sosafe

Tendances en cybercriminalité 2023

Le point sur les menaces
et les bonnes pratiques

Table des matières

En matière d'innovation, les cybercriminels mènent la course

Plus la technologie évolue et permet à la cybercriminalité de se démocratiser, plus il est important de bien se préparer à d'éventuelles attaques. Avec l'intelligence artificielle et toutes les innovations qui en découlent, les cyberattaques exploitant la fragmentation croissante du monde, les attaques de grande portée ciblant la chaîne d'approvisionnement numérique, le rançongiciel-as-a-service ou le phishing multicanal, les cybercriminels ne cessent d'innover et d'enrichir leur répertoire. En cas d'échec de la technologie à protéger votre entreprise, c'est la vigilance de vos équipes et la solidité de votre culture de sécurité qui feront toute la différence.

Il est donc essentiel de renforcer la résilience face aux risques cyber en gardant toujours une longueur d'avance. Voici les huit dernières tendances en cybercriminalité pour 2023, ainsi que quelques conseils pratiques pour aider les entreprises à se protéger.

01

Essor de l'intelligence artificielle : un moteur pour l'innovation en cybercriminalité

L'intelligence artificielle (IA) s'immisce progressivement dans notre quotidien et les cybercriminels n'hésitent pas à sauter sur l'occasion qu'elle leur offre : ils n'ont pas mis longtemps à comprendre qu'en utilisant l'IA pour leurs tentatives d'ingénierie sociale, ils pouvaient augmenter leurs profits.

Les hypertrucages, et notamment le clonage vocal, ont compté parmi les premières méthodes d'IA utilisées par les pirates pour leurs attaques de vishing (phishing vocal). Ils ont ainsi réussi à duper des employés en leur faisant croire qu'ils s'entretenaient avec des membres de leur entreprise. En 2019 déjà, des criminels s'étaient servis d'un logiciel d'intelligence artificielle pour imiter le PDG d'une société allemande et obtenir que son subordonné, le président d'une filiale britannique, leur transfère 220 000 €.[1] Ces appels assistés par IA peuvent aussi être associés à d'autres stratégies. Il est, par exemple, arrivé que des criminels contactent leurs victimes par téléphone pour leur annoncer l'arrivée d'un e-mail important. Elles ne se méfient donc pas lorsqu'elles reçoivent ce message, qui est en réalité une tentative de phishing. Cette tactique augmente dangereusement les chances de succès des criminels, en rendant leurs e-mails malveillants plus difficiles à déjouer. Et comme si cela ne suffisait pas, le lancement de VALL-E, cette année, menace d'empirer encore la situation. Ce modèle de synthèse vocale développé par Microsoft est en effet capable de générer un discours en imitant n'importe quelle voix à partir d'un enregistrement de seulement 3 secondes.[2]

Pour aussi inquiétante qu'elle soit, l'arnaque vocale n'est cependant qu'une partie du problème, car les cybercriminels attaquent également au moyen de montages vidéo. Début 2022, une fausse capitulation du président ukrainien Volodymyr Zelensky est devenue virale sur les réseaux sociaux. Elle montre les conséquences que peut avoir ce type d'attaques, surtout si l'IA continue d'être perfectionnée.[3] Dans le même ordre d'idées, la maire de Berlin a également été victime d'un deepfake dans lequel son homologue de Kiev, Vitali Klitschko, prétendait s'entretenir avec elle de la guerre en Ukraine par visioconférence. Il lui a fallu 15 minutes d'échange avant de réaliser qu'il ne s'agissait pas du maire de Kiev en personne, mais d'un « cheapfake » utilisant une bande-son truquée pour doubler une vidéo existante. Cet incident illustre bien jusqu'où les imposteurs sont prêts à aller dans la manipulation et avec quelle facilité ils parviennent à dissimuler leurs intentions réelles.[4]

Alors que les hypertrucages ne cessent de gagner en qualité, il est probable que les tentatives d'ingénierie sociale perpétrées cette année soient plus crédibles et donc enregistrent un plus grand taux de réussite. Les experts en droit et en cybersécurité craignent, en effet, que la prolifération des deepfakes sape la confiance dans les vidéos de surveillance, les caméras d'intervention et les autres sources de preuve. Cette situation pourrait ouvrir la porte à toute sorte de cyberharcèlement, de chantage ou de manipulations boursières irrégulières, aggravant l'instabilité politique ambiante.[5]

Toutefois, les deepfakes et toutes les autres méthodes assistées par IA, telles que les systèmes automatisés pour deviner les mots de passe et craquer les CAPTCHA, ne font que marquer le début d'une nouvelle ère. L'IA permet de réaliser des cyberattaques qui gagnent en sophistication et en portée d'heure en heure, et beaucoup d'entreprises ne commencent à s'y préparer que maintenant. L'un des exemples les plus saisissants est l'utilisation de l'IA générative pour envoyer des e-mails malveillants capables de contourner les filtres anti-spam.

Une étude menée en 2021 par l'Agence gouvernementale de technologie de Singapour a révélé que l'IA générative était capable de créer des e-mails de spear phishing très convaincants, avec des taux de clics plus élevés que les messages rédigés par des humains.[6] L'outil utilisé dans le cadre de ces recherches n'était autre que l'ancêtre de ChatGPT, le chatbot aujourd'hui accessible au grand public.

De fait, le lancement de ChatGPT à la fin de l'année dernière confronte les professionnels de la cybersécurité à de nouveaux défis. De nombreux chercheurs se disent préoccupés par ces solutions d'IA générative qui pourraient démocratiser le cybercrime.[7] Avec cet outil gratuit et accessible à tous, n'importe qui peut aujourd'hui générer du code malveillant et des e-mails de phishing réalistes sans avoir besoin de posséder une grande expertise technique. Certains experts affirment même avoir réussi à créer, avec l'aide de ChatGPT, un logiciel malveillant « polymorphe » capable d'échapper à la surveillance des solutions de sécurité traditionnelles.[8]

Les attaques par rançongiciel sont, elles aussi, susceptibles de devenir plus destructrices avec l'aide du ciblage assisté par IA qui permet aux pirates de trouver de nouvelles failles et de nouvelles victimes. D'ailleurs, vu la vitesse à laquelle l'IA évolue, il est probable qu'elle surpassera bientôt certains systèmes biométriques ou sera en mesure d'imiter le comportement humain de telle manière que les comptes dérobés ne puissent pas être repérés par les systèmes de sécurité comportementaux.[9]

Naturellement, l'intelligence artificielle est également utile aux experts en cybersécurité à des fins de défense, par exemple pour la génération de codes de tests ou le cyberrenseignement. Mais, on ne peut nier qu'elle a beaucoup complexifié et exacerbé le paysage des menaces. L'avenir seul nous dira qui, des équipes de cybersécurité ou des hackers, retirera le plus de bénéfices de cette technologie.

CONSEILS PRATIQUES

Comme pour tout nouveau type de cyberattaque, la prévention est la meilleure parade. Il faut que les équipes de sécurité continuent de s'approprier les nouvelles solutions techniques et organisationnelles qui émergent, afin de pouvoir tenir le rythme face aux capacités d'innovation des criminels.

Les outils de threat intelligence alimentés par IA ou l'évaluation des risques de violation des données assistée par IA sont, entre autres, des moyens techniques pour limiter les attaques.

Dans le même temps, la formation continue des employés pour les préparer aux nouveaux scénarios, stimuler leur vigilance et mettre à leur disposition des outils intelligents qui les aident à détecter les attaques permettra aux sociétés de tirer leur épingle du jeu.

Il en est de même pour les équipes de sécurité : en se formant régulièrement, elles pourront limiter les risques de manière constante et réagir rapidement si, malgré toutes les précautions prises, un problème survient.

1 Le Monde (2019). « Deepfake » : dupée par une voix synthétique, une entreprise se fait dérober 220 000 euros.
2 Debugbar (2023). L'IA VALL-E de Microsoft peut cloner votre voix à partir d'un clip audio de trois secondes.
3 NPR (2022). Deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn.
4 Le Progrès (2022). Un deep fake du maire de Kiev a trompé plusieurs maires de capitales européennes.
5 The New York Times (2023). As deepfakes flourish, countries struggle with response.
6 Wired (2021). AI wrote better phishing emails than humans in a recent test.
7 France24 (2023). L'intelligence artificielle ChatGPT et la démocratisation de la cybercriminalité.
8 Gizmodo (2023). ChatGPT is pretty good at writing malware, it turns out.
9 Techmonitor (2022). How AI will extend the scale and sophistication of cybercrime.

02

Indétrônable phishing : l'arme de prédilection des attaquants

En 2023 encore, l'une des tactiques préférées des cybercriminels restera la manipulation psychologique de leurs victimes pour leur dérober des informations confidentielles. Au cours des quelques dernières années écoulées, les attaquants sont devenus des experts en la matière : ils savent influencer les réactions humaines, établir un climat de confiance, créer une sensation de manque, adopter un ton autoritaire ou véhiculer un sentiment d'urgence pour pousser leurs victimes à cliquer sur du contenu malveillant et/ou à divulguer des informations sensibles.

Qu'elles jouent sur la corde de la séduction amoureuse ou du devoir professionnel, ces stratégies d'ingénierie sociale ont déjà rapporté plusieurs milliards à leurs auteurs, ce qui n'empêche pas les attaquants de chercher à les perfectionner toujours plus. L'une de leurs dernières trouvailles est le « Pig Butchering », une escroquerie qui consiste littéralement à « engraisser le cochon avant de le tuer ». Les criminels cherchent à appâter une victime en la contactant par SMS ou sur les réseaux sociaux, les sites de rencontre ou les plateformes de communication. L'échange commence par une simple salutation. Si le destinataire répond, le hacker va tenter d'instaurer une relation d'amitié. Cela fait, il commencera à lui parler des sommes considérables qu'il a réussi à gagner grâce à des investissements en cryptomonnaies pour convaincre la victime d'investir à son tour. Il va alors le diriger vers des sites Web malveillants créés de toutes pièces ou des sites officiels qu'il a détournés. Pour rassurer sa victime, il peut lui proposer un appel vidéo avec son nouvel « ami » ou lui suggérer de retirer un peu d'argent de la plateforme. En 2022, un américain de 52 ans vivant à San Francisco a perdu 1 million de dollars dans un « Pig Butchering » après avoir été contacté par une personne qui prétendait être une ancienne collègue.[10] La conversation de 271 000 mots qu'ils ont entretenue a révélé toute la sophistication des stratégies employées par les cybercriminels pour parvenir à leurs fins odieuses. Il faut s'attendre à ce qu'en 2023, les malfaiteurs exploitent encore davantage les craintes des populations face aux questions économiques et environnementales, et développent tout un éventail de nouvelles techniques.

Dans le cadre professionnel, ces attaques pourraient se présenter sous la forme d'un faux profil LinkedIn, d'une invitation à une réunion sur Zoom envoyée par un pirate qui se fait passer pour un collègue, d'un e-mail frauduleux cachant un logiciel malveillant ou d'un message sur WhatsApp émanant d'un « responsable informatique de l'entreprise » qui vous demande de lui accorder l'accès à l'Intranet. Tous ces exemples sont réellement tirés du contexte de cybermenaces dans lequel nous évoluons aujourd'hui, et ils peuvent tous causer de graves dommages aux sociétés. La plateforme marketing tout-en-un Mailchimp a récemment annoncé avoir été victime d'une violation de données. C'est la seconde attaque de ce genre lancée contre l'entreprise en moins d'une année. L'acteur non autorisé a mené une attaque d'ingénierie sociale sur les employés de Mailchimp. Après avoir dérobé leurs informations d'identification, il a pu accéder à certains comptes Mailchimp via l'un des outils utilisés par les équipes de la société qui sont en contact avec la clientèle.[11] Autre cas impressionnant : certains attaquants ont même organisé un appel Zoom avec leur victime, puis envoyé une URL malveillante dans la barre de discussion pendant l'appel.[12]

Comme nous l'évoquions en parlant de la tendance précédente, ChatGPT-3 et les autres solutions d'IA générative qui imitent le comportement humain peuvent devenir les outils d'ingénierie sociale et de phishing les plus redoutables de notre siècle. Il sera ainsi de plus en plus facile de rédiger des e-mails de phishing qui ne contiennent aucune faute d'orthographe et ont ces caractéristiques de style et de format qui nous servent aujourd'hui d'indices pour distinguer les vrais e-mails des faux. Les pirates pourront même ajouter des nuances en utilisant différents réglages tels que « faire en sorte que l'e-mail semble urgent » ou « créer un e-mail avec le maximum de probabilité que les destinataires cliquent sur le lien ».[13]

Alors que 82 % des compromissions de données impliquent le facteur humain[14], il devient vital de se tenir à la page et de connaître les dernières inventions des cybercriminels, afin de se préparer au nombre incalculable d'attaques d'ingénierie sociale qui vont envahir nos boîtes de réception, outils de communication et réseaux sociaux en 2023.

CONSEILS PRATIQUES

Outre les précautions d'usage telles que les pare-feu et les solutions EDR, il est essentiel de mettre en place une solide culture de la sécurité, au sein des sociétés, pour éviter d'être pris au piège des attaques de phishing.

Les entreprises doivent communiquer avec leurs employés sur l'importance de la sécurité des informations, le mode de fonctionnement des différentes cyberattaques et l'intérêt de signaler à l'équipe responsable de la cybersécurité toute activité suspecte, tout en les incitant à respecter les règlements en vigueur.

La bonne nouvelle est qu'il existe des méthodes efficaces pour y parvenir : des formations de sensibilisation aux simulations d'attaque, en passant par les plateformes d'apprentissage en ligne.

10 Forbes (2022). How one man lost $1 million to A crypto 'super scam' called pig butchering.
11 TechCrunch (2023). Mailchimp says it was hacked — again.
12 ZDNet (2023). Hameçonnage : ces méthodes de plus en plus sophistiquées pour vous tromper.
13 Le Monde Informatique (2023). Comment ChatGPT change la donne dans le phishing.
14 Verizon (2022). 2022 Data Breach Investigations Report.

03

Crises géopolitiques : exploiter la fragmentation croissante de l'espace mondial

Quand il s'agit de manipulation psychologique, les cybercriminels n'ont aucun scrupule. Ils n'hésitent pas, en particulier, à exploiter des sujets de société comme amorces pour leurs attaques de phishing. L'une de leurs méthodes favorites est de semer la panique et l'incertitude pour pousser leur victime à cliquer sur du contenu malveillant ou à divulguer des informations sensibles sous la pression. Ils ont donc fait leurs choux gras de la pandémie de coronavirus : quelques semaines à peine après que la propagation du variant omicron, le Royaume-Uni était la cible d'une attaque massive de SMS et d'e-mails, parfois porteurs du logo de la NHS, le service de santé britannique, et proposant à leurs destinataires des tests PCR gratuits. L'objectif de cette campagne était en réalité de pousser les gens à communiquer leurs informations personnelles.[15]

Cet exemple montre bien que les cybercriminels ne laissent passer aucune occasion pour sévir. Les crises géopolitiques ne font pas exception à la règle. La guerre menée par la Russie contre l'Ukraine s'est ainsi doublée de cyberattaques massives et coordonnées visant aussi bien des infrastructures dans ces deux pays que dans le monde entier. Ainsi, un groupe de hackers basé en Russie a ciblé plusieurs ONG aux États-Unis, les armées de plusieurs pays d'Europe de l'Est et un centre d'excellence de l'OTAN afin de dérober les identifiants de connexion à des fins d'espionnage ou de propager des logiciels malveillants.[16]

Et ce ne sont là que quelques-uns des grands événements qui ont bouleversé notre société au cours de ces dernières années. Après des décennies de mondialisation croissante, le monde semble maintenant s'engager dans la voie de la démondialisation. Si les premiers signes de cette nouvelle tendance sont apparus dès 2008, elle s'est récemment accélérée avec la compétition stratégique que se livrent les États-Unis et la Chine en matière de commerce bilatéral, de flux d'investissement et de technologie.[17] Or, alors que les relations entre Washington et Pékin ne cessent de se détériorer en raison d'événements tels que la pandémie de coronavirus et la crise taïwanaise[18], nous commençons d'ores et déjà à en constater les effets : plus grande volatilité dans les chaînes d'approvisionnement, inflation, changements démographiques, et même pénurie alimentaire et énergétique.

Ces crises mondiales ont mêlé de manière inextricable la géopolitique et la cybersécurité. C'est ainsi que, l'année dernière, plusieurs sites officiels taïwanais ont été désactivés à la suite de cyberattaques par déni de services (DDoS). Les soupçons se sont portés sur la Chine qui venait de manifester son opposition à la visite de la présidente de la Chambre des représentants des États-Unis, Nancy Pelosi, à Taïwan.[19] Ces piratages n'ont pas seulement affecté les organismes publics, mais aussi des structures privées dans le monde entier. Au cours du second semestre 2021, la Chine a largement été blâmée pour une série de cyberattaques visant à s'emparer de secrets industriels, d'informations commerciales et d'études sur des vaccins.[20] Les États-Unis, la Grande-Bretagne et d'autres alliés ont ainsi été visés et ont attribué ce piratage de Microsoft Exchange à des hackers affiliés au gouvernement chinois.[21]

Dans un contexte où les DDoS, ainsi que d'autres types de cyberattaques, sont de plus en plus utilisés sur l'échiquier géopolitique, les cybercriminels vont, de toute évidence, s'adapter aux principales vulnérabilités des zones géographiques et des secteurs d'activité qu'ils ciblent. Il n'y a pas de marche arrière possible : la technologie et l'informatique se sont politisées. Désormais, les institutions publiques comme les entreprises privées des pays où les tensions géopolitiques s'intensifient devront mettre en place des stratégies de sécurité cohérentes pour réduire au maximum leurs risques cyber.

CONSEILS PRATIQUES

En tant qu'individus ou sociétés, nous n'avons généralement aucune influence sur les conflits géopolitiques, mais nous pouvons nous préparer à ces nouveaux défis du cyberespace pour savoir comment y répondre. Les exigences légales se durcissent et il est temps, pour les entreprises, d'investir dans un renforcement de leurs mesures de sécurité, de revoir leurs procédures actuelles et de corriger leurs vulnérabilités.

Face à un contexte géopolitique dans lequel les attaques se diversifient et se multiplient, la cyberrésilience dépend fortement du sérieux avec lequel les sociétés se préparent aux différentes menaces. Cette préparation inclut aussi des mesures au niveau de la chaîne d'approvisionnement. Il faut identifier les processus sensibles et les ressources qu'ils requièrent pour prévoir des plans afin d'assurer la continuité des opérations en cas d'attaque réussie chez un fournisseur.

Dans la lutte sans merci que se livrent hackers et cyberexperts, la capacité à adapter constamment les procédures de réponse aux incidents et de récupération en fonction des évolutions du contexte peut faire une grande différence. D'ailleurs, puisque la cybersécurité est devenue affaire de politique, il est temps pour les entreprises de faire remonter cette thématique au niveau de l'exécutif et de lui accorder toute l'attention et les ressources qu'elle mérite.

15 The Independent (2021). Scam warning over fake omicron testing text messages.
16 L'Usine Digitale (2022). Des cyberattaques ont ciblé des structures militaires internationales, d'après Google.
17 Bruegel (2020). Deglobalisation in the context of United States-China decoupling.
18 Reuters (2022). U.S.-China relationship bleeds by a thousand cuts.
19 NBC News (2022). Taiwanese websites hit with DDoS attacks as Pelosi begins visit.
20 InfoSecurity Magazine (2022). How geopolitical tension creates opportunities for cyber-criminals.
21 Siècle Digital (2021). Piratage de Microsoft Exchange : l'UE, l'OTAN, et les États-Unis désignent la Chine.

ENTRETIEN

« La cybersécurité est un processus d'adaptation constante, car les vecteurs d'attaque ne cessent de changer. »

Ulrich Irnich
Directeur des systèmes d'information et responsable du « Modernization Garage », chez Vodafone Allemagne

Ulrich Irnich est directeur informatique au sein du groupe européen de télécommunications Vodafone depuis 2020 et responsable d'un système informatique axé sur le client. Il dirige également le « Modernization Garage » international, dont la mission est d'impulser une modernisation BSS au sein de Vodafone. Il était auparavant directeur informatique chez Unitymedia où il s'est occupé de la transformation agile de l'informatique et des opérations. Il a fait évoluer la société d'une vision orientée projets à une approche davantage centrée sur le produit. Sa grande expérience des télécommunications lui permet d'avoir une compréhension très fine du monde de l'entreprise et de la transformation numérique.

Tôt ou tard, toutes les entreprises sont la cible d'une cyberattaque. Pourtant, on n'en parle pas beaucoup. Pensez-vous qu'il faudrait davantage de dialogue autour de ce problème ?

Oui. Mais les gens ne sont pas encore assez ouverts sur la question. Les sociétés peuvent avoir l'impression qu'attirer l'attention sur ce genre d'incidents est perçu comme un aveu de faiblesse, de culpabilité ou de gêne. Les hacktivistes et les hackers éthiques font leur possible pour s'assurer que chacun apprenne de ses erreurs. Récemment, au cours de notre « Vodafone Elevation Tour », nous avons essayé d'aborder le sujet des cyberattaques qui ont réussi, mais le public est resté plutôt réservé.

Les sociétés ayant déjà été touchées n'ont réellement surmonté leurs hésitations que lorsque les intervenants sur le podium ont commencé à parler ouvertement de cyberattaques.

Les cyberattaques qui sévissent actuellement sur fond de crises géopolitiques et de guerres ne sont que la partie émergée de l'iceberg. Quel est votre avis sur la question ?

Il est vrai que nous avons assisté, dans le sillage de la guerre en Ukraine, à une démultiplication des incidents de cybersécurité. Mais beaucoup ignorent que nous avancions en terrain miné, avant même que la guerre ne soit déclarée.

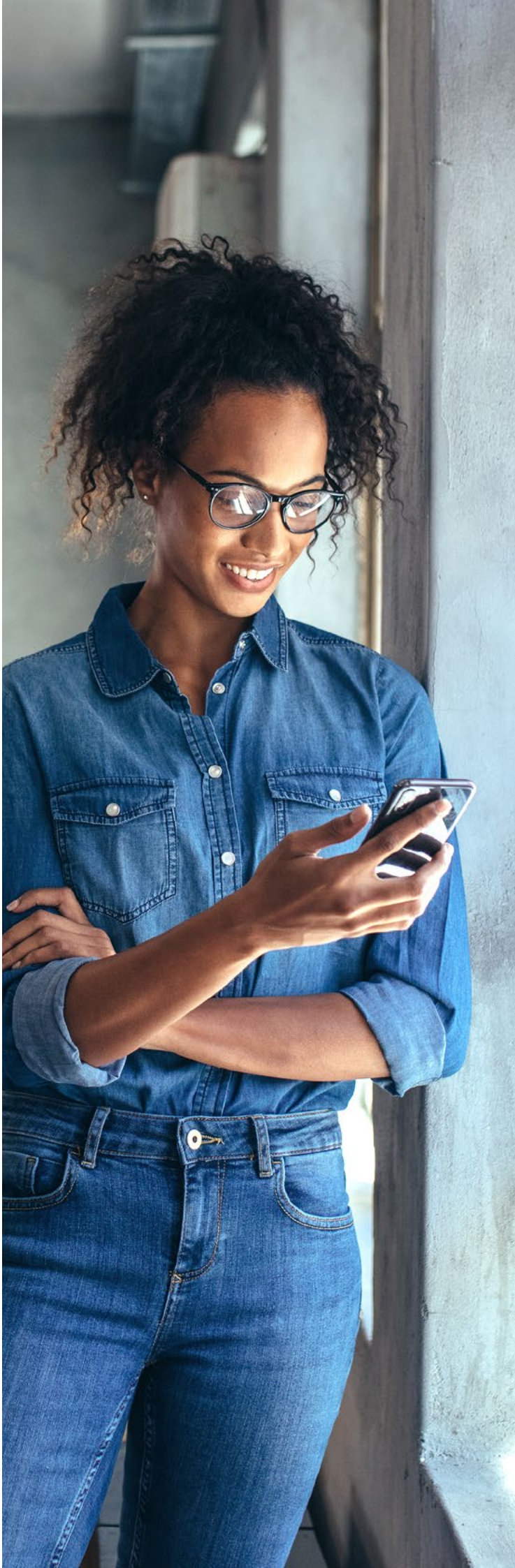
C'est particulièrement le cas concernant la prolifération des attaques par rançongiciel : le nombre de cas non signalés est probablement très élevé. Ces attaques à large échelle sont de plus en plus fréquentes, parce que les schémas exploités par les cybercriminels dans les contextes professionnels ont gagné en attractivité.

Les stratégies d'attaques évoluent-elles à mesure que la cybercriminalité se professionnalise?

Les stratégies se professionnalisent également. Jusqu'ici, nous pouvions repérer les e-mails de phishing du premier coup d'œil, mais aujourd'hui les attaquants ont des tactiques plus sophistiquées et jouent sur davantage de canaux, avec plus de données. Il suffit, par exemple, qu'un seul compte soit compromis pour qu'une attaque soit menée sur toutes sortes de plateformes. Cependant, la plupart des attaques suivent un schéma type : elles commencent par de petites « bombes » lancées à large échelle pour déterminer quelles sont les cibles valables. C'est une sorte d'étude de marché qui précède l'attaque en elle-même.

À votre avis, quels sont les plus grands dangers auxquels sont actuellement exposées les sociétés ?

Outre les rançongiciels que j'ai déjà évoqués, les plus grands dangers sont l'ingénierie sociale, les attaques par force brute, les menaces persistantes sophistiquées et les attaques qui sont lancées de l'intérieur.



En 2013, Vodafone a été la cible d'une attaque par rançongiciel importante. Ces méthodes d'extorsion ont-elles évoluées depuis, que ce soit pour votre groupe ou pour vos partenaires commerciaux ?

Je tiens avant tout à souligner que, depuis 2013, nous avons énormément investi dans notre cybersécurité pour augmenter son niveau de maturité en améliorant à la fois les mesures de prévention et notre capacité à réagir de manière appropriée. Cela ne veut pas dire que nous sommes désormais hors d'atteinte, mais nous avons beaucoup limité les risques.

Le problème est qu'aujourd'hui, les cybercriminels peuvent rentabiliser les données clients bien davantage qu'il y a encore quelques années. Celles-ci sont revendues sur le marché noir pour des sommes colossales. Les rançongiciels restent la principale menace, en particulier pour les entreprises, mais les méthodes d'extorsion ont changé. Autrefois, les logiciels malveillants étaient plutôt envoyés de manière aléatoire, tandis qu'aujourd'hui, les cybercriminels ciblent spécifiquement les entreprises ayant les reins solides sur le plan financier. Lorsqu'ils ont infiltré leurs systèmes, ils espionnent le réseau, les comptes et les mots de passe tout poursuivant l'infection par rançongiciel avant de demander une rançon.

Vodafone est un groupe opérant sur des infrastructures critiques, et nous devons donc, tout spécialement, protéger notre système, ainsi que les données clients.

À votre avis, quelle est la meilleure réponse en cas d'attaque par rançongiciel : faut-il payer ou non ?

La réponse va dépendre du contexte. Il peut y avoir des situations où vous n'avez pas le choix. Linus Neumann a dit un jour : « pas de back-up, pas de pitié ». Il est vital de mettre en place une procédure de réponse aux incidents et de récupération propre à l'entreprise. À titre personnel, instinctivement, je ne paierais pas et je veillerais à ce que les données puissent être reproduites en cas d'incident grave. J'estime que la prévention, la détection, l'expertise en cybercriminalité et la reproduction comptent parmi les étapes les plus importantes. J'encourage les directeurs exécutifs à bien connaître les processus qui sont essentiels à l'activité de leur société. Plus ils peuvent être rapidement opérationnels après une attaque, moins le risque est grand. Plus on laisse de zones d'incertitudes, plus la récupération des données prendra de temps. S'il faut plusieurs semaines, cela peut souvent menacer l'existence même de l'entreprise.

Avez-vous l'impression que la menace qui pèse actuellement au niveau de la direction a entraîné une prise de conscience plus aiguë de ce qu'est la sécurité de l'information ?

Nous faisons régulièrement des simulations de gestion d'incidents cyber avec nos cadres dirigeants. La dernière était sur le thème des rançongiciels et incluait toutes les exigences de notre secteur : communication avec les partenaires commerciaux, négociations, demandes émanant des médias.

La simulation d'une situation de crise place les dirigeants dans un contexte de pression qui leur donne une autre perspective sur les risques encourus.

Il est essentiel d'assurer la continuité dans ce domaine. En effet, si, pendant longtemps, tout fonctionne sans encombre, l'absence d'incidents entraîne une baisse de la vigilance… et c'est précisément à ce moment-là que les criminels frappent. C'est le moment qu'ils attendent pour lancer leurs attaques.

La question n'est pas de savoir si votre société va être piratée, mais quand elle le sera, et dans quelle mesure vous vous y êtes préparé. Vous devez connaître, dès le départ, les risques encourus en cas d'attaque, y compris les risques de responsabilité pour les cadres. Il est également important d'ancrer dans les esprits que la cybersécurité est l'affaire de tous : la protection de l'entreprise n'incombe pas uniquement à l'équipe de sécurité informatique.

> « La protection de l'entreprise n'incombe pas uniquement à l'équipe de sécurité informatique. »

Quels indicateurs utilisez-vous pour attirer l'attention des cadres sur l'importance de la sécurité de l'information ?

Ils donnent une idée claire des risques d'attaques, des conséquences qu'elles peuvent avoir et le profil de risque de la société. Chaque année, nous faisons le point sur les principaux risques et les évaluons.

Les hommes d'affaires ont toujours une bonne compréhension des risques parce qu'ils se traduisent en dommages pécuniaires. Les principales questions qui se posent alors sont de savoir l'ampleur des dommages potentiels et la probabilité d'un événement grave. La menace cyber est le plus grand risque technique qui pèse, à l'heure actuelle, sur l'économie mondiale.

Qui dit sécurité, dit investissements. Or, si les mesures sont efficaces, le retour sur investissement n'est pas visible. Le fait que la cybercriminalité constitue, de loin, le risque le plus important a-t-il contribué à une augmentation des budgets ?

La cybersécurité ne se discute même pas. Nous avons atteint un tel niveau de croissance et de maturité qu'elle est devenue primordiale. C'est une obligation pour nous, dans la mesure où nous sommes un prestataire de services essentiels.

Et qu'en est-il de vos partenaires commer-ciaux ?

Les sociétés qui ont déjà subi des attaques sont beaucoup plus familiarisées avec la question de la cybersécurité. On constate, en particulier, que les entreprises de taille moyenne font de grands progrès en matière de sensibilisation.

Le facteur humain est généralement considéré comme le maillon faible. Psychologiquement parlant, ce n'est pas très motivant de présenter les choses ainsi. Quelles leçons avez-vous apprises en ce qui concerne l'instauration d'une culture de la sécurité ?

Il vaut mieux présenter les choses autrement. Nos ressources humaines ne sont pas le maillon faible, mais plutôt nos meilleurs alliés en matière de cybersécurité. Et par-dessus tout, il est important de partager nos connaissances et d'échanger pour que nous puissions tous apprendre ensemble.

Comment cela se passe-t-il chez Vodafone ? Quelle approche avez-vous adoptée par rapport au facteur humain ?

Chez Vodafone, nous cherchons avant tout à stimuler la vigilance et la résilience de nos équipes. Des collaborateurs bien préparés mentalement sauront mieux se protéger en cas de problème. Nous cherchons, dans tous les cas, à privilégier une approche positive, que ce soit en cybersécurité ou dans d'autres domaines.

Nous avons plusieurs lignes de défense. Et chaque employé est un élément de la stratégie d'ensemble. L'une d'entre elles est l'obligation à se former.

Pour mesurer notre niveau de maturité, nous nous servons d'un modèle « Cyber Security Baseline » avec différents points de contrôle à tous les niveaux de l'entreprise. Nous évaluons ensuite les indicateurs avec un système de notation. Cela représente beaucoup de travail. Certains se plaignent parfois d'avoir toujours trop de choses à faire, mais, en comparaison des conséquences que pourrait avoir une éventuelle attaque, ces plaintes sont vraiment peu de choses. La plupart des gens comprennent la nécessité d'être vigilants et de faire partie intégrante du système de défense de l'entreprise.

> « Nous avons plusieurs lignes de défense. Et chaque employé est un élément de la stratégie d'ensemble. »

Comment faites-vous pour maintenir la vigilance des employés sur le long terme ?

Notre culture de la sécurité a atteint un bon niveau de maturité. Comme les gens se sentent protégés, ils peuvent parfois se montrer négligents au quotidien. C'est la raison pour laquelle nous sensibilisons continuellement nos collaborateurs aux risques, par exemple, au moyen de formations régulières.

On nous a souvent demandé : « Est-ce qu'on ne peut pas être un peu moins rigide sur certains points ? » Or, l'infiltration et l'ingénierie sociale comptent parmi les principales sources de danger. Le secret pour s'en protéger, c'est de maintenir la vigilance sur le long terme.

Selon vous, quelles sont les tendances qui se dessinent pour l'avenir ?

Nous vivons une époque fascinante, à la croisée des chemins : des bandes passantes sans limites, une énorme puissance de traitement à très faible coût, une explosion des volumes de données. Les possibilités sont incroyables.

Prenez le métavers par exemple. Comment savoir si, derrière un avatar, se trouve une personne en chair et en os. C'est tout de suite l'idée de « deepfake » qui vient à l'esprit. Les identités numériques vont devenir un sujet délicat à traiter

Il y a aussi la question des chaînes de blocs. En matière de technologie, il nous reste encore beaucoup de chemin à parcourir, car les processus actuels sont encore trop exigeants pour nos ordinateurs.

Le métavers va également entraîner l'émergence de nouveaux modèles commerciaux. L'intelligence artificielle va se démocratiser. Les méthodes de paiements vont évoluer (NFT, cryptomonnaie…) et les répercussions sur les banques traditionnelles seront énormes.

On peut dire que les mondes numériques et analogiques vont de plus en plus fusionner et le nombre de cibles va augmenter à mesure que les modèles économiques des attaquants se multiplient.

Dès 2018, nous avons commencé à mettre en garde contre des tactiques de deepfake comme le clonage vocal. Selon vous, dans quelle mesure l'intelligence artificielle représente-t-elle un danger ?

De toute évidence, le nombre de nouveaux risques va exploser. Si la technologie permet de systématiser l'information, elle peut aussi devenir une arme. Les progrès de la technologie comportent de nombreux avantages, mais ils ont aussi leur côté obscur.

Si nous ne voyons pas encore, à l'heure actuelle, circuler beaucoup d'e-mails de phishing générés par IA, malgré l'émergence de nouveaux outils comme ChatGPT, c'est plutôt parce que les attaquants parviennent déjà facilement à leurs fins sans avoir besoin de recourir à cette technologie. Mais, dans la mesure où nous sommes tous en train de chercher à renforcer notre sécurité, un jour ou l'autre, ils y viendront. La cybersécurité est un processus d'adaptation constante, et notamment d'adaptation aux nouvelles technologies.

Avez-vous des méthodes concrètes à recommander pour accompagner les employés à cet égard ?

Nous avons, par exemple, un bouton intégré à notre gestionnaire de messagerie qui permet aux utilisateurs de signaler immédiatement les e-mails, en un clic.

Et, naturellement, nous avons aussi pris toutes nos précautions sur le plan technique pour réduire l'impact au maximum en cas de scénario catastrophe. Dans le même temps, nous félicitons ceux qui réussissent. Nous avons lancé un prix spécial, le « Spirit Awards », que nous décernons aux personnes qui contribuent à renforcer la sécurité de notre entreprise. Nous croyons au pouvoir de l'éducation positive plutôt qu'aux réprimandes qui n'offrent que des solutions à court terme. Il s'agit simplement d'inclure le facteur humain, de veiller à ce que chacun ait l'envie et les capacités pour apporter sa contribution active.

En conclusion : comment envisagez-vous les 12 prochains mois ?

Commençons par les points positifs : je pense que l'univers numérique va nous ouvrir beaucoup de nouvelles opportunités pour résoudre des problèmes d'ordre mondial, de nouvelles approches pour lutter contre le réchauffement climatique, par exemple.

Pour le côté négatif, je pense que les attaques vont devenir de plus en plus fréquentes et destructrices. Il nous faut rester vigilants, nous adapter à cette nouvelle réalité et nous préparer tous activement à ce qui se profile.

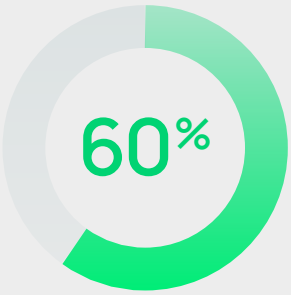
04

Burn-out parmi les équipes de sécurité et le personnel : une autoroute pour les cybercriminels

Un personnel démotivé s'implique incontestablement moins dans les objectifs de son entreprise et cela pèse sur la productivité générale de la société. Pourtant un danger bien plus grand guette : le burn-out chez les collaborateurs, au sein de l'équipe informatique et parmi les professionnels de la cybersécurité pourrait augmenter la vulnérabilité des entreprises aux cyberattaques.

Dans un contexte où les menaces s'intensifient, l'épuisement professionnel sévit chez un grand nombre d'employés en cybersécurité. Au cours des deux dernières années, la pandémie de la COVID-19, la situation géopolitique mondiale et le télétravail ont mis les responsables informatiques et les professionnels de la sécurité à rude épreuve. Les formes de travail hybrides, par exemple, offrent aux pirates la possibilité d'exploiter les failles de sécurité créées par des connexions non sécurisées depuis les domiciles des employés, par l'utilisation de périphériques privés pour des tâches professionnelles et par le recours massif aux outils collaboratifs tels que Microsoft Teams et Slack. Afin de limiter ces risques, les salariés du secteur de la sécurité assument une charge de travail excessive : selon une étude de l'organisme britannique CIISEC (Chartered Institute of Information Security), environ 12 % d'entre eux travaillent entre 51 et 70 heures par semaine.[22]

La surcharge de travail et le burn-out poussent de nombreux professionnels de la sécurité à quitter leur emploi. Une étude menée en 2022 par l'ISACA (Information Systems Audit and Control Association) a révélé que 60 % des entreprises éprouvaient des difficultés à retenir les professionnels qualifiés en cybersécurité. Les niveaux élevés de stress au travail comptaient parmi les cinq principaux motifs de démission.[23] Une pénurie de talents dans le secteur de la sécurité informatique, estimée à 3,5 millions de postes vacants, vient encore aggraver la situation.[24]



des entreprises éprouvaient des difficultés à retenir les professionnels qualifiés en cybersécurité

Résultat : les équipes de cybersécurité en sous-effectif ne parviennent pas à endiguer l'afflux massif de cybermenaces au niveau mondial.

Dans le contexte actuel, il est de la plus haute importance d'allouer les ressources et le budget suffisants aux équipes de sécurité informatique. Le rapport du CIISEC a également montré qu'en 2021, seuls 64 % des entreprises ont augmenté les budgets dédiés à la cybersécurité contre 17 % qui ont conservé un budget identique et 9 % qui l'ont réduit. Parmi les 64 % de sociétés ayant augmenté leur budget, seuls 9 % accordent à leurs équipes de sécurité un financement suffisant pour doubler de vitesse les attaquants. Par rapport aux années précédentes, les statistiques montrent une légère hausse du nombre de sociétés n'augmentant pas leur budget, tandis que le nombre de sociétés qui l'augmente a plutôt tendance à diminuer. Nous sommes donc aujourd'hui dans un contexte où la cybersécurité se complexifie alors que les entreprises n'ont pas les ressources suffisantes.

Le stress, le manque de motivation et les insuffisances budgétaires font le bonheur des cybercriminels. Ceux-ci profitent de l'épuisement des cyberexperts qui sont alors davantage susceptibles de négliger de petits détails et ont plus de mal à trouver des solutions aux problèmes qui surviennent.[25]

Sans compter que ces professionnels surchargés peuvent facilement ne pas percevoir les signes d'une attaque, voire faire eux-mêmes des erreurs (oublier de mettre à jour un logiciel, par exemple), créant des failles dans lesquelles les hackers s'engouffrent.[26] Connaissant les erreurs que peuvent commettre des équipes de sécurité sous pression, les cybercriminels peuvent s'informer pour savoir qui est aux commandes et cibler les entreprises qui semblent les plus vulnérables, vues de l'extérieur.

CONSEILS PRATIQUES

L'amélioration de la santé mentale au sein des équipes chargées de la sécurité informatique doit devenir l'une des priorités des entreprises.

C'est d'elle que peut dépendre leur capacité à empêcher d'éventuels attaquants de tirer parti d'un éventuel épuisement. Il est possible de remédier à ces problèmes de burn-out et de baisse de moral par une série de mesures : accorder à ces professionnels un budget adéquat pour mener à bien leur mission, proposer des évolutions de carrière pour retenir ces talents, mais aussi éviter les sous-effectifs et les heures supplémentaires excessives.

De nombreuses équipes se plaignent également d'avoir à porter la charge mentale supplémentaire d'une mauvaise réputation : ils sont pointés du doigt parce qu'ils perturbent ou ralentissent les procédures de travail, lorsqu'ils sont contraints de restreindre les droits de téléchargement de logiciels, par exemple. Or, le rôle et l'objectif de la direction devraient être de soutenir les efforts des équipes de sécurité en soulignant leur importance pour l'entreprise et en insistant pour que les employés se soumettent à un programme de sensibilisation continu.

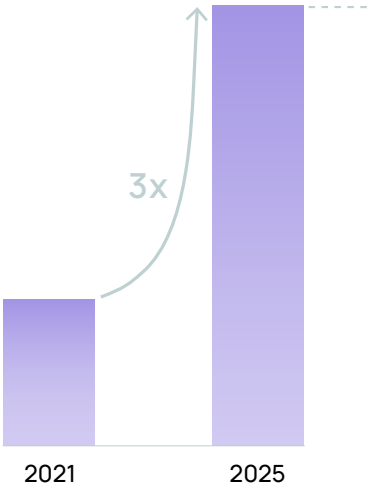
Il est temps d'investir dans la formation des cyberexperts de demain : ceux qui assureront notre sécurité dans un contexte de plus en plus dangereux et complexe.

22 Chartered Institute of Information Security (2022). The security profession 2021/2022.
23 ISACA (2022). State of cybersecurity 2022: cyber workforce challenges.
24 Chartered Institute of Information Security (2022). The security profession 2021/2022.
25 ZDNet (2022). Cybersécurité : le burn-out guette, et cela va devenir un problème pour nous tous.
26 Bleeping Computer (2023). IT burnout may be putting your organization at risk.

05

Attaques de la chaîne d'approvisionnement numérique : nous sommes tous connectés les uns aux autres

L'augmentation alarmante du nombre d'attaques de la chaîne d'approvisionnement en 2022 n'était qu'un avant-goût de ce qui nous attend en 2023 où la tendance ne peut qu'aller en s'intensifiant. Ces attaques toucheront en particulier les chaînes d'approvisionnement numériques. Gartner prédit, en effet, que d'ici 2025, 45 % des entreprises dans le monde auront subi des attaques contre leurs chaînes d'approvisionnement numérique, soit trois fois plus qu'en 2021.[27]



45%

des entreprises auront subi des attaques contre leurs chaînes d'approvisionnement numérique d'ici 2025

Les événements des deux dernières années nous ont rappelé, avec force, que la sécurité des uns dépend de celle des autres. Les cybercriminels cherchent constamment à améliorer leurs chances de succès en exploitant les partenaires et les fournisseurs de leurs cibles, voire des technologies open source. Ils sont prêts à tirer parti de la moindre faille dans la chaîne d'approvisionnement pour s'infiltrer dans les systèmes ou infecter le réseau d'une société avec un logiciel malveillant.

Survenu en mars 2022, le piratage d'Okta, l'éditeur de logiciels dédiés à la gestion d'accès sécurisés, illustre bien l'effet domino de telles attaques : l'intrusion a commencé par un ancien réseau de Sykes, société de service client rachetée par Sitel, un fournisseur d'Okta. L'attaque menace à son tour de compromettre les clients du spécialiste de l'authentification, parmi lesquels on compte Engie, Foncia ou encore la Croix Rouge française. Les données sensibles ainsi collectées par le groupe Lapsus$ se sont retrouvées exposées sur la messagerie sécurisée Telegram.[28] Il ne s'agit pas là d'un cas isolé. Les premières violations de données de 2023, en lien avec des vulnérabilités chez des partenaires, ont déjà été signalées : en janvier, la filiale nord-américaine de Nissan a, par exemple, annoncé que l'un de ses fournisseurs de logiciels avait été victime d'un piratage exposant les noms et les dates de naissance de milliers de clients de Nissan.[29]

Dans la mesure où ces attaques ciblent l'ensemble des chaînes d'approvisionnement et non des sociétés isolées, elles réussissent à affecter de grands groupes comme Okta et Nissan, ainsi que des entreprises locales ayant moins de ressources à leur disposition et donc beaucoup plus de difficultés à se remettre de ces attaques. Un rançongiciel a récemment paralysé les services d'expédition internationale de la poste britannique Royal Mail et entraîné des retards de plusieurs jours dans l'acheminement du courrier de nombreux clients. Les pertes financières pour les petites entreprises ont été énormes.[30]

Les logiciels open source se sont également avérés être des terrains de jeu de choix pour les hackers. Des plateformes comme Codecov en ont déjà fait la triste expérience. Les pirates ont, en effet, eu accès aux informations clients de Codecov en exploitant une vulnérabilité du processus de création d'image Docker.[31] Autre exemple de la complexité et des retombées à long terme que peut avoir ce type d'incidents : la faille Log4j, découverte en décembre 2021. On estime que Log4j est utilisé dans quelque 36 000 logiciels, ce qui signifie que les conséquences de cet incident perdureront jusqu'à ce que l'intégralité de ces applications soit mise à jour.[32]

Ces évolutions, dans un contexte où de nombreuses équipes de sécurité informatique souffrent de sous-effectif, sont du pain bénit pour les cybercriminels. Comme de nombreuses sociétés ont recours à des solutions externalisées pour des opérations de cybersécurité que leurs équipes ne sont pas à même d'effectuer en interne, leur surface de frappe augmente. En fin de compte, l'utilisation de logiciels (et même de logiciels de sécurité) constitue toujours une prise de risques. C'est également ce qu'a montré l'incident de sécurité qui a frappé LastPast et ses clients en août 2022.[33] Il est essentiel que les sociétés renforcent leurs stratégies de cybersécurité afin de pouvoir tirer leur épingle du jeu au sein du paysage de logiciels interconnectés dans lequel nous évoluons aujourd'hui.

CONSEILS PRATIQUES

Avant d'entamer une relation avec un prestataire de services ou un fournisseur, une société doit se renseigner sur son niveau de sécurité et de conformité afin de réduire les risques.

Il faut, par exemple, vérifier que le partenaire détient les certifications (logicielles) requises et remplit les obligations de conformité aux règlements comme le RGPD de l'Union européenne et aux normes telles que ISO/CEI-27001. Des audits et des évaluations indépendantes de la société et de ses clients, une enquête sur les récentes attaques dont le fournisseur a fait l'objet peuvent aider à mieux cerner son profil.

L'étape suivante consiste à limiter au maximum les risques en convenant, avec le fournisseur, des droits qui lui sont octroyés, ainsi que du plan de notification et de réponse en cas d'incident.

La société peut aussi gérer l'accès à distance, le restreindre et le renforcer en ajoutant des couches de protection, à l'aide d'une authentification multifacteur, par exemple.

Il est vital de procéder à des contrôles réguliers : vérifier la performance du fournisseur et assurer le suivi de l'évolution de la relation pour limiter les risques. En résumé, votre sécurité est étroitement liée à celle de vos partenaires et de vos fournisseurs.

27 Gartner (2022). Gartner identifies top security and risk management trends for 2022.
28 Le Monde Informatique (2022). Un chercheur détaille le piratage d'Okta.
29 Cybernews (2023). Nissan data breach exposed clients' full names and dates of birth.
30 Le Monde (2023). Lockbit revendique l'attaque ayant bloqué le service postal britannique Royal Mail.
31 Data Security Breach (2021). Les pirates ont eu accès à un code source de Rapid7 à la suite du piratage de Codecov.
32 Siècle Digital (2022). La faille Log4j considérée comme une « vulnérabilité endémique ».
33 Le Monde Informatique (2022). LastPass annonce le vol d'une partie de son code source.

06

Rançongiciel-as-a-service : comment extorquer en ligne, en un clic

Depuis son invention à la fin des années 1980, le rançongiciel est devenu l'une des méthodes de cyberattaque les plus fréquentes, faisant trembler entreprises et particuliers. Ces dernières années, cette pratique s'est énormément professionnalisée : les cybercriminels diversifient aujourd'hui leurs modèles économiques et l'on assiste à une réelle explosion de rançongiciel-as-a-service (RaaS).

Il n'est plus nécessaire, aujourd'hui, d'avoir de grandes connaissances en informatique ou des compétences en matière de piratage pour lancer une attaque par rançongiciel : une simple recherche sur le dark web suffit, avec un paiement en cryptomonnaie. Sur le même modèle que les fournisseurs de Software-as-a-service, avec une procédure d'inscription similaire et même des services clients dédiés (comme nous l'ont appris les fuites sur le rançongiciel Conti[34]), les opérateurs de RaaS permettent à n'importe qui de mener des attaques à grande échelle. Ce système a multiplié de manière exponentielle le nombre de cybercriminels potentiels.

Les conséquences sont aussi effrayantes qu'impressionnantes : de 2021 à 2022, les attaques par rançongiciel ont augmenté de 13 %, une croissance qui dépasse celle des cinq années précédentes cumulées.[35] En 2021, 1 entreprise française sur 5 a été victime d'un rançongiciel, la France étant le pays le plus impacté de l'Union européenne.[36] Le récent rapport publié par IBM a mis en lumière tous les effets dévastateurs de cette méthode sur l'économie en chiffrant le coût moyen d'une attaque par rançongiciel à 4,54 millions de dollars, hors rançon.[37]

Dans le monde entier, des sociétés ont déjà eu affaire à des attaques par RaaS. L'une des plus célèbres est celle qui a frappé, en 2021, le réseau d'oléoducs de Colonial Pipeline à l'initiative du groupe cybercriminel DarkSide.[38]

4,54 millions d'$

Coût moyen d'une attaque par rançongiciel, hors rançon

Cette attaque a entraîné l'interruption temporaire de l'exploitation des oléoducs et une pénurie de pétrole sur la côte Est des États-Unis. Le mode d'opération de cette cyberattaque a été clarifié ultérieurement : il a suffi aux attaquants d'un mot de passe compromis et de l'absence d'authentification multifacteur pour s'introduire dans le réseau interne.[39]

Le groupe REvil utilise également un modèle RaaS pour nombre de ses attaques. L'attaque de la chaîne d'approvisionnement qu'il a perpétrée, en 2021, sur le fournisseur de logiciels Kaseya s'est notamment répercutée sur des milliers d'entreprises. La compagnie d'assurance CNA Financial et le producteur brésilien de viande JBS comptent parmi les autres victimes tristement célèbres de REvil. Elles ont fait la une de l'actualité en réglant certaines des rançons les plus fortes jamais payées, à savoir 40 millions et 11 millions de dollars respectivement. Bien que les autorités aient annoncé le démantèlement de REvil, début 2022, on pense qu'il a déjà commencé à renaître de ses cendres sous d'autres noms.[40]

Cependant, la nouvelle étoile montante du RaaS est sans doute LockBit. Durant l'été 2022, le fournisseur de pièces automobiles Continental a été victime de l'une de ses attaques. Le groupe de hackers avait, à cette occasion, dérobé un volume de données estimé à 40 To et, devant le refus de Continental de payer la rançon exigée, avait mis ces données en vente sur le dark net pour environ 50 millions de dollars.[41]

Ce principe de double extorsion est de plus en plus fréquent, avec les RaaS, et place de nombreuses sociétés dans une impasse, les forçant à céder au chantage des criminels. LockBit a également fait parler de lui récemment en annonçant le lancement d'un programme de prime de bug pour récompenser les « idées brillantes ». Le groupe externalise ainsi efficacement la recherche de vulnérabilités et multiplie ses chances de succès avec l'aide de sa communauté.[42]

Avec la possibilité de mener des attaques à fort impact en quelques clics, l'explosion des techniques d'extorsion multifacette et l'interconnectivité accrue des chaînes d'approvisionnement, le rançongiciel est devenu un marché extrêmement lucratif pour les cybercriminels du monde entier. Et comme les exemples que nous venons d'évoquer semblent n'être que les signes avant-coureurs d'une véritable épidémie, il est fortement recommandé aux entreprises de sécuriser au maximum leurs systèmes.

CONSEILS PRATIQUES

La prévention contre les rançongiciels est une entreprise de longue haleine. Les experts admettent généralement que toutes les sociétés sont, tôt ou tard, victimes de ce type d'attaques. Il ne faut donc pas uniquement se concentrer sur des mesures de prévention, mais envisager également des solutions pour limiter au maximum les dégâts éventuels.

Avant tout autre chose, les responsables doivent veiller à maintenir à jour les logiciels, à corriger constamment les vulnérabilités détectées et à mettre en place des outils fiables de détection des menaces et de protection des terminaux.

Il peut également être bénéfique de restreindre les droits administratifs des employés sur les différents périphériques, de revoir les politiques de gestion des mots de passe et de les durcir le cas échéant, mais aussi de mettre en place une solide gestion des accès au niveau du serveur. Dans la mesure où ils empêchent les attaquants de diffuser leur logiciel malveillant dans l'ensemble du système, ces gestes permettront de limiter les dommages éventuels causés par un rançongiciel.

Les entreprises doivent également garder à l'esprit que de nombreuses cyberattaques commencent par une forme d'ingénierie sociale. La sensibilisation des collaborateurs est donc un moyen efficace pour réduire les risques d'incidents.

Enfin, la première chose à faire pour ne pas se trouver dans l'obligation de céder à une demande de rançon est de sauvegarder les données et de définir un plan de réponse pour réagir rapidement en cas d'incident.

34 TechCrunch (2022). Conti ransomware gang's internal chats leaked online after declaring support for Russian invasion.
35 Verizon (2022). 2022 Data Breach Investigations Report.
36 L'Usine Nouvelle (2021). Une grande entreprise française sur cinq victime d'un rançongiciel.
37 IBM (2022). Coût d'une violation de données en 2022. Détecter et répondre aux menaces : la course qui valait des millions.
38 Le Monde (2021). Comment un rançongiciel a semé la panique dans un grand réseau d'oléoducs aux Etats-Unis.
39 Reuters (2021). One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators.
40 Le Monde Informatique (2022). Un énième retour du cybergang Revil ?
41 Tech Monitor (2022). FBI joins investigation into Continental ransomware attack.
42 Bleeping Computer (2022). LockBit 3.0 introduces the first ransomware bug bounty program.

07

Phishing multicanal : quand la sécurité des e-mails ne suffit plus

L'époque où les e-mails étaient le seul canal utilisé par les hackers pour nuire aux sociétés en dérobant des informations de connexion et des données privées est bel et bien révolue. Le phishing est désormais plus sophistiqué et prend plusieurs visages : les attaquants jettent leur dévolu sur de nouvelles plateformes, voire utilisent plusieurs canaux pour une même attaque, afin de piéger les particuliers et les entreprises.

De plus en plus, les réseaux sociaux deviennent un de leurs terrains de jeu favoris : le récent détournement du défi « Invisible Body » sur TikTok n'a fait que le confirmer. Ce défi incitait les gens à se filmer nus en utilisant un filtre qui faisait disparaître leur corps. Les pirates y ont vu l'occasion de tirer profit du voyeurisme des utilisateurs en faisant la promotion d'une application censée leur permettre de retirer le filtre d'« invisibilité ». Les curieux étaient donc redirigés vers un serveur Discord sur lequel ils pouvaient récupérer un lien contenant le logiciel malveillant WASP Stealer. De cette façon, les hackers ont pu dérober à des milliers d'utilisateurs des informations sensibles, telles que des mots de passe et des numéros de carte de crédit.[43]

Or, les cybercriminels reprennent également des tactiques inspirées d'applications comme Telegram et Discord sur des plateformes plus professionnelles telles que LinkedIn, Slack et Microsoft Teams. Le télétravail a énormément flouté les frontières entre l'utilisation personnelle et professionnelle de nos périphériques, ce qui permet aux intrus d'accéder à des informations sensibles et à des identifiants de connexion aux systèmes des entreprises par le biais de ces canaux. C'est ce qui a, par exemple, mené à la faille de sécurité qui a affecté Uber, après qu'un salarié est tombé dans le piège d'une fausse notification MFA. Les malfaiteurs l'ont contacté par message WhatsApp en se faisant passer pour des collègues du service informatique et lui ont demandé de leur accorder l'accès aux réseaux de l'entreprise.[44]

Les cybercriminels sont aussi passés par LinkedIn pour piéger des personnes en quête d'un nouvel emploi. Le but était de les pousser à cliquer sur des e-mails de phishing ou sur de fausses offres d'emploi en échange de paiements anticipés ou de coordonnées bancaires.[45] La plateforme offre aussi une bonne source d'informations pour les attaques de spear phishing : les criminels peuvent se renseigner sur les dernières personnes recrutées dans l'entreprise, se faire passer pour leurs supérieurs hiérarchiques en leur demandant de cliquer sur tel ou tel lien et de saisir leurs identifiants de connexion sur de faux sites Internet qui déroberont leurs données.[46]

Les hackers ne se servent évidemment pas uniquement de LinkedIn, mais de nombreux autres outils professionnels. Le studio Rockstar Games a, lui aussi, souffert d'une attaque qui a entraîné une fuite massive de vidéos issues de la version test du jeu Grand Theft Auto 6 (GTA 6). Les pirates ont réussi à s'introduire dans le canal Slack de la société et pu accéder à un grand nombre de séquences, ainsi qu'à d'autres informations telles que les codes source de GTA 5 et GTA 6. Ils ont ensuite publié 90 vidéos pour environ 50 minutes de visionnage et menacé les développeurs de Rockstar Games de divulguer le code source s'ils refusaient de payer une somme d'argent considérable.[47]

43 CNet (2022). Des hackers détournent le défi "Invisible Body" de TikTok pour pirater les utilisateurs.
44 The Verge (2022). Uber's hack shows the stubborn power of social engineering.
45 We Live Security (2022). Common Linkedin scams: beware of phishing attacks and fake job offers.
46 Under News (2023). Comment les cybercriminels utilisent-ils le phishing pour cibler les nouveaux employés ?
47 The Guardian (2022). Grand Theft Auto 6 leak: who hacked Rockstar and what was stolen?
48 ReviewGeek (2022). That computer virus you can't remove might be a browser notification.

De nos jours, le phishing peut se cacher presque partout, même dans des notifications de navigateur apparemment inoffensives. Détournées par des personnes malveillantes, elles peuvent en effet servir de point d'entrée dans nos périphériques et être utilisées pour dérober des identifiants de connexion et des informations sensibles. Il faut, par exemple, se méfier des notifications survenant sur les navigateurs Web pour faire croire aux utilisateurs que leur ordinateur est infecté et leur demander de cliquer sur le message pour éradiquer le virus. En créant un contexte anxiogène et un sentiment d'urgence, les malfaiteurs poussent ainsi la victime à télécharger un logiciel malveillant ou à s'enregistrer en utilisant ses identifiants de connexion.[48]

En exploitant de nouveaux canaux tels que les réseaux sociaux et les applications de messagerie pour s'infiltrer dans nos périphériques, les hackers parviennent à élaborer des techniques d'attaque de plus en plus difficiles à éviter et à détecter. C'est la triste réalité de notre contexte actuel : lorsqu'un nouveau canal est créé, les cybercriminels ne mettent pas longtemps avant de trouver comment le détourner pour servir leurs intérêts.

CONSEILS PRATIQUES

Les êtres humains sont encore et toujours dans le collimateur des attaques d'ingénierie sociale.

Il paraît donc logique de renforcer la sensibilisation à la cybersécurité et d'insister sur l'importance de rester vigilant, quels que soient les canaux utilisés. Les salariés doivent être considérés comme des éléments essentiels du SMSI au sein d'une entreprise qui souhaite développer une culture solide et intégrale de la sécurité.

Étant eux-mêmes propriétaires de leurs périphériques mobiles et des logiciels qu'ils ont demandés, ils ont la responsabilité d'observer les exigences de sécurité. En outre, l'utilisation d'outils de détection des menaces sur différents canaux peut permettre aux collaborateurs d'identifier plus facilement et de signaler d'éventuelles attaques.

Comme beaucoup de ces attaques de phishing exploitent des vulnérabilités zero-day, le meilleur moyen, pour les entreprises, de se protéger est de renforcer le facteur humain.

08

Quand la MFA échoue : une sécurité moins imparable qu'on ne le pensait

Depuis longtemps, les entreprises considèrent l'authentification multifacteur (MFA) comme une méthode fiable pour se protéger des incidents de cybersécurité. Pourtant, s'il est prouvé que la MFA est un obstacle de taille pour les hackers, sa capacité à assurer la sécurité des accès a malheureusement été surestimée.

Il existe plusieurs manières d'instaurer une authentification multifacteur. L'une des plus fréquentes consiste à générer des notifications pop-up sur le téléphone de l'utilisateur pour obtenir son autorisation. Les cybercriminels ont cependant trouvé un moyen pour contourner ce mode d'authentification : une forme d'ingénierie sociale baptisée « Fatigue MFA » ou, en anglais, « MFA push spam ». Elle consiste à bombarder les victimes de notifications pop-up à répétition, jusqu'à ce qu'ils finissent par les accepter, soit par erreur, soit par lassitude. Comme nous le disions au chapitre précédent, les hackers contactent ensuite généralement la victime sur un autre canal, en se faisant passer pour le service d'assistance informatique et en incitant la personne à accepter l'invitation. C'est la méthode qui a récemment causé beaucoup de dégâts chez Uber, Microsoft et Cisco.[49]

Autre tactique fréquente pour contourner l'authentification multifacteur : l'attaque de l'homme du milieu (MitM) qui, tout en s'apparentant à une attaque de phishing standard, est en réalité un peu plus sophistiquée. Tout commence généralement par un e-mail de phishing qui redirige l'utilisateur vers une page de connexion factice, en tout point semblable à l'original. Un proxy, situé entre la page d'origine et son imitation, permet aux attaquants de sauvegarder le cookie de session généré lorsque l'utilisateur a saisi ses informations de connexion et son mot de passe MFA. Ils vont alors utiliser ces cookies dans leurs propres navigateurs pour se connecter automatiquement au compte de leur victime sans avoir à passer, de nouveau, la barrière de l'authentification. C'est ce type d'attaque qui, associé à des techniques de spear phishing, a été récemment utilisé pour compromettre les comptes Microsoft 365 de cadres dirigeants et détourner des transactions financières importantes vers les comptes bancaires des pirates.[50]

Certains attaquants ont également tenté d'utiliser la MFA comme un vecteur d'attaque pour des violations de données de grande échelle. C'est, par exemple, ce qu'il s'est produit lors de l'attaque de la chaîne d'approvisionnement de SolarWinds. La tentative a été découverte lorsque quelqu'un a cherché à enregistrer un second téléphone pour l'autorisation.[51] Toutefois, les attaques de la MFA par téléphone interposé ne sont pas toujours faciles à repérer. En 2021, des pirates ont eu recours à la méthode dite du « SIM swapping » pour vider le portefeuille crypto de leurs victimes : ils ont dupé les opérateurs de téléphonie mobile afin de les convaincre d'affecter le numéro de téléphone de l'utilisateur à une carte SIM différente. Les escrocs recevaient alors les SMS d'authentification multifacteur sur la nouvelle carte SIM et pouvaient ainsi accéder aux comptes de cryptomonnaie de leurs victimes.[52]

Des logiciels malveillants peuvent également être utilisés pour contourner la MFA en compromettant le terminal de la victime (attaque de type « man-in-the-endpoint »). Il s'agit d'installer un malware sur l'appareil de l'utilisateur qui permette aux criminels de démarrer des sessions non autorisées en arrière-plan (et donc, visibles d'eux seuls), une fois que l'utilisateur a passé la barrière de l'authentification multifacteur. Ils se servent alors de ces sessions à des fins malhonnêtes, par exemple, pour détourner des salaire vers leurs propres comptes bancaires.[53] Dans les systèmes qui utilisent des codes à usage unique, ils peuvent aussi réinstaller un générateur de mots de passe pour court-circuiter l'authentification.

Cette seconde technique requiert un haut niveau de compétences et implique de détourner l'algorithme, ainsi que le nombre de seed du générateur pour en prendre le contrôle. Ceci fait, l'attaquant peut lui-même envoyer les codes secrets à l'utilisateur pour contourner la MFA.[54]

Quelle que soit la technique utilisée, la MFA est devenue un vecteur d'attaque dans des violations de données à large échelle. Bien qu'elle ajoute des couches de sécurité supplémentaires, son efficacité dépend de la manière dont elle est configurée et du nombre de mesures complémentaires qui sont mises en place.

CONSEILS PRATIQUES

Pour tirer le meilleur parti de la MFA et de la protection qu'elle offre à votre entreprise, il est important de bien concevoir les processus d'organisation internes et de ne pas négliger la sensibilisation des utilisateurs.

Sur le plan technique, l'utilisation de la correspondance de numéro dans les notifications MFA et/ou la limitation du nombre de demandes d'authentification acceptées ou du temps imparti pour les valider permet déjà de réduire les risques.

Les entreprises doivent également veiller à supprimer les comptes orphelins, contrôler régulièrement les droits d'accès et mettre en place le principe du moindre privilège pour les accès à leurs systèmes. Certains recommandent même d'adopter des pratiques de MFA résistante au phishing, en ayant recours, par exemple, à des tokens physiques ou en utilisant une connexion SSO sur un maximum de comptes pour éviter complètement la MFA.

Sur le plan organisationnel, la sensibilisation des collaborateurs offre un avantage considérable. Il est extrêmement précieux, pour une société, de pouvoir compter sur des utilisateurs qui savent prévenir les attaques et réagir en cas d'activité suspecte. Ce sont eux, en particulier, qui pourront déjouer les tentatives de contournement de la MFA et de « Fatigue MFA ».

49 Bleeping Computer (2022). MFA fatigue: hackers' new favorite tactic in high-profile breaches.
50 Bleeping Computer (2022). Hackers use AiTM attack to monitor Microsoft 365 accounts for BEC scams.
51 Gartner (2021). How to respond to a supply chain attack.
52 Le Monde (2019). Qu'est-ce que le « SIM swapping », qui a permis de pirater le compte du patron de Twitter ?
53 Beyond Identity (2020). How your MFA can be hacked (with examples).
54 Beyond Identity (2020). How your MFA can be hacked (with examples).

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.

ÉDUQUER

Micro-apprentissage stimulant

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 et percutante qui joue sur différents canaux pour développer, sans efforts, des réflexes de sécurité qui durent.

- Une pédagogie narrative et gamifiée conçue pour favoriser l'engagement et la mémorisation
- Une bibliothèque de contenus présélectionnés prêts à être implémentés pour faire évoluer votre formation
- Des options de personnalisation et de gestion de contenu qui ne demandent que peu d'efforts et s'adaptent à chaque entreprise

TRANSMETTRE

Simulations de spear phishing

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 : un moyen efficace pour réduire les risques et le temps de signalement des menaces dans un scénario où chaque minute peut compter.

- Des simulations de cyberattaques personnalisées et réalistes
- Des explications pédagogiques contextualisées qui consolident les habitudes de sécurité des employés
- 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 désastreuses grâce à notre solution tout-en-un d'évaluation du risque humain. Bénéficiez d'un bilan complet sur l'état de votre couche de sécurité humaine afin de pouvoir anticiper toute vulnérabilité éventuelle. Suivez l'impact de vos programmes de sensibilisation, 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 »

SoSafe GmbH
Lichtstrasse 25a
50825 Cologne, Allemagne

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