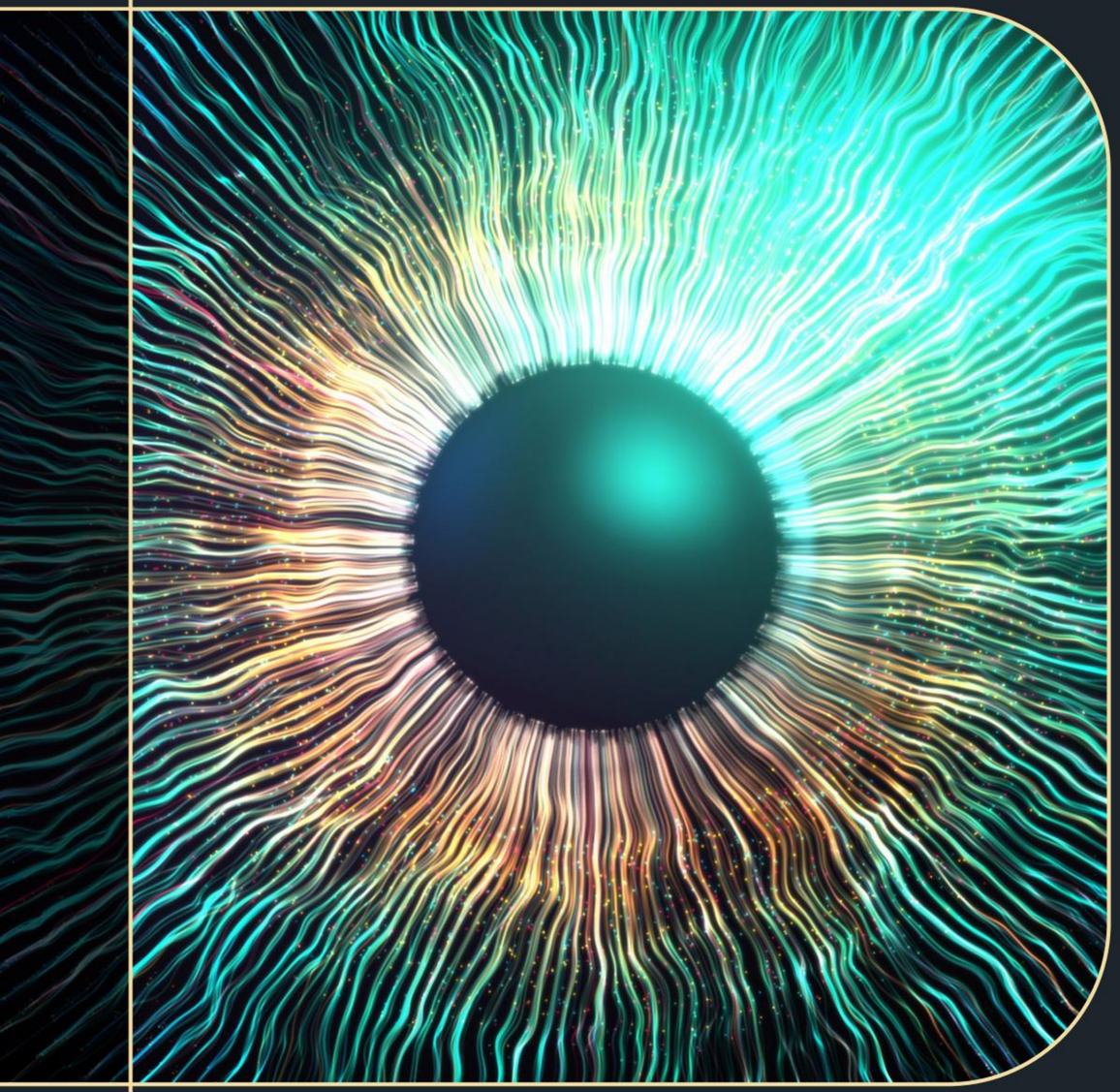


Forcepoint

Perspectives d'avenir 2025

Quelles seront les répercussions de l'année 2025 sur la sécurité ? Dans cet eBook Future Insight 2025, les dirigeants et experts de Forcepoint proposent quatre prévisions sur les tendances qui, selon eux, façonneront les efforts de sécurité au cours de l'année à venir et au-delà.

Découvrez l'eBook 2025 Future Insights de Forcepoint.

Vous approfondirez des sujets tels que l'AISPM, la législation sur l'IA, les tendances des pirates informatiques, la confidentialité des données à l'ère de l'IA et bien plus encore.

L’intelligence artificielle a continué de dominer l’actualité technologique en 2024. Quel sera son impact sur la cybersécurité dans les années à venir ?
C’est la question que nous avons posée à nos hauts dirigeants et à nos technologues.

Consultez l’eBook 2025 Future Insights pour entendre ce qu’ils avaient à dire.

Téléchargez le rapport pour en savoir plus :

→ AISPM : un concept de sécurité critique pour 2025

→ Apprendre à vivre sans : l’impact de la législation sur l’IA

→ Les pirates informatiques créeront de plus en plus de campagnes de logiciels malveillants sur des services d'infrastructure légitimes

→ L’émergence d’un ordre multilatéral en matière de réglementation de la vie privée

AISPM : un concept de sécurité essentiel pour 2025

Une sécurité efficace des données ne se limite pas à la simple mise en place de mesures visant à bloquer l'exfiltration d'informations sensibles. Elle nécessite également une compréhension précise de la nature et de l'emplacement des données, ainsi que l'élimination des données ROT (redondantes, obsolètes et triviales). C'est pourquoi, en plus de notre célèbre programme de prévention des pertes de données, (DLP), Forcepoint propose une gestion de la posture de sécurité des données (DSPM). Cette solution adopte une approche proactive de la sécurité en découvrant, classant et orchestrant les données tout en utilisant l'automatisation pour détecter rapidement les facteurs de risque émergents.

Dans le paysage technologique en constante évolution d'aujourd'hui, l'intelligence artificielle (IA) est devenue un élément essentiel de nombreuses opérations d'entreprise. De l'amélioration de l'expérience client à la rationalisation des processus internes, les outils d'IA sont à l'origine d'avancées significatives dans tous les secteurs. Cependant, un grand pouvoir implique de grandes responsabilités, et il est essentiel pour les entreprises de comprendre les risques associés à l'IA et de savoir les gérer efficacement. C'est là qu'entre en jeu la gestion de la posture de sécurité de l'IA (AISPM).

L'importance de comprendre les risques liés à l'IA

Les systèmes d'IA, bien que transformateurs, introduisent un ensemble unique de risques qui diffèrent considérablement des menaces informatiques traditionnelles. Ces risques peuvent avoir de profondes implications pour une entreprise, allant des violations de données aux perturbations opérationnelles. Il est essentiel de comprendre ces risques pour protéger les actifs, la réputation et la fonctionnalité globale de votre entreprise.

1. Confidentialité et sécurité des données : les outils d'IA nécessitent souvent Il est nécessaire de disposer de grandes quantités de données pour fonctionner efficacement. Ces données peuvent contenir des informations sensibles, et toute violation ou utilisation abusive peut entraîner de graves violations de la vie privée et des conséquences juridiques.

2. Vulnérabilités des modèles : les modèles d'IA ne sont pas à l'abri des attaques. Les attaques adverses, où des acteurs malveillants manipulent les données d'entrée pour tromper les systèmes d'IA, peuvent conduire à des résultats et des décisions incorrects, pouvant potentiellement causer des dommages importants.

3. Biais et équité : les systèmes d'IA peuvent par inadvertance perpétuer ou amplifier les biais présents dans les données d'apprentissage. Cela peut entraîner un traitement injuste des individus ou des groupes, ce qui peut susciter des préoccupations éthiques et juridiques.

4. Risques opérationnels : les systèmes d'IA peuvent mal fonctionner ou produire des résultats inattendus dus à des défauts dans le modèle ou à des changements dans les modèles de données, susceptibles de perturber les opérations commerciales.

AISPM : un concept de sécurité essentiel pour 2025

Qu’est-ce que l’AISPM exactement et qu’en faites-vous ?

Alors que CSPM se concentre sur l’infrastructure cloud et que DSPM englobe les données à toutes les étapes de leur cycle de vie, AISPM se concentre sur la sécurité des systèmes d’IA et d’apprentissage automatique (ML) partout où ils sont utilisés dans votre organisation.

L'AISPM est conçu pour traiter les vulnérabilités associées aux systèmes d'IA et à la manière dont ils interagissent avec les données et l'infrastructure. Les principales fonctionnalités de l'AISPM que vous pouvez utiliser pour résoudre les problèmes de sécurité de l'IA sont les suivantes :

→ Découverte de l'IA : pour obtenir une visibilité sur les outils d'IA utilisés
Pour utiliser l’IA fantôme, commencez par une évaluation approfondie des outils d’IA utilisés. Identifiez les risques potentiels liés aux données, à l’intégrité du modèle et à l’impact opérationnel. Mettez régulièrement à jour cette évaluation à mesure que la technologie et le paysage des menaces évoluent. Exploitez des outils qui peuvent aider à identifier les outils d’IA fantômes qui peuvent être utilisés par des individus ou des équipes dans toute l’organisation sans avoir été entièrement approuvés par votre entreprise.

→ Détection de mauvaise configuration : utilisez ceci pour identifier
services d'IA mal configurés et appliquer des règles de configuration.

→ Gouvernance des données : mettre en œuvre une gouvernance des données robuste
pratiques visant à garantir que les données utilisées à des fins de formation et d'exploitation sont sécurisées, exactes et conformes aux réglementations en matière de confidentialité. Cela comprend le cryptage des données, les contrôles d'accès et les audits réguliers.

→ Correction du chemin d'attaque : identifier et éliminer
vulnérabilités et éviter le mélange d'informations sensibles avec les données de formation.

→ Application de la conformité : s'assurer que toute utilisation de l'IA est
réalisée conformément aux exigences réglementaires applicables, de la configuration au reporting.

→ Surveillance et amélioration continues : la sécurité de l'IA est
Il ne s'agit pas d'une tâche ponctuelle, mais d'un processus continu. Surveillez en permanence les systèmes d'IA pour détecter les menaces et les vulnérabilités émergentes et adaptez vos mesures de sécurité en conséquence.

À mesure que l’AISPM gagne en popularité en tant que catégorie de solutions – et je m’attends pleinement à ce que cela continue – nous pourrions assister à l’émergence d’un ensemble de fonctionnalités plus détaillées et standardisées que chaque fournisseur d’AISPM proposera comme mise de départ.

AISPM : un concept de sécurité essentiel pour 2025

Qu'est-ce qui fait de Forcepoint un acteur majeur pour l'AISPM ?

Forcepoint est bien placé pour jouer un rôle de premier plan dans la conversation AISPM, avec notre spécialisation dans la sécurité des données qui, depuis le début, a été fortement axée sur la lutte contre les menaces émergentes associé à l'IA générative. Le maillage AI Le modèle qui alimente actuellement la classification de notre solution DSPM peut améliorer radicalement la précision avec lesquels les organisations identifient les données sensibles et les protègent contre l'exfiltration via des systèmes d'IA.

Dans cette vidéo, Je vous propose un aperçu de ce qui différencie AI Mesh et le rend si transparent et efficace. Au cœur de cette performance se trouve le Small Language Model (SLM) génératif de l'IA, qui nécessite beaucoup moins de puissance de calcul et est donc plus rapide et plus facilement personnalisable qu'un LLM.

Une stratégie proactive de classification et d'organisation des données avant leur interaction avec les systèmes d'IA est mieux complétée par une DLP qui peut bloquer la saisie d'informations sensibles et exclusives dans les outils d'IA. La sécurité de l'IA organisationnelle peut être encore renforcée en utilisant une protection adaptative aux risques pour analyser le comportement des utilisateurs et ajuster les niveaux d'accès automatiquement, en temps réel. L'utilisation de ces outils en combinaison donne lieu à l'approche que nous appelons Data Security Everywhere, une stratégie efficace pour sécuriser les données importantes et maintenir la sécurité de l'utilisation de l'IA générative.

L'AISPM définit une nouvelle norme en matière de sécurité proactive

Une grande partie du travail à effectuer pour prévenir les violations de données ne consiste pas à contrer les menaces avancées, mais à être constamment vigilant sur les petits détails. Par exemple, si vous souscrivez à une solution d'IA d'entreprise pour vous aider dans une tâche particulière, comment pouvez-vous vous assurer que vos employés n'utilisent que cette solution et non une version publique plus facilement accessible et dépourvue des contrôles de sécurité nécessaires ? Comment éviter qu'un fichier contenant des informations stratégiques confidentielles ne soit accidentellement enregistré dans le dossier de messagerie de la marque que vous êtes sur le point de mettre à la disposition de votre outil de rédaction d'IA ?

Alors que l'IA continue de remodeler le paysage des entreprises, il est essentiel de comprendre et de gérer la posture de sécurité des outils d'IA pour protéger votre entreprise contre les risques potentiels. En adoptant une approche proactive et globale de la gestion de la posture de sécurité de l'IA, vous pouvez protéger vos données, maintenir l'intégrité opérationnelle et respecter les normes éthiques. Ce faisant, vous améliorerez non seulement la sécurité de vos systèmes d'IA, mais renforcerez également la confiance de vos parties prenantes.

Investir dans l'AISPM ne consiste pas seulement à atténuer les risques : il s'agit de garantir que vos initiatives d'IA contribuent positivement à votre entreprise tout en maintenant un cadre sécurisé et éthique.
Adoptez l'avenir de l'IA en toute confiance, sachant que vous disposez des outils et des stratégies nécessaires pour gérer efficacement sa sécurité.

Jaimen Hoopes

Vice-président, Gestion des produits

Apprendre à vivre sans l'IA : l'impact de la législation sur l'IA

Les entreprises se dirigent à grands pas vers une ligne d'arrivée où leurs technologies et les services qu'elles fournissent sont indéniablement liés à l'intelligence artificielle.

Bien que le jury n'ait pas encore rendu son verdict sur des produits tels que les clubs de golf alimentés par l'IA , L'IA est rapidement passée d'un simple chatbot à la technologie sous-jacente derrière certains des services logiciels les plus impactants du marché actuel.

Parallèlement, les législateurs et les régulateurs du monde entier peaufinent leurs lignes directrices pour une approche plus réfléchie et plus prudente de l'intégration de l'IA. Pour que les entreprises restent à la pointe, elles devront réfléchir à la manière dont leurs logiciels basés sur l'IA peuvent fonctionner sans l'IA.

La législation suit l'innovation

ChatGPT a ouvert la boîte de Pandore. Peu après son lancement fin 2022, des dizaines de milliers d'entreprises d'IA ont afflué sur le marché libre, promettant des solutions plus rapides et plus performantes.

Avec la vague d'introductions en bourse et de lancements de produits, vous avez peut-être manqué ce qui se passait en coulisses. Les législateurs se sont rapidement mis au travail pour établir des lignes directrices et des garde-fous pour la technologie la plus transformatrice depuis Internet.

Plusieurs pays ont présenté leurs propres cadres mondiaux d'IA. Ces derniers fournissent des orientations pratiques aux entreprises du secteur privé pour tenter de répondre aux principales questions d'éthique et de gouvernance lors de la conception et du déploiement de solutions d'IA.
Ces cadres mettent l'accent sur la transparence, l'équité et la responsabilité.
Parmi les exemples de cadres d'IA, on peut citer :

→ Cadre éthique de l'IA en Australie

→ Modèle de cadre de gouvernance de l'IA à Singapour

→ Stratégie nationale de l'Inde en matière d'IA

→ Stratégie nationale de l'IA en Corée du Sud

→ Lignes directrices des Émirats arabes unis en matière d'éthique de l'IA

Certains de ces cadres sont arrivés parallèlement aux lois mondiales sur l'IA conçu pour faire avancer les choses au niveau national :

→ Loi européenne sur l'IA : Se concentre sur la réglementation basée sur les risques des systèmes d'IA, en les classant en risques inacceptables, élevés, faibles ou minimes.

→ Décret exécutif américain sur l'IA : Met l'accent sur la transparence, la sécurité et la confidentialité dans le développement et le déploiement de l'IA, et appelle à de nouvelles normes et meilleures pratiques dans divers secteurs.
De nombreux États américains sont en attente d'une législation ou ont promulgué leurs propres lois sur l'IA au niveau de l'État.

→ Directive canadienne sur la prise de décision automatisée :
Garantit que les systèmes de décision automatisés sont utilisés de manière transparente, responsable et conforme aux droits de l'homme. Nécessite des évaluations d'impact et un suivi continu.

Bon nombre de ces politiques s'appuient sur les lois sur la protection des données et la confidentialité déjà en vigueur, dont certaines tiennent déjà compte de la manière dont l'IA interagit avec les données. Il s'agit notamment du RGPD, du CCPA, du LGPD, du PIPA, de l'APPI et de la loi australienne sur la confidentialité de 1988. Comprendre à quoi servent ces réglementations, jusqu'où elles s'étendent (ou pas) et à qui elles s'appliquent est une première étape souvent négligée dans l'adoption réelle de l'IA.

Apprendre à vivre sans l'IA : l'impact de la législation sur l'IA

Beaucoup de bruit pour quelque chose

La législation incite les entreprises à se préoccuper davantage de l'IA et de son impact sur les utilisateurs finaux. Les entreprises ont la responsabilité de veiller à ce que les données soient entre de bonnes mains, comme pour toute autre application, et les utilisateurs doivent garder le contrôle des données transmises à l'IA, au cas où ils souhaiteraient les supprimer.

De nombreuses entreprises intègrent une interface utilisateur à l'IA et s'attendent à ce que le tour soit joué : le financement de série A est imminent. Mais pour beaucoup de ces startups, l'intégralité du back-end du produit est open source et l'IA s'entraîne sur ces données.

Dans le cadre de la législation sur l'IA, les organisations doivent conserver un contrôle total sur les données. Dans certains cas, cela signifie s'assurer que l'IA est prête à l'emploi plutôt qu'une solution universelle. Tenez compte des éléments suivants :

→ Les données sont une voie à sens unique. L'IA doit fonctionner comme une entreprise, modèle fermé.

→ L'IA varie selon les fonctions. Évaluez les investissements en IA en fonction de votre activité : support client, développement de logiciels ou marketing, par exemple. La criticité ou la sensibilité des données que vous partagez avec cette IA doit refléter les mesures de sécurité qu'elle a mises en place.

→ L'IA doit être transparente. Documentez tout et s'assurer que les gens comprennent comment l'IA est utilisée dans un produit. Ne divulguez pas de propriété intellectuelle, mais expliquez comment les données passent de l'entrée à la sortie. Voici un exemple de la manière dont Forcepoint procède avec AI Mesh.

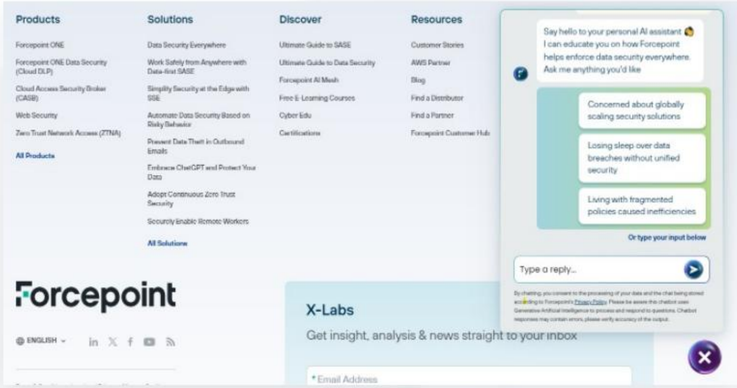
Gardez l'interrupteur « Off » en vue

Plus important encore, les entreprises doivent réfléchir de plus en plus à la manière dont l'IA est intégrée dans la pile de services.
Cela est dû au fait que, sur une base individuelle, les organisations doivent permettre aux utilisateurs de demander la désactivation de l'IA.

Considérez ceci : si vous avez passé l'année dernière à créer un tout nouveau chatbot IA et qu'une loi prévoit que les utilisateurs peuvent refuser de participer, comment allez-vous gérer cette demande ? Il faut tenir compte des flux de travail en place et de l'impact que la réglementation peut avoir sur eux.

À titre d'exemple, Forcepoint informe les utilisateurs, à la fois dans la fenêtre d'invite et pendant la sortie générée, qu'ils interagissent avec l'IA et avant d'utiliser les fonctionnalités de chatbot IA fournies par Forcepoint.

Forcepoint fournit également une liste de nos sous-traitants de données que nous utilisons pour soutenir nos produits et nos opérations. C'est pourquoi nos outils et services d'IA sont indiqués par (*), via notre liste de sous-traitants Forcepoint sur notre site internet.



Apprendre à vivre sans l'IA : l'impact de la législation sur l'IA

« En discutant, vous consentez au traitement de vos données et au stockage du chat conformément à la politique de confidentialité de Forcepoint. Veuillez noter que ce chatbot utilise l'intelligence artificielle générative pour traiter et répondre aux questions. Les réponses du chatbot peuvent contenir des erreurs, veuillez vérifier l'exactitude des résultats.

Cette utilisation binaire de l'IA deviendra la norme en 2025 et au-delà, car les entreprises continuent de réfléchir à la manière de fournir des services logiciels basés sur l'IA tout en offrant aux utilisateurs la possibilité de se retirer de la partie IA de ces services.

Outre la possibilité de refus, les organisations doivent également avoir la capacité d'identifier les individus spécifiques qui interagissent avec l'IA et les données personnelles qu'ils partagent au sein de celle-ci. Gestion de la posture de sécurité des données (DSPM) vous aide ici en identifiant et en classant les données dont vous disposez afin que vous puissiez surveiller les interactions avec des plateformes comme ChatGPT Enterprise pour garantir que l'activité de l'utilisateur final n'entraîne pas de non-conformité.

Les utilisateurs sont impatients de profiter des avantages de l'IA et les entreprises ont raison de se lancer dans l'innovation.
Toutefois, les fournisseurs de logiciels doivent tenir compte de la législation dans la conception de leurs services le plus tôt possible.

Michel Leach

Directeur de la conformité mondiale

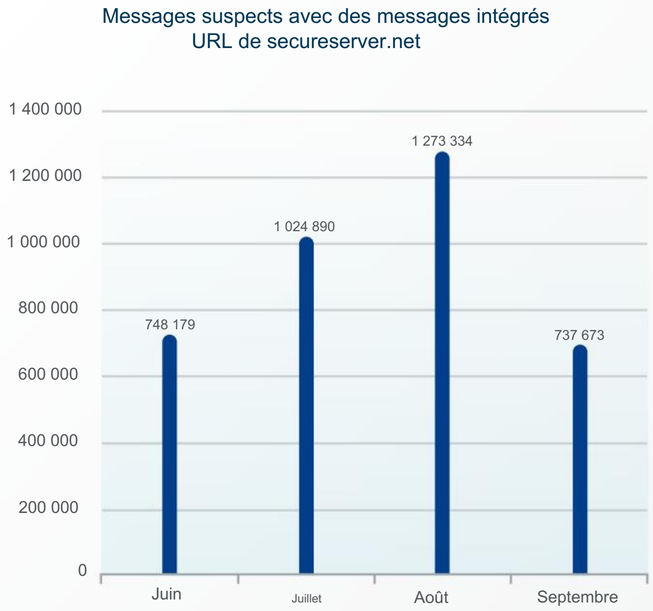
Les pirates informatiques vont de plus en plus créer des campagnes de logiciels malveillants sur des services d'infrastructure légitimes

Tout au long de l'année 2024, alors que nous continuions à suivre l'activité autour des dernières campagnes de malware et de phishing, nous avons remarqué une tendance : les pirates informatiques abandonnaient l'utilisation de sites Web compromis pour héberger des malwares au profit de services d'infrastructure légitimes. Sur la base de nos données, nous prévoyons que cette tendance s'accélérera en 2025 et au-delà.

Exemples de campagnes de logiciels malveillants

Prenons blogspot.com, le service de domaine gratuit de Google qui fournit un sous-domaine pour Blogger. C'est là que nous avons découvert le malware Agent Tesla les auteurs y hébergent des charges utiles. En juillet, nous avons assisté à une vague d'activité où les pirates informatiques ont exploité Trycloudflare.com et Python pour déployer le malware AsyncRAT. Et l'activité RAT de Remcos dont nous avons parlé sur notre blog en juin également exploité Trycloudflare.com. Les pirates ont utilisé TryCloudflare pour XWorm et d'autres logiciels malveillants des campagnes également. La campagne de malware Snakekeylogger a utilisé Discord CDN comme réseau de distribution de contenu public pour héberger des fichiers malveillants.

Les pirates informatiques ont également largement exploité Secureserver.net pour leurs activités malveillantes. C'est ce qui a donné naissance à une campagne de logiciels malveillants dont nous avons parlé dans notre blog et qui visait principalement les institutions financières en Amérique latine. D'autres logiciels malveillants comme Grandoreiro et NetSupport RAT ont exploité Secureserver.net également. Pour donner une idée de l'ampleur du problème, Forcepoint a intercepté plus de 3,7 millions d'e-mails suspects contenant des URL Secureserver.net au cours des derniers mois seulement :



Les pirates informatiques vont de plus en plus créer des campagnes de logiciels malveillants sur des services d'infrastructure légitimes

Dans le cas de Remcos et d'Agent Tesla, nous avons trouvé des exemples de ces deux sociétés utilisant des services gratuits pour héberger des images de stéganographie ou d'autres téléchargements d'étapes :

1. uploaddeimagens.com.br

2.archive.org

3. raw.githubusercontent.com

Pour l'exfiltration de données et la communication de commande et de contrôle, plusieurs campagnes de logiciels malveillants ont exploité les services légitimes suivants :

→ Services DNS dynamiques : les pirates utilisent ces services pour modifier les adresses IP afin d'échapper à la détection.

- freeddns.noip.com (servequake.com)
- freeddns.dynu.com
- duckdns.org

→ Telegram Bot API : L'API Telegram Bot permet aux mauvais acteurs créer des bots pour interagir avec les utilisateurs sur la plateforme Telegram.

- api.telegram.org/bot

→ Services d'hébergement de petits fichiers : stockage de fichiers à l'aide de Les services de stockage gratuits connus rendent plus difficile le suivi des activités malveillantes.

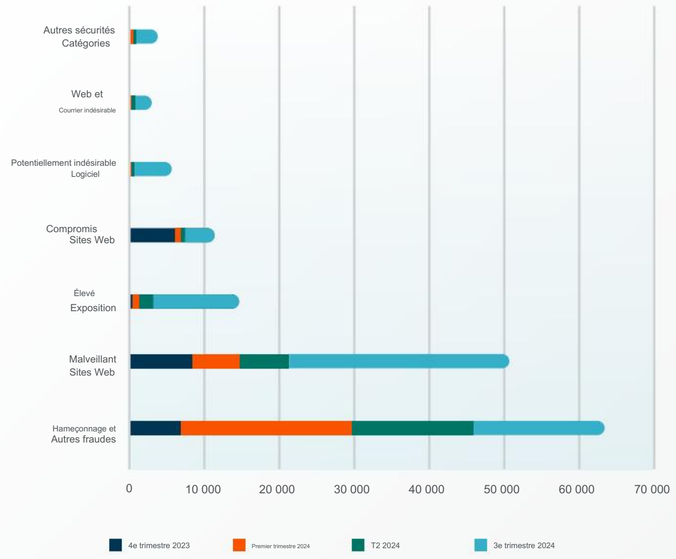
- qu.ax
- store2.gofile.io/téléchargement

→ Services de redirection de port : le stockage de fichiers dans plusieurs emplacements distants bien connus rend plus difficile le suivi des activités malveillantes en cours.

- ply.gg
- portmap.hôte

Pour avoir une idée de l'ampleur du phénomène de basculement des pirates vers des services légitimes, nous avons analysé l'activité des menaces observée sur les 50 principaux services d'hébergement Web. Cette liste comprenait plusieurs des principaux acteurs comme Windows.net, Wordpress.com, Bluehost, Wix, Firebase de Google et bien d'autres. Voici le graphique qui montre les plateformes d'hébergement Web présentant des risques de sécurité sur les sous-domaines

Plateformes d'hébergement présentant des risques de sécurité sur les sous-domaines



Les pirates informatiques vont de plus en plus créer des campagnes de logiciels malveillants sur des services d'infrastructure légitimes

Services légitimes utilisés pour les campagnes de phishing

En ce qui concerne le phishing, nous avons rencontré des campagnes de phishing dans lesquelles les pirates exploitent divers services Cloudflare : Pages pour déployer des pages Web statiques et Workers pour déployer du code sans serveur vers plusieurs emplacements potentiels dans le monde. Les acteurs malveillants profitent également du CDN Cloudflare pour accélérer la livraison d'applications SaaS partout dans le monde.

Nous avons observé des niveaux d'activité importants sur Windows.
net où les pirates exploitent Azure Blob Storage pour héberger et diffuser du contenu Web statique, des fichiers et des applications. Les attaquants en profitent en hébergeant des pages de phishing, des logiciels malveillants ou des escroqueries au support technique sur des sous-domaines tels que web.core.windows.net ou azurewebsites.net. Ces sous-domaines rendent les sites malveillants
le contenu semble plus crédible car il est associé à l'infrastructure de confiance de Microsoft.

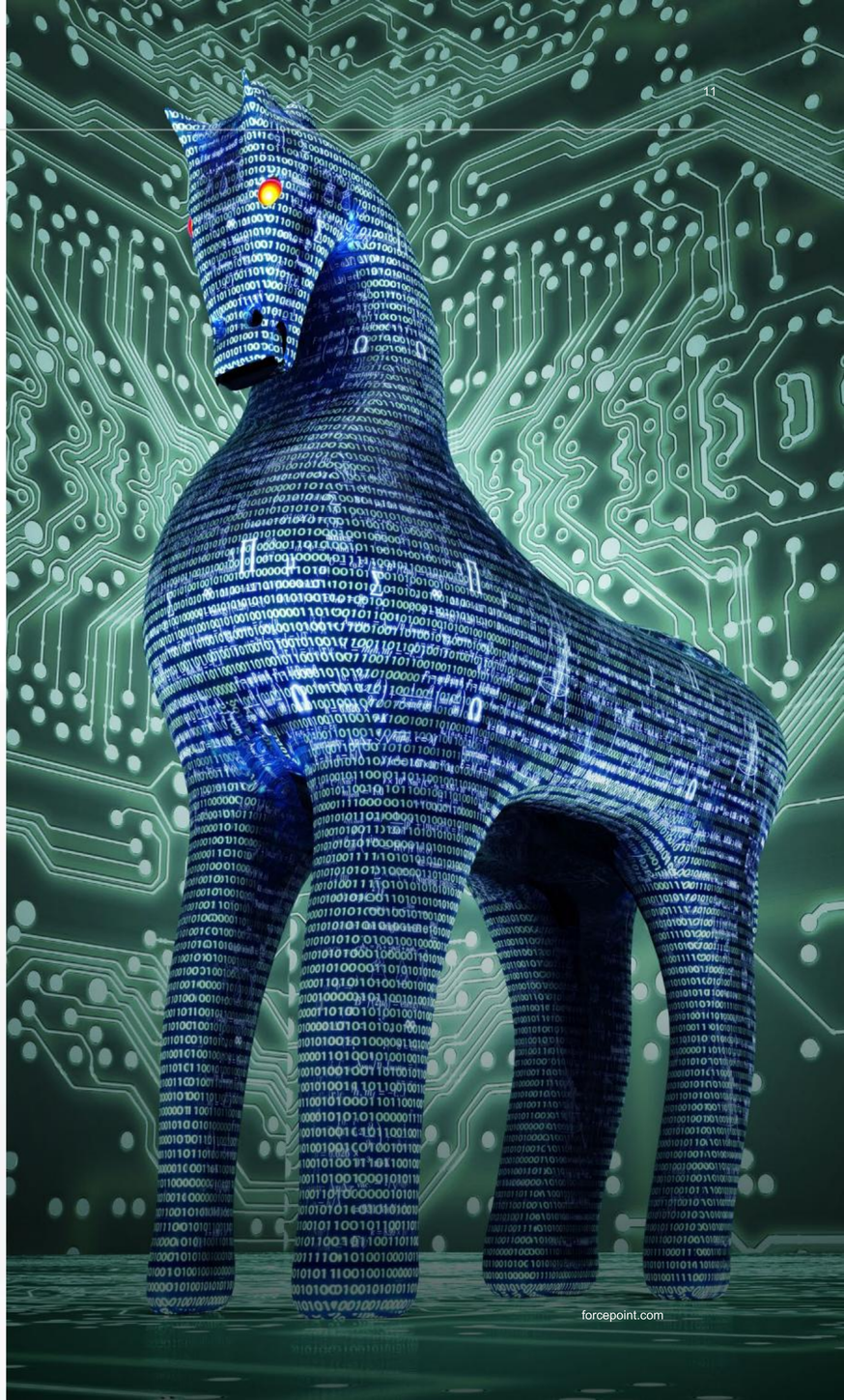
Et bien sûr, les pirates informatiques s'appuient également sur des services open source comme IPFS. Sa nature décentralisée le rend plus difficile à démanteler
pages Web, fichiers ou applications car ils sont répartis sur plusieurs serveurs. Les pirates informatiques comptent sur le fait que les méthodes traditionnelles de suppression d'hébergement Web (comme contacter le fournisseur d'hébergement) ne fonctionnent pas efficacement avec IPFS, car le contenu est réparti sur de nombreux nœuds.

Les attaquants utilisent des URL malveillantes tournantes, hébergées sur des plateformes comme AWS ou Azure, pour échapper à la détection et au blocage.

Les pirates informatiques pensent comme des spécialistes du marketing numérique

Pour les campagnes de phishing, les attaquants utilisent parfois leur casquette de marketing numérique. À cet égard, ils ont recours à des tactiques telles que l'empoisonnement SEO, où ils utilisent des mots-clés populaires ou tendance dans le contenu de leurs sites Web malveillants pour tromper les moteurs de recherche et les amener à mieux les classer. Ces mots-clés sont souvent liés à l'actualité, à des logiciels populaires ou à des problèmes de sécurité (par exemple, « antivirus gratuit », « Google Authenticator », etc.).

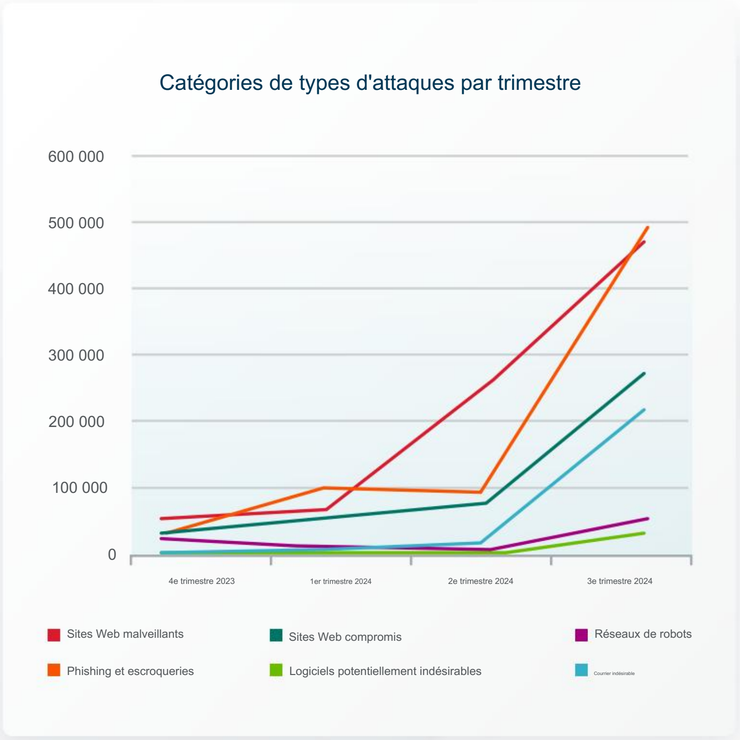
En parlant de penser comme des spécialistes du marketing numérique, les pirates informatiques utilisent également Google Ads pour promouvoir leurs produits auprès de victimes sans méfiance. Nous avons observé des scénarios dans lesquels ils se font passer pour des produits de la gamme de produits de Google, comme Google Authenticator ou Google Maps par exemple. Ils utilisent Looker Studio de Google pour créer de fausses pages d'accueil. Sur ces fausses pages, ils affichent des images qui ressemblent à ce que l'on attend d'une page de recherche Google, pour inciter les utilisateurs à interagir avec la fausse page. Ils utilisent des publicités pour attirer les utilisateurs vers ces fausses pages Google.



Les pirates informatiques vont de plus en plus créer des campagnes de logiciels malveillants sur des services d'infrastructure légitimes

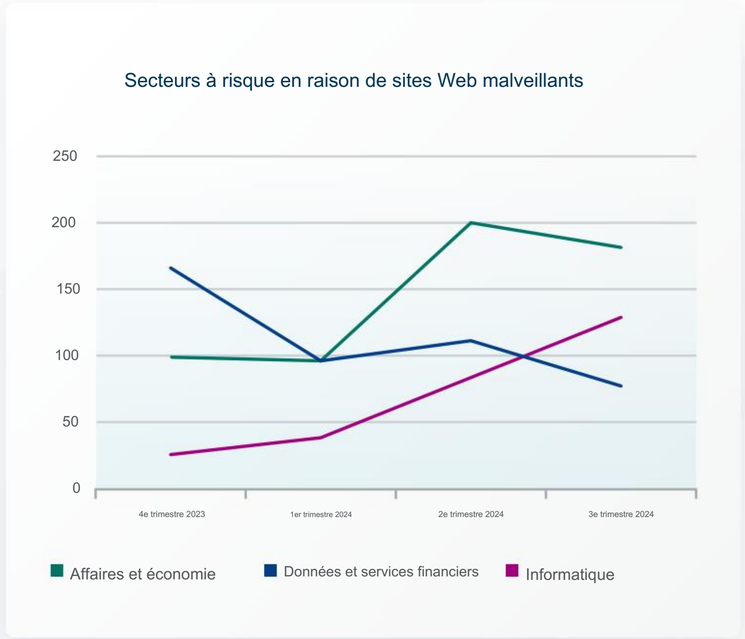
Tendances des catégories de logiciels malveillants en 2025

Nous avons comparé différentes catégories de malwares détectées via nos signatures en temps réel au cours des derniers mois pour avoir une idée des tendances des catégories de malwares en 2025. Dans le graphique ci-dessous, le nombre de sites Web malveillants a plus que quadruplé, passant de moins de 100 000 au premier trimestre 2024 à près de 500 000 instances à la fin du troisième trimestre. Nous nous attendons à ce que cette tendance se poursuive. Le phishing et les escroqueries représentent la deuxième catégorie la plus importante en termes de volume, passant d'environ 125 000 instances au premier trimestre à près de 400 000 à la fin du troisième trimestre 2024. En comparaison, nous nous attendons à ce que la catégorie des sites Web compromis continue d'être à la traîne par rapport aux principales catégories de malwares.



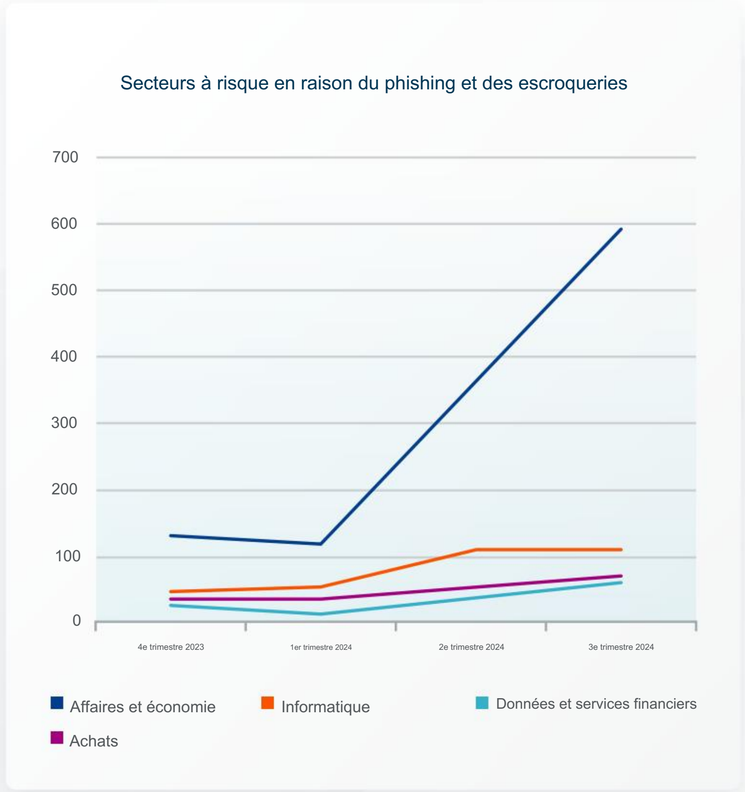
Les pirates informatiques vont de plus en plus créer des campagnes de logiciels malveillants sur des services d'infrastructure légitimes

À partir de là, nous avons décidé d'examiner de plus près les secteurs les plus exposés aux risques liés aux sites Web malveillants, la principale catégorie de logiciels malveillants que nous avons examinée. Le graphique ci-dessous met en évidence les tendances des différents secteurs exposés aux risques liés à l'hébergement de sites Web malveillants. Le secteur des affaires et de l'économie a été le plus touché en termes de volume au cours de l'année dernière. Mais nous nous attendons à ce que le secteur des données financières et des services plateforme pour la dépasser puisque les sociétés de services financiers continuent d'être ciblées à un taux plus élevé du premier au troisième trimestre 2024.



Les pirates informatiques vont de plus en plus créer des campagnes de logiciels malveillants sur des services d'infrastructure légitimes

Enfin, nous avons examiné les secteurs les plus exposés au risque de phishing et d'escroqueries, la deuxième catégorie de logiciels malveillants la plus répandue. Sans surprise, le secteur des affaires et de l'économie est le plus exposé, avec une trajectoire qui augmente le plus du premier au deuxième trimestre 2024 et dans une moindre mesure entre le deuxième et le troisième trimestre 2024. Les technologies de l'information sont le deuxième secteur le plus exposé, bien qu'il soit nettement en retrait par rapport à la catégorie principale. Voir le graphique ci-dessous :



Les pirates informatiques créeront de plus en plus de campagnes de logiciels malveillants sur

Services d'infrastructure légitimes

Mayur Sewani
X-Labs, chercheur principal en sécurité

Ben Gibney
X-Labs, chercheur en sécurité III

Hassan Faizan
X-Labs, chercheur en sécurité III

Comment l'IA s'intègre dans le mix de logiciels malveillants

Comme la plupart d'entre nous, les pirates informatiques continuent d'exploiter l'IA dans leurs efforts. Ils l'utilisent pour créer des composants d'une campagne. Les attaquants peuvent ainsi rédiger des textes convaincants pour de faux sites Web, rédiger des e-mails authentiques, créer des tentatives de phishing bien structurées par SMS ou même des tentatives sophistiquées de phishing vocal. Ils peuvent s'en servir pour créer des documents convaincants tels que des factures, des détails sur un emploi ou des éléments de référence contenant une charge utile de malware. Ils peuvent également utiliser des chatbots pour engager des victimes potentielles via des conversations en temps réel, en les incitant à partager des informations sensibles. De même, les LLM peuvent également être exploités pour générer des réponses contextuelles, en répondant rapidement à une victime qui répond à un e-mail de phishing par exemple. Dans ces cas, les conversions en temps réel peuvent contribuer grandement à augmenter la crédibilité d'une attaque.

L'autre réalité est que l'IA rend la technologie plus accessible à une nouvelle génération de pirates informatiques. Avec l'aide de l'IA, un jeune peut créer de nombreux éléments d'une campagne de malware en utilisant des services légitimes comme infrastructure pour héberger et déployer le tout. Si l'on additionne tout cela, il semble y avoir de bonnes chances que les script kiddies cèdent la place aux malware kiddies ou aux phishing kiddies. Le temps nous le dira.

L'émergence d'un ordre multilatéral en matière de réglementation de la vie privée

Il y a deux ans, j'ai donné la première d'une série de conférences prospectives examinant l'impact de la géopolitique et de la démographie sur le paysage mondial de la cybersécurité. L'une de mes principales prédictions était qu'un ordre mondial plus multilatéral était en train de naître, avec des répercussions importantes sur la cybersécurité. De l'utilisation des technologies à leur développement, de l'embauche de cyber-guerriers à la mise en œuvre de l'automatisation de l'IA, du financement des start-ups au respect de la réglementation, tout cela deviendrait beaucoup plus difficile, plus complexe et plus coûteux.

Je vais ici examiner de plus près un aspect de ce tableau général : à savoir, comment la balkanisation de la réglementation mondiale sur la confidentialité aura un impact sur la sécurité des données. Je vois l'adoption de l'IA accélérer cette tendance, conduisant à des développements et des défis majeurs en 2025.

Une vieille tendance qui prend de l'ampleur

Les réglementations en matière de protection de la vie privée ne sont pas nouvelles. Elles existent sous une forme ou une autre depuis des décennies. Nous avons des réglementations aux niveaux national, infranational et supranational, couvrant toutes des domaines différents et qui se chevauchent.

Ce domaine a toujours été complexe, mais l'ère d'Internet a accentué cette complexité à mesure que les régulateurs se sont tous efforcés de se moderniser. Nous avons assisté à des changements importants et à l'introduction de nouvelles lois dans toutes les grandes juridictions au cours des années 1990 et 2000. Dans certaines juridictions, nous avions même des réglementations concurrentes, généralement en matière de collecte et de conservation, où le respect de l'une signifiait que vous n'étiez pas en conformité avec l'autre.

Au milieu des années 2010, les entreprises avaient du mal à se conformer à la myriade de règles, et les choses allaient devenir encore plus compliquées avec les implications extra-juridictionnelles du règlement général européen sur la protection des données (RGPD), qui a étendu la capture réglementaire à toute personne traitant des informations sur les citoyens de l'UE.

Depuis un certain temps, des efforts concertés semblent être déployés pour rationaliser les réglementations, dans le but non pas d'harmoniser les réglementations mais plutôt de les reconnaître mutuellement. Cette démarche s'appuie sur la manière dont la reconnaissance croisée a aidé d'autres secteurs hautement réglementés, tels que les télécommunications, l'électronique et la construction aéronautique et automobile.

Il est bien connu que la surréglementation a un impact négatif important sur la croissance économique et l'innovation.
Les régulateurs de tous les domaines cherchent à trouver un équilibre entre réglementation et innovation. Malheureusement, la nature des règles est telle qu'elles évoluent constamment. Il faut des changements majeurs et de réels efforts pour les rationaliser et les optimiser, et pendant un certain temps, j'ai eu l'espoir que cela se produirait ici.

Mais aujourd'hui, un ensemble de forces s'opposent à ce phénomène, dans un contexte où les entreprises collectent, traitent et stockent plus de données que jamais, mais alimentent également désormais leurs modèles d'IA gourmands en données.

L'émergence d'un ordre multilatéral en matière de réglementation de la vie privée

Expansion réglementaire et balkanisation

Je pense qu'il ne faut plus trop espérer de rationalisation de la réglementation. L'une des principales raisons en est le glissement géopolitique vers un ordre mondial multilatéral.

Je prédis que nous assisterons à une certaine rationalisation, mais elle se fera par groupes, en fonction des groupements géopolitiques des pays. Quand je dis cela, on me demande généralement : « Mais n'est-ce pas une bonne chose si cela réduit le fardeau de la conformité ? » Le gros problème est que je pense qu'il y aura un manque forcé de reconnaissance croisée et une introduction intentionnelle de différences entre les clusters. La friction et la complexité seront inhérentes à la conception.

Je pense également que nous assisterons à des réglementations très contradictoires, où ce qui est obligatoire dans une juridiction sera explicitement interdit dans une autre. Par exemple, des entreprises pourraient être obligées de collecter certaines informations dans une juridiction, mais interdites dans une autre. Certaines informations collectées pourraient être autorisées à certaines fins dans une juridiction, mais interdites à ces mêmes fins dans une autre.

Les entreprises opérant dans ces juridictions de marché devront savoir quelles sont leurs obligations, envers quels régulateurs, envers quels utilisateurs, envers quelles données, où ces données sont stockées, comment ces données sont utilisées en aval et comment ces données sont gérées tout au long de leur cycle de vie.

Tout cela semble coûteux et compliqué, car c'est le cas. Cela entraînera probablement une duplication des infrastructures et des services, des problèmes de conformité plus importants, des risques résiduels importants et une multitude de politiques et de procédures en vigueur au sein des organisations.

L'émergence d'un ordre multilatéral en matière de réglementation de la vie privée

La révolution de l'IA

Ce débat ne serait pas contemporain si nous n'évoquions pas l'IA. Les entreprises se bousculent pour l'utiliser et les gouvernements se bousculent pour la réglementer. L'IA a captivé l'imagination non seulement des créateurs, mais aussi des régulateurs.

Nous en sommes encore aux prémices de l'IA générative et de l'externalisation de la prise de décision vers l'IA, mais les régulateurs évoluent rapidement. Nous avons déjà vu de nouvelles réglementations importantes et des propositions de réglementation autour de l'IA. Malheureusement pour l'innovation, nous voyons également dans certaines juridictions une réglementation qui va de légèrement excessive à extrêmement onéreuse.

Il y a quelques semaines, j'ai été invité à participer à un panel de discussion sur les considérations de sécurité des données lors de l'adoption de l'IA à GovWare. Aujourd'hui, GovWare est la plus grande conférence sur la cybersécurité en Asie-Pacifique, avec plus de 13 000 participants. Il est probablement superflu de le dire, mais l'immense hall d'exposition était absolument couvert des lettres « IA ». Malgré tout cela, je ne pense pas que nous ayons atteint le pic de battage médiatique autour de l'IA.

Le panel a eu lieu le deuxième jour de la conférence et les participants avaient déjà été inondés de contenu et de messages sur l'IA. On aurait pu penser que le public en avait assez du sujet, mais il n'en avait jamais assez. Après une conversation très large, nous avons été bombardés de questions, non pas sur la technologie de l'IA, mais plutôt sur la gouvernance et la sécurité, avec un réel accent sur la façon de gérer toutes les données que l'IA exige.

Et c'est là que se situe le problème du multilatéralisme. Pour que l'IA soit efficace, productive et génératrice, il faut d'énormes volumes de données.

Il s'agit d'un problème lorsque ces données sont couvertes non seulement par des réglementations balkanisées et contradictoires sur la confidentialité des données, mais également par des réglementations sur l'IA.

Nous sommes confrontés à la perspective que les organisations ne puissent utiliser l'IA qu'avec des données collectées dans certaines juridictions. Les œuvres dérivées (le résultat génératif) et les résultats commerciaux peuvent être différents selon les juridictions. Des données mélangées auxquelles un humain peut accéder peuvent ne pas être autorisées pour l'IA.

Pire encore, qu'advient-il des modèles basés sur des données, dont l'autorisation d'utilisation par l'IA peut être révoquée à tout moment par la personne concernée ?

Il ne s'agit pas simplement de considérations liées à la conception ; il s'agit de considérations opérationnelles et continues.

L'IA est devenue un substitut aux objectifs stratégiques géopolitiques, et je m'attends à ce que les défis actuels autour de l'accès aux semi-conducteurs, aux outils et aux logiciels d'IA se répercutent sur l'environnement de la protection des données.

Apprendre à vivre sans l'IA : l'impact de la législation sur l'IA

Nous ne pouvons pas renoncer à la réglementation sur la confidentialité des données

Après avoir lu tout cela, il est facile de dire que nous allons tous nous battre : certains seront victimes d'infractions, d'autres enfreindront les lois, certains recevront de lourdes amendes et d'autres encore passeront des années devant les tribunaux. Et même si cela contient une part de vérité, nous pouvons faire certaines choses pour nous préparer.

Une rubrique qui m'a bien servi dans ce domaine a été de demander et répondez à deux questions :

1. « Suis-je un bon gardien des données que je détiens ? »

2. « Est-ce que je fais ce qu'on attend de moi pour protéger les données ? »

Ces questions sont toujours d'une grande utilité aujourd'hui, même dans un monde multilatéral. En règle générale, lorsqu'un problème survient, les autorités et les régulateurs raisonnables évaluent la situation à l'aune de ces questions et les utilisent pour déterminer les mesures de suivi à prendre.

J'ai délibérément choisi le terme de dépositaire car il implique de nombreuses choses. Pour être un bon dépositaire, vous devez savoir quelles données vous détenez, où elles se trouvent, par quoi elles sont réglementées et qui y a accès. De la protection découlent l'observabilité et le contrôle de l'utilisation des données.

C'est un bon début, mais l'ordre multilatéral exige que nous accordions également la priorité à l'efficacité. Cela peut paraître surprenant, compte tenu du grand nombre d'autres facteurs à prendre en compte, mais je crois que l'efficacité est le facteur décisif pour tout le reste.

Les organisations doivent adopter des technologies qui leur permettront d'adapter leurs pratiques de sécurité et de confidentialité des données à ce nouvel environnement complexe. Si cela n'est pas fait, les programmes s'effondreront pour faire face à leurs principales juridictions, et les autres seront abandonnés. Si cela a pu être regrettable par le passé, cela pourrait aujourd'hui être catastrophique.

Des outils d'efficacité des flux permettant aux employés d'identifier rapidement les réglementations applicables aux données qu'ils utilisent doivent être associés à des programmes de formation repensés pour améliorer la compréhension et la gestion des données par les utilisateurs.

Même si certains ne sont pas d'accord avec ma thèse, je pense que nous pouvons tous convenir que les problèmes de sécurité des données, de confidentialité et de réglementation ne vont faire que s'aggraver et devenir plus complexes. Il nous appartient d'identifier et de mettre en œuvre des solutions qui empêcheront ces problèmes de devenir incontrôlables.

Nick Savvides

Directeur technique de terrain et directeur des affaires stratégiques, Asie-Pacifique

Perspectives d'avenir 2025 : les points à retenir

→ La gestion de la posture de sécurité par intelligence artificielle (AISPM) représente une approche de la cybersécurité axée sur l'avenir, utilisant l'IA pour s'adapter de manière dynamique, réduire les erreurs humaines et prédire les menaces, garantissant ainsi une gestion proactive et automatisée des risques.

→ À mesure que les réglementations mondiales autour de l'IA évoluent, les organisations doivent donner la priorité à la transparence, Responsabilité et gouvernance solide. L'accent doit être mis sur la protection des données, l'élaboration de stratégies d'IA adaptables et la préparation de l'autonomie des utilisateurs pour qu'ils puissent se retirer des systèmes d'IA.

→ En 2025, les pirates informatiques utiliseront de plus en plus des plateformes fiables pour donner vie à des campagnes de logiciels malveillants, contournant la détection grâce à des infrastructures légitimes et imitant au passage les stratégies marketing.

→ Le consensus international croissant qui donne la priorité à la protection et à la conformité des données transfrontalières sera essentiel en 2025. La balkanisation de la réglementation mondiale sur la confidentialité à l'ère de l'IA aura un impact sur la sécurité des données dans les années à venir. Les entreprises doivent s'adapter à cette tendance en mettant en œuvre des mesures de protection des données robustes pour garder une longueur d'avance sur l'évolution des cadres réglementaires.

Forcepoint

forcepoint.com/contact

À propos de Forcepoint

Forcepoint simplifie la sécurité des entreprises et des gouvernements mondiaux. La plateforme cloud native tout-en-un de Forcepoint facilite l'adoption du Zero Trust et empêche le vol ou la perte de données sensibles et de propriété intellectuelle, quel que soit l'endroit où les personnes travaillent. Basée à Austin, au Texas, Forcepoint crée des environnements sûrs et fiables pour les clients et leurs employés dans plus de 150 pays. Communiquez avec Forcepoint sur www.forcepoint.com, Gazouillement et LinkedIn.

[FP-Ebook-Future Insights 2025-FR] 09/12/2024