la messagerie instantanée permet de :

- **Réduire les délais :** Les discussions sont instantanées, ce qui élimine les attentes causées par les réponses aux e-mails.
- **Favoriser la collaboration :** Les membres de l'équipe peuvent rapidement poser des questions, partager des idées et résoudre des problèmes en temps réel.
- **Créer un sentiment de présence :** Même à distance, la messagerie instantanée crée une sensation de proximité entre les membres de l'équipe.

3. Partagez et collaborez sur des documents

La collaboration virtuelle exige un moyen efficace de partager et de collaborer sur des documents. Whaller facilite cela en permettant aux utilisateurs de téléverser des fichiers directement dans leurs espaces de travail. Vous pouvez ainsi collaborer sur des documents, les réviser en temps réel et assurer la cohérence de vos projets.

Pourquoi c'est important ?

Le partage et la collaboration sur des documents offrent de nombreux avantages, notamment :

- **Réduction des frictions :** Évite les échanges de fichiers par e-mail,

qui peuvent entraîner des versions désynchronisées.

- **Facilitation de la révision :** Plus besoin de jongler avec des versions différentes. Les modifications peuvent être apportées directement sur le document en cours.
- **Centralisation des ressources :** Tous les documents liés à un projet sont accessibles depuis l'espace de travail correspondant.

4. Planifiez des réunions à distance

Bien que la communication écrite soit essentielle, rien ne remplace une réunion virtuelle en face à face pour renforcer la connexion entre les membres de l'équipe. Whaller propose des fonctionnalités de planification et de tenue de réunions virtuelles, ce qui facilite l'organisation de rencontres collaboratives, de discussions en temps réel et de présentations visuelles.

Pourquoi c'est important ?

La planification de réunions à distance présente plusieurs avantages :

- **Communication en temps réel :** Les réunions virtuelles permettent des discussions en direct, éliminant les délais dans la communication.
- **Partage visuel :** Vous pouvez partager des écrans, des documents et des présentations pour une compréhension plus approfondie.
- **Maintien de la connexion humaine :** Les réunions visuelles renforcent les relations et favorisent la compréhension mutuelle, ce qui est essentiel pour les équipes distantes.

5. Priorisez la sécurité et la confidentialité

La sécurité et la confidentialité des données sont primordiales lors de la collaboration virtuelle. Whaller met l'accent sur la protection des informations sensibles en proposant des mesures de sécurité avancées et un contrôle d'accès personnalisé. Cette approche assure que seules les personnes autorisées ont accès aux données cruciales.

Pourquoi c'est important ?

La sécurité et la confidentialité sont cruciales pour :

- **Protéger les données sensibles :** En garantissant que vos informations sont en sécurité, vous évitez les fuites de données potentielles.
- **Construire la confiance :** Les membres de l'équipe peuvent collaborer en toute confiance, sachant que leurs informations sont protégées.
- **Conformité réglementaire :** En respectant les réglementations de sécurité, vous évitez des problèmes juridiques et des amendes potentielles.

En optimisant la collaboration virtuelle au sein de votre équipe avec Whaller, vous pouvez renforcer l'efficacité de votre travail à distance. En créant des espaces de travail dédiés, en utilisant la messagerie instantanée, en favorisant la collaboration sur des documents, en organisant des réunions virtuelles et en priorisant la sécurité, vous créez un environnement où la productivité et la cohésion d'équipe prospèrent.

Whaller s'impose comme une plateforme de premier choix pour répondre à ces besoins de collaboration virtuelle. Grâce à ces 5 meilleures pratiques, vous pouvez tirer le meilleur parti de cette plateforme et optimiser la manière dont votre équipe col-labore, quels que soient les défis de distance qui se dressent devant vous.

Réussir le flex office : Whaller, votre atout pour une collaboration sans frontières

Transformation numérique

Le flex office, cette approche qui permet aux employés de choisir où et quand ils travaillent, est de plus en plus adopté par les entreprises soucieuses de s'adapter à un environnement en constante mutation. Mais comment réussir cette transition vers le flex office et en faire un véritable atout pour votre organisation ?

Le flex office : une réalité incontournable

Le flex office n'est plus une simple tendance, c'est une réalité qui s'impose dans le monde professionnel moderne. Il offre aux employés la liberté de choisir leur espace de travail, que ce soit au bureau, à domicile, dans un espace de coworking ou ailleurs. Cette flexibilité accrue favorise la productivité, l'équilibre entre vie professionnelle et vie personnelle, et peut même réduire les coûts liés à l'espace de bureau.

Les défis du flex office

Cependant, le flex n'est pas sans défis. La gestion de la communication, de la collaboration et de la sécurité des données peut devenir complexe lorsque les équipes sont dispersées dans différents lieux. C'est là qu'intervient Whaller.

Whaller : votre allié pour la collaboration sans frontières

Whaller, la plateforme collaborative, sociale et sécurisée française, est conçue pour répondre aux besoins des organisations engagées dans le flex office. Imaginez Whaller comme une salle de réunion virtuelle, accessible de n'importe où, à tout moment. Cette salle de réunion, appelée « sphère », peut être votre bureau virtuel où les membres de votre équipe se réunissent pour échanger des idées, partager des documents, organiser des visioconférences et collaborer de manière transparente.

Les Avantages de Whaller pour le Flex Office

- **Flexibilité absolue :** Avec Whaller, vous pouvez créer des sphères dédiées à chaque projet, équipe ou département, et inviter les membres pertinents à les rejoindre. Cela signifie que peu importe où se trouvent vos employés, ils ont un espace de collaboration dédié.
- **Sécurité renforcée :** La sécurité est une préoccupation majeure en matière de flex office. Whaller offre un contrôle total sur la confidentialité des données. Vous pouvez choisir qui peut accéder à chaque sphère et quelles informations sont partagées.
- **Communication transparente :** Avec des fonctionnalités telles que les discussions, les partages de fichiers, les sondages, les événements et les visioconférences, Whaller garantit que la communication au sein de votre organisation reste fluide et transparente, quel que soit le lieu de travail.
- **Suivi des projets :** La gestion de projets est simplifiée grâce à la possibilité de créer des tâches, des listes de tâches et des calendriers au sein de chaque sphère. Votre équipe peut ainsi suivre les avancements et rester organisée.

Réussir et faire du flex office un atout

Le succès du flex office repose sur une combinaison d'éléments : une culture d'entreprise favorable, une gestion experte du changement et des outils de collaboration adaptés.

Whaller se positionne comme l'outil essentiel pour garantir que la collaboration sans fron-tières soit non seulement pos-sible, mais aussi bénéfique pour votre organisation.

Le flex office est plus qu'une tendance, c'est un atout stra-tégique pour les entreprises qui souhaitent s'adapter à un environnement de travail en constante évolution. En choi-sissant Whaller comme parte-naire de flex office, vous inves-tissez dans la productivité, la sécurité et la flexibilité, tout en offrant à vos employés la liber-té de travailler comme ils le souhaitent. Alors, prépa-rez-vous à réussir et à faire du flex un atout majeur pour votre organisation, avec Whaller à vos côtés.

Whaller accompagne la transformation numérique des universités

Transformation numérique

L'EUt+ est un réseau de huit, bientôt neuf universités partenaires, universités de technologie au niveau européen qui vise à terme à devenir une seule université et, pour les étudiants, à obtenir un diplôme européen.

Nous avons interviewé Laetitia Roggero Directrice de la Communication à l'Université de Technologie de Troyes en Champagne, responsable de la communication au niveau de l'initiative Université de technologie européenne (EUt+).

Comment avez-vous connu Whaller ?

En juillet 2020, on a eu une réponse positive de la Commission européenne qui a accordé un financement pour cette initiative EUt+. A partir de là, il a fallu que nous commencions à travailler sur l'ensemble des thématiques de l'université, telles que la recherche et l'éducation, avec nos sept autres partenaires européens et pour cela, nous cherchions une plateforme de collaboration.

Nous avions entendu parler de la plateforme et nous nous sommes dit que nous allions faire un essai. Nous avions également regardé la concurrence, qui, pour des raisons de protection des données, pour des raisons d'usage, ne correspondait pas à ce que nous cherchions. Ce que nous avons apprécié dans Whaller, c'est que nous avons pu discuter avec toute l'équipe. Nous avons vraiment apprécié le côté sur-mesure de la solution et l'ensemble des fonctionnalités qui répondaient à nos besoins.

Pourquoi le choix de Whaller ?

Premièrement, c'est vraiment le côté sur-mesure et service client. Il y a eu un vrai échange, un accompagnement pour la mise en place de l'ensemble de nos groupes de travail, puisque c'est un projet européen avec énormément de groupes de travail sur des thématiques très variées. Cela nous permettait d'avoir cette souplesse pour organiser notre travail. L'une des fonctionnalités que nous avons vraiment appréciée, c'est pour démarrer le travail. C'est bien sûr le côté visioconférence, mais aussi d'avoir dans un même espace tous ces outils, que ce soit la box de sphère pour pouvoir mettre nos documents et travailler collaborativement sur des documents. La visio-sphère, comme je vous le disais, il y a aussi la partie calendrier. Nous utilisons beaucoup cet outil lorsque nous sommes en déplacement.

Quels usages faites-vous de Whaller ?

Nous avons décidé que chaque sphère correspondait à un groupe de travail. Nous avons des numéros de work packages, c'est-à-dire de groupe de travail et de tâches associées à ces work packages. Une sphère correspond à la tâche 7.1 par exemple, qui correspond à la communication. Nous avons vraiment façonné ça.

Une fois par mois environ, nous nous réunissons. Nous sommes une centaine de participants à nous réunir chez un de nos partenaires. Actuellement, nous sommes à Troyes pour la semaine de travail autour de la recherche et Whaller nous sert pour diffuser ces informations, que ça soit l'emploi du temps, les informations pratiques en lien avec le logement, les activités sociales qui vont être organisées, les salles dans lesquelles vont avoir lieu les groupes de travail.

Cela nous a permis petit à petit de capturer cette audience sur Whaller et ensuite de diffuser de l'information. Il y a notamment la section "Breaking news" où nous partageons notre actualité.

Comment s'est déroulé le déploiement et l'adoption de l'outil ?

Nous nous sommes dit qu'il faut absolument que sur Whaller, il y ait des informations indispensables pour que les personnes puissent se connecter et doivent se connecter pour y avoir accès. Une des pistes que nous avons explorée, c'est tout ce qui est les infos pratiques autour de nos semaines de travail.

Un peu plus tard, nous avons travaillé vraiment sur la partie intranet, parce que nous sommes huit universités distinctes, chacun ayant ses propres réseaux de communication interne. Il y avait une volonté de créer aussi un outil, un intranet EUt+ à l'échelle du consortium de l'Alliance.

Nous avons travaillé sur cet intranet pour permettre à toutes les personnes, que ce soit personnel ou étudiant, d'avoir accès aux informations en lien avec cette initiative.

Une grande étape que nous avons passée, c'est la mise en place d'une connexion SSO. Ceux qui souhaitent aller voir les informations en lien avec les progrès de l'initiative, ils peuvent le faire grâce à leur login habituel de leur université.

Quelles fonctionnalités vous sont utiles ?

Le panel est vraiment large et je dirais qu'au sein de l'alliance EUt+, ce qui est le plus utilisé c'est tout d'abord la visio-sphère, ça permet pour nos partenaires de se rencontrer facilement au sein d'une sphère et à tout moment elle est disponible.

Par exemple : Je suis à l'UTT, j'ai besoin de discuter en visio avec ma collègue Eva qui est en Espagne. Nous nous retrouvons sur une sphère pour avancer sur un sujet. La deuxième option, je dirais que ça serait la box de sphère avec les documents collaboratifs.

Forcément avec EUt+, nous nous connaissons bien, ce qui nous permet aussi d'identifier des opportunités de partenariat. Nous répondons à beaucoup d'appels à projets européens annexes à l'EUt+. Pour répondre à ces appels à projets, il y a des dossiers conséquents à remplir et ça nous permet d'avoir ce travail collaboratif au sein des documents, de commenter, d'échanger et de modifier. Cela est très apprécié également.

Depuis sa mise en place, quelles sont les évolutions ?

Au niveau des évolutions de Whaller, le moteur de recherche, il y a déjà une première évolution que je vois pour rechercher des informations. Ça va encore aller plus loin, j'ai vu ça dans la feuille de route et ça, effectivement, c'est très important pour nous parce que le projet, l'initiative grandit. Nous avons de plus en plus de documents et c'est très important de pouvoir avoir ce système de tags et ce système de recherche à la fois sur les messages, sur les documents et aussi sur les personnes.

Comment Whaller répond à votre initiative ?

Un travail que nous avons effectué avec l'équipe Whaller, c'est le passage en marque blanche. Pour nous, c'était important que l'intranet ait vraiment une identité forte EUt+ et que ce soit marqué visuellement.

Nous avons utilisé un design spécifique EUt+, une charte graphique que nous avons développés sur la première phase du projet. Je vous donne un exemple quand nous nous connectons à Whaller, désormais nous avons ce graphique avec les différents campus, nous sélectionnons son campus et nous nous connectons. Nous avons un visuel 100 % EUt+. Nous sommes dans un écosystème EUt+, ce qui permet de développer ce sentiment d'appartenance : Nous sommes sur l'intranet EUt+.

Quels sont les projets à venir à mener sur la plateforme ?

Selon moi, un des enjeux, c'est développer la partie application mobile. Je pense que cela permettrait de créer encore plus ce sentiment d'appartenance à l'alliance EUt+.

D'avoir dans sa poche, avoir son portable, l'application Whaller, avec du push d'informations. Nous avons que nous allons retrouver toutes les informations utiles au bon déroulé du projet à l'intérieur de cette application.

C'est vrai que la partie Chat, nous ne l'avons pas encore trop utilisée. Il y a beaucoup de développements en cours et je souhaiterais lancer un message à l'équipe Whaller. Si nous pouvons développer les Chat groupés, ça serait vraiment un gros plus parce que nous le voyons notamment en déplacement.

Les gens ont besoin de se parler en petits groupes de travail et ça permettrait de prendre aussi une autre dimension au niveau de l'usage de Whaller dans le quotidien de l'EUt+.

En savoir plus :

- Comment Whaller facilite la communication interne et externe ?
- Comment Whaller contribue au développement d'un projet universitaire ?

> 🎥 Retrouvez tous nos témoignages clients sur notre chaîne Youtube.

Conclusion

Alors que nous tournons la page de l'année 2023, riche en enseignements et en avancées, les perspectives pour 2024 s'annoncent tout aussi palpitantes dans l'univers de la cybersécurité, de la transformation numérique et de la souveraineté numérique.

Le monde digital continue d'évoluer à un rythme effréné, et avec lui, les défis de sécurité qui nous tiennent à cœur chez Whaller. En 2024, l'accent sera mis sur la consolidation des stratégies de cybersécurité, notamment en prévision d'événements d'envergure comme les Jeux Olympiques. La cyberrésilience restera un pilier central, garantissant la sécurité et l'intégrité des infrastructures numériques face à des menaces toujours plus sophistiquées.

En parallèle, la transformation numérique continuera de remodeler nos façons de travailler et d'interagir. Les outils numériques, tels que les plateformes collaboratives offertes par Whaller, joueront un rôle crucial dans le soutien de cette transformation, en permettant des échanges plus fluides, sécurisés et efficaces.

La souveraineté numérique, quant à elle, restera au cœur des débats et des actions. L'année 2024 sera probablement marquée par des initiatives renforcées pour assurer une autonomie numérique, notamment en termes de données et de gestion des infrastructures. Ce sera un moment clé pour les organisations et les individus de s'engager dans la construction d'un écosystème numérique plus robuste et souverain.

En conclusion, Whaller s'engage à rester à l'avant-garde de ces évolutions. Nous continuerons de fournir des outils innovants et des insights pertinents pour accompagner nos utilisateurs dans cette ère de transition numérique. L'année 2024 s'annonce comme une période charnière, riche en opportunités et en défis, mais surtout en solutions prometteuses pour un avenir numérique sécurisé et souverain.

L'équipe Whaller

Whaller

Communiquer et collaborer en toute sécurité

Déployez une plateforme sociale et collaborative complète. De l'intranet collaboratif au réseau social d'entreprise, Whaller s'adresse aux organisations qui veulent accélérer leur transformation numérique, sans délaisser leur cybersécurité. Whaller convient aussi bien aux petites équipes qu'aux très grands réseaux.

Nous contacter

01.47.92.82.18

contact@whaller.com

3, rue Salomon de Rothschild - 92150 Suresnes