Tendances en cybercriminalité 2024

Le point sur les menaces et les bonnes pratiques en cybersécurité

sosafe

Contenu

En 2023, tout a changé. Il faut se préparer à l'avenir.

L'année 2023 a marqué un tournant dans notre contexte mondial. L'annonce du lancement de ChatGPT-3 par OpenAI en novembre 2022 a déclenché innovation sur innovation en matière d'intelligence artificielle et profondément modifié notre rapport à la technologie. C'est surtout dans le domaine de la sécurité de l'information que cette évolution s'est fait sentir puisque l'IA s'y est imposée comme une force motrice, non seulement du côté de la cyberdéfense, mais aussi entre les mains des cyberattaquants.

Après la vive impression qu'ont laissée sur nous ces avancées fulgurantes de l'innovation technologique, l'année 2024 s'ouvre maintenant sur une série de défis sans précédent : l'implication croissante de l'IA dans les cyberattaques, l'émergence de technologies comme la 5G ou l'informatique quantique qui se révèlent être des armes à double tranchant, ou encore l'évolution de la cybercriminalité qui s'organise en un secteur d'activité fortement professionnalisé… Sur ce contexte déjà difficile viennent se greffer d'autres paramètres inquiétants : la recrudescence de l'hacktivisme et des cyberattaques au sein d'un monde agité par les crises politiques, la prolifération des campagnes de désinformation… Chacun de ces facteurs contribue à dessiner un paysage des menaces de plus en plus complexe, où les incidents peuvent avoir de très grandes répercussions. Les tensions se multiplient tandis que, du côté des professionnels de la cybersécurité, les équipes luttent contre le burn-out.

Alors que la probabilité augmente de voir une erreur humaine ouvrir la porte à une cyberattaque, notre seul espoir est de bâtir une solide culture de la sécurité au sein de nos entreprises. C'est dans cette optique que ce rapport s'articule autour de neuf tendances de la cybercriminalité en 2024 et cherche à définir de bonnes pratiques pour se préparer à y faire face.

1 Le rôle croissant de l'IA dans les cyberattaques : une épée de Damoclès

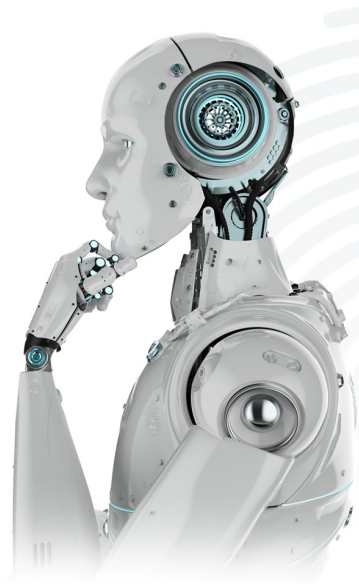
De plus en plus de personnes utilisent l'intelligence artificielle. D'après les statistiques, le nombre d'utilisateurs devrait dépasser les 300 millions en 2024 et atteindre approximativement les 700 millions d'ici 2030[1] : c'est donc une véritable révolution qui est en marche et elle suscite de nombreuses inquiétudes quant à ce que cette technologie peut impliquer à large échelle et aux risques qu'elle présente pour la sécurité. Lorsque l'on évoque les problèmes de sécurité causés par l'IA, c'est inévitablement la question des **deepfakes** et du **clonage vocal** qui vient à l'esprit.

Cela fait déjà quelque temps que les hackers jouent sur ces deux tableaux, mais la récente prolifération d'outils capables de générer des hypertrucages vidéo de grande qualité rend aujourd'hui cette technologie accessible au plus grand nombre.

1 sur 4

avait déjà été confrontée à une attaque par clonage vocal, soit parce qu'elle a été visée personnellement, soit parce qu'elle connaît quelqu'un qui l'a été.

Source : Global Security Mag[3]



On assiste donc à une utilisation croissante des deepfakes dans **le cadre de campagnes de désinformation et de manipulation sociale**[2] (voir la section sur la tendance du DaaS ou « disinformation-as-a-service » pour plus d'informations).

Et le clonage vocal n'est pas en reste. Une récente étude a montré que plus d'une personne sur quatre avait déjà été confrontée à une attaque par clonage vocal, soit parce qu'elle a été visée personnellement, soit parce qu'elle connaît quelqu'un qui l'a été.[3] La police d'Everett, à Washington, a averti de la recrudescence d'arnaques à caractère financier qui se servent de clonages vocaux pour escroquer des particuliers.[4] Si les cybercriminels exploitent

1 **Statista (2023).** Artificial Intelligence Worldwide.

2 **Zdnet (2023).** L'ère des deepfakes : cette nouvelle arme nucléaire de désinformation.

3 **Global Security Mag (2023).** Étude McAfee - Clonage de voix par intelligence artificielle : les arnaques en hausse piègent plus d'1 Français sur 4.

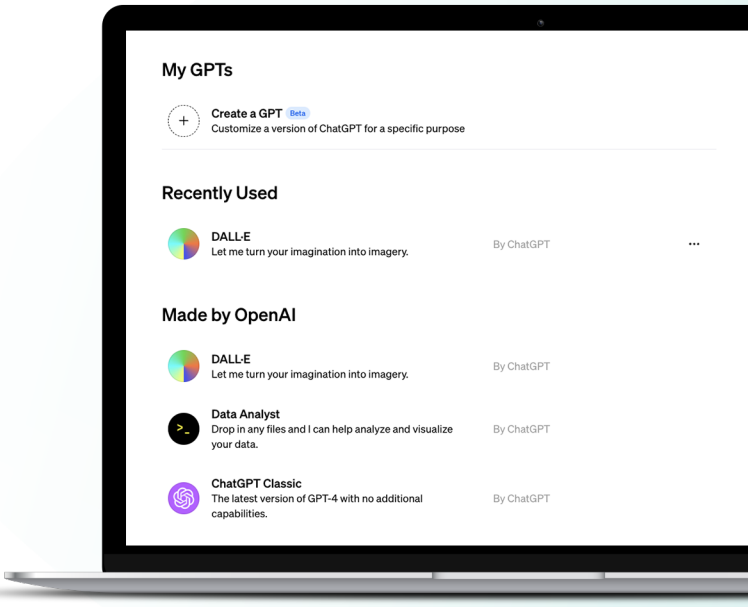
4 **Fox 13 Seattle (2023).** Everett Police warn of AI voice-cloning phone scam after case reported in Snohomish County.

principalement cette technologie pour soutirer de l'argent à leurs victimes - certains d'entre eux sont même parvenus à simuler le rapt d'une jeune femme[5] - quelques-uns commencent à utiliser le clonage vocal pour **tromper les systèmes de MFA basés sur la reconnaissance vocale**. C'est ainsi que, début 2023, un journaliste a annoncé avoir réussi à accéder à son compte en banque en utilisant[6] un clonage de sa propre voix. Bien que l'expérimentation menée par ce journaliste ne présente aucun risque personnel, on comprend toute la portée de la menace qui, elle, est bien réelle.

Or, c'est loin d'être la seule manière dont les cybercriminels détournent l'intelligence artificielle. Les progrès de l'IA générative au cours de l'année écoulée ont permis l'ajout de nombreuses fonctionnalités innovantes à des outils déjà bien connus : certaines d'entre elles, comme la capacité de ChatGPT à lire des images, par exemple, peuvent être exploitées à des fins malveillantes. Avec la technique de **l'injection de prompt**[7] par exemple, il est possible d'amener l'outil à suivre les instructions contenues dans une image, au lieu de celles données par l'utilisateur. Un détournement, qui, s'il peut sembler inoffensif de prime abord, ouvre des perspectives illimitées pour les escrocs.

Cette fonction permettant de charger des images suscite aussi d'autres inquiétudes, notamment parce qu'elle pourrait permettre de **court-circuiter les codes CAPTCHA** qui sont, à l'heure actuelle, l'une des protections les plus connues contre l'usage abusif de la technologie. Jusqu'à récemment, les hackers ne pouvaient pas exploiter l'intelligence artificielle pour lire les CAPTCHA, en raison, principalement, des restrictions éthiques des outils d'IA. Cependant, Bing Chat[8] s'est avéré capable de déchiffrer ces codes lorsque l'utilisateur saisit une excuse ou un prétexte rationnel. Ce phénomène pousse des sociétés et des sites Internet du monde entier à envisager la **nécessité d'adopter d'autres méthodes de sécurité**.

À mesure que la technologie progresse, les **hackers commencent aussi à développer leurs propres outils d'IA en se basant sur les modèles de langage existant**. C'est ainsi que sont apparus des jumeaux maléfiques de ChatGPT[9], tels que FraudGPT et WormGPT. Pourtant, jusqu'à fin 2023, la création (mais pas l'utilisation) de tels outils était réservée à ceux qui possèdent des connaissances techniques. Or, OpenAI a récemment lancé une fonction qui



5 **01 net (2023).** Grâce à l'IA, un criminel clone la voix d'une jeune fille pour extorquer de l'argent à sa mère.

6 **Le monde informatique (2023).** La voix générée par l'IA, un moyen simple d'usurper une identité bancaire.

7 **Futura (2023).** « Prompt injection » : quelle est cette nouvelle attaque contre les IA ?

8 **International Business Times (2023).** Voici comment le chat Bing peut résoudre les CAPTCHA.

9 **ZDNet (2023).** Ce qu'il faut savoir à propos de WormGPT, la réponse des cybercriminels à ChatGPT.

permet de créer très facilement un GPT, c'est-à-dire un chatbot que l'utilisateur peut entraîner pour qu'il l'assiste dans une tâche donnée. La procédure est même plus facile d'accès que chez ses homologues du dark web : aucune connaissance technique ni savoir-faire en matière de codage n'est requis. Si la possibilité de créer des GPT personnalisés ouvre naturellement une perspective très intéressante, qui aidera beaucoup de gens dans leurs tâches quotidiennes, il faut néanmoins s'attendre à ce qu'**en 2024, des cyberattaquants se saisissent de cette opportunité pour la détourner à leur avantage et créer des assistants de piratage**[10] capables de générer des textes de smishing percutants, des e-mails de phishing et des virus polymorphes.[11]

Les **limites** de l'IA présentent tout autant de risques que ses capacités. La possibilité de rédiger du code à l'aide de modèles d'IA perfectionnés constitue un progrès majeur, adopté à large échelle par quelque 92 % des développeurs[12], sur leur lieu de travail comme à l'extérieur. Mais certains commencent à s'inquiéter de **la fiabilité du code généré par l'IA**. Plusieurs[13] experts ont en effet remarqué que l'intelligence artificielle avait tendance à privilégier la fonctionnalité du code sur la sécurité, ce qui pose un réel problème. Parmi les défauts relevés, en matière de sécurité, on trouve[14] notamment la probabilité d'une injection SQL, le codage en dur d'identifiants de connexion ou l'utilisation d'algorithmes non sécurisés pour le hachage de mots de passe.

La faille la plus connue de l'IA est peut-être sa tendance à fournir des informations fausses ou inventées de toutes pièces, un phénomène que l'on a surnommé **« hallucinations ». Les hackers commencent à exploiter ces hallucinations pour injecter des fichiers malveillants**.[15] Si l'utilisateur saisit une requête spécifique, l'outil se met à « halluciner » en recommandant des noms de bibliothèques de code qui n'existent pas. Il suffit alors aux cyberattaquants de créer des bibliothèques de code ou des packages infectés, de leur attribuer ces noms et de les charger sur des bases de données publiques. Ainsi, la prochaine fois qu'un utilisateur se verra recommander l'un de ces packages, il téléchargera la bibliothèque de code mise à disposition par les hackers.

Étant donné les menaces qui émergent avec l'utilisation de l'IA et la vitesse fulgurante à laquelle la technologie progresse, **il faut impérativement mettre en place des techniques de défense bien pensées pour les contrer**. Il devient essentiel d'adopter une approche proactive en matière de cybersécurité pour préserver à la fois nos entreprises et les personnes qui les composent des dangers d'un monde où l'IA prend de plus en plus de place.

10 **BBC News Afrique (2023).** ChatGPT Builder aide à créer un outil de cybercriminalité.

11 **Developpez.com (2023).** Des experts en sécurité sont parvenus à créer un logiciel malveillant polymorphe « hautement évasif » à l'aide de ChatGPT.

12 **Développez.com (2023).** 92 % des développeurs utiliseraient des outils d'intelligence artificielle.

13 **Futura (2022).** Les IA qui génèrent du code ajoutent des failles de sécurité !

14 **Le monde informatique (2023).** Des codes moins sécurisés avec les assistants à base d'IA.

15 **COMK (2023).** Quand les hallucinations de ChatGPT facilitent le travail des pirates.

CHECKLIST

Bonnes pratiques en matière de sécurité

- **Vérifiez les codes générés par l'IA avant de les utiliser :** même si vous avez pris la précaution de demander à l'outil de générer du code sécurisé, il vaut toujours mieux en vérifier la fiabilité à l'aide de logiciels de revue de test automatisée ou en appliquant un ensemble normalisé de critères de sécurité.

- **Restez informé des dernières tendances de l'IA et adaptez votre stratégie en conséquence :** au fur et à mesure que la technologie progresse, certaines mesures de sécurité peuvent tomber dans l'obsolescence. Vous devez donc trouver d'autres solutions pour continuer à protéger votre société. Il peut valoir la peine de créer, au sein de votre société, un groupe de travail ou un service de cyberrenseignement qui se concentre sur le suivi et l'analyse des attaques menées avec l'aide de l'IA et sur leur impact pour votre cybersécurité.

- **Faites un usage responsable des outils d'IA :** évitez de saisir des données personnelles lorsque vous utilisez ces outils ou de prendre les informations qu'ils vous fournissent pour argent comptant. Gardez toujours à l'esprit que certaines des réponses apportées peuvent être dépassées ou incorrectes. Il vaut toujours mieux en vérifier l'exactitude.

- **Servez-vous de l'IA pour renforcer votre sécurité :** l'intégration d'outils augmentés par l'IA peut significativement optimiser l'analyse de larges bases de données et assurer une meilleure détection des anomalies, ainsi qu'une identification plus efficace des menaces en temps réel. En associant l'IA à la technologie SOAR (Security Orchestration, Automation and Response), on favorise ainsi une prise de décision automatisée et intelligente, mais aussi une plus grande réactivité dans le traitement des incidents. En outre, l'utilisation de l'IA dans l'automatisation no code permet d'adapter rapidement les procédures de cybersécurité pour suivre l'évolution des menaces. L'implémentation de systèmes d'authentification perfectionnés s'appuyant sur l'IA est également bénéfique puisque ces solutions apprennent et perfectionnent les mesures de sécurité en continu. Un contrôle humain adapté doit cependant être mis en place pour veiller à ce qu'elles restent en phase avec vos politiques d'entreprise et vos principes éthiques.

- **Soyez sur vos gardes lorsque vous recevez des messages vidéo ou vocaux suspects :** si les messages semblent authentiques, mais qu'ils contiennent des demandes ou des affirmations inhabituelles, il est conseillé de chercher un moyen de vérifier leur authenticité.

- **Formez vos employés aux menaces de sécurité posées par l'IA :** s'ils savent comment se protéger et préserver votre société contre les menaces, ils seront votre meilleure défense. Apprenez-leur à utiliser l'IA générative de manière responsable tout en protégeant les données sensibles.

2 L'IA, mais pas seulement : les cybercriminels surfent sur toutes les nouvelles technologies

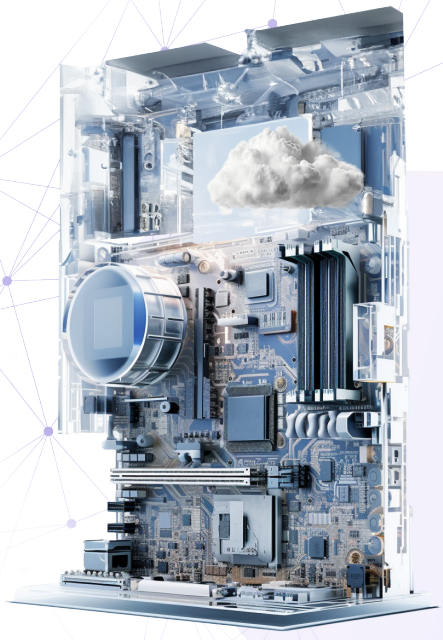
L'intelligence artificielle a beau être l'innovation du siècle, les cybercriminels ne jouent pas que sur ce seul tableau. Ils **élargissent leur horizon** en faisant feu de tout bois, parmi les technologies émergentes. L'objectif est d'augmenter la surface d'attaque et d'atteindre le maximum de victimes possible. Chaque nouvelle **technologie est donc à la fois un outil et une cible** pour les menaces cyber sophistiquées.

Cette tendance n'est pas totalement nouvelle : nous avons déjà connu des schémas similaires lors de l'avènement d'autres technologies comme le **cloud, par exemple**. Ces dernières années, les entreprises ont investi des milliards de dollars dans le stockage sur le cloud, en délaissant peu à peu les solutions traditionnelles. Cette transition n'a bien sûr pas échappé aux cybercriminels. Selon le rapport Global Threat Report de CrowdStrike[1], les attaques ciblant les systèmes sur le cloud ont quasiment doublé en 2022, et le nombre de groupes cybercriminels capables de perpétrer de telles attaques va tripler.

L'une des attaques les plus frappantes en la matière est le rançongiciel qui[2] a infiltré le cloud du gouvernement srilankais, début août, en envoyant des liens corrompus à ses employés. Le pays, qui n'avait pas mis en place de services de back-up, a ainsi perdu quatre mois de données officielles.

Les technologies émergentes d'aujourd'hui, comme **l'informatique quantique**, sont très certainement vouées à subir le même sort. Les cybercriminels procèdent selon le principe « Harvest now, decrypt later (HNDL) »[3] ou, en français, « Récolter maintenant, décrypter plus tard » : cela signifie qu'ils collectent aujourd'hui un très grand nombre de données cryptées avec l'espoir que les avancées futures de l'informatique quantique leur permettront de les décrypter. Si tel est le cas, nous allons au-devant de violations de données, de vols de la propriété intellectuelle et de divulgations de secrets relatifs à la sécurité nationale sans précédent.

Pour anticiper cette menace, le Centre canadien pour la cybersécurité[4] a, dès 2021, publié une série de conseils. L'objectif est d'aider les entreprises à se préparer à la menace que pose l'informatique



1 **CrowdStrike (2023).** Global Threat Report 2023 de CrowdStrike Résumé.

2 **Infosecurity Magazine (2023).** Ransomware attack wipes out Sri Lankan government data. (Une attaque par rançongiciel supprime les données du gouvernement srilankais).

3 **Horizons (2022).** État d'alerte à cause de l'ordinateur quantique.

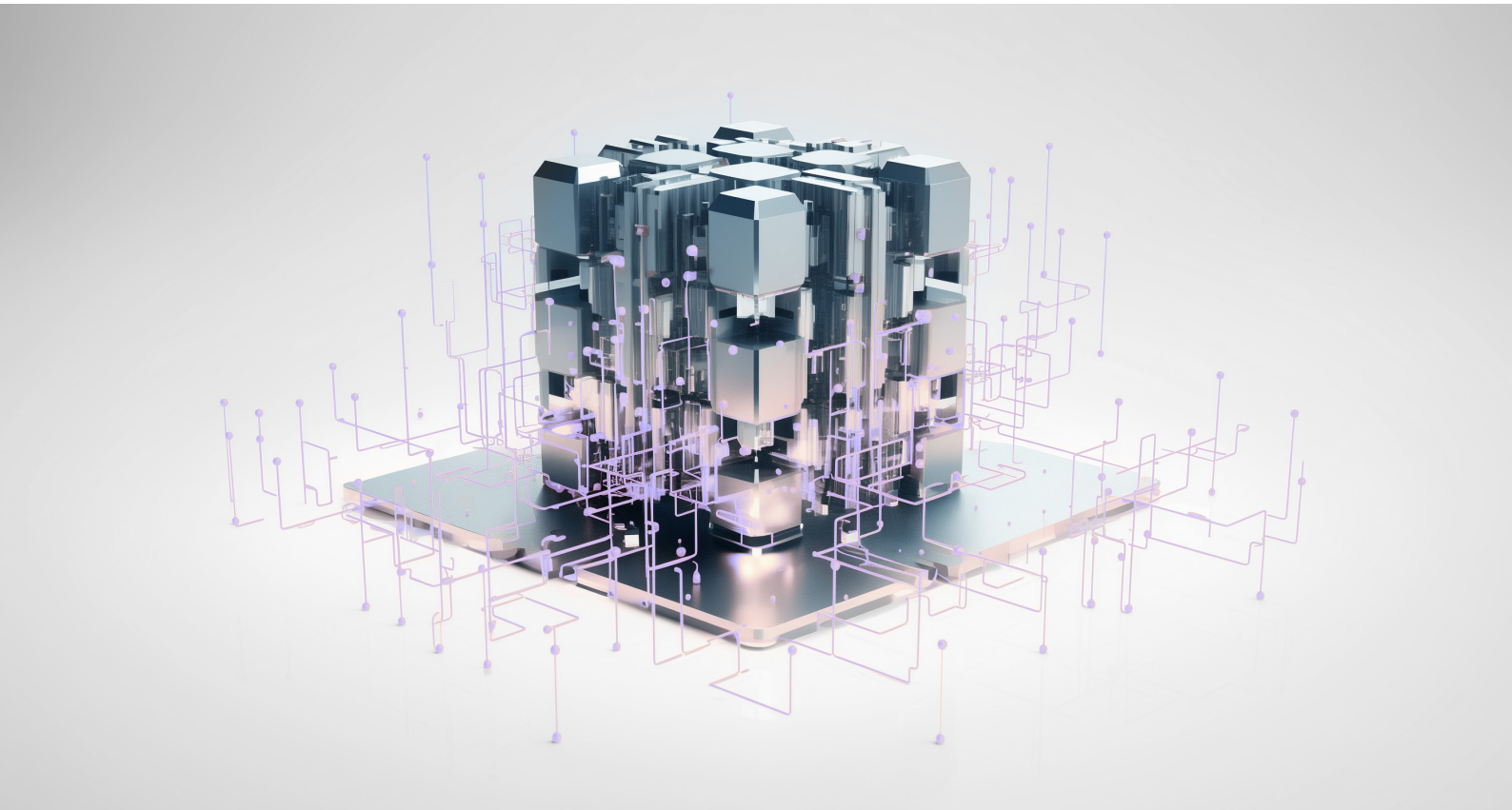
4 **Gouvernement du Canada (2021).** Préparez votre organisation à la menace que pose l'informatique quantique pour la cryptographie.

quantique pour la cryptographie et sensibiliser à la nécessité d'enclencher suffisamment tôt ce processus de défense. Malheureusement, la question est complexe, en particulier en raison des incertitudes quant aux délais qu'il nous reste avant que les progrès de l'informatique quantique ne constituent un réel danger. Dans ce contexte, les entreprises pèsent le pour et le contre entre le coût des mesures de protection contre la menace quantique et le risque de ne pas être prêt en cas de soudaine avancée dans ce domaine.

La technologie 5G illustre, elle aussi, comment les nouvelles technologies peuvent être à double tranchant. Elles sont la promesse d'une connectivité et d'une rapidité sans précédent, mais ouvrent aussi la voie à de nouveaux modes d'attaque de la part des cybercriminels. Un rapport spécial de la Cour des comptes européenne[5] identifie un certain nombre de risques liés à la 5G : surface de frappe plus importante qu'avec la 3G ou la 4G, nombre restreint d'équipementiers impliquant une plus grande exposition aux risques de rupture d'approvisionnement et une dépendance potentielle vis-à-vis d'acteurs à haut risque, possibilité d'ingérence de pays tiers susceptibles de prendre le contrôle d'infrastructures critiques et menace pour la confidentialité et la vie privée dans la mesure où les données peuvent être stockées dans des pays n'offrant pas le même niveau de protection que l'Union européenne.

Il faut retenir de tout cela un point essentiel : puisque toutes les **nouvelles technologies sont appelées à évoluer encore, il est évident que les cybercriminels vont adapter, au fur et à mesure, leurs méthodes et leurs cibles**. C'est une constante course contre la montre où chaque nouvelle technologie émergeant sur le marché représente aussi, potentiellement, une menace. Il est donc essentiel de définir des stratégies de cybersécurité agiles et évolutives, capables de s'adapter aux progrès de la technologie pour endiguer les risques.

5 **Cour des comptes européenne (2022)**. Déploiement des réseaux 5G au sein de l'UE : des retards et des questions de sécurité encore sans réponse.



CHECKLIST

Bonnes pratiques en matière de sécurité

- **Renforcez votre sécurité dans le cloud :** investissez dans un back-up intégral et dans des systèmes de récupération pour les données stockées sur le cloud. Mettez à jour vos outils régulièrement et téléchargez tous les correctifs pour vous protéger contre les menaces en perpétuelle évolution.
- **Limitez le risque de violations de données chiffrées :** protégez les données à l'aide de la microsegmentation, changez régulièrement de clé de chiffrement sur la base de la classification des données, et veillez à mettre constamment à jour les logiciels et les mesures de sécurité.
- **Adoptez une approche crypto-agile :** préparez-vous à changer rapidement d'algorithmes et de méthodes cryptographiques au fur et à mesure que de nouvelles menaces font leur apparition.
- **Sécurisez les réseaux 5G :** éliminez les vulnérabilités au sein des réseaux complexes et des déploiements locaux. Vérifiez la sécurité de la chaîne d'approvisionnement, y compris celle des composants logiciels et matériels.
- **Limitez les vulnérabilités des infrastructures existantes :** mettez à niveau ou remplacez les systèmes existants susceptibles de présenter des failles inhérentes de sécurité. Intégrez vos réflexions en matière de sécurité dans la conception des nouvelles technologies.
- **Surveillez les menaces émergentes et adaptez les mesures en fonction :** tenez-vous informé des menaces cyber qui émergent, adaptez vos stratégies en conséquence et instaurez une surveillance continue, ainsi qu'une analyse des menaces en temps réel.
- **Consolidez les compétences en cybersécurité de votre équipe :** comme avec l'IA, il est essentiel de former en continu votre équipe de sécurité, mais aussi le reste de votre personnel, pour les préparer à réagir rapidement aux nouvelles menaces et à s'y adapter.

3 La cybercriminalité s'organise en un marché de plus en plus professionnalisé, en quête de rentabilité

La cybercriminalité ne cesse de se professionnaliser et devrait atteindre un nouveau degré de maturité en 2024. C'est en partie à la mise sur le marché et à l'expansion des **offres de rançongiciel-as-a-service (RaaS)** que nous devons cette évolution. L'an dernier, nous soulignions déjà que ces outils sophistiqués, non contents de mettre la cybercriminalité à la portée de tous ou presque, avaient également fait monter d'un cran la complexité et l'impact des attaques.

Le contexte a évolué très rapidement au cours de l'année écoulée : on enregistre, en effet, **une augmentation spectaculaire de 112 % du nombre d'attaques par rançongiciel** entre janvier 2022 et juillet 2023.[1] Cette tendance alarmante prouve que les ransomwares **continuent d'être le talon d'Achille des organisations de toutes sortes au sein de l'espace EMEA**.[2]

Le ciblage de plus en plus marqué des attaques par rançongiciel en dit long sur le tournant pris dans ce domaine. Comme nous l'évoquerons plus tard dans ce rapport, **les attaques sont nettement dirigées vers le secteur public et les infrastructures critiques**, et tout particulièrement vers les secteurs de la santé et de l'éducation, ainsi que vers les instances gouvernementales. La raison en est que ces entités manquent souvent de ressources en matière de sécurité et sont donc davantage susceptibles de payer une rançon afin d'assurer la continuité des services essentiels et la protection des données sensibles.

En décembre 2023, par exemple, le ministère français de l'Éducation nationale a annoncé que la plateforme du service national universel (SNU) avait subi une cyberattaque. Cet incident a provoqué **un vol de données personnelles touchant 150 000 personnes** qui voient leurs noms, adresses, dates de naissance, etc. ainsi exposées.[3]

Le secteur public n'est cependant pas le seul à être affecté. MGM Resorts, géant mondial de l'hôtellerie et des casinos, a été la cible d'une attaque perpétrée par Scattered Spider, un sous-groupe d'ALPHv, en septembre 2023.[4] La méthode utilisée est celle de l'ingénierie sociale : les attaquants ont identifié un employé sur LinkedIn, puis ont appelé le service d'assistance. **L'entreprise évaluée à plusieurs milliards de dollars a été vaincue par une conversation de 10 minutes**. L'attaque a semé la panique, les machines à sous et les cartes-clés de milliers de chambres d'hôtel ont cessé de fonctionner et les transferts électroniques de gains ont été ralentis. Ce chaos a entraîné la fermeture temporaire des sites Web et des systèmes de réservation des établissements de MGM Resorts aux États-Unis. Le groupe estime le coût des dégâts à 100 millions de dollars et précise qu'il a également dû engager, pendant cette crise, 10 millions de dollars pour du conseil en technologie, des frais juridiques et d'autres dépenses externes.

1 **flare (2023).** Rapport - Ransomware d'extorsion de données et chaîne d'approvisionnement de la cybercriminalité : principales tendances en 2023.

2 **ITChannel (2023).** Le nombre des victimes de ransomware est en pleine explosion dans la région EMEA.

3 **Le monde informatique (2023).** Après une cyberattaque sur le SNU, les données de 150 000 personnes volées.

4 **Développez.com (2023).** Un simple appel téléphonique au service d'assistance serait à l'origine du piratage de l'exploitant de casinos MGM.

«

Il faut, en moyenne, 23 jours pour restaurer les opérations de base après une attaque par rançongiciel de grande ampleur. Cela peut prendre des mois avant que le système ait retrouvé sa pleine fonctionnalité.

Inge van der Beijl
Facilitatrice en résilience humaine et experte en communication avec les pirates informatiques chez Northwave, lors de la Human Firewall Conference 2023

Cette intensification des demandes de rançons est assez révélatrice de l'agressivité croissante des cybercriminels. Ceux-ci **ont de plus en plus recours à la double extorsion**, en chiffrant les données tout en menaçant de les publier. Bien que loin d'être récente, cette méthode est devenue de plus en plus fréquente au cours des derniers mois.[5] On voit même poindre une nouvelle tendance à la triple extorsion qui ajoute un niveau supplémentaire d'attaque, comme les DDoS, voire à la quadruple extorsion, qui implique des pressions supplémentaires sur les clients, les fournisseurs et les employés de l'entreprise ciblée. Lorsque le spécialiste en matériel informatique Quanta Computer a, par exemple, refusé d'accéder aux demandes de rançon du groupe REvil, celui-ci s'est tourné vers Apple, l'un des clients du fournisseur.[6] Ils l'ont menacé de dévoiler des schémas confidentiels de produits, mais lui ont aussi posé un ultimatum en annonçant que la divulgation aurait lieu à la date prévue pour le lancement du produit Apple et en attirant l'attention du public et des médias pour accroître la pression et décupler l'impact de l'attaque.

La professionnalisation de la cybercriminalité va bien au-delà du RaaS et commence à conquérir des technologies émergentes comme le clonage vocal. Le « **voice-cloning-as-a-service** » (VCaaS) est une menace qui se dessine de plus en plus, comme nous l'avons vu dans le paragraphe sur l'IA. Elle met, entre les mains de cybercriminels même peu qualifiés en informatique, les moyens de mener à bien des escroqueries de haut vol.[7] Les plateformes, comme celle d'ElevenLabs, qui permettent de générer des échantillons de voix personnalisés, contribuent à ouvrir un peu plus les portes de la cybercriminalité.

Alors que les cyberattaques se multiplient, plus complexes et professionnelles que jamais, il apparaît essentiel de protéger aussi les chaînes d'approvisionnement. Il est de plus en plus nécessaire de sous-traiter, mais cette externalisation des services crée de nouvelles vulnérabilités et les cybercriminels parviennent à **pénétrer dans les réseaux de grandes entreprises en passant par leurs partenaires ou leurs fournisseurs**. C'est ce qui est arrivé à Airbus en 2023. En pénétrant dans le système d'information du groupe aéronautique par le biais de l'un de ses fournisseurs, la compagnie Turkish Airlines, les pirates ont dérobé les données de plus de 3 000 fournisseurs.[8] La force de nos chaînes d'approvisionnement se mesure à leurs maillons les plus faibles. Si nous voulons garantir notre sécurité, nous ne pouvons plus nous permettre de faire l'impasse sur celle de nos fournisseurs, de nos partenaires et de nos clients.

Les pronostics sont sans appel : **la cybercriminalité va se professionnaliser de plus en plus et s'imposer comme un marché extrêmement juteux**. Nous ne pouvons plus fermer les yeux sur cette vérité ou la sous-estimer. L'heure est venue, pour les sociétés, d'investir sérieusement dans leur cybersécurité, car les tendances de ces dernières années ne sont que le début d'un processus qui est appelé à s'intensifier : la cybercriminalité va développer des méthodes de plus en plus sophistiquées pour parvenir à ses fins.

5 **TechCrunch (2023).** Why extortion is the new ransomware threat.

6 **Les Numériques (2021).** Quanta Computer et Apple visés par une cyberattaque à 50 millions de dollars.

7 **CIO (2023).** Le Deepfake Voice, nouvelle menace sur la sécurité des entreprises.

8 **Franceinfo (2023).** Airbus victime d'une nouvelle cyberattaque, les données de plus de 3000 fournisseurs dévoilées sur le dark web.

CHECKLIST

Bonnes pratiques en matière de sécurité

- **Créez une infrastructure résiliente contre les rançongiciels :** développez une stratégie de cybersécurité intégrale qui inclut, à la fois, des mesures préventives et des plans de réponse efficaces. Il est essentiel d'intégrer des systèmes de détection des menaces, notamment des méthodes augmentées par l'IA, et d'adopter une architecture Zero Trust qui renforce la sécurité. Réalisez régulièrement des audits et prévoyez des plans de récupération en cas d'incident. Repensez constamment vos stratégies de back-up et veillez à mettre en place un plan d'intervention éprouvé pour être capable de réagir rapidement et efficacement en cas d'incident.

- **Protégez-vous contre l'ingénierie sociale et le phishing :** formez vos équipes en les sensibilisant aux risques de l'ingénierie sociale et aux tactiques utilisées par les groupes de rançongiciel. Les micro-modules et les simulations de phishing peuvent stimuler la vigilance des employés et les aider à détecter les menaces éventuelles. L'intégration d'expériences gamifiées et de parcours d'apprentissage personnalisés les motivera tout en favorisant la rétention des informations en matière de sécurité.

- **Anticipez les vulnérabilités zero-day :** élaborez des stratégies qui vous permettront de réagir rapidement en cas d'attaques zero-day. Instaurez une gestion des correctifs pour mettre à jour efficacement les logiciels et pallier rapidement les vulnérabilités.

- **Renforcez la sécurité de la chaîne d'approvisionnement :** sécurisez votre chaîne d'approvisionnement, en vérifiant notamment les protocoles de sécurité de vos partenaires et fournisseurs, et en mettant en place des contrôles d'accès rigoureux, ainsi que des systèmes de suivi.

- **Assurez une meilleure sécurité et intégrité des données :** aidez-vous de techniques de chiffrement sophistiquées et optez pour une protection des données en plusieurs étapes avec un modèle de sécurité centré sur les données et des technologies de prévention des pertes de données (data loss prevention ou DLP). Vous limiterez ainsi les risques de vol ou de fuite de données.

- **Appuyez-vous sur le cyberrenseignement et les analyses :** utilisez le cyberrenseignement pour identifier et analyser les menaces émergentes. Vous pourrez ainsi prendre des mesures préventives et augmenter votre réactivité en cas d'attaque.

INTERVIEW

Ralf Schneider

Senior Fellow d'Allianz et Head of Cybersecurity au sein du groupe de réflexion NextGenIT

Titulaire d'un doctorat en informatique de l'Université Ludwig Maximilian de Munich, Ralf Schneider poursuit, depuis plus de 20 ans, une impressionnante carrière dans le domaine de l'informatique et de la cybersécurité, marquée par les 13 années passées chez Allianz en tant que DSI du groupe. Il a également fait partie du conseil d'administration d'Allianz Managed Operations & Services et a récemment pris les fonctions de Senior Fellow et de Head of Cybersecurity, chez Allianz, au sein du groupe de réflexion NextGenIT.

« Pour lancer une cyberattaque efficace, il est de moins en moins nécessaire de disposer de compétences spécifiques ou d'une structure organisée. C'est précisément ce qui laisse présager de graves difficultés.

Qu'est-ce qui vous a amené à travailler dans le domaine de la sécurité informatique ?

J'ai commencé à travailler dans ce domaine lorsque j'ai été nommé DSI du groupe Allianz en janvier 2011. Pour gérer les 3 000 bureaux et les 63 unités commerciales que nous possédons dans le monde, j'ai rapidement compris qu'il nous fallait une infrastructure de communication permettant, entre autres, des visioconférences. Nous devions organiser notre système informatique de façon à pouvoir accéder aux ressources numériques depuis n'importe quel périphérique dans le monde. Pour ce faire, il faut une infrastructure de réseau, un centre de données consolidé qui permette aux applications de fonctionner dans le monde entier et un espace de travail final virtualisé. Tous ces éléments doivent être sécurisés. Nous ne nous sommes jamais posé la question de savoir si la cybersécurité devait être

un élément important de notre stratégie.

Les révélations d'Edward Snowden en 2013, puis le piratage du téléphone portable de la chancelière allemande Angela Merkel, nous ont fait réaliser que la cybersécurité devenait un sujet de plus en plus brûlant. Cette même année, nous avons donc ajouté aux éléments déjà mis en place une infrastructure de cybersécurité, une gestion internationale des identités et des accès, une gestion internationale des privilèges, ainsi que le centre de cyberdéfense d'Allianz à l'échelle mondiale.

Quel regard jetez-vous sur le paysage actuel des menaces et comment va-t-il, selon vous, évoluer dans les prochaines années ?

Après le début du conflit armé en Ukraine, il est devenu rapidement évident que nous étions au beau milieu d'une guerre cyber. En cybersécurité, nous sommes confrontés à des criminels de haut vol, à des forces militaires, mais aussi à des acteurs étatiques. Les attaquants cherchent constamment à se perfectionner et sont de mieux en mieux organisés. Ils tendent également à « industrialiser » les cyberattaques et en font un marché frauduleux et extrêmement juteux.

On observe également que la cybersécurité suit un schéma cyclique. Le DDoS était un problème majeur en 2013 avant de disparaître. Aujourd'hui, on assiste à son grand retour. Il faut s'attendre à ce que les activistes et les kits de hacking reviennent sur le devant de la scène, notamment avec des variantes augmentées par l'IA. Pour lancer une cyberattaque efficace, il est de moins en moins nécessaire de disposer de compétences spécifiques ou d'une structure organisée. C'est précisément ce qui laisse présager de graves difficultés. Nous ne concentrons plus notre attention sur quelques groupes de criminels, nous sommes face à des centaines, voire des milliers d'acteurs malveillants.

L'écart qui se creuse entre les pauvres et les riches aggrave encore la situation. À l'heure actuelle, il n'est plus besoin d'être un athlète de haut niveau pour gagner beaucoup d'argent… Il suffit de faire du piratage. La bonne nouvelle, c'est que nous sommes de plus en plus performants en matière de cyberdéfense.

Vous venez de mentionner l'essor de l'IA générative. Pensez-vous que les technologies comme le deepfake ou le clonage vocal vont être massivement utilisées dans les attaques ?

Le clonage vocal et les méthodes similaires sont déjà très répandus à l'heure actuelle, mais je crois qu'ils cachent un autre danger. Les attaquants n'en sont plus à chercher les failles de sécurité ou la personne qui pourra être le maillon faible. Ils s'en prennent aujourd'hui aux moyens de réponse, en cherchant à désactiver ou à contourner les outils de détection. C'est à ce niveau-là que l'IA va être de plus en plus utilisée.

Outre le fait que l'IA permet des attaques plus sophistiquées, je ne pense pas que nous courrions actuellement de grands risques de subir des piratages automatisés avec l'IA. Cette technologie fait encore trop d'erreurs et il faut savoir l'utiliser correctement. Nous n'en sommes qu'aux débuts, mais nous devons nous préparer au pire scénario possible. Nous sommes actuellement en sursis en attendant qu'une évolution majeure ait lieu. Et chaque attaque, qu'elle aboutisse ou non, est pour nous l'occasion d'apprendre et d'améliorer notre ligne de défense. Le risque n'est cependant pas uniquement dans la quantité, mais aussi dans le fait que l'IA permet de faire coïncider les attaques. Ces campagnes simultanées de grande ampleur vont constituer le grand défi de demain.

Comment devons-nous faire, selon vous, pour ne pas être dépassés par le rythme effréné auquel évoluent les menaces ?

Cela tient en quelques mots : une cyberhygiène adaptée et un œil ouvert sur les menaces émergentes. La cyberhygiène doit être posée comme un fondement… Et c'est déjà un défi en soi. Je pense qu'on ne peut pas faire l'impasse sur l'authentification multifacteur. Avant de conduire,

vous attachez votre ceinture ; avant de surfer sur le Web, vous devez passer l'authentification multi-facteur. Chez Allianz, nous avons mis ce type d'authentification en place pendant la pandémie du coronavirus, en raison des taux élevés de télétravail. La meilleure manière de ne pas se laisser dépasser par la rapidité avec laquelle les menaces apparaissent, c'est de poser des bases de travail saines et complètes dès le départ. Puis, de suivre le marché. Nous sommes en train de refaire à neuf notre plateforme de cyberdéfense en l'augmentant par l'IA. Nous avons acheté les solutions auprès des leaders du marché. Le gros du travail va maintenant être de les intégrer et de les utiliser dans notre environnement. C'est sur ce point que nous investissons. Tout revient, en fin de compte, au facteur humain : il faut trouver les bonnes personnes et leur donner l'occasion d'apprendre en toute autonomie. Si vous n'avez pas, au sein de votre entreprise, les capacités ou les connaissances qu'il faut, toute la technologie du monde ne vous servira à rien.

Tout revient, en fin de compte, au facteur humain : il faut trouver les bonnes personnes et leur donner l'occasion d'apprendre en toute autonomie. Si vous n'avez pas, au sein de votre entreprise, les capacités ou les connaissances qu'il faut, toute la technologie du monde ne vous servira à rien.

La cybercriminalité s'oriente aussi vers la numérisation, à une époque où tout est de plus en plus interconnecté. Quels sont, à votre avis, les risques cyber à ce niveau ?

Il est extrêmement risqué d'administrer un site Internet sans se protéger contre les menaces de base en utilisant un proxy. Toute entreprise a besoin d'un bon proxy, mais cela a un prix.

Aujourd'hui, tout est interconnecté et les informations circulent à la vitesse de la lumière, pour ainsi dire. En outre, tout est géré par des logiciels qui réalisent des opérations en quelques millisecondes. Il n'est plus possible d'assurer la surveillance et le contrôle sans automatisation, mais l'on peut s'attendre à ce que l'IA fasse toutes ces tâches à notre place. Ceux qui nous attaquent exploitent les possibilités de l'intelligence artificielle. Nous avons donc besoin, pour nous défendre, de personnes qui savent également l'utiliser, de professionnels dûment formés, disposant de connaissances adaptées. Il faut aussi tenir compte du fait que les points d'entrée dans les systèmes informatiques ne sont pas des machines. Ce sont généralement des êtres humains. Or, chacun de ces points de contact doit être suivi et sécurisé contre d'éventuelles attaques.

C'est un dilemme qui revient fréquemment : les sociétés doivent-elles remédier en priorité à leurs vulnérabilités sur le plan technique, avant de se concentrer sur les gens, ou faut-il procéder dans l'ordre inverse ? Avez-vous une stratégie à proposer qui soit holistique et inclue le facteur humain ?

Si vous vous jetez tête baissée dans toutes les batailles, vous allez perdre. Si vous connaissez votre ennemi, vous avez une chance sur deux de gagner. Si vous connaissez non seulement votre ennemi, mais aussi vous-même, vous avez de grandes chances de pouvoir gagner à chaque fois. La cybersécurité est un jeu d'attaque et de défense. Au début, en 2013, nous nous sommes concentrés sur deux contrôles que nous avons déployés à tous les niveaux. Nous avons commencé par la sensibilisation et par une protection à grande échelle contre les attaques DDoS en sécurisant d'abord les terminaux mobiles, puis toutes les autres couches de notre défense comme la protection, la détection, la réponse et la récupération.

Deux mille ans de sagesse nous ont appris qu'en situation d'attaque et de défense, il était essentiel

de se connaître soi-même et de connaître l'ennemi. Aujourd'hui, cela passe par une étude approfondie du paysage des menaces cyber, mais aussi de vos propres systèmes informatiques, de vos réseaux et de leurs vulnérabilités. On ne peut pas défendre ce que l'on connaît mal. Derrière toute infrastructure informatique, il y a des personnes qui les ont construites et qui les utilisent : vous devez connaître ces gens et leur degré de sensibilisation à la cybersécurité.

À propos de sensibilisation, certaines formations proposent aux sociétés de ne plus se contenter de répondre aux exigences légales de conformité, mais d'adopter des mesures continues qui transforment le facteur humain en une ligne de défense efficace. Quel est votre avis sur ce point ?

À l'ère de la transition numérique, nous ne pouvons plus nous contenter d'une informatique fonctionnelle. Elle doit être à la fois sécurisée et conforme aux exigences. Mais tout ce qui est bon pour la conformité n'est pas nécessairement bon pour renforcer la sécurité. La sensibilisation illustre bien ce principe. Imaginons que vous mettiez en place un programme de sensibilisation via une formation en ligne. Vous cochez les cases des exigences de conformité et les organismes de réglementation sont satisfaits. Mais vous n'avez pas pour autant amélioré votre sécurité si les utilisateurs n'ont pas compris le rôle qu'ils y jouent.

C'est là que l'autonomie des employés entre en jeu. Nous avons assez tôt compris qu'il fallait sensibiliser en adoptant une approche ludique et en cessant de faire pression sur les gens. Il faut aussi trouver le bon moment pour les former. L'idéal est lorsque je viens de recevoir une campagne de phishing ou un véritable e-mail de phishing. Une autre difficulté consiste à maintenir la vigilance au sein du personnel. Sur ce point, le bouton d'alerte phishing de SoSafe est un outil extrêmement utile. Lorsque les employés hésitent, ne sachant pas si l'e-mail qu'ils ont reçu est vraiment une tentative de phishing, ils peuvent utiliser ce bouton pour savoir si c'est une attaque et comment l'identifier. L'impact pédagogique est énorme. Il s'y ajoute une dimension ludique, ainsi qu'une grande motivation suscitée par le plaisir d'apprendre par soi-même et d'utiliser le bouton d'alerte phishing comme une sorte d'assistant. C'est très gratifiant, car les utilisateurs peuvent directement mettre en pratique ce qu'ils ont appris.

> **Ceux qui nous attaquent exploitent les possibilités de l'intelligence artificielle. Nous avons donc besoin, pour nous défendre, de personnes qui savent également l'utiliser, de professionnels dûment formés, disposant de connaissances adaptées.**

Les équipes d'informatique sont soumises à toutes sortes de pressions, que ce soit sur le plan de la défense ou sur celui de la sensibilisation à la cybersécurité. À votre avis, quelles mesures pourrait-on prendre pour essayer de les décharger ?

Dll faut aller à la racine du problème : mener des exercices de gestion de crise à tous les niveaux, y compris parmi les cadres dirigeants et le conseil d'administration. Chez Allianz, nous en faisons régulièrement, depuis des années. Il y a différents facteurs psychologiques en jeu dans ce contexte. Il faut, d'abord, tenir compte du fait que les gens n'aiment pas montrer qu'ils ne savent pas faire quelque chose. Ensuite, il est important que les avantages soient très rapidement évidents et justifient le temps investi. Ne perdons pas de vue qu'une formation de sensibilisation coûte beaucoup d'argent et de ressources.

L'une des plus grandes difficultés consiste à faire toucher du doigt aux dirigeants toute l'urgence du problème. Aux yeux de ceux qui définissent les objectifs de l'entreprise, l'informatique doit être à la fois fonctionnelle et sécurisée. Tant que la société n'a pas été confrontée à des incidents graves, vous aurez du mal à expliquer en quoi les mesures que vous avez prises ont contribué à renforcer la sécurité. Il est très difficile de démontrer l'efficacité

de votre stratégie et de convaincre les sceptiques, parce que vous n'avez aucun moyen de prouver que l'infrastructure informatique est plus sécurisée qu'avant. Dans ce contexte, les simulations d'attaques peuvent être très convaincantes : elles doivent montrer que vous êtes plus réactifs et plus efficaces au niveau de la défense de votre entreprise.

Pensez-vous que certains ICP peuvent aider à convaincre les instances dirigeantes ?

Chez Allianz, nous avons six indicateurs de cybersécurité définis d'après les critères du NIST : Gouvernance, Identification, Prévention, Détection, Réponse, Récupération après une cyberattaque. Nous utilisons un code couleur pour les évaluer : rouge, orange, jaune, vert clair et vert foncé. Nous procédons exactement comme lorsqu'on mesure la tension artérielle, le pouls ou les taux de cholestérol. Pour attester de la bonne santé de notre cybersécurité, les six indicateurs doivent se trouver dans une plage de valeurs donnée.

Deux de ces indicateurs se sont avérés particulièrement efficaces. Le premier est lié à la technique : il s'agit de notre tolérance zéro vis-à-vis des composants toxiques lorsque les correctifs de sécurité ne sont plus disponibles. Cette politique nous a amenés à faire la chasse à toutes les applications trop anciennes ou insuffisamment protégées. Nous avons également commencé à automatiser, à analyser toutes les bases de données et les systèmes d'exploitation obsolètes, à identifier les composants toxiques et à renouveler systématiquement toute notre infrastructure. La tolérance zéro avait, à l'origine, été mise en place par souci de sécurité, mais elle va aujourd'hui bien au-delà. Le deuxième indicateur efficace est notre score de sensibilisation qui nous permet de mesurer les campagnes de phishing partout dans le monde. Nous enregistrons les taux de clics et le nombre de personnes ayant signalé un e-mail malveillant.

Lors d'une précédente interview, vous disiez que les structures hiérarchiques pouvaient être un obstacle à la cybersécurité au sein des sociétés. Qu'entendez-vous par là ?

Les attaques externes menées à l'aide d'outils ne peuvent être empêchées que par des experts ayant à leur disposition les outils correspondants. C'est aux professionnels de la sécurité qu'il revient de décider de la marche à suivre. Le rôle de l'exécutif est de garder un œil sur la situation globale et de fournir, en temps et en heure, les ressources, les initiatives et l'assistance nécessaires. Tout cela a pourtant lieu « sur site » et nécessite de l'autonomie. Les cadres dirigeants posent les fondements, apportent les ressources adaptées pour une cyberdéfense efficace et mettent les professionnels de la sécurité en contact avec des partenaires internes ou externes.

« C'est aux professionnels de la sécurité qu'il revient de décider de la marche à suivre. Le rôle de l'exécutif est de garder un œil sur la situation globale et de fournir, en temps et en heure, les ressources, les initiatives et l'assistance nécessaires.

4 Dissidence numérique et cyberextorsion : les deux visages de l'hacktivisme et de la cybercriminalité dans un monde fragmenté

La complexité du paysage des menaces va bien au-delà d'individus mus par l'appât du gain ou la recherche de profits personnels. L'intensification des tensions politiques et sociales alimente une autre forme, non négligeable, de piratage informatique : **l'hacktivisme**. Motivés par le désir d'exprimer leur opposition ou de soutenir des causes - dans le cadre de conflits armés ou d'injustices sociales, par exemple - ces hackers **exploitent les vulnérabilités et les failles de sécurité afin de faire passer leur message**. Il s'agit là d'une forme de piratage qui ne cesse de prendre de l'ampleur au fil des mois.

Les recherches montrent que l'hacktivisme a augmenté de 8 % dans le monde en 2023, ce qui représente la plus forte hausse en deux ans.[1] L'initiative pro-russe **DDoSia** est un exemple frappant d'hacktivisme. Lancé à l'été 2022, ce projet de déni de service distribué (DDoS) a connu une croissance massive de 2 400 % en moins d'un an[2], avec plus de 45 000 abonnés sur son canal Telegram principal (il y en a sept au total).

La guerre qui fait rage, depuis près de deux ans, entre la Russie et l'Ukraine a montré que les conflits modernes se déroulent sur **un mode hybride, aussi bien sur site que dans la sphère cybernétique**. Perpétrées par des hacktivistes et par des entités opérant avec le soutien des gouvernements, les **cyberattaques** sont, dans ce contexte, devenues une **arme importante dans l'arsenal des belligérants**. De leur côté, les hacktivistes ukrainiens Cyber. Anarchy.Squad s'en sont pris à la société russe de télécommunications Infotel[3] qui joue un rôle vital en tant que lien entre la Banque Centrale de Russie et les banques et systèmes de crédits russes. Cette attaque a fait perdre à certaines grandes institutions financières russes leur accès au système banquier du pays, les empêchant d'effectuer des échanges sécurisés en ligne pendant plusieurs heures.

Plus récemment, le conflit entre Israël et Gaza illustre aussi la montée en puissance de ces menaces et toutes leurs possibles répercussions. Peu après le début de la guerre, le groupe Anonymous Sudan lançait sa première attaque[4] dirigée contre les systèmes israéliens d'alerte à la roquette et leurs applications d'information aux civils. Presque en même temps, KillNet lançait une offensive contre les sites Web du gouvernement israélien. En représailles contre la pluie de cyberattaques qui s'est abattue sur l'État hébreu, le groupe d'hacktivistes pro-israélien Indian Cyber Force[5], basé en Inde, a revendiqué le

1 **ZDNet (2023).** L'hacktivisme en 2023 : des mouvements populaires aux menaces commanditées par les États.

2 **Hfrance (2023).** Le projet hacktiviste pro-russe DDoSia enregistre une augmentation de 2 400 % du nombre de ses membres.

3 **Geo (2023).** L'économie russe paralysée après plusieurs attaques de hackers.

4 **i24NEWS (2023).** Les Anonymous soudanais affirment avoir piraté les alertes du Dôme de fer.

5 **Israel Valley (2023).** Les cyberattaques contre Israël s'intensifient alors que la guerre contre le Hamas fait rage.

piratage de plusieurs sites Web du gouvernement palestinien.

Cependant, l'hacktivisme va bien au-delà de la guerre cybernétique et des tensions politiques : il embrasse également différentes **causes sociales**. C'est ainsi qu'Anonymous Sudan s'en est aussi pris aux sites de cinq aéroports français, en mars 2023, provoquant la panne de trois d'entre eux.[6] Le groupe a indiqué mener ces attaques « en représailles des caricatures de Mahomet » publiées par Charlie Hebdo en 2015. Les mêmes hackers avaient revendiqué la campagne lancée contre les administrations suédoises et danoises après que des militants d'extrême droite ont brûlé le Coran dans ces deux pays.

Plus tard dans le courant de l'année 2023, le groupe de hackers VulzSec a annoncé avoir compromis et dérobé à la police nationale française des données sensibles[7] en représailles contre les violences policières. Quelque 7 092 enregistrements de données et les profils de 30 policiers ont ainsi été exposés. Cet incident est révélateur d'une tendance plus générale : les cyberattaques perpétrées contre les forces de l'ordre ont augmenté de 28 %[8] et l'hacktivisme joue un rôle majeur dans cette recrudescence.

Il faut pourtant rappeler que les hacktivistes n'agissent pas par intérêt financier. Ils s'engagent dans le piratage informatique afin de soutenir des causes qui leur tiennent à cœur. Il existe, par ailleurs, d'autres cybercriminels qui, eux, profitent de l'instabilité sociale pour en tirer des avantages personnels. Certains, par exemple, ont repris les tactiques déjà utilisées dans le cadre du conflit entre la Russie et l'Ukraine, et créé des sites Web d'arnaque aux dons humanitaires[9] afin d'escroquer les personnes qui souhaitent aider les victimes de la crise de Gaza. Mais ce n'est pas tout. Des hackers soutenus par des États se jettent également dans la mêlée : il semble ainsi qu'une série de cyberattaques visant Israël soit le fait de pirates affiliés au Hamas. Ceux-ci ont utilisé un malware sophistiqué appelé « SysJoker »[10] capable d'échapper à la détection et à l'analyse des organismes qui en sont infectés. Nous sommes donc au cœur d'un paysage très complexe où les menaces émanent de différents profils de hackers, chacun agissant pour des raisons qui lui sont propres.

> ↗ **28 %**
>
> d'augmentation du nombre de cyberattaques perpétrées contre les forces de l'ordre, l'hacktivisme étant l'un des principaux moteurs de cette recrudescence
>
> Source : Motorola Solutions[8]

Alors que les tensions mondiales s'intensifient et qu'aucun dénouement ne semble se profiler à l'horizon, il est quasiment certain que les attaques de cybermilitants vont encore augmenter en 2024. Les hacktivistes, tout comme les cybercriminels, contribuent à alimenter l'instabilité de notre cyberespace. Ils opèrent dans une sorte de synergie agressive, chaque groupe exploitant les vulnérabilités révélées par l'autre. Cette interaction façonne un contexte dynamique où les menaces cyber sont en perpétuelle évolution, image d'un espace numérique complexe et imprévisible.

6 **numerama (2023).** Les sites de 3 aéroports français attaqués par des hackers « pro-russes » et « islamistes ».

7 **The Cyber Express (2023).** Cyber Attack on French National Police: VulzSec Hacking Group Claims to Leak Sensitive Data.

8 **Motorola Solutions (2023).** New Report Outlines Q3 2023 Cyber Threats to Public Safety.

9 **BFMTV (2023).** Conflit au Proche-Orient : comment repérer les faux appels aux dons.

10 **HFrance (2023).** La nouvelle porte dérobée SysJoker, basée sur Rust, est liée à des pirates du Hamas.

CHECKLIST

Bonnes pratiques en matière de sécurité

Mettez en place une infrastructure de réseau redondante : si vous disposez de plusieurs voies d'accès, vous pourrez maintenir la disponibilité du réseau même en cas d'attaque DDoS. Ce processus implique aussi l'ajout de serveurs, de centres de données supplémentaires ou de services sur le cloud. Si la voie principale est compromise ou surchargée, le trafic pourra être basculé sur un autre chemin de réseau afin d'assurer la continuité des services.

Procédez régulièrement à des tests de charge : soumettez votre infrastructure à des tests de charge pour observer comment elle se comporte en cas de forte affluence. Il peut être très utile, lors de ces tests, d'organiser des exercices de type « red team » pour simuler des scénarios d'attaque.

Adoptez une solution de limitation du débit, des services de nettoyage du trafic et un surprovisionnement en bande passante : ces stratégies vous aideront à contrôler le débit de trafic accepté par un serveur sur un laps de temps donné, à filtrer le trafic malveillant et maintenir une grande capacité de bande passante pour gérer les brusques pics d'affluence.

Sauvegardez régulièrement les données en back-up et dans une solution de stockage externe : réalisez régulièrement des sauvegardes des données critiques et stockez-les sur une plateforme externe ou sur le cloud, pour éviter de tout perdre en cas de compromission du site principal. Il est recommandé de privilégier les sauvegardes immuables et de suivre la règle du 3-2-1 qui consiste à conserver trois copies des données : deux en local, stockées sur des appareils différents, pour garantir la facilité d'accès et de récupération, et une copie conservée en externe pour plus de sécurité.

Segmentez le réseau : segmentez votre réseau pour limiter la propagation des malwares. Si un segment est compromis, l'incident n'affectera pas nécessairement l'ensemble du réseau. Il est conseillé d'avoir recours à la micro-segmentation pour améliorer la granularité et la protection des données sensibles au sein des segments.

CHECKLIST

Bonnes pratiques en matière de sécurité

Restreignez les privilèges utilisateurs : adoptez le principe du moindre privilège en n'accordant aux utilisateurs que les autorisations requises pour l'exercice de leurs fonctions. Cette approche est un élément essentiel d'une architecture zero trust et permet de réduire efficacement les risques de menaces internes. Veillez à contrôler régulièrement ces autorisations et à les mettre à jour.

Utilisez un WAF ou pare-feu d'applications Web : un WAF est un type de pare-feu qui régit le trafic à destination et en provenance d'une application Web. Il empêche que des modifications non autorisées soient apportées au site Internet. Les WAF peuvent être intégrés dans d'autres outils de sécurité. Leur utilisation est recommandée pour la création d'un système UTM (unified threat management). Vous pouvez aussi envisager d'optimiser les WAF en les combinant à la technologie d'apprentissage automatique qui leur permettra de s'adapter de manière dynamique aux menaces cyber émergentes et à l'évolution de celles existantes.

Adoptez des méthodes d'authentification fortes : appliquez des politiques strictes en matière de mots de passe et implémentez une authentification multifacteur (MFA) pour ajouter une couche de sécurité supplémentaire, en particulier pour protéger l'accès aux systèmes sensibles et au back-end du site Internet. Lorsque c'est possible, privilégiez les technologies d'authentification sans mot de passe et les contrôles biométriques pour augmenter encore le niveau de protection.

Aidez-vous de systèmes de surveillance et d'alerte : utilisez des outils de surveillance pour garder un œil sur le trafic réseau, les performances du système et les registres d'accès. Pour compléter votre arsenal de surveillance, d'analyse et de réponse automatisée, installez également des systèmes de gestion des informations et des événements de sécurité (SIEM) et des solutions SOAR (Security Orchestration, Automation, and Response). Paramétrez des alertes en cas d'activités inhabituelles ou de changements : ils permettront à l'équipe de sécurité de réagir rapidement si des incidents surviennent.

5 La « désinformation-as-a-service » : un outil redoutable entre les mains des hackers

Depuis le scandale de Cambridge Analytica, les campagnes de désinformation contribuent de manière significative à exacerber la polarisation sociale. Différents acteurs ont de plus en plus recours à cette tactique qui consiste à **répandre délibérément de fausses informations** afin de manipuler l'opinion publique, de nuire à la réputation de certaines personnalités ou d'influer sur les contextes commercial et politique.[1] L'année 2023 a cependant marqué un tournant majeur dans cette tendance, avec **l'avènement de l'IA générative.** Celle-ci soulève des inquiétudes parce qu'elle laisse présager d'un avenir où n'importe qui peut facilement générer, à moindre coût, des textes fallacieux d'une qualité telle qu'il est **quasiment impossible de les distinguer de contenus authentiques.**

Les élections présidentielles aux États-Unis sont, par exemple, l'un des principaux théâtres des campagnes de désinformation. En 2016, de fausses informations s'étaient propagées à grande échelle sur les réseaux sociaux, alimentés par des militants d'extrême droite, par l'ingérence de pays étrangers ou par des sites de fake news. En 2020, les élections se sont déroulées sur fond de théories du complot et d'accusations de fraude électorale sans aucun fondement[2] : celles-ci ont pourtant touché des millions de personnes et suscité un mouvement anti-démocratique. À la veille des élections 2024, les craintes augmentent de voir les récentes avancées de l'IA être utilisées[3] pour générer **des formes encore plus subtiles de désinformation**, de deepfakes et de campagnes de propagande ciblées.

En fait, cette **menace pour la démocratie** s'était déjà manifestée lors des élections en Slovaquie lorsqu'un deepfake utilisant des voix générées par IA[4] a été utilisé pour diffuser de fausses informations sur les réseaux sociaux. Dans ce faux enregistrement, écouté par des milliers de personnes, on entend le chef de file du parti Slovaquie progressiste, Michal Simecka, converser avec une célèbre journaliste d'investigation de la façon dont « le vote rom » va être « manipulé » pour favoriser sa candidature. Bien que l'authenticité de cet entretien ait été immédiatement démentie et que plusieurs agences de fact-checking aient attesté de sa fausseté, la vidéo s'est propagée comme une traînée de poudre. L'heure de sa diffusion avait été soigneusement choisie à cet effet, puisqu'elle a été publiée dans la période de 48 h qui précède les élections et durant laquelle les médias et les personnalités politiques sont tenus au silence électoral. Ceux-ci étaient donc dans l'impossibilité de réfuter immédiatement ces propos sur la scène publique.

L'avènement de la **désinformation-as-a-service (DaaS)** dans ce contexte menace de faire monter d'un cran encore la portée et la sophistication

1 **Les Échos (2024).** La désinformation, risque mondial majeur, selon Davos.

2 **Le Monde (2020).** Elections américaines : « La désinformation a pris un rôle de premier plan ».

3 **Le Télégramme (2023).** À un an de la présidentielle américaine, la désinformation à la sauce IA menace la campagne.

4 **Le Monde (2023)** Lutte contre la désinformation : les élections en Slovaquie, premier test raté de la politique européenne.

des campagnes de désinformation. La **guerre de l'information prend un nouveau visage** : désormais, particuliers et organisations pourront acheter et propager des fake news et des campagnes de désinformation avec une effrayante facilité. Alimentée par les rapides progrès de l'IA générative et par tout un réseau de trolls professionnels, de bots et d'outils de manipulation en ligne[5], la DaaS met la possibilité de mener des campagnes de désinformation à la portée de tous, tout comme le RaaS l'avait fait pour les attaques par rançongiciel. Nul doute que les cybercriminels et les hacktivistes exploiteront cette nouvelle offre.

L'année **2024 sera donc marquée par un déferlement des campagnes de désinformation diffusées à des fins politiques ou financières**. Il est probable qu'elles ciblent de nombreux secteurs : la santé, la finance, la technologie, l'éducation et les médias, par exemple. Les hacktivistes et les cybercriminels à la solde des États vont poursuivre leurs efforts pour tenter de déstabiliser les gouvernements et les instances politiques, et répandre de fausses informations pour influencer l'opinion publique afin de rallier davantage de monde à leur cause. C'est ce qui s'est passé en 2023, par exemple, lorsqu'une image truquée publiée sur les réseaux sociaux a montré les supporters de l'Atlético Madrid[6] en train de manifester leur soutien aux Palestiniens en plein match. Certaines attaques ont des retombées économiques plus importantes encore et vont même jusqu'à influer sur le marché boursier. Ainsi, en mai 2023, une fausse image montrant une explosion près du Pentagone est devenue virale sur les réseaux sociaux et a été relayée par différents médias, provoquant un bref affaissement des marchés.[7]

Par ailleurs, des cybercriminels motivés par l'appât du gain cherchent, eux aussi, à déstabiliser les sociétés et les organismes officiels par différents moyens. La DaaS leur permettra **d'avoir recours aux fake news à moindre coût, et de mener des attaques sophistiquées d'ingénierie sociale et de phishing**. Ils profiteront ainsi de la panique et du sentiment d'urgence provoqués par la propagation de nouvelles inquiétantes sur le compte d'une entreprise pour manipuler psychologiquement les gens. Sans compter que, si elles sont largement relayées à l'externe, les campagnes de désinformation peuvent aussi **nuire à la réputation d'une entreprise**. Le site de commerce Wayfair en a fait la triste expérience lorsqu'il s'est retrouvé au cœur d'une théorie du complot. Dans le contexte anxiogène de la pandémie, le réseau QAnon avait entaché la réputation du revendeur[8] en propageant une rumeur sur des plateformes comme Twitter, Instagram et Reddit, accusant le site d'être impliqué dans un réseau de pédophilie. Malgré tous les efforts déployés par la société pour réfuter ces allégations, les fausses informations ont continué de se répandre en ligne. L'épisode illustre avec force les risques que présentent de telles fake news pour l'image des sociétés.

Dans la mesure où les PDG sont des personnalités qui apparaissent sur la scène publique, ils constituent des cibles privilégiées pour les deepfakes. Puisqu'ils prennent régulièrement la parole pour des appels de fonds, des réunions d'actionnaires et des interviews télévisées, les cybercriminels n'ont aucun mal à se procurer des échantillons de leur voix ou des clips vidéo. Et nous avons déjà vu, dans le passage consacré à l'IA, ce qu'ils sont capables d'en faire.

Alors que les campagnes de désinformation gagnent en puissance et menacent le monde de l'information à l'échelle planétaire, les sociétés prennent de plus en plus conscience du risque qu'elles représentent, des importantes pertes financières qu'elles peuvent provoquer et des dommages à long terme qu'elles sont susceptibles de causer. Par conséquent, face à la sophistication et à la démocratisation constante de ces tactiques, il est essentiel que les entreprises mettent en place des contre-mesures pour protéger leur intégrité et conserver la confiance du public.

5 **Sensorts TechForum (2022).** Désinformation-as-a-service maintenant offert sur les forums Dark Web.

6 **franceinfo (2023).** « Info ou Intox » : images générées par l'IA, le front virtuel de la guerre Israël - Hamas.

7 **20 minutes (2023).** Une fausse image d'une explosion au Pentagone brièvement virale.

8 **Le Monde (2020).** Comment le site de commerce Wayfair s'est retrouvé accusé d'organiser un réseau pédophile.

CHECKLIST

Bonnes pratiques en matière de sécurité

Évaluez les menaces éventuelles : les sociétés doivent évaluer régulièrement leur vulnérabilité aux campagnes de désinformation. Pour ce faire, il est essentiel d'intégrer une solide modélisation des menaces qui analyse non seulement la probabilité d'être ciblé, mais aussi les conséquences éventuelles que de telles rumeurs pourraient avoir. Utilisez des outils d'analyse de sentiments et de suivi des tendances : ils permettent de se faire une idée de l'opinion publique et fournissent aux sociétés des informations utiles pour anticiper les éventuelles menaces de désinformation et développer une stratégie efficace pour les contrer.

Formez et entraînez les employés : informez les employés sur les tactiques utilisées lors des campagnes de désinformation et les répercussions qu'elles peuvent avoir sur l'entreprise. Enseignez-leur à vérifier les faits, à reconnaître les sources crédibles et à utiliser leur esprit critique pour remettre en question les contenus auxquels ils sont exposés. Instaurez une culture de scepticisme et de contrôle des informations pour armer l'entreprise contre les effets des fake news.

Améliorez la qualité de la communication en interne : intensifiez l'usage des canaux de communication en interne pour être en mesure de réagir rapidement aux fausses informations et d'en limiter la propagation. Des outils comme Sofie Rapid Awareness, la fonctionnalité de SoSafe intégrée dans MS Teams, vous permettent d'informer rapidement vos employés lorsque vous constatez l'émergence d'une campagne de désinformation concernant votre entreprise.

Mettez en place une équipe dédiée à la communication de crise : formez une équipe d'intervention rapide, spécialisée dans la communication de crise, pour être en mesure de contredire rapidement de fausses informations avec des faits à l'appui.

CHECKLIST

Bonnes pratiques en matière de sécurité

Incitez à la vigilance et au signalement : les sociétés doivent installer un cadre qui favorise la vigilance des employés et les incite à signaler tout élément inhabituel qu'ils peuvent rencontrer en ligne, par exemple de fausses informations, des photos truquées, des deepfakes vidéo ou audio. Les collaborateurs doivent avoir la liberté de faire remonter ce genre d'incidents, sans crainte d'être jugés. L'utilisation d'un système de signalement anonyme et facile d'utilisation peut s'avérer d'une grande aide à cet égard. Les employés pourront faire part des cas de désinformation qu'ils rencontrent sans crainte de représailles.

Automatisez la veille sur les réseaux sociaux : gardez un œil sur les réseaux sociaux pour y dépister d'éventuelles opérations de DaaS, rechercher des fake news, des photomontages et de faux enregistrements audio. Pour ce faire, il est essentiel de collaborer avec les équipes de marketing et de relations publiques. Il existe également des logiciels de veille augmentés par l'IA qui peuvent détecter les éventuelles campagnes de désinformation sur les réseaux sociaux et les signaler en temps réel pour permettre une réaction immédiate.

Collaborez avec le cyberrenseignement : travaillez en partenariat avec des réseaux externes de cybersécurité, notamment avec des pairs, des organismes gouvernementaux et des alliances mondiales pour la cybersécurité afin d'échanger sur les tendances de la désinformation et les meilleures pratiques.

6 2024 : une année riche en défis pour la cybersécurité du secteur public et des infrastructures essentielles

Alors que l'hacktivisme est une menace bien connue des institutions publiques, ce n'est pas le seul problème auquel elles sont confrontées. Le secteur public est également menacé par des **cybercriminels mandatés par des États, ainsi que par des hackers indépendants** qui cherchent à détruire les données, perturber les systèmes, extorquer de l'argent et espionner. Les conséquences peuvent être désastreuses. Le Rapport 2023 sur le coût d'une violation de données d'IBM a en effet montré que[1] **le coût moyen d'une cyberattaque contre le secteur public pouvait atteindre les 2,60 millions de dollars.**

La transition numérique au sein du secteur public et les services essentiels dispensés par celui-ci en font **une cible de choix pour les cybercriminels désireux de dérober des données sensibles ou de perturber les réseaux**. Ne serait-ce qu'au cours de l'année 2022, le nombre de **cyberattaques entre États visant les infrastructures critiques est passé de 20 % à 40 %** à l'échelle mondiale.[2] Cette évolution est majoritairement liée aux attaques commanditées dans le cadre du conflit russo-ukrainien. Dans la mesure où celui-ci fait toujours rage, alors que d'autres, comme la guerre entre Israël et Gaza, viennent de se déclarer, il faut s'attendre à ce que cette tendance persiste en 2024, envenimant encore la situation.

De toute évidence, la quantité d'informations à caractère personnel traitées par ces instances est une véritable mine d'or qui attise la convoitise

> **La cybernétique est un instrument de pouvoir géopolitique et un nouveau vecteur d'attaques utilisé par les États pour parvenir à leurs fins.**

Katrin Suder
Experte en stratégie (technologies numériques, entrepreneuriat et politique)

de personnes malintentionnées. L'enseignement public en a notamment fait les frais. L'an dernier, l**e coût moyen d'une violation de données perpétrée avec succès contre le secteur de l'éducation était de 3,65 millions de dollars**.[3] En 2023, le groupe Vice Society[4] a été l'un des cartels de cybercriminels les plus actifs contre les écoles et les universités, avec pas moins d'une cinquantaine d'établissements pris en otage depuis ses débuts en 2021. Ces attaques, dont beaucoup étaient dirigées contre le Royaume-Uni, se soldaient par la divulgation d'informations sur les étudiants, de scans de passeports, de détails sur le salaire du personnel, ainsi que sur les contrats de travail. Partout en Europe, les hackers sont parvenus à mettre à mal des réseaux et des infrastructures informatiques : les universités françaises[5] et allemandes ont ainsi été visées[6], tout comme la plateforme d'examen en ligne du lycée

1 **IBM (2023).** Rapport 2023 sur le coût d'une violation de données.
2 **Microsoft (2022).** Rapport sur la défense numérique de 2022 de Microsoft.
3 **IBM (2023).** Rapport 2023 sur le coût d'une violation de données.
5 **Le Figaro étudiant (2023).** L'université d'Aix-Marseille a été secouée par une cyberattaque.
6 **B2B Cyber Security (2023)** Attaque de pirate informatique : l'université des Sciences appliquées de Karlsruhe complètement paralysée.

national grec, qui a été sérieusement perturbée par une attaque DDoS.[7]

De plus en plus menacées par les cyberattaques, les administrations publiques du monde entier sont soumises à une énorme pression. Le mois de juillet 2023 a été marqué par un incident de grande ampleur qui a touché le portail eCitizen du Kenya.[8] Le piratage de cette plateforme qui permettait l'accès à plus de 5 000 services publics numériques a paralysé des fonctionnalités essentielles comme les demandes de passeports, de visas touristiques, de permis de conduire, de cartes d'identité ou de dossiers de santé. Cette attaque a également interrompu, par ricochet, les services de banque en ligne et de transport : des dommages collatéraux qui montrent combien nos systèmes modernes sont interdépendants et vulnérables.

Cet incident a souligné une triste réalité : dans la complexité du contexte géopolitique actuel, les **gouvernements sont vulnérables aux menaces cyber**, que ce soit au niveau local, étatique ou fédéral. Ces attaques peuvent avoir **de lourdes conséquences, et compromettre non seulement des données sensibles, mais aussi la sécurité publique**. Les effets potentiels ne se limitent pas aux interruptions de services. Les infrastructures essentielles peuvent, elles aussi, être impactées, ce qui pourrait provoquer des crises économiques, voire mettre en danger des vies humaines. Sans compter que le processus de restauration, après ces attaques, est souvent long et coûteux, qu'il puise dans les ressources publiques et sape la confiance qu'inspiraient les entités concernées. La vulnérabilité de plus en plus marquée de ces instances est particulièrement manifeste dans le secteur de la santé, un domaine où la protection et la disponibilité des données sont d'une importance vitale. Dans la partie consacrée à cette question de son dernier rapport, l'Agence de l'Union européenne

7 **News 24 (2023).** Le ministère grec de l'Education cible d'une cyberattaque, la plus importante de l'histoire du pays.

8 **Africa Cybersecurity Magazine (2023).** Cyberattaque par Anonymous Sudan : de nombreux services en ligne paralysés au Kenya.

pour la cybersécurité (ENISA)[9] révèle que **près de la moitié des attaques par rançongiciel lancées contre les établissements de santé publics aboutissent à des fuites ou à des violations de données**. En mars dernier, l'hôpital public de Barcelone, en Espagne, a ainsi été victime du ransomware « RansomHouse »[10] et contraint, face à l'ampleur de la cyberattaque, de suspendre 150 opérations chirurgicales non urgentes et près de 3 000 consultations externes.

Au cours de l'année écoulée, le nombre d'attaques perpétrées contre des institutions sanitaires en Europe n'a cessé d'augmenter. En décembre 2023, ce fut au tour du réseau hospitalier allemand Katholische Hospitalvereinigung Ostwestfalen (KHO) d'être frappé par un rançongiciel[11] qui a provoqué des interruptions de service dans trois hôpitaux. Quelques mois plus tôt, un hôpital de Bruxelles avait lui aussi fait les frais d'une cyberattaque obligeant la centrale[12] à dévier les ambulances vers d'autres établissements hospitaliers. Dans ce dernier cas, un plan d'urgence mis au point avant l'incident a permis de relancer rapidement les serveurs, de sorte qu'ils étaient de nouveau pleinement opérationnels dès le lendemain de l'attaque. Cet épisode souligne **l'intérêt de la prévention et d'un plan de réponse rapide aux cyberattaques.**

Il est **malheureusement assez rare** que des entités du secteur public **parviennent à se remettre rapidement de telles cyberattaques**, car elles pâtissent souvent de **budgets insuffisants, d'outils obsolètes et d'équipes en sous-effectif**. Beaucoup d'instances publiques manquent de moyens pour mettre en place des mesures préventives adéquates en matière de sécurité. Le rapport de l'ENISA a, par exemple, révélé que[13] seulement 27 % des établissements de santé disposaient d'un programme de défense dédié aux rançongiciels et que 40 % d'entre eux négligeaient la sensibilisation du personnel qui ne travaille pas dans le domaine informatique. Il faut inverser cette tendance **et adopter des mesures de prévention**, telles que des audits de sécurité et une architecture Zero Trust. Il est également essentiel **d'instaurer une culture de la cybersécurité par le biais d'une formation de sensibilisation personnalisée** et adaptée aux besoins de chaque entité. Ces points sont, non seulement, essentiels pour protéger les structures ciblées par les cyberattaques, mais aussi pour la sécurité de tous, dans la mesure où ces organismes sont au service du public.

9 **ENISA (2023).** ENISA Threat Landscape: Health Sector.

10 **IT-Connect (2023).** Un hôpital public de Barcelone victime du ransomware RansomHouse.

11 **The Breach Trace (2023).** Le ransomware Lock bit perturbe les soins d'urgence dans les hôpitaux allemands.

12 **Le soir (2023).** Retour à la normale au CHU Saint-Pierre cible d'une cyberattaque.

13 **ENISA (2023).** ENISA Threat Landscape: Health Sector.

CHECKLIST

Bonnes pratiques en matière de sécurité

- **Analysez et évaluez les risques :** considérez l'analyse et la gestion des risques comme des rouages essentiels de votre activité. Intégrez-les aux processus à intervalles réguliers, en particulier lorsque vous implémentez de nouvelles technologies ou planifiez les opérations. L'évaluation des risques cyber est indispensable pour établir une base de référence en matière de risques, garantir la conformité aux réglementations en vigueur et préserver l'intégrité des données.

- **Nommez des responsables de la transition numérique :** les dirigeants du secteur public doivent penser à nommer un chef de service expert en transition numérique, par exemple un responsable de la sécurité des systèmes d'information (RSSI). C'est à lui que revient la charge de diriger les stratégies de sécurité numérique.

- **Adoptez une architecture Zero Trust :** cette approche a, pour principe directeur, de « ne jamais faire confiance sans avoir vérifié auparavant ». Chaque requête est donc soumise à authentification comme si elle provenait d'un réseau ouvert. Étant donné la multiplication des cyberattaques complexes visant le secteur public, il est particulièrement important, aujourd'hui, d'avoir recours à une telle architecture.

- **Tirez des leçons des incidents passés et anticipez :** mettez à profit ce que vous avez appris lors des incidents antérieurs pour améliorer votre procédure générale de gestion des risques. Élaborez également un plan d'intervention en cas d'incident et mettez-le régulièrement à jour. Ce plan doit préciser les différentes étapes à suivre en cas de cyberattaque pour garantir une réponse rapide et efficace qui limitera les dégâts.

- **Faites régulièrement des audits de sécurité :** réalisez des audits de sécurité fréquents et complets. Ils vous aideront à identifier les points faibles du système. Grâce à cette approche proactive, vous pourrez remédier aux éventuelles vulnérabilités avant que les cybercriminels ne s'y engouffrent.

- **Proposez des programmes de formation personnalisés :** formez régulièrement le personnel en adaptant les enseignements aux besoins de l'organisme et aux fonctions des différents collaborateurs. Proposez, par exemple, des modules spécialement conçus pour les établissements de santé, qui traitent des techniques d'ingénierie sociale les plus utilisées dans ce secteur. Pensez également à personnaliser les simulations de phishing en fonction du domaine d'activité concerné.

INTERVIEW

John Noble

Non-executive director et chair of the Cyber Security Committee de NHS Digital en Angleterre

John Noble a dirigé, de 2016 à 2018, le service de gestion des incidents au National Cyber Security Centre (NCSC) britannique. Il y a organisé la réponse à près de 800 cyberincidents majeurs, contribuant à faire du Royaume-Uni le pays le plus sécurisé pour les activités commerciales en ligne. Il est aujourd'hui l'un des non-executive directors du NHS Digital (rattaché au système de santé publique britannique, le National Health Service) où il préside le comité de cybersécurité et d'assurance de l'information.

« Le partage d'informations entre gouvernements et l'instauration de collaborations entre le privé et le public nous permettront de mieux comprendre les menaces émergentes.

Qu'est-ce que le National Cyber Security Center (NCSC) et quelle est sa principale raison d'être?

Nous devons la création du NCSC à une prise de conscience politique de Gordon Brown qui était, à l'époque, Premier ministre. Constatant que la société s'orientait vers une transition numérique, avec tous les risques propres aux activités sur le Net, le gouvernement a compris qu'il était nécessaire de créer un organisme capable de prodiguer des conseils et de l'assistance.

Pourquoi avez-vous décidé d'intégrer le NCSC au service de renseignement GCHQ ?

L'intégration du centre NCSC dans le service de renseignement Government Communications Headquarters (GCHQ) était une décision stratégique. Du fait de son expertise en défense des réseaux et de son statut bien établi d'agence spécialisée en cybersécurité, le GCHQ était l'instance idéale pour chapeauter le NCSC.

Quel est le rôle du NCSC ?

Au début, il nous a fallu comprendre comment le service public, et le NCSC en particulier, pouvaient le mieux contribuer à faire du Royaume-Uni l'endroit le plus sûr pour les activités commerciales en ligne. Nous avons réalisé qu'il nous fallait partager notre expérience au niveau du gouvernement et instaurer un partenariat entre le public et le privé.

Pourquoi une collaboration entre le public et le privé est-elle si importante dans le cadre des efforts de cybersécurité ?

Chacun de ces deux secteurs a des atouts qui lui sont propres en matière de cybersécurité. Le NCSC analyse donc comment les instances gouvernementales peuvent fournir les moyens nécessaires à une collaboration entre les deux. Deux initiatives sont nées de cette réflexion : le partenariat de partage d'informations « Cyber Information Sharing Partnership » (CISP) qui permet aux sociétés d'échanger des informations sur les menaces cyber en temps réel de manière anonyme, et l'initiative Cyber 100 dans le cadre de laquelle des experts du secteur privé sont sollicités pour partager leurs connaissances avec le NCSC.

Certaines sociétés hésitent à faire connaître leurs vulnérabilités aux entités publiques parce qu'elles craignent que ces informations ne se retournent contre elles. Comment leur faire comprendre que le but du gouvernement est d'aider les entreprises, et non de leur nuire ?

La notion de confiance et de transparence est essentielle. Si un service de renseignement découvre une vulnérabilité dans un élément logiciel, mais ne communique pas cette information, les cybercriminels vont s'y engouffrer. Les entités comme le NCSC doivent construire une relation de confiance avec les sociétés afin de pouvoir partager les preuves de ces vulnérabilités. Ces échanges peuvent être le début de relations très précieuses et très profitables avec les entreprises.

« Au sein du gouvernement, nous assistons aussi à une évolution des mentalités : notre priorité no 1 est désormais de protéger notre économie en ligne et donc, les sociétés qui la font vivre.

Je pense qu'au sein du gouvernement, nous assistons aussi à une évolution des mentalités : notre priorité no 1 est désormais de protéger notre économie en ligne et donc, les sociétés qui la font vivre. Les gens doivent comprendre que la protection de notre économie numérique passe nécessairement par le partage d'informations avec les instances gouvernementales.

D'après ce que vous avez pu observer au cours des dernières décennies, quelles sont les grandes thématiques qui se dégagent du paysage des menaces ?

Le paysage des menaces, et notamment la cybercriminalité, ont énormément évolué au cours de ces dernières décennies. L'un des points les plus frappants est l'explosion du rançongiciel qui s'est transformé en un écosystème complexe et spécialisé. Les groupes de hackers comme Conti s'organisent désormais en structures qui ressemblent à celles de véritables entreprises, avec des hiérarchies, différents départements et des postes bien distincts. Lorsque les autorités parviennent à démanteler certaines de ces organisations, ces dernières en tirent des leçons, changent de mode de fonctionnement et s'adaptent.

Nous assistons de plus en plus à un phénomène étrange : les cybercriminels parviennent à pénétrer dans des systèmes, mais ils n'y font rien de spécial. Comment expliquer ces agissements ?

Lorsqu'une vulnérabilité est découverte, les pirates informatiques s'y engouffrent et vont poser un implant dans plusieurs entreprises différentes.

Ainsi, ils pourront revenir plus tard. C'est souvent ce qu'il se passe avec les infrastructures critiques : il est important de corriger rapidement les vulnérabilités.

La résolution des vulnérabilités peut s'avérer particulièrement compliquée dans le secteur public, puisque les entités exploitent des systèmes qui fonctionnent 24 h/24. Pouvez-vous nous expliquer comment le NHS, le système de santé britannique, gère cette difficulté ?

Le NHS a tiré d'importantes leçons des incidents passés comme l'attaque de WannaCry qui avait tiré parti d'une vulnérabilité que nous connaissions, mais que de nombreuses structures hospitalières n'avaient pas corrigée. Cet incident a non seulement eu un impact financier sur les établissements touchés, mais a aussi affecté la prise en charge des patients.

Pour remédier aux vulnérabilités dans les systèmes de santé, nous avons mis en place deux stratégies principales. La première consiste à identifier clairement les vulnérabilités critiques que les hackers exploitent activement et qui nécessitent un correctif de toute urgence. La seconde implique la définition de normes explicites auxquelles les entités sont tenues de se conformer.

Quel impact la centralisation des systèmes de santé, comme c'est le cas au Royaume-Uni avec le NHS, a-t-elle sur la gestion des risques cyber et des vulnérabilités ?

Les conséquences sur la gestion des difficultés liées à la cybersécurité sont à la fois positives et négatives. Ce qui est positif, c'est que plus un système est centralisé, plus les critères et les attentes sont bien définis, ce qui facilite la communication et le renforcement des mesures de cybersécurité dans tout le réseau. Cette approche centralisée améliore également la prise en charge des patients et la réactivité en cas de vulnérabilité. Mais elle s'accompagne d'autres problèmes : lorsqu'un système est centralisé, il suffit qu'un élément soit compromis pour que d'autres parties soient également touchées. Une seule faille peut donc avoir des répercussions plus importantes dans l'ensemble du système.

En quoi les événements géopolitiques contribuent-ils à alimenter les menaces cyber ? De quelle manière cela influe-t-il sur les relations entre les entités publiques et privées ?

Dans l'analyse d'une menace, il y a deux aspects à prendre en considération : les intentions de l'attaquant et ses capacités. Lors d'événements comme l'invasion de l'Ukraine, nous avons vu des États-nations mener des cyberattaques dans l'intention de soutenir leur effort de guerre. Pour ce qui est des capacités, nous constatons que ces États-nations développent des moyens qu'ils retournent ensuite contre nous.

Qu'en est-il de l'hacktivisme ?

Le conflit russo-ukrainien a entraîné une recrudescence de l'hacktivisme, dans les deux camps. Tandis qu'une cyberarmée ukrainienne menait des attaques contre les sociétés russes, les médias, etc., de nombreux groupes, comme KillNet par exemple, se sont rangés aux côtés de la Russie, en perpétrant des attaques DDoS explicitement dirigées contre les pays soutenant l'Ukraine.

Existe-t-il une zone grise entre le piratage informatique motivé par le gain financier et celui qui sert une cause politique ?

Normalement, un État renonce à l'utilisation de la cybernétique en raison des conséquences potentielles, notamment des désagréments qui peuvent en résulter. Cependant, dans un contexte comme celui de la guerre en Ukraine, les États n'accordent aucune importance à ce que les autres peuvent penser de leurs actions, ni aux retombées possibles.

Alors que nous avions mis en place des mesures très efficaces pour lutter contre les groupes de hackers, nous sommes aujourd'hui dans une

situation où ces mêmes criminels collaborent avec des gouvernements. Les principaux responsables politiques russes en sont même à envisager la légitimation des cyberattaques. Ce serait terrible d'en arriver là et j'espère sincèrement que nous n'irons pas aussi loin, car cela signifierait qu'un pays autorise les crimes perpétrés contre d'autres nations.

Dans le cadre de ces collaborations entre États-nations et cybercriminels, quelles sont les autres stratégies utilisées par les gouvernements ?

Le déni avant tout : les pays s'efforcent de cacher le fait qu'ils ont tiré les ficelles de certaines actions. Ces États-nations utilisent, par exemple, de nombreux outils également exploités par les groupes de cybercriminels, afin de pouvoir nier toute implication dans les attaques qu'ils ont menées. Par exemple, si un implant disponible dans le commerce est découvert au niveau d'une infrastructure essentielle pour un pays, il sera très difficile de prouver si c'est le fait ou non d'un État-nation. Le gouvernement qui se cache derrière cette attaque aura beau jeu de le nier. Comme ces outils sont accessibles facilement, l'État peut puiser dans cet arsenal de piratage en toute impunité.

Nous parlions à l'origine de la Russie, mais vous venez d'évoquer d'autres pays. Quels autres acteurs jouent un rôle important dans le paysage des menaces cyber ?

Si l'on considère certains aspects stratégiques très importants, on ne peut pas ne pas aborder l'influence croissante de la Chine : dans le conflit en mer de Chine méridionale, dans son attitude vis-à-vis de Taïwan, mais aussi de ses autres voisins comme les Philippines. Les capacités de la Chine en matière de cybernétique se sont considérablement accrues, avec une sophistication de plus en plus marquée et le recours à de nouvelles attaques zero-day. Pour éviter les conflits, le gouvernement a réformé son service de renseignement et adopté une structure beaucoup plus professionnelle. La Chine a également diversifié ses centres d'intérêt. Elle cultive une vision à long terme qui lui permet de renforcer ses capacités au fil du temps.

En Europe et au Royaume-Uni, en revanche, nous avons une approche cohérente en matière de cybersécurité et nous avons réalisé qu'il nous fallait être plus stratégiques, plutôt que de nous contenter de réagir aux derniers événements.

Que peut-on faire pour endiguer les menaces cyber, notamment celles posées par les APT (Advanced Persistent Threats) ?

Le partage d'informations entre gouvernements et l'instauration de collaborations entre le privé et le public nous permettront de comprendre plus en profondeur les menaces émergentes. En partageant les indicateurs de compromission (IoC) et en instaurant une relation de confiance entre le public et le privé, nous pouvons dépasser les sensibilités d'ordre commercial et faire front ensemble pour détecter les menaces et y réagir efficacement.

Écouter le podcast →

Cette interview vous a plu ?

Écoutez-la dans **sa version intégrale**, dans notre podcast Human Firewall. Suivez l'échange entre notre PDG, Niklas Hellemann, et John Noble, avec de nouveaux éclairages sur l'importance d'une collaboration internationale en matière de cybersécurité.

7 Le pretexting et les attaques menées sur plusieurs canaux rendent les cyberattaques plus dangereuses

Pour tromper et manipuler leurs victimes en vue d'obtenir un gain financier ou de dérober des données sensibles, les cybercriminels ont de plus en plus recours à des méthodes sophistiquées d'ingénierie sociale. Le **pretexting** est l'une d'entre elles : les hackers se font passer pour une personne de confiance et présentent à leur victime un faux scénario pour la piéger. Selon le rapport 2023 publié par Verizon, **50 % des attaques par ingénierie sociale utilisent le pretexting**, c'est dire à quel point les attaquants misent sur la psychologie humaine qu'ils manipulent avec brio.[1]

Les cybercriminels qui pratiquent le pretexting poussent parfois la perversité jusqu'à **faire des recherches sur leur victime en croisant plusieurs canaux** : réseaux sociaux, blogs ou sites Internet, par exemple. L'objectif est de collecter des informations très précises sur la personne pour les réutiliser dans le scénario qu'ils lui raconteront afin de rendre l'histoire encore plus crédible et d'augmenter leurs chances de réussite.[2] Il peut s'agir d'informations sur son lieu de travail, sur sa vie sociale, sur ses animaux domestiques, ses partenaires ou de tout autre détail personnel susceptible de les aider à inventer des histoires convaincantes pour gagner la confiance de leur cible.

Les canaux sur lesquels les cybercriminels trouvent ce type de données ne sont cependant pas uniquement des sources d'informations : ce sont aussi des vecteurs d'attaque. Selon notre Analyse du risque humain 2023, le phishing par e-mail continue de dominer le paysage des menaces et cible encore 61 % des sociétés.[3] Mais les formes d'attaques se diversifient et 34 % d'entre elles passent désormais par les réseaux sociaux. De très nombreuses PME les utilisent, par exemple, pour démarcher de nouveaux clients. L'occasion est trop belle pour les hackers qui cherchent à les ruiner en piratant leurs comptes. C'est ce qu'a vécu une petite entreprise qui vendait du granola sur Instagram.[4] Les attaquants ont contacté la propriétaire sur ce réseau social en se faisant passer pour une autre société qu'elle connaissait et en qui elle avait confiance. Ils lui ont fait croire que l'entreprise participait à un concours et lui ont demandé de cliquer sur un lien pour voter pour elle. Lorsque la revendeuse de granola s'est exécutée, les pirates ont pris le contrôle de son

1 **Verizon (2023).** Data Breach Investigations Report (DBIR) 2023.

2 **The Wall Street Journal (2021).** What Hackers Can Learn About You From Your Social-Media Profile.

3 **SoSafe (2023).** Analyse du risque humain.

4 **CNBC (2023).** Phishing scams targeting small business on social media including Meta are a 'gold mine' for criminals.

compte Instagram et exigé qu'elle leur verse 10 000 dollars pour pouvoir poursuivre son activité sur le réseau social, ce qu'elle a fait. Et il ne s'agit pas là d'un cas isolé. Les cybercriminels ont mille et une façons d'exploiter les réseaux sociaux : par exemple, ils piratent les comptes d'employés pour converser avec des collègues et leur demander des informations sensibles ou les pousser à télécharger des pièces jointes infectées qu'ils présentent comme des documents professionnels.

Les applications de messagerie comme WhatsApp et Microsoft Teams sont également l'un des terrains de jeu favoris des hackers pour interférer dans nos vies privées et professionnelles. Récemment, la police de Calcutta a signalé une série d'attaques menées sur WhatsApp à l'occasion de la journée internationale du yoga. Les hackers envoyaient des messages proposant des cours de yoga.[5] Les destinataires étaient invités à cliquer sur un lien et à partager un code OTP à six chiffres qui, en réalité, permettait aux attaquants d'accéder au compte WhatsApp de leur victime. Ceci fait, les pirates envoyaient des messages pressants à ses contacts pour leur demander de l'argent. L'application professionnelle Microsoft Teams a, elle aussi, été le théâtre de procédés similaires : les attaquants contactaient leurs victimes en expliquant qu'ils faisaient partie de l'équipe de RH et qu'ils souhaitaient les informer de modifications dans leur planning de congés.[6] Les destinataires étaient invités à télécharger un fichier contenant le nouveau calendrier de vacances qui, en réalité, lançait l'installation du malware DarkGate.

Et les cybercriminels ne s'arrêtent pas en si bonne voie. Ils cherchent constamment à perfectionner leurs méthodes pour les rendre plus convaincantes. Ils mènent aujourd'hui des **attaques extrêmement sophistiquées dans lesquelles ils contactent leurs victimes sur plusieurs canaux**, par SMS, par e-mail ou par téléphone. Une habitante d'Archiac, en Charente-Maritime, a ainsi été la cible d'une arnaque par téléphone et par SMS.[7] L'escroc l'a d'abord appelée en se faisant passer pour un agent de la répression des fraudes. Devant la méfiance de la victime, il lui a envoyé la copie de ses relevés bancaires par SMS, y compris le dernier paiement effectué le matin même par carte bancaire. Un dernier message indiquant qu'elle était bien en ligne avec un conseiller de sa banque a achevé de la convaincre. Elle s'est alors laissée guider par son interlocuteur et a effectué les virements qu'il demandait se faisant extorquer, au total, 3 800 euros.

Avec l'essor de l'IA, ces attaques multicanaux gagnent encore en efficacité et en force de conviction. Un employé de Retool, éditeur américain de solutions logicielles pour les entreprises, a ainsi mordu à l'hameçon d'un phishing par SMS.[8] Le message semblait provenir d'un membre de l'équipe informatique et demandait au collaborateur de se connecter sur un faux site Internet pour résoudre un problème avec sa couverture santé. Une fois que l'employé a passé la MFA, les cybercriminels l'ont appelé. En utilisant une voix générée par l'IA qui imitait celle de l'expéditeur du SMS, ils ont réussi à soutirer à leur victime un autre jeton MFA qui, de fil en aiguille, leur a permis d'accéder aux systèmes internes de l'entreprise. Les attaquants ont alors pu prendre le contrôle des comptes de 27 clients et dérober plusieurs dollars en cryptomonnaie.

Alors que les pirates informatiques perfectionnent de plus en plus leurs méthodes et entrent dans une logique de professionnalisation, **nous devons redoubler de prudence et veiller à ce que la cybersécurité devienne une seconde nature au sein de nos équipes**.

5 **The Times of India (2023).** Police warns netizens about WhatsApp hacking, here's how fraudsters hack accounts.

6 **lebigdata.fr (2023).** Microsoft Teams : faites extrêmement attention à cette attaque de phishing.

7 **La Nouvelle République (2023).** « Il m'a envoyé la copie de mes comptes par SMS » : comment une Française s'est fait extorquer 3 800 euros.

8 **Silicon (2023).** La synchronisation cloud des codes MFA pointée du doigt.

CHECKLIST

Bonnes pratiques en matière de sécurité

- **Formez vos équipes à vérifier la provenance des messages et les numéros appelants :** il est essentiel que vos employés sachent contrôler, par eux-mêmes, l'identité des personnes qui les appellent ou leur envoient des messages. Même lorsqu'un appel semble authentique, il vaut toujours mieux contacter l'interlocuteur directement, via un autre canal de confiance, si les demandes semblent suspectes ou concernent des informations sensibles.

- **Vérifiez les interlocuteurs externes :** étendez votre procédure de vigilance à toute personne externe qui interagit avec vos systèmes. S'ils demandent l'accès à des données sensibles, assurez-vous qu'ils respectent les critères de cybersécurité de votre entreprise.

- **Encouragez les collaborateurs à signaler les incidents rapidement, sans les culpabiliser :** instaurez une culture où les employés ont la liberté de signaler immédiatement les tentatives de phishing et les activités inhabituelles, sans craindre les éventuelles répercussions. Ce type d'environnement permet aux équipes de sécurité de réagir rapidement, leur donnant la possibilité de bloquer l'attaque avant qu'elle ne prenne une trop grande ampleur.

- **Actualisez vos politiques de cybersécurité :** pensez à mettre à jour régulièrement vos politiques de cybersécurité pour y inclure les formes d'ingénierie sociale émergentes, comme le pretexting. Ainsi, vos défenses resteront efficaces et solides.

- **Améliorez vos plans d'intervention en cas d'incident :** mettez régulièrement à jour votre stratégie de réponse afin de minimiser l'impact d'attaques par pretexting ou d'autres formes de piratage. Définissez des procédures claires pour détecter, gérer et endiguer ces cyberattaques tout en assurant la continuité de l'activité et la sécurité de l'entreprise. Veillez également à renforcer constamment votre plan d'intervention en cas d'incident et à organiser, de temps en temps, des exercices pratiques pour éviter que les bons réflexes se rouillent.

- **Assurez une formation continue des équipes :** informez-les, en continu, des dernières menaces cyber, telles que le pretexting et les attaques multicanal. Consolidez leurs connaissances en organisant des simulations qui les placent en situation réelle. Enseignez-leur à reconnaître les activités suspectes et à les gérer : vous aurez ainsi des collaborateurs vigilants, capables d'identifier et de désamorcer les éventuelles tentatives d'extorsion.

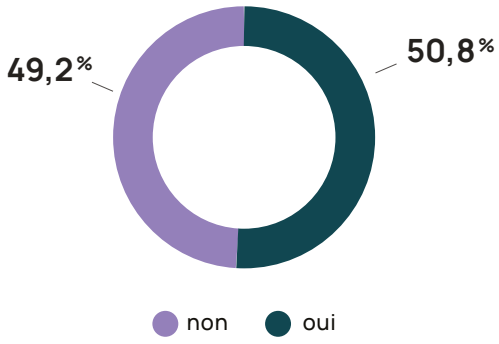
8 L'augmentation des taux de burn-out plonge les équipes de cybersécurité dans des difficultés sans précédent

L'an dernier, nous avions déjà abordé la question du burn-out au sein des équipes de cybersécurité. Or, les récentes tensions sur la scène internationale et la professionnalisation croissante de la cybercriminalité, aujourd'hui assistée par l'intelligence artificielle, ne contribuent pas seulement à dessiner un paysage des menaces plus complexe et plus difficile à détecter. Elles accroissent également la pression qui pèse sur les professionnels. Face à ces déferlements incessants de sollicitations, la résilience et les capacités d'adaptation de nos équipes sont mises à très rude épreuve.

Or, la pénurie en main-d'œuvre qualifiée qui sévit dans ce secteur ne fait qu'empirer la situation. Selon le dernier rapport de l'ISC2, 4 millions de postes restent vacants dans le secteur de la cybersécurité à l'échelle mondiale.[1] L'écart entre le nombre de personnes nécessaires et le nombre de personnes disponibles a ainsi augmenté de 12,6 % entre 2022 et 2023, et se creuse majoritairement en Asie du Pacifique (surtout au Japon et en Inde), ainsi qu'en Amérique du Nord. L'Europe n'est guère en reste puisque son manque de main-d'œuvre en cybersécurité a augmenté de 9,7 % par rapport à l'an dernier. Mais il y a plus grave encore. Selon une étude menée par l'ISACA, les équipes de cybersécurité sont en sous-effectif dans 62 % des sociétés, ce qui augmente dramatiquement la charge de travail pour le personnel en place et pousse souvent **les professionnels à l'épuisement professionnel, voire à la démission**.[2]

Une enquête menée auprès de plus d'un millier de spécialistes de la cybersécurité aux États-Unis et en Europe le confirme : **66 % des personnes interrogées souffrent de stress au travail**, 51 % d'entre elles sont traitées pour des pathologies psychologiques et 19 % consomment plus de trois verres d'alcool par jour pour tenter de décompresser.[3] Or, cette situation ne pèse pas seulement sur les personnes. Elle provoque **un manque d'attention au sein des équipes et les amène à négliger certains détails importants, elle affecte leur réactivité et leur efficacité face aux menaces** et augmente donc significativement le risque de violations de sécurité au sein de leurs entreprises. D'autant que, comme nous l'avons vu, les cybercriminels ne cessent de perfectionner leurs techniques et lancent des attaques de plus en plus sophistiquées.

Un médecin vous a-t-il déjà prescrit un médicament pour traiter votre santé mentale ?



Source : MtoM-mag.com[3]

1 **Le Monde informatique (2023).** 4 millions de personnes manquent à l'appel en cybersécurité.

2 **solutions-magazine (2023).** L'état de la cybersécurité : selon de nouvelles recherches, par manque de cybercompétences, les entreprises sont vulnérables aux attaques.

3 **MtoM-mag.com (2023).** Pénurie de main-d'œuvre qualifiée en cybersécurité : récession ou stress ?

Le piratage d'AccessPress illustre les énormes difficultés auxquelles sont confrontées les équipes de sécurité.[4] Le fournisseur de WordPress a, en effet, connu une cyberattaque de grande ampleur compromettant 40 thèmes et 53 plugins utilisés par plus de 360 000 sites actifs. Image de la grande portée que peut avoir une attaque de la chaîne d'approvisionnement, la porte dérobée installée par les hackers leur a donné accès à de très nombreux sites Internet. Cet incident montre combien les menaces actuelles peuvent être terribles et complexes, impliquant des défis techniques, mais aussi de nombreux aspects humains et psychologiques qui épuisent les équipes de sécurité.

Alors que les services de cybersécurité ont pour mission de protéger les autres unités de l'entreprise et de réagir rapidement en cas d'attaque, ils comptent eux-mêmes parmi les cibles les plus visées par les hackers, comme l'a révélé notre Analyse du risque humain 2023.[5] Les cybercriminels, bien conscients du stress qui pèse sur le personnel de cybersécurité et le rend plus vulnérable, n'hésitent pas à profiter du burn-out ambiant pour mener à bien leurs attaques. Ils traquent les sociétés, identifient celles dont les délégués à la cybersécurité donnent des signes de faiblesse dus à la tension et à la surcharge de travail, et les ciblent en priorité.

Dans ce contexte aussi dynamique que compliqué, **il est important que les entreprises investissent dans leurs équipes de sécurité** en veillant au bien-être de leurs collaborateurs. Il faut voter des budgets appropriés, proposer des plans de carrière qui fidélisent les talents, soulagent le burn-out et prévoient des ressources suffisantes pour mettre en place les mesures de sécurité qui s'imposent. C'est la seule manière pour permettre aux professionnels de travailler efficacement, de contrer les cyberattaques et de renforcer la sécurité.

> **À l'heure actuelle, le problème numéro 1, dans le secteur de la cybersécurité, est le burn-out : il y a trop de données, trop de dossiers et pas assez de temps.**

Stéphane Duguin
PDG de CyberPeace Institute

4 **it-connect (2022).** Une attaque supply chain cible WordPress : 93 thèmes et plugins infectés !

5 **SoSafe (2023).** Analyse du risque humain.

CHECKLIST

Bonnes pratiques en matière de sécurité

Donnez la priorité à la santé mentale et à l'équilibre vie privée-vie professionnelle : développez des programmes pour accompagner les membres de votre équipe de cybersécurité au niveau de leur santé mentale et de leur bien-être. Vous pouvez, par exemple, proposer des horaires de travail flexibles, un accès à des services de conseil et des pauses régulières pour éviter le burn-out.

Installez des outils efficaces de détection des menaces : ayez recours à des outils perfectionnés, tels que des systèmes de détection des menaces augmentés par l'IA, des boutons d'alerte phishing et d'autres outils comme l'assistant d'e-mail de SoSafe PhishFeedback, pour que l'identification des menaces demande moins de temps et de travail.

Automatisez l'analyse des e-mails : installez des outils automatisés spécifiques pour assister l'équipe du Centre des opérations de sécurité (SOC) dans l'analyse des e-mails signalés comme suspects. Ils simplifieront grandement l'évaluation des e-mails susceptibles de contenir des menaces et permettront aux membres du SOC de se concentrer sur des problèmes de sécurité plus importants et plus complexes.

Automatisez les opérations de routine : ayez recours à l'automatisation pour les tâches répétitives, afin de permettre aux professionnels de la cybersécurité de se concentrer sur des aspects plus stratégiques et plus complexes de la cybersécurité.

Encouragez vos équipes à se former et à monter en compétences : proposez des programmes de formation et de perfectionnement qui fourniront à votre équipe les connaissances dont elle a besoin pour gérer les menaces cyber et les technologies qui émergent. Favorisez également l'interdisciplinarité et nommez des responsables de la sécurité au sein d'autres équipes travaillant dans le domaine technologique.

Investissez dans la rétention du personnel : mettez en place des plans de carrière et des programmes de développement personnel pour retenir les talents et limiter le turn-over.

Organisez régulièrement des sessions de feedback et des entretiens d'évaluation : ayez régulièrement des entretiens individuels avec les collaborateurs pour leur faire un retour sur leur travail et recueillir leurs impressions afin de mieux comprendre leurs attentes et d'y répondre.

Il faut s'attendre à ce que l'année 2024 soit marquée par davantage de violations impliquant le facteur humain

Au vu de toutes les tendances de l'année, une conclusion s'impose : **si nous ne concentrons pas nos efforts sur le personnel, notre stratégie de cybersécurité demeure incomplète**. Les hackers l'ont bien compris : ils savent que, pour se donner toutes les chances de réussir, ils doivent jouer sur les émotions humaines. C'est la raison pour laquelle ils continuent à miser énormément sur l'ingénierie sociale, comme nous l'avons vu à plusieurs reprises dans ce rapport.

Selon le Rapport d'investigations sur les violations de données publié par Verizon, 74 % des violations de données étaient attribuables au facteur humain en 2023.[1] Même les secteurs d'activité très tournés vers la technologie prennent aujourd'hui conscience du rôle de l'humain dans ce contexte. Et nous n'en sommes encore qu'au début. **En 2024, le taux de violations impliquant le facteur humain va encore augmenter**, selon le guide des prévisions 2024 de Forrester.[2] Alors que la cybercriminalité se professionnalise et que l'IA fait son entrée sur le terrain, les hackers ont désormais tout en main pour mettre au point des attaques d'ingénierie sociale convaincantes et sophistiquées. Il est donc plus difficile que jamais de faire la différence entre les messages qui sont authentiques et ceux qui sont malveillants. Et plus nos moyens de communication numérique se diversifient, plus les menaces se propagent rapidement.

D'après le baromètre des risques Allianz 2024, les cyberincidents s'annoncent comme le risque no 1 pour les entreprises du monde entier en 2024.[3] Les délégués à la cybersécurité ne peuvent donc plus se permettre de négliger le facteur humain dans leurs stratégies de défense. Le point positif, c'est qu'il existe une mesure efficace pour parer à ce danger : **la sensibilisation et la formation à la cybersécurité**. En mettant la cybersécurité à la portée de tous au point qu'elle devienne une seconde nature, il est possible d'inverser la vapeur. Gardons toujours à l'esprit qu'il ne s'agit pas uniquement d'informatique : les cibles des cyberattaques et ceux qui en paient les conséquences, ce sont les gens. Or, ce sont aussi **les gens qui ont le pouvoir de faire barrage à ces attaques**. Établir une culture de la cybersécurité n'est pas simplement une mission de l'entreprise : c'est aussi une mission personnelle. Ensemble, nous pouvons repousser la menace que fait peser sur nous une cybercriminalité de plus en plus sophistiquée et bâtir notre avenir sous le signe de la sécurité.

1 **Verizon (2023).** Data Breach Investigations Report (DBIR) 2023.

2 **Forrester (2024).** Predictions 2024: Exploration Generates Progress.

3 **Atlas-mag (2024).** Baromètre des risques Allianz 2024 : la cybercriminalité en tête de liste.

Établissez une ligne de défense humaine efficace

La plateforme de sensibilisation SoSafe permet aux entreprises de consolider leur culture de la sécurité en limitant les risques humains. Elle propose une expérience d'apprentissage stimulante ainsi que des simulations d'attaques personnalisées qui enseignent aux employés comment protéger activement la société des menaces en ligne. Chaque outil est développé selon les principes des sciences comportementales pour assurer une formation à la fois ludique et efficace. Des analyses détaillées mesurent les fruits de ce programme en matière d'évolution des comportements et révèlent précisément aux sociétés les lacunes à combler pour assurer une réponse proactive face à d'éventuelles menaces. Facile à déployer et évolutive, la plateforme de SoSafe inscrit en chaque employé des réflexes de sécurité, sans lui demander d'efforts démesurés.

APPRENDRE — Micro-apprentissage intelligent

Une plateforme de formation inspirée des sciences comportementales qui enthousiasme les collaborateurs. Améliorez votre résilience face aux menaces cyber et assurez votre conformité aux obligations légales grâce à une formation dynamique qui joue sur différents canaux pour développer, des réflexes de sécurité qui durent.

- Une pédagogie narrative et gamifiée
- Une bibliothèque de contenus présélectionnés
- Des options de personnalisation et de gestion de contenu qui s'adaptent à chaque entreprise

ENTRAÎNER — Simulations de spear phishing

Des simulations de phishing axées sur l'utilisateur pour développer des réflexes de sécurité. Grâce à nos simulations de spear phishing régulières et automatisées, formez vos employés pour qu'ils sachent détecter les cyberattaques. Vous les aiderez ainsi à adopter des réflexes de sécurité durables dans leurs activités quotidiennes.

- Des simulations de cyberattaques personnalisées et réalistes
- Des explications pédagogiques contextualisées
- Bouton d'alerte phishing qui permet de signaler les menaces en un clic

AGIR —

Suivi stratégique des risques

Protégez votre entreprise contre les incidents et leurs conséquences financières grâce à notre solution d'évaluation du risque humain. Bénéficiez d'un bilan sur l'état de votre couche de sécurité humaine afin de pouvoir anticiper toute vulnérabilité éventuelle. Suivez l'impact de vos programmes, analysez les comportements et prenez des décisions éclairées en matière de protection des données.

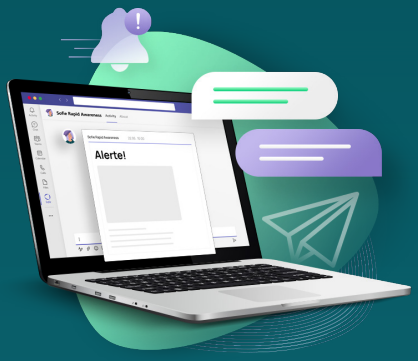
- Des données contextuelles, incluant notamment les ICP techniques et psychologiques
- Des références propres au secteur de l'entreprise et des directives pratiques
- Une solution développée pour répondre aux exigences de la norme ISO/CEI 27001 et conçue selon une approche de « privacy by design »

CONNECTER —

Sofie Rapid Awareness

Les cybercriminels progressent à un rythme effréné… Vous pouvez en faire autant. La formation rapide à la sensibilisation vous permet de vous connecter rapidement avec vos collaborateurs dans MS Teams, pour gérer les menaces qui surgissent avec des micro-apprentissages express, envoyer des alertes en temps réel à votre équipe et leur donner le pouvoir de devenir votre meilleure défense.

- Connexion directe avec votre équipe dans MS Teams
- Gain de temps et facilité de communication
- Envoi de micro-alertes de sécurité faciles à assimiler pour les collaborateurs
- Possibilité de visualiser le nombre de personnes qui ont lu l'alerte pour assurer un maximum de suivi



Human Firewall Conference

HuFiCon est un événement européen dédié à la cybersécurité. Son but est d'aider les professionnels de la sécurité à transformer leurs collaborateurs en **cyber-héros**. Assistez à des débats entre experts et à des ateliers pratiques, et rejoignez une communauté qui s'investit pour placer l'humain au cœur de la cybersécurité.

Ferez-vous partie de celles et de ceux qui façonneront la cybersécurité de demain ?

OÙ ? Halle Tor 2, Cologne

QUAND ? Les 14 et 15 novembre 2024

Inscrivez-vous pour participer à HuFiCon24

Contact

Pour toute question relative à ce rapport et à l'étude réalisée dans ce cadre, veuillez contacter :

Laura Hartmann
Responsable de la communication d'entreprise
press@sosafe-awareness.com

sosafe

SoSafe GmbH
Lichtstrasse 25a
50825 Cologne, Allemagne

info@sosafe.de
www.sosafe-awareness.com/fr
+49 221 65083800