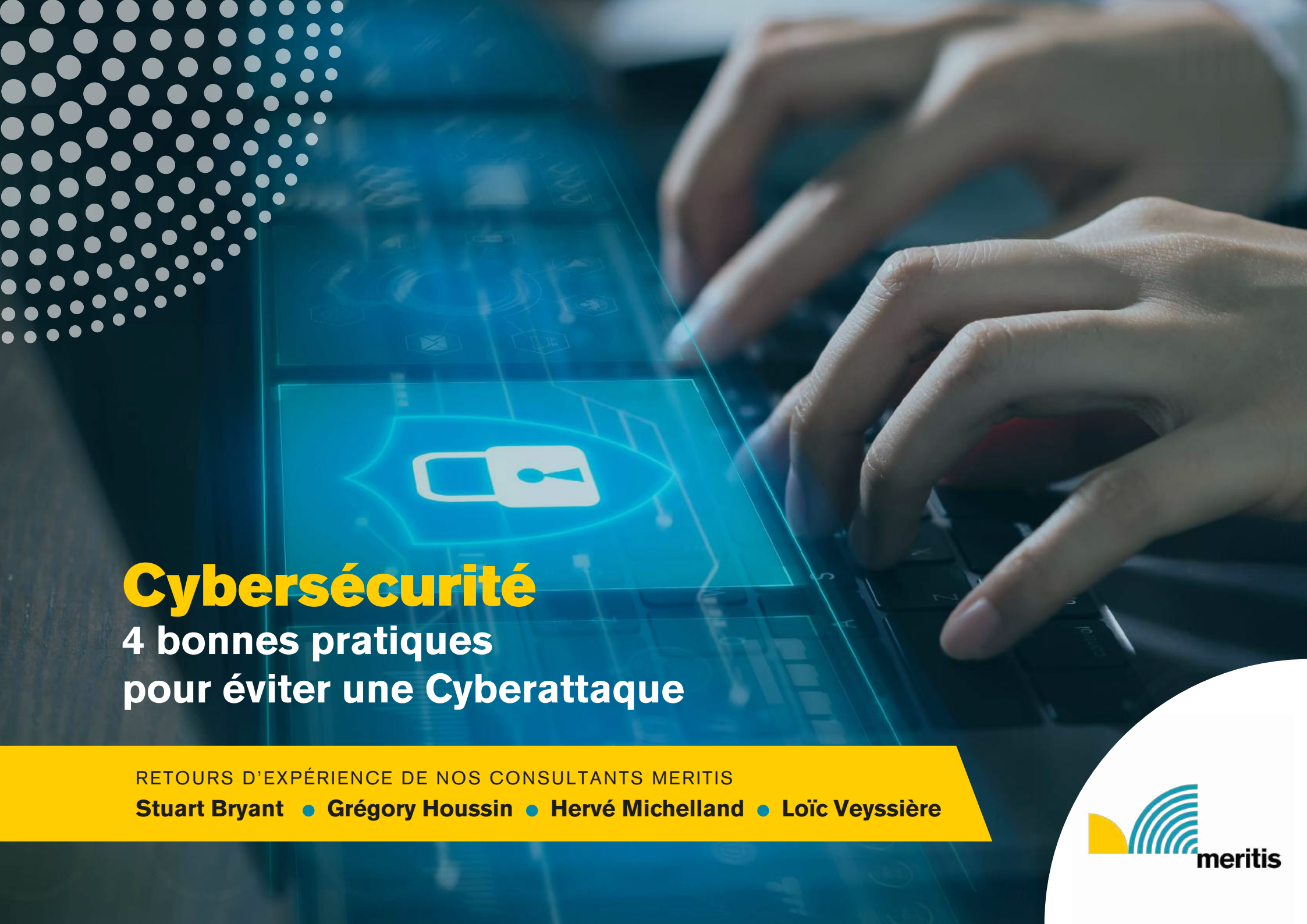


Cybersécurité

4 bonnes pratiques pour éviter une Cyberattaque

RETOURS D'EXPÉRIENCE DE NOS CONSULTANTS MERITIS

Stuart Bryant • Grégory Houssin • Hervé Michelland • Loïc Veyssière

meritis

[Sommaire]

[Les minibios des consultants]

Loïc Veyssiere
Senior Machine Learning Engineer

Loïc a commencé sa carrière en faisant de la recherche chez Intel sur des problématiques de calculs intensifs sur les supercalculateurs. Il a ensuite développé des solutions de machine learning dans différents domaines comme l'IoT ou dans l'estimation de risques dans l'assurance avant de rejoindre Meritis. Ce qui lui plaît aujourd'hui c'est de comprendre et de construire des architectures logicielles.

Hervé Michelland
Chief Information Security Officer et DPO

Après avoir géré le Centre de Sécurité Opérationnel d'un opérateur télécom, puis occupé les fonctions de Directeur de la sécurité d'une grande collectivité, Hervé a appris à apporter une réponse efficiente aux cybers menaces tout en diffusant un message positif autour de la cyber sécurité.
Hervé a permis au groupe Meritis d'obtenir une des certifications sécurité les plus exigeantes : Iso 27001. Elle démontre la capacité du groupe Meritis à protéger les informations confiées par nos clients. Il accompagne également plusieurs clients sur leurs besoins en sécurité technique ou de gouvernance.

Grégory Houssin
Consultant architecte sécurité réseau

Gregory a rejoint Meritis en 2021. Il a une expérience réussie, de plus de 20 ans dans la Cyber-Securité dans le domaine de l'Aéronautique.
En tant qu'Architecte Sécurité et Réseaux, j'aide les clients afin de mettre en place une stratégie de Sécurité des SI adaptée à leurs besoins et leur environnement, sensibiliser leurs utilisateurs, partager les bonnes pratiques, déployer des solutions dans leur réseau et apporter mon expérience afin d'améliorer en continue la sécurité au sein des entreprises.

Stuart Bryant
Consultant en technologies

Stuart, Tech Lead innovant, accompagne des équipes de développeurs pour construire des solutions performantes et développer de nouvelles opportunités commerciales. Il possède une expertise spécifique dans les domaines de services cloud, de la sécurité, de l'IOT, des médias et du divertissement et des interfaces utilisateur conversationnelles vocales

La cybersécurité sur le podium des priorités en 2022

+ 569 % ! C'est le niveau de hausse des enregistrements malveillants (relatifs aux logiciels malveillants et à l'hameçonnage) relevé par INTERPOL entre février et mars 2020[1]. Une augmentation qui s'élève même à + 788 % concernant les enregistrements présentant un risque élevé. Une explosion de la menace cyber à mettre en regard du passage massif en télétravail qui a affecté le monde entier du jour au lendemain en réponse à la pandémie. En conséquence, des millions de personnes ont dû apprendre à travailler dans un environnement personnel peu ou pas sécurisé.

Nos consultants ont regroupé dans ce livre blanc 4 bonnes pratiques issues de leurs propres retours d'expérience pour anticiper ou éviter une cyberattaque.

Une hyperconnexion qui a fait le bonheur des cyberhackers ouvrant considérablement la surface d'attaque. Quelles ont été les 3 menaces les plus importantes ? Les rançongiciels – ou ransomwares – qui bloquent l'accès aux données et menacent de les publier ou de les supprimer à moins qu'une rançon ne soit versée. Leur nombre a augmenté de 255 % en 2020[2] ! Mais aussi l'usurpation d'identité et les chevaux de Troie. Des attaques de plus en plus sophistiquées et industrialisées, mais qui n'en utilisent pas moins les canaux « traditionnels » : plus de 80 % des intrusions commencent tout simplement par un email[3].

Si l'expansion de la menace est « née » avec la globalisation du travail à distance, le nouveau mode de travail hybride, appelé à se pérenniser, fait aujourd'hui craindre le pire. En effet, 92 % des entreprises françaises ont connu en 2020 au moins une cyberattaque avec des répercussions sur leur activité[4] (perte de productivité, de données clients et/ou de données employés).

Résultat, les entreprises sont aujourd'hui prises en tenaille entre des technologies d'attaques et de défense qui évoluent très vite et une pénurie de compétences à tous les niveaux de la cybersécurité. Alors que 2022 est déjà considérée comme l'année du Ransomware as a Service, voilà les cartes avec lesquelles les ETI doivent composer. À elles alors de jouer sur l'effet levier de la cybersécurité : plus la sécurité sera intégrée tôt, plus elle sera efficiente !

1 • Selon un rapport d'Interpol, août 2020
2 • Selon l'ANSSI, février 2021
3 • Étude Email Security: Maintaining a High Bar When Moving to Office 365, IDC, janvier 2022
4 • Étude « Au-delà des frontières : l'avenir de la cybersécurité dans le nouveau monde du travail », menée par Forrester Consulting pour le compte de Tenable, septembre 2021

[Bonne pratique #1]

Réaliser une analyse de risque

Véritable « Alpha et Oméga » de votre sécurité, cette étape consiste à identifier les menaces auxquelles vous êtes exposé, et à mesurer leur probabilité d'occurrence et leur impact. Vous serez alors à même de définir une stratégie et d'y associer les ressources nécessaires.

Les 3 points clés de l'analyse de risques

Cette phase d'analyse de risques est un exercice critique en termes de sécurité. Pour le Responsable de la Sécurité des Systèmes d'Information (RSSI), l'enjeu est double : établir le plan d'actions à mener et surtout convaincre le comité de direction ! Pour cela, 3 éléments sont à prendre en considération.

L'avis de l'expert

Grégory Houssin
Consultant architecte sécurité réseau

C'est comme le diagnostic de performance énergétique (DPE) et l'état des lieux quand vous achetez une maison. Le rapport d'analyse va vous permettre d'orienter votre stratégie, mais aussi de définir les forces et faiblesses de votre entreprise, et de mettre en place un plan adéquat.

1/ La sécurité absolue n'existe pas

Par conséquent, soit vous mettez en place un écosystème extrêmement onéreux qui va scléroser toute l'entreprise, soit vous acceptez le risque… mais de façon raisonnable et raisonnée. Consultez la direction générale (DG) et les directions métiers pour comprendre quels sont leurs enjeux les plus importants et en déduire les conséquences en cas d'intrusion.

2/ La sécurité est chère

En donnant cette visibilité intelligible à la DG, elle en acceptera d'autant mieux les moyens alloués pour réduire le risque à un niveau acceptable. Car la sécurité a un coût ! Il importe alors de faire en sorte de dépenser le budget là où la plus-value sécuritaire sera la plus importante.

3/ La sécurité est contraignante

Enfin, n'oubliez pas que la course à la faille de sécurité n'est pas efficiente. La mise en œuvre de mesures très contraignantes ne s'avère légitime que si elle fait écho aux plus grandes craintes de la DG. Il appartient au responsable de tirer un fil d'Ariane pour expliquer ces mesures prises à la suite de cette analyse de risques.

[Bonne pratique #1]

La méthode de nos consultants

Mener un audit de sécurité

Si la liste des points à auditer relève du cas par cas, la méthode utilisée ne diffère pas :

- **Préparez votre audit :** vous devez définir son objectif et effectuer un état des lieux du réseau. Ensuite, vous pourrez établir votre stratégie selon votre infrastructure réseau, de ses composantes physiques et clouds, des profils de l'entreprise, etc.
- **Réaliser votre audit de sécurité :** il s'agit d'obtenir un diagnostic et une cartographie de votre réseau via des tests de charge, de panne, d'intrusion, de pénétration intérieure et extérieure, de vulnérabilité, des audits OS… La liste est loin d'être exhaustive.
- **Rédigez votre rapport d'audit :** présentez une synthèse technique et fonctionnelle de votre SI, détaillez les failles observées et proposez vos recommandations.

Vous souhaitez réaliser un audit de sécurité ?

CONTACTEZ-NOUS

En 2020,
Le nombre de cyberattaques en France a été

multiplié par 4

Source : ANSSI, février 2021

Les tips Meritis

Pour réaliser votre audit de sécurité, plusieurs méthodes existent, telles Cobit, Mehari ou EBIOS Risk Manager proposée par l'ANSSI.

[Bonne pratique #2]

Définir votre stratégie de Cybersécurité

Une fois les risques et le taux de couverture de ces risques bien compris par la DG, vous pouvez décliner votre stratégie de sécurité à court, moyen et long terme.

Les 5 rôles clés de la cybersécurité

Quelle organisation mettre en place ? Les experts doivent-ils être internalisés ou externalisés ? Si le référent de votre cybersécurité est le RSSI, de nombreux profils l'accompagnent répartis au sein de 5 expertises principales.

L'avis de l'expert

Stuart Bryant
Consultant en technologies

Il appartient à chacun, même au sein de départements autres que l'IT, de porter la responsabilité en matière de sécurité. Votre stratégie doit être envisagée à l'échelle horizontale. Pour le cloud, la sécurité doit impérativement faire partie du processus de développement dès la conception de l'environnement. C'est ce qu'on appelle le DevSecOps

1/ Pilotage, organisation et gestion des risques (POG)

L'objectif est de gérer le Plan de Sécurité des Systèmes d'Information (PSSI).

2/ Management de projet et cycle de vie (MPC)

L'architecte va alors designer les architectures à mettre en place une fois la stratégie définie.

3/ Opération et maintien en condition opérationnelle (OMCO)

Les métiers opérationnels ayant en charge la configuration et le déploiement de correctifs de sécurité, et l'application de mesures de sécurité sur l'infrastructure technique.

4/ Conseil, audit et expertise (CAE)

Les consultants interviennent directement chez le client en amont de la stratégie.

5/ Support et gestion des incidents (SGI)

Les analystes surveillent le réseau, principalement via le Security Operations Center (SOC), et interviennent en cas d'incidents.

[Bonne pratique #2]

La méthode de nos consultants

Focus sur le cloud

Quel que soit le type de cloud, public, privé ou hybride, les méthodes de sécurisation sont les mêmes :

- **Implémentez un système d'authentification forte :** les niveaux de connexion au cloud sont adaptés à chaque département en interne et à chaque utilisateur cloud.
- **Tracez toutes les personnes autorisées :** vous devez comprendre ce qu'il se passe en temps réel au sein de vos environnements cloud.
- **Déployez de multiples points de contrôle de sécurité :** dans les machines virtuelles, les systèmes d'exploitation…
- **Automatisez la sécurité :** indispensable pour pouvoir réagir en temps réel lorsqu'une activité inhabituelle est détectée.
- **Protégez les données transmises depuis le cloud :** pensez à encrypter vos données sensibles au repos et lors de leur transmission.
- **Privilégiez des responsabilités partagées :** à vous de gérer les systèmes d'exploitation et les réseaux superposés. À votre fournisseur cloud de s'occuper de la sécurité de l'environnement matériel et de certains services.

En 2020

95%

des professionnels IT

constataient toujours un déficit de compétences en cybersécurité, pénalisant ainsi près de 6 entreprises sur 10 (57 %).

Source : Enquête The Life and Times of Cybersecurity Professionals, ESG, juillet 2021

Les tips Meritis

Pensez à contracter une cyber-assurance. Celle-ci couvrira vos préjudices à hauteur de 100 000 à 1 million d'euros en cas d'attaque : pertes d'exploitation, dommages en responsabilité civile, frais de notification ou liés à une enquête de la CNIL, assistance et conseil juridique, éventuelles sanctions pécuniaires… Surtout, l'assureur vous assiste en cas de gestion de crise.

[Bonne pratique #3]

Mettre en œuvre votre plan d'actions

Place au Build ! À vous de construire votre sécurité à travers la mise en œuvre d'un certain nombre de mesures organisationnelles, physiques ou techniques.

L'avis de l'expert

Hervé Michelland
Chief Information Security Officer et DPO

Le temps est votre pire ennemi : plus vous attendez, plus l'infection se répandra. D'autant que les pirates poussent habituellement leur attaque lorsque vos équipes ne sont pas devant leur écran : la nuit, pendant les fêtes, le week-end, les vacances… Donc cloisonnez au maximum vos systèmes et surtout effectuez des exercices réguliers pour que la procédure devienne un réflexe.

Les 10 différents types de sécurité à mettre en place

La liste n'est pas exhaustive mais elle permet d'assurer un haut niveau de sécurité.

- ☐ **Respectez une politique rigoureuse de mot de passe**
  Il doit impérativement être individuel, difficile à deviner et demeurer confidentiel.
- ☐ **Déployez une procédure de création et de suppression des comptes utilisateurs**
  L'accès aux postes de travail et aux applications doit se faire uniquement via des comptes nominatifs.
- ☐ **Sécurisez au maximum les postes de travail**
  Verrouillez automatiquement les postes de travail au-delà d'un certain temps d'inactivité.
- ☐ **Identifiez de manière précise qui peut avoir accès aux données à protéger**
  Et limitez cet accès aux seules personnes qui en ont légitimement besoin dans leurs missions.
- ☐ **Assurez la confidentialité des données vis-à-vis des prestataires**
  C'est imposé par la loi !
- ☐ **Sécuriser le réseau local vis-à-vis des attaques extérieures**
  Emails, accès internet, communications entre sites distants : tout doit être sécurisé !
- ☐ **Assurer la sécurité de l'accès physique aux locaux**
  À quoi bon protéger les données si tout le monde a accès aux serveurs ou aux sauvegardes ?
- ☐ **Anticiper la perte ou la divulgation de données**
  Stocker les serveurs et les sauvegardes dans des espaces distincts. Et nettoyez vos supports mobiles !
- ☐ **Consigner dans un document la politique de sécurité du système d'information**
  Ce document doit être accessible à l'ensemble des salariés et mis à jour si besoin.
- ☐ **Sensibiliser les salariés à la loi Informatiques et Libertés et aux risques informatiques**
  Formations, diffusion de notes de service, envoi périodique de fiches pratiques, etc.

[Bonne pratique #3]

La méthode de nos consultants

L'effet Titanic

Si tous les composants réseau communiquent les uns avec les autres, l'attaque affectera l'ensemble du système d'information. C'est pourquoi vous devez segmenter votre réseau :

- Raccordez les imprimantes à un réseau, les serveurs à un autre, les backups situés à un 3e endroit, et les ordinateurs encore ailleurs.
- Installez des sens uniques. Par exemple, vous pouvez autoriser les serveurs à pousser de l'information vers les PC, mais pas l'inverse.
- Les posts administrateurs doivent également bénéficier de mesures spécifiques pour, en cas d'infection, pouvoir gérer la crise.

En 2020

57%

des entreprises

ont été victimes d'une attaque de phishing fructueuse

Source : Rapport State of the Phish 2021, Proofpoint

Les tips Meritis

Pensez à formaliser une charte informatique, laquelle regroupe, à destination de l'ensemble des salariés, les bonnes pratiques à adopter dans le cadre de l'utilisation de leur poste de travail.

[Bonne pratique #4]

Former et sensibiliser en interne

Le principal risque de sécurité demeure l'erreur humaine. C'est pourquoi l'ensemble des utilisateurs du SI doivent être sensibilisés aux différents risques inhérents à l'utilisation d'une base de données.

L'avis de l'expert

Loïc Veyssiere
Senior Machine Learning Engineer

La plus grande crainte du développeur est de laisser passer une faille et donc de manquer de compétences. Le hacker fait peur. C'est pourquoi la culture web doit s'articuler autour de la cybersécurité, et intégrer des notions aussi simples que le chiffrage des flux en HTTPS, ou le chiffrement de l'information avec des clés asymétrique et symétrique. Ce sont des points que tout développeur doit avoir appris au moins une fois.

Les 4 règles d'or de la sensibilisation des utilisateurs

Les experts se faisant rares, les entreprises n'ont d'autre choix que de former en interne pour éviter au maximum les risques.

1/ La sensibilisation concerne toutes les parties prenantes

Membres du codir, équipes IT, responsables fonctionnels et opérationnels, managers mais aussi (et surtout) collaborateurs métiers : tous les utilisateurs doivent être formés. La sensibilisation est inclusive !

2/ Former les collaborateurs dès leur arrivée dans l'entreprise

Cette formation doit être cohérente par rapport à votre analyse de risques. Vous devez informer les utilisateurs des principaux risques identifiés dès leur recrutement.

3/ Former de façon récurrente

Idéalement 1 fois par trimestre, et 1 à 2 fois par an minimum. Donc envoyez régulièrement des messages pour rappeler les bonnes pratiques.

4/ Adapter la sensibilisation à l'interlocuteur

Sur la base d'un cursus commun, il est essentiel de proposer une déclinaison adaptée au métier de l'utilisateur et aux enjeux spécifiques de son poste. Tous les profils ne sont pas concernés par les mêmes risques.

[Bonne pratique #4]

La méthode de nos consultants

Le cas du développeur

N'oubliez pas les développeurs dans votre politique de sensibilisation. Votre culture informatique doit intégrer les 4 grands principes de développement suivants :

- **L'isolation des environnements :** il s'agit en résumé de ne pas mettre tous ses œufs dans le même panier ;
- **La security by design :** intégrer la sécurité dès la phase de conception du produit ;
- **La sécurité en profondeur :** il ne faut jamais « croire » la couche supérieure qui a transmis les informations ;
- **Le principe de frugalité :** on n'échange que les informations dont on a réellement besoin.

85%

des fuites des données

sont causées par une erreur humaine… Mais la formation et la sensibilisation à la sécurité ont réduit leur vulnérabilité aux attaques de phishing pour 80 % des organisations.

Source :
Rapport d'enquête sur les compromissions de données Rapport State of the Phish 2021, Proofpoint (DBIR), Verizon, 2021

Les tips Meritis

Le Top 10 OWASP est un document de sensibilisation standard à la sécurité des applications web destiné aux développeurs.
Il représente un large consensus sur les risques de sécurité les plus critiques pour les applications web.

Conclusion

Pour une approche globale de la sécurité

66 % des DSI prévoient d'augmenter le montant qu'ils consacrent à la cybersécurité et à la sécurité de l'information selon les prédictions 2022 du cabinet Gartner. Désormais, la sécurité se classe en 3e position des priorités derrière l'intelligence artificielle / le machine learning, et le cloud distribué. Des technologies émergentes qui constituent autant de portes d'entrée potentielles pour les hackers.

À commencer par les objets connectés dont les usages ont explosé avec l'arrivée de la 5G. Les défis de sécurité sont ainsi amenés à être renforcés par les fonctionnalités même de la 5G, telles que « la virtualisation, l'hyper précision de la géolocalisation, et l'explosion du volume et de la vitesse du réseau ». En effet, la nature distribuée des réseaux 5G sur lesquels vont se greffer une multitude d'objets connectés peu sécurisés élargit considérablement la zone d'attaque.

Autre technologie à risque : l'intelligence artificielle… dont les entreprises ne peuvent pourtant pas se passer. Et les pirates informatiques en ont parfaitement conscience ! Selon la liste des menaces actuelles et futures des intelligences artificielles rédigée par Europol, l'IA serait déjà utilisée pour deviner des mots de passe, casser des CAPTCHA ou encore cloner des voix. Imaginez que les hackers parviennent à modifier le comportement de certaines de vos innovations. Sans aller jusqu'à l'exemple des voitures autonomes, votre image et votre activité en pâtiraient fortement.

La cybersécurité a aujourd'hui pris une tout autre dimension en pénétrant la sphère géopolitique. D'une « simple » obligation de protection des données personnelles, les entreprises font désormais face à de véritables enjeux de souveraineté nationale. Résultat, votre responsabilité s'étend bien au-delà des murs de votre entreprise.

C'est pourquoi vous devez intégrer au plus tôt la cybersécurité dans une approche globale impliquant tous les acteurs de votre écosystème.

Meritis, le talent d'aller plus loin.

CONSEIL, PILOTAGE ET DÉVELOPPEMENT IT

Meritis est une société de conseil en transformation des Systèmes d'Information et Organisations.

➔ **Notre approche ?**
Accompagner nos clients sur l'ensemble de la chaîne de valeur : cadrage personnalisé, pilotage & développement applicatif pour les projets IT.

➔ **Notre mission ?**
Connecter les meilleurs talents au service de la transformation numérique pour donner un temps d'avance aux entreprises.

Nos +750 consultants vous accompagnent avec agilité dans tous vos projets de transformation digitale. Un seul objectif : vous emmener plus loin.

Meritis Cybersécurité

NOTRE EXPERTISE AU SERVICE DE VOTRE SECURITE !

Ransomware & malware (logiciels malveillants), **phishing** (hameçonnage par des fraudeurs) ou **intrusion au niveau du système d'information** (vol de données, usurpation d'identité , espionnage industriel) ; les sociétés sont toutes vulnérables face à ces menaces. Selon l'Autorité nationale de la sécurité des systèmes d'information (ANSSI), les **cyberattaques** ciblant des sociétés Françaises sont **de plus en plus nombreuses avec des pertes estimées à plusieurs millions d'euros.**

Pour répondre au plus près à vos besoins, nous avons composé une **équipe d'experts pluridisciplinaires** : RSSI, Consultant Cybersécurité, auditeur Cybersécurité, Risk Manager, Architecte Sécurité, Pentester ou encore experts DevSecOps

Quelques soient vos besoins, Meritis vous accompagne dans chaque étape de votre projet :

- ➔ **Analyse des menaces et des risques**
- ➔ **Détection des activités suspectes ou malveillantes**
- ➔ **Mise en place d'une stratégie cybersécurité**

EN SAVOIR PLUS

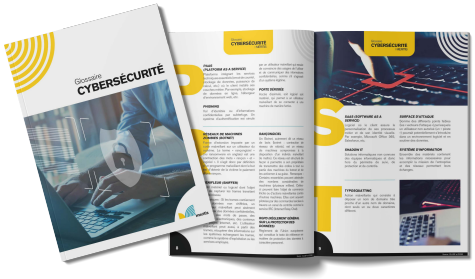
Nos dernières publications

Cliquez sur l'image pour les découvrir

Livre Blanc

Cyberattaque et gestion de crise : quel protocole mettre en place ?

Télécharger



Glossaire

le lexique à connaître

Télécharger

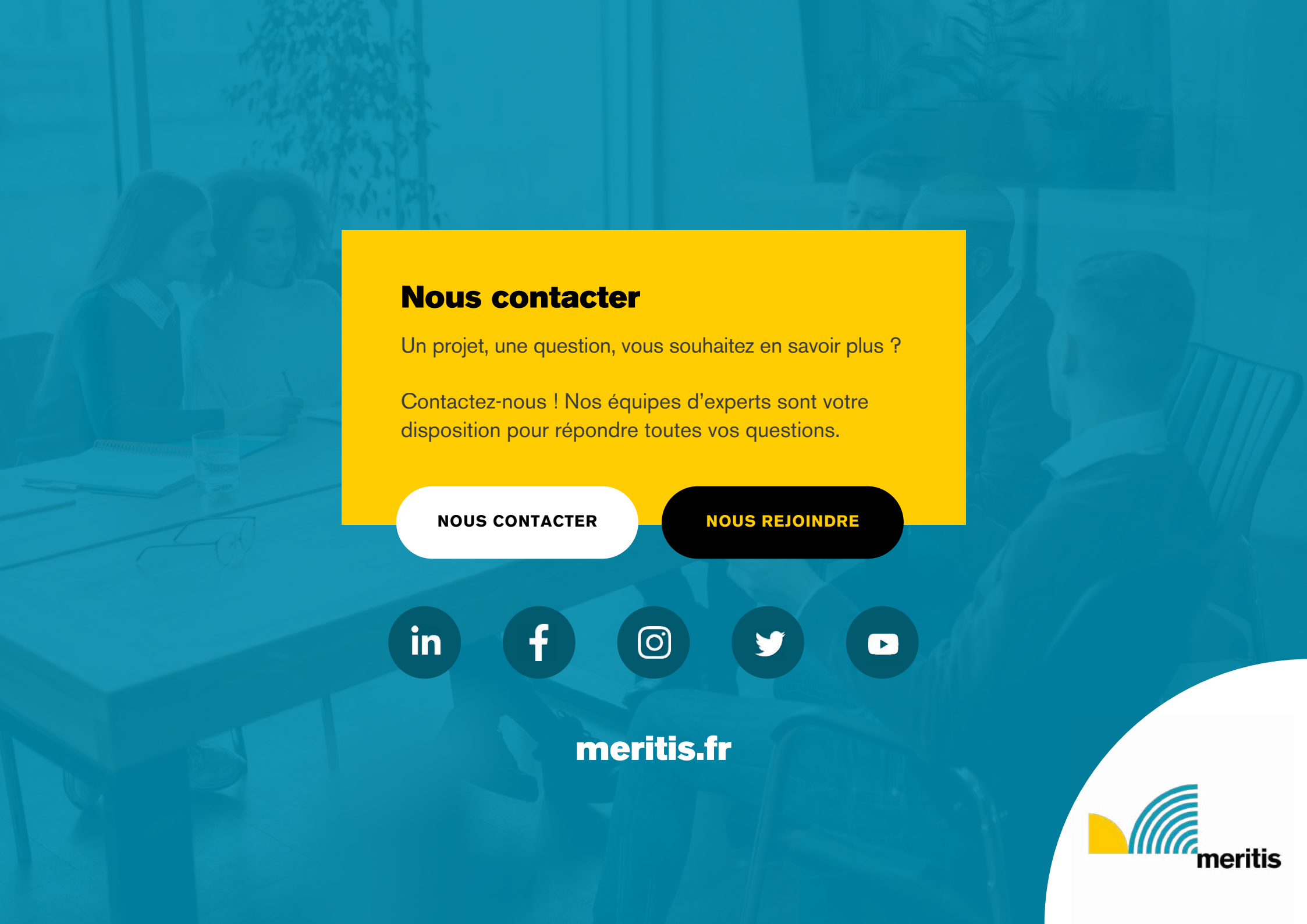
Use Case

Comment un piratage a déclenché la restructuration de tout un système d'information ?

Télécharger

Retrouvez l'ensemble de nos publications ici

ou sur notre site
https://meritis.fr/livres-blancs/



Nous contacter

Un projet, une question, vous souhaitez en savoir plus ?

Contactez-nous ! Nos équipes d'experts sont votre disposition pour répondre toutes vos questions.

NOUS CONTACTER

NOUS REJOINDRE

meritis.fr

meritis