sosafe

Analyse du risque humain 2023

Avis d'experts et stratégies pour mieux se préparer aux menaces cyber en Europe

« Nous devons mettre la cybersécurité à la portée de tous, développer de bons réflexes qui entrent en action dans tous les domaines de notre vie et réaliser la fusion entre la cybersécurité et le monde de l'entreprise.

Niklas Hellemann, PhD
PDG de SoSafe

Éditorial

Ce n'est un secret pour personne : le paysage des menaces cyber est extrêmement tendu et se développe avec une incroyable rapidité d'innovation.

Au cours de ces dernières années, et tout particulièrement en 2022, le contexte a évolué à une vitesse folle. Les tensions sur la scène internationale, les conflits géopolitiques et les constantes interruptions de l'activité dans les entreprises ont modelé un monde volatile, augmentant de manière inquiétante le périmètre de frappe des cybercriminels et favorisant une professionnalisation croissante de leurs modes d'action. Dans le même temps, les progrès technologiques, et notamment les outils d'IA générative, ont mis « l'art de la cybercriminalité » à la portée de tous. Nous nous trouvons donc aujourd'hui confrontés à des

pirates potentiels sans nombre, ayant à leur disposition les outils nécessaires non seulement pour étendre la portée de leurs attaques, mais aussi pour en décupler le taux de réussite.

Voici maintenant plusieurs années que nous avons, chez SoSafe, averti que les cybercriminels pourraient avoir recours à des tactiques sophistiquées exploitant l'intelligence artificielle, par exemple au deepfake, pour mener des attaques à large échelle. Avec l'émergence d'outils d'IA générative plus facile d'accès, cette menace se fait aujourd'hui plus précise. Une petite étude que nous avons menée récemment a révélé que ChatGPT, par exemple, permettait de créer des e-mails de phishing 40 % plus vite qu'un humain, et ce n'est qu'un avant-goût des possibilités qu'offre l'IA aux cybercriminels pour parvenir à leurs fins.

Il faut donc se faire une raison : en matière de sécurité informatique, nous ne pouvons pas nous permettre de nous reposer sur nos lauriers. Par définition, la sécurité nécessite des améliorations et des adaptations constantes. Les nouvelles technologies permettent, certes, de mieux se protéger contre les stratégies d'attaques émergentes, mais elles ne sont qu'une partie de la solution. Car nous pouvons être sûrs d'une chose : les attaquants continueront à chercher (et à trouver) des moyens pour contourner les obstacles technologiques, même les plus sophistiqués. Ils ne savent que trop bien que leur plus grande chance de succès réside dans la manipulation des émotions humaines, comme l'ont montré les récentes violations de grande ampleur subies par Uber ou Reddit. L'ingénierie sociale est une véritable poule aux œufs d'or. Pourtant, il existe des méthodes efficaces qui permettent de réduire considérablement ce risque.

Ce n'est d'ailleurs pas sans raison que les formations de sensibilisation à la cybersécurité figurent en tête des priorités en matière de sécurité au sein des entreprises que nous avons interrogées dans le cadre de ce rapport. L'un des facteurs qui pèsent le plus sur leur capacité à investir correctement leurs ressources dans leur culture de la sécurité est le niveau de conscience des risques cyber chez les dirigeants. Cela rejoint, en quelque sorte, l'objectif que nous nous sommes fixé en publiant chaque année notre rapport « Analyse du risque humain » : fournir des données qui ouvrent de nouvelles perspectives. Nous partageons ici des informations de première main sur les stratégies des cybercriminels et le rôle du facteur humain dans ce contexte, ainsi que des ressources pour initier des débats autour de la sécurité de l'information et de la sensibilisation.

Une analyse approfondie des données recueillies sur notre plateforme, une enquête à grande échelle menée auprès de professionnels européens de la cybersécurité et des échanges avec des experts issus de différents secteurs n'ont fait que nous conforter dans notre conviction : nous devons mettre la cybersécurité à la portée de tous, développer de bons réflexes qui entrent en action dans tous les domaines de notre vie et réaliser la fusion entre la cybersécurité et le monde de l'entreprise. C'est la seule manière de lutter contre le fléau de la cybercriminalité dont les conséquences se chiffrent aujourd'hui à plus d'un milliard de dollars : dans un contexte de menaces qui évolue vite, nous devons être plus rapides encore.

Niklas Hellemann, PhD
PDG de SoSafe

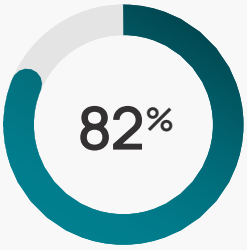
Contenu

Résumé exécutif

Le paysage des menaces cyber est tendu...

1 société sur 2

a été victime d'une cyberattaque réussie au cours des 3 dernières années.



des entreprises pensent que la situation ne se décantera pas dans l'année qui vient.

> Nous vivons à l'ère du numérique. Tout, ou presque, est interconnecté et peut être piraté.

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

Top 3 des stratégies d'attaques qui réussissent le mieux :

1. Logiciel malveillant
2. Phishing
3. Rançongiciel

Top 3 des services ciblés au sein des entreprises :

1. Informatique
2. Finance
3. Sécurité

... et le cybercrime vit son âge d'or ; voici pourquoi :

3 experts sur 4

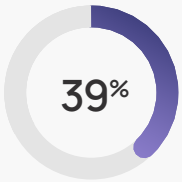
estiment que la **géopolitique**, l'**IA** et le **télétravail** ont augmenté les risques cyber qui pèsent sur leur société.

« 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.

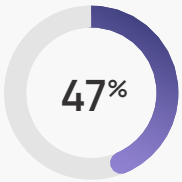
Stéphane Duguin
PDG de CyberPeace Institute

8 sur 10

trouvent que leur société est de plus en plus **dépendante de la sécurité de ses partenaires et fournisseurs**.



Parmi les sociétés victimes d'**attaque par rançongiciel**, plus d'un tiers ont payé la rançon.



Dans le cas des petites entreprises, c'est **même la moitié** d'entre elles qui ont été contraintes de payer.

Des possibilités encore inexploitées en cybercriminalité

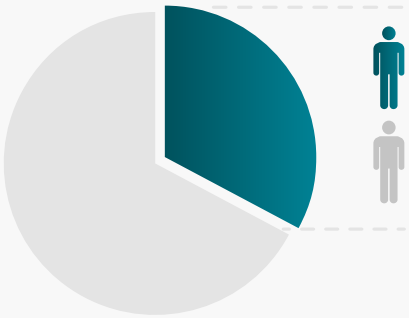
« Depuis quelque temps déjà, les cybercriminels ont une technologie extrêmement perfectionnée à leur disposition, notamment le clonage vocal. Pourtant, nous n'avons pas encore vu surgir d'attaques à grande échelle utilisant ces techniques sophistiquées d'ingénierie sociale. C'est donc que les procédés les plus simples continuent de fonctionner. Cependant, avec le partage illégal des accès à de grands modèles de langage et l'explosion de l'IA générative dans tous les domaines, la situation va très certainement évoluer.

Niklas Hellemann, PhD
PDG de SoSafe

80 % des experts estiment que l'ingénierie sociale et le phishing constituent des risques majeurs pour leur entreprise :

1 utilisateur sur 3

clique sur les e-mails de phishing malveillants. Parmi eux…



1 utilisateur sur 2

va jusqu'à divulguer des données sensibles.

Dans un contexte où les menaces s'intensifient, les techniques d'ingénierie sociale qui jouent sur la pression ou l'autorité pour générer

des émotions négatives

sont celles qui réussissent le mieux.

« Nous recevons de plus en plus souvent des e-mails malveillants. Chaque nouvelle vague est plus forte que la précédente.

Sascha Czech
RSI au CHU Uniklinikum de Münster

« Beaucoup d'utilisateurs relâchent leur vigilance lorsqu'ils travaillent de chez eux, dans un cadre moins formel. Ils intègrent beaucoup d'activités privées dans leur flux de travail et sont donc moins attentifs.

Stefan Lüders, PhD
Responsable de la sécurité informatique au CERN

Les natifs du numérique sont

↗ 65 %

plus susceptibles de cliquer sur des e-mails de phishing que les utilisateurs plus âgés.

Perspectives : les entreprises sont-elles prêtes à faire face ?

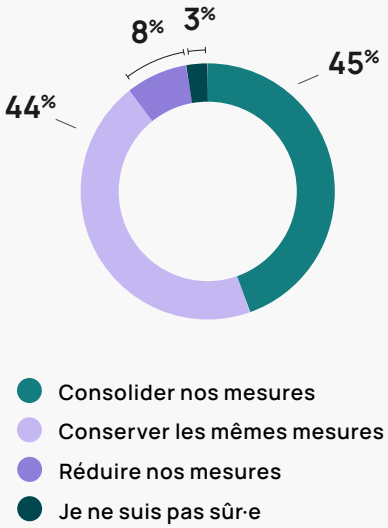
« J'entends souvent le même refrain : « Pourquoi changer ce qui fonctionne bien ? » Pourtant, en cas d'attaque, les conséquences peuvent être désastreuses.

Thomas Tschersich
RSI chez Deutsche Telekom

Top 3 des priorités pour les professionnels de la sécurité informatique :

1. **Sensibiliser davantage les employés à la cybersécurité**
2. **Renforcer la gestion des identités et des accès**
3. **Sécuriser le travail hybride**

9 sociétés sur 10 envisagent de conserver ou d'accroître leur niveau de sensibilisation au cours de l'année qui vient.



« Tout ce qu'une entreprise peut protéger en sensibilisant ses employés la rend plus résiliente. Elle économise ainsi de l'argent, gagne du temps et s'épargne bien du stress en évitant d'amplifier les risques.

Thomas Schumacher
Directeur général d'Accenture Security

Selon les professionnels du secteur, **les meilleures méthodes** pour garantir un réel impact des formations de sensibilisation sont :

1. **Les mesures de sensibilisation utilisant les applications de messagerie**
2. **Les formations personnalisées**
3. **La personnalisation des programmes**

Méthodologie et sources

Enquête auprès des professionnels de la cybersécurité

Pour mener cette enquête à grande échelle sur l'état de la cybersécurité au sein des entreprises, nous nous sommes associés à Censuswide, un cabinet international d'études de marché dont le siège se trouve à Londres. Plus d'un millier de professionnels de la cybersécurité, issus de 6 pays européens (Royaume-Uni, Allemagne, Autriche, Suisse, France et Pays-Bas) ont été interrogés en février 2023. Ils représentaient des entreprises de 10 à plus de 5 000 employés, tous secteurs confondus

Données de la plateforme SoSafe

Pour l'analyse des différentes techniques d'ingénierie sociale, 8,4 millions d'e-mails de simulations de phishing menées dans 3 000 sociétés clientes de la plateforme SoSafe ont été analysés de manière anonyme pour identifier les niveaux de risque humain et le taux de réussite des différentes stratégies d'attaque.

Test de phishing

Dans cette étude portant sur la sensibilisation au phishing de manière générale, plus de 9 000 e-mails de simulation de phishing ont été envoyés aux utilisateurs qui se sont inscrits en 2022. En l'espace d'une semaine, les participants ont reçu trois simulations d'attaque, d'une complexité intermédiaire. Les utilisateurs devaient identifier ces e-mails. S'ils cliquaient dessus, ils étaient redirigés vers des ressources pédagogiques en rapport avec le contenu du message.

La cybercriminalité classée risque numéro 1 pour les entreprises : l'impact des comportements humains sur ce phénomène

Tous les experts en matière de sécurité informatique sont d'accord pour affirmer que la cybercriminalité constitue un risque majeur pour les sociétés du monde entier. Depuis plusieurs années, les rapports analytiques dans ce domaine, tels que le Baromètre des risques d'Allianz ou le Coût d'une violation de données d'IBM, montrent que la négligence vis-à-vis des principes de sécurité peut avoir des conséquences désastreuses pour les entreprises, non seulement en termes de pertes financières, mais aussi de dégradation de leur réputation.

Risque n°1
pour les entreprises

Les cyberincidents constituent le risque majeur pour les sociétés

Source : Allianz Risk Barometer 2023 [1]

4,35 M$

Coût moyen d'une violation de données

Source : Coût d'une violation des données 2022 d'IBM [2]

De nombreux événements, des crises géopolitiques à l'essor de l'intelligence artificielle en passant par une pénurie de talents dans les secteurs de l'informatique et de la sécurité, tendent à aggraver une situation déjà compliquée. Dans un contexte où les cybercriminels perfectionnent de plus en plus leurs modes d'action et les adaptent aux évolutions technologiques et sociétales, de nombreux organismes et entreprises ont du mal à suivre le rythme de cette course effrénée et à trouver les bons outils pour se protéger efficacement.

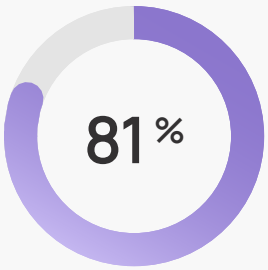
1 société sur 2

a été victime d'une cyberattaque réussie au cours des 3 dernières années et 64 % estiment qu'elles courent encore un risque élevé de subir une nouvelle attaque

La perspective pour les mois et les années à venir n'est pas brillante. Les experts en sécurité interrogés dans le cadre de ce rapport ont été sans équivoque : 82 % d'entre eux pensent que la situation ne se décantera pas dans les mois qui viennent.

Le dénominateur commun

Malgré la complexité du contexte actuel, toutes les menaces ont un point commun : le facteur humain. Quelle que soit la performance des mesures techniques de protection mises en place, les gens continuent à tomber dans le piège d'une ingénierie sociale sophistiquée. Pour donner une meilleure idée de la situation : le phishing, une des méthodes d'ingénierie sociale par excellence, arrive en deuxième position parmi les tactiques de cyberattaque faisant le plus de victimes. Seuls les logiciels malveillants et les rançongiciels présentent un risque comparable, d'après les experts. Il est d'ailleurs intéressant de souligner que ces deux types d'attaques sont souvent déclenchées par une interaction humaine, lorsqu'un employé communique par mégarde des informations de connexion, par exemple.



des professionnels de la cybersécurité estiment que le phishing et la manipulation psychologique représentent un risque significatif pour leur entreprise

On comprend mieux alors pourquoi ces techniques d'ingénierie sociale restent le choix numéro 1 des cybercriminels et pourquoi ces derniers ne cessent d'innover en la matière : ce sont, en effet, des outils simples et économiques permettant de s'infiltrer dans les systèmes des sociétés. La bonne nouvelle, cependant, c'est que les entreprises peuvent mettre en place des mesures pour renforcer leur pare-feu humain et l'intégrer à part entière dans leur stratégie globale de sécurité de l'information.

1 **Allianz (2023).** Allianz Risk Barometer.

2 **IBM (2022).** Coût d'une violation de données en 2022. Détecter et répondre aux menaces : la course qui valait des millions.

Le facteur humain : première et dernière ligne de défense

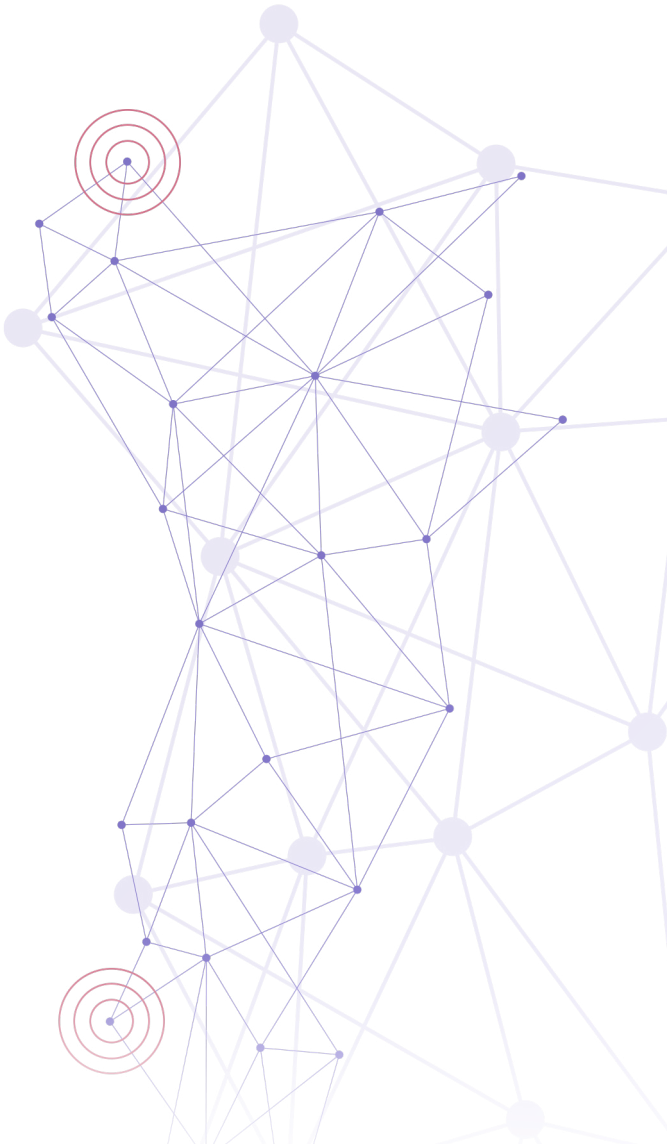
Si les sociétés inversent la tendance et entreprennent d'exploiter les comportements et la psychologie humaine comme le font les cybercriminels, elles peuvent transformer leurs employés en véritables gardiens de leur sécurité et de l'accès à leurs systèmes.

> **Tout ce qu'une entreprise peut protéger en sensibilisant ses employés la rend plus résiliente. Elle économise ainsi de l'argent, gagne du temps et s'épargne bien du stress en évitant d'amplifier les risques.**

Thomas Schumacher
Directeur général d'Accenture Security

Le cyberincident qu'a subi Reddit[3] ne l'illustre que trop bien : au début 2023, la société a souffert d'une violation de données provoquée par une attaque de phishing extrêmement sophistiquée qui a permis aux attaquants d'avoir accès à des documents internes et à du code source. Mais cet événement a parfaitement illustré la force d'une solide culture de la sécurité : l'employé qui a cliqué sur l'e-mail de phishing a, en effet, réalisé immédiatement qu'il venait d'être victime d'une attaque. Il l'a tout de suite signalé à l'équipe interne de sécurité informatique qui a alors pu restreindre les accès de l'attaquant. Sans cette réaction salutaire, l'histoire aurait pu avoir des conséquences autrement plus graves.

Notre principal atout pour contrer les attaques des cybercriminels est de les battre à leur propre jeu : en cherchant à comprendre les schémas comportementaux qu'ils exploitent et en adoptant une approche proactive. Dans ce rapport, nous nous proposons d'étudier plus en détail la situation actuelle en matière de cybersécurité et de sensibilisation, en analysant plus spécifiquement le paysage européen. Nous examinerons également les méthodes inspirées des sciences comportementales qui permettent aux entreprises de mieux se protéger dans un contexte où les menaces se complexifient. Bien que les données parlent déjà d'elles-mêmes, nous laisserons aussi la parole à des experts issus de différents secteurs d'activité. Ils nous donneront leur avis sur ce qu'ils considèrent être les priorités pour les professionnels de la cybersécurité d'aujourd'hui.



3 **Le Big Data (2023).** Reddit piégé par le phishing : le code source volé par les hackers.

« Nous vivons à l'ère du numérique. Tout, ou presque, est interconnecté et peut être piraté.

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

Experte réputée en technologies numériques, entrepreneuriat et politique, Katrin Suder est consultante pour différentes sociétés, notamment de grands groupes allemands ou américains. Spécialiste en physique et en neuro-informatique, titulaire d'un doctorat en intelligence artificielle, elle a des années d'expérience dans le monde des affaires et de la politique. Elle a dirigé, jusqu'en 2021, le Conseil numérique du gouvernement allemand sous Angela Merkel. De 2014 à 2018, elle a également été secrétaire d'État au ministère allemand de la Défense. Elle a travaillé 14 ans chez McKinsey, en partie comme directrice, et elle est membre de plusieurs conseils de surveillance en Allemagne et à l'international, notamment chez Cloudflare.

Lors de notre Human Firewall Conference, vous avez déclaré que les cyberattaques étaient votre cauchemar. Pour quelle raison ?

La cybernétique est une arme militaire dangereuse et un outil aussi redoutable que rentable entre les mains des criminels. La plupart du temps, les pirates peuvent, en effet, perpétrer des attaques sans être détectés. Il n'est pas, à proprement parler, impossible de trouver le coupable, mais cela prend énormément de temps. C'est également un moyen extrêmement économique, comparé, par exemple, à un avion de combat. Le risque personnel est faible : personne ne risque sa vie, mais les cyberattaques n'en sont pas moins potentiellement dévastatrices. À l'époque où je travaillais au ministère allemand de la Défense, la question de la sécurité a commencé à s'étendre de plus en plus à l'espace cybernétique et nous avons dû ajouter une nouvelle dimension à notre stratégie de défense : celle de la cybersécurité. Les cyberincidents sont l'un des principaux risques que je rencontre dans mon travail avec les entreprises. Celles-ci sont constamment ciblées par des hackers. La question n'est pas de savoir si vous serez attaqués, mais quand, comment vous allez gérer la situation et si vous saurez réagir rapidement.

La situation géopolitique est de plus en plus instable et fragmentée. Quels sont les effets de cette évolution sur les dangers qui menacent déjà le cyberespace ?

La cybernétique est un instrument de pouvoir géopolitique et un nouveau vecteur d'attaques utilisé par les États pour parvenir à leurs fins. Notre nouvel ordre mondial entraîne un effritement continu des forces de réglementation

globales, tandis que les intérêts nationaux prennent de plus en plus le dessus, par de l'espionnage ou des tentatives d'agression, par exemple. En investissant dans la cybernétique, les États se dotent d'une technologie armée qui leur permet de provoquer des dégâts considérables, à peu de frais. Il ne s'agit pas uniquement de données et d'argent : ce sont parfois même des vies humaines qui sont en jeu.

Dans le contexte actuel, la prolifération des cyberattaques est-elle uniquement motivée par des questions (géo)politiques ?

Non, pas uniquement. Beaucoup de cyberattaques sont menées par des acteurs paragouvernementaux qui se comportent un peu comme des soldats qui n'auraient pas prêté allégeance à un pays en particulier. Ils ne sont liés par aucune loi. Vous ne pouvez pas imputer leurs actions à un pays en particulier. Vous ne pouvez pas les accuser d'avoir violé une convention précise. Et c'est ce qui complique terriblement la situation. Dans notre nouvel ordre mondial, où les intérêts nationaux jouent un rôle majeur, ces structures peuvent continuer à prospérer. Les hackers paragouvernementaux exploitent les événements géopolitiques pour en tirer un profit, en soutenant, par exemple, des intérêts politiques ou en revendant des données volées pour des sommes exorbitantes. La géopolitique alimente la cybercriminalité en ce sens que les crises géopolitiques s'accompagnent d'une prolifération de cyberattaques dont les motivations ne sont plus uniquement politiques, mais aussi criminelles.

Quelles sont les autres évolutions qui impactent notre cybersécurité ?

Nous vivons à l'ère du numérique. Tout, ou presque, est interconnecté et peut être piraté. La transition numérique a aussi donné une place plus importante à la technologie, ce qui ouvre de nouvelles perspectives pour les attaquants.

Comment cela va-t-il affecter les services essentiels dont nous dépendons ? Autrefois, par exemple, les centrales électriques n'étaient pas connectées à Internet. Sommes-nous toujours protégés alors que les fournisseurs d'énergie sont décentralisés ?

Il y aura, bien sûr, toujours quelques domaines qui ne dépendent pas d'Internet, par exemple dans les forces armées allemandes. Mais, de plus en plus, les services essentiels dont nous dépendons sont interconnectés. Et cela m'inquiète. Les attaques et les manipulations dirigées directement contre des personnes se multiplient à une vitesse alarmante et ces victimes peuvent, à leur tour, avoir accès à des réseaux isolés. Il existe bien une législation et des ordonnances visant à réglementer le secteur des services essentiels, mais les réseaux d'approvisionnement décentralisés, tels que les petits fournisseurs municipaux, par exemple, ont plus de mal à se protéger : ils n'ont pas les ressources financières ni le personnel nécessaire pour installer des systèmes informatiques appropriés.

Est-il même possible de conserver une vue d'ensemble de toutes les nouveautés qui surgissent dans le domaine de la cybersécurité ?

On entend souvent dire que tout ce qui touche au cyberespace est nouveau et inédit. Ce n'est pas tout à fait vrai. Les principes de base, pour la sécurité et la protection, restent les mêmes : le fait de changer fréquemment les mots de passe, par exemple, devrait être aussi évident que de se laver régulièrement les mains. Je pense qu'il est important de ne pas se comporter comme si tout, dans le monde numérique, était nouveau, imprévisible et incontrôlable. Ce n'est pas vrai et ça véhicule un sentiment d'impuissance.

« Ces 10 dernières années, les entreprises ont davantage investi dans la technologie que dans les personnes. Elles commencent à comprendre que la technologie ne fait pas tout et que l'ingénierie sociale, en particulier le phishing, pose un réel problème.

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

Abordons la question de la défense. Vous êtes membre du comité consultatif chez Cloudfare. La cybersécurité est-elle un sujet abordé à l'échelon exécutif, aujourd'hui ?

Absolument. Cela varie d'un secteur à l'autre, car moins un secteur est numérisé, moins il est concerné par la cybersécurité. Mais, en règle générale, d'après mon expérience, les cyberincidents sont considérés comme un risque majeur. Il faut noter que tous les comités consultatifs ne comptent pas forcément un membre spécialisé dans cette question. C'est aussi un phénomène de génération. Ces comités sont généralement dirigés par des personnes qui ont davantage d'expérience de la vie, mais sont souvent moins familiarisées avec les problèmes de transition numérique et de cyberincidents. Sans compter que la cybersécurité est une véritable course de vitesse : tout change très vite, il faut constamment se former et se tenir à jour. Il est donc essentiel de développer de nouveaux modèles, en investissant plus massivement dans les formations, par exemple, ou en intégrant, au sein des comités consultatifs, des personnes plus jeunes, disposant d'une expertise spécifique, même si elles n'ont pas d'expérience en direction d'entreprise. La question qu'il faut se poser, c'est : où en est votre société en termes de sensibilisation aux risques cyber et comment rester à jour dans ce domaine ? De nombreuses entreprises, notamment celles de taille moyenne, sont aujourd'hui confrontées à ce nouveau défi.

Les sociétés se protègent-elles assez, en particulier au niveau de leurs ressources humaines ?

Les sociétés n'investiront jamais assez dans la sensibilisation à la sécurité. Elles n'ont pris conscience de l'importance du facteur humain qu'il y a à peine quelques années. Il va donc leur falloir un certain temps pour développer des bonnes pratiques et des méthodes pour se tenir à jour.

Ces 10 dernières années, les entreprises ont davantage investi dans la technologie que dans les personnes. Elles commencent à comprendre que la technologie ne fait pas tout et que l'ingénierie sociale, en particulier le phishing, pose un réel problème.

« Technologie ou être humain » : le débat revient souvent dans le contexte de la sécurité informatique. À quoi faut-il donner la priorité et de quelle manière ? Qu'en pensez-vous ?

C'est un faux débat. Personne n'irait débattre sur la nécessité d'investir en priorité dans l'infrastructure d'une entreprise ou dans son personnel. Il est bien sûr naturel que les entreprises cherchent à pallier leurs points faibles à l'aide de la technologie ou à optimiser leurs défenses en installant des logiciels, mais il est impératif d'investir aussi dans le facteur humain.

Vous avez dit que la sécurité de l'information était une véritable course de vitesse. Les sociétés continuent-elles à envisager la formation à la cybersécurité comme une mesure ponctuelle ? Ou ont-elles compris qu'il faut constamment investir dans ce domaine ?

Aujourd'hui, le phishing affecte les entreprises et la plupart d'entre elles réalisent que les efforts constants sont la clé pour résoudre ce problème. Cependant, beaucoup de sociétés ont du mal à prendre ce tournant et continuent à recourir aux méthodes traditionnelles : des présentations PowerPoint interminables, des vidéos qui sont censées être « drôles » ou des séminaires académiques en présentiel visant à former les employés à la cybersécurité.

Or, étant donné la quantité d'informations à communiquer aux collaborateurs, non seulement sur le cyberespace, mais aussi sur les questions de conformité, de protection des données, de critères ESG, etc., il est nécessaire d'adopter des approches comme la gamification ou certaines méthodes pédagogiques utilisées dans la formation d'adultes. Bien des entreprises en sont encore au point mort à cet égard.

Quelles sont les questions posées par les comités consultatifs pour évaluer les aspects humains et techniques de la cybersécurité au sein de l'entreprise ?

Nous ne sommes pas encore totalement au point à ce sujet au sein des comités consultatifs. Les questions et les échanges tournent souvent autour des moyens de contrôle et des processus, alors que nous devrions aller plus loin et poser des questions telles que : « Quel est le risque encouru dans notre modèle entrepreneurial ? Quelles données stockons-nous et où ? À l'heure actuelle, dans quelle mesure une cyberattaque pourrait-elle impacter notre modèle entrepreneurial ? Quels sont les vecteurs d'attaque géopolitiques qui nous concernent ? Quels sont les plans d'action prévus en cas d'urgence ? » Cette démarche peut sembler compliquée de prime abord, mais elle ne l'est pas. Dans le cadre de la production, par exemple, on aborde aussi des questions précises, telles que les coûts en cas d'interruption de l'activité ou les taux d'erreurs.

Dans quelle mesure les sociétés devraient-elles inscrire la cybersécurité au nombre de leurs exigences internes ?

La cybersécurité est un sujet qui relève typiquement de la gestion des risques. Soit les entreprises l'intègrent dans leurs procédures de gestion des risques, soit elles créent un chevauchement en instaurant leur propre évaluation des risques cyber. J'ai déjà vu les deux manières de faire, et les deux fonctionnent.

Peut-on considérer la cybersécurité comme une forme d'impôt numérique ? Faut-il se faire une raison et considérer que l'essor de la numérisation va nécessairement de pair avec une augmentation des dépenses ?

Cette nouvelle dimension de la sécurité informatique a évidemment son prix. Le problème est que les primes d'assurance ont augmenté : pour la santé (COVID), pour les politiques industrielles, pour la sécurité physique, pour l'énergie et pour la cybersécurité. Les sociétés sont donc confrontées à des dépenses supplémentaires conséquentes, sans compter que les marges d'EBIT (REX en français) sont aussi mises à rude épreuve par les événements géopolitiques. Globalement, cela implique que nous perdons de la richesse, puisque les marges d'EBIT (REX) qui n'ont pas été générées ne peuvent pas être employées pour les investissements, les employés, etc. D'un point de vue géopolitique, je ne vois pas pourquoi les primes d'assurance baisseraient. L'État non plus n'a pas la possibilité de tout réguler ou compenser, et nous en voyons les conséquences en temps réel. Je pense donc que l'analogie avec un « impôt » n'est pas adaptée, ici.

Quel rôle l'État doit-il jouer dans la gestion des problèmes de cybersécurité ?

L'un des principaux rôles de l'État est d'investir dans des formations modernes. Nous en manquons cruellement dans le domaine de l'informatique. Il faudrait que tout le monde apprenne à l'école les bases de la cybersécurité et de la manipulation des données, a minima. Outre la formation, nous avons besoin d'une police (numérique) active, ainsi que de points de contact et d'assistance supplémentaires, car nous n'en avons pas assez dans le cyberespace.

Comment pallier la pénurie de talents dans le secteur informatique ?

Il faut viser au-delà de l'automatisation en informatique, si nous voulons renforcer notre sécurité. Il n'est plus question de licenciements ou de gagner en efficacité grâce à l'automatisation, mais de savoir si nous sommes encore en mesure de garantir la cybersécurité. La pénurie de talents, de manière générale, est une réalité et beaucoup en payent déjà les conséquences. Elle se fait encore plus cruellement sentir dans les secteurs de la science, des technologies, de l'ingénierie et des mathématiques, alors que la demande, elle, ne cesse d'augmenter. Cette situation nécessite de trouver de nouvelles solutions, telles que le renforcement des défenses grâce à l'automatisation. Nous devons également continuer à libérer des capacités dans tous les domaines où c'est possible, à l'aide de ChatGPT ou d'autres technologies.

Vous parlez de ChatGPT : à votre avis, comment l'intelligence artificielle influe-t-elle sur la cybersécurité ?

L'IA générative m'inquiète davantage sur le plan de l'éducation et de la démocratie que sur celui des ressources humaines. Elle nous fixe une nouvelle mission en matière de formation : si l'IA générative prend de plus en plus d'ampleur, nous devons commencer à penser notre manière de catégoriser l'innovation ou les contenus. Comment évaluons-nous les textes ? Comment menons-nous nos recherches ? Les résultats fournis par ces outils proviennent de machines. Leurs destinataires n'ont pas de source humaine pouvant servir de référence pour les évaluer. Les utilisateurs doivent donc apprendre à évaluer les réponses fournies par les outils d'IA.

Un champ de bataille à l'échelle mondiale : comment les événements géopolitiques façonnent le paysage de la cybercriminalité

> Nous vivons à l'ère du numérique. Tout, ou presque, est interconnecté et peut être piraté.

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

Les paroles de l'experte Katrin Suder soulignent une grande vérité du monde d'aujourd'hui : les progrès fulgurants de la technologie et l'interconnectivité croissante de tous nos systèmes et périphériques numériques ont ouvert des perspectives de communication, de commerce et d'innovation sans précédent. Mais ils mettent aussi notre résilience à rude épreuve. Les **interactions des mondes numérique et géopolitique** ont favorisé l'émergence d'une **industrie complexe de la cybercriminalité** : des attaquants commissionnés par des États, des organisations criminelles ou des pirates isolés exploitent les vulnérabilités des infrastructures numériques pour des raisons politiques et économiques. Dans cette véritable jungle, la cybersécurité est devenue une préoccupation majeure pour les gouvernements, les entreprises et les particuliers.

Mise en danger du pouvoir : l'impact sur la cybersécurité au sein des gouvernements

Paradoxalement, après une transition numérique rapide et des années de mondialisation croissante, on voit se dessiner aujourd'hui, à l'échelle mondiale, une nouvelle tendance géopolitique : **la démondialisation**. Si les premiers signes de ce processus sont apparus dès 2008, il s'est récemment accéléré avec la compétition stratégique que se livrent les États-Unis et la Chine.[1] Les relations se sont durcies entre ces deux superpuissances et leur rivalité s'est étendue jusque dans le cyberespace : elles s'accusent l'une l'autre de vols de propriété intellectuelle, d'espionnage et de financement de cyberattaques. C'est ainsi que, l'année dernière, plusieurs sites officiels taïwanais ont été désactivés à la suite d'attaques DDoS. Dans la mesure où celles-ci coïncidaient avec la visite de la présidente de la Chambre des représentants des États-Unis, Nancy Pelosi, la Chine a été soupçonnée de les avoir commanditées.[2]

Le conflit actuel entre Israël et l'Iran offre un autre exemple de cette réalité : voilà déjà des années que les deux pays se livrent, dans l'ombre, une guerre cybernétique. Après le ver informatique tristement célèbre, Stuxnet, qui ciblait le programme nucléaire iranien, de nombreuses autres frappes ont été perpétrées entre les deux États : tentative de violation de données sur le réseau hydraulique israélien en avril 2020, cyberattaque du port iranien de Shahid Rajaee en mai 2020, cyberattaques visant les systèmes de transports iraniens en juillet 2021 ou piratage d'un site d'hébergement israélien en octobre 2021 avec fuites de données à caractère personnel.[3] Les cyberattaques de ce type ne cessent de se multiplier, y compris dans le contexte de la guerre russo-ukrainienne. Elles inquiètent, car **elles ont dévié de leurs objectifs premiers et ne ciblent plus essentiellement des points stratégiques pour la défense, mais des infrastructures essentielles et des civils**. Au vu des tensions politiques qui ne cessent de s'exacerber, les gouvernements actuels partagent désormais cette crainte.

1 **Ouest France (2022).** Entre la Chine et les États-Unis, une confrontation à tous les niveaux.

2 **Clubic (2022).** Taïwan a subi un pic de cybermenaces en marge de la visite de l'Américaine Nancy Pelosi.

3 **RFI (2022).** Moyen-Orient : cyberguere entre Israël et l'Iran.

« Le nombre de tentatives de cyberattaques a augmenté de près de 8 000 % depuis février 2022.

Sascha Czech
RSI chez Uniklinik Münster

Responsable de la sécurité informatique au CHU de Münster (Uniklinik Münster), en Allemagne, Sascha Czech assure, à ce titre, la cybersécurité de tout l'établissement. Celui-ci est le premier hôpital allemand à avoir mis en place un Centre des opérations de sécurité (SOC) géré par une équipe interne. En reconnaissance des efforts qu'il a déployés dans ce cadre, Sascha Czech a été nommé RSSI de l'année, en 2022, par l'organisme délivrant la Certification Information Security (CIS).

Vous avez occupé différents postes à responsabilité, liés à la sécurité informatique, dans le secteur de la santé. Quels sont les plus grands défis que vous ayez rencontrés ?

Nous voyons bien que le contexte cyber actuel est de plus en plus dangereux, et cela ne date pas d'hier. Ce n'est pas uniquement dû à la démocratisation des nouvelles stratégies d'attaques, mais aussi à ces « rumeurs constantes » qui circulent. Selon moi, la sécurité sur le net, mais aussi physique, est le plus grand défi qui se pose aujourd'hui pour le secteur de la santé.

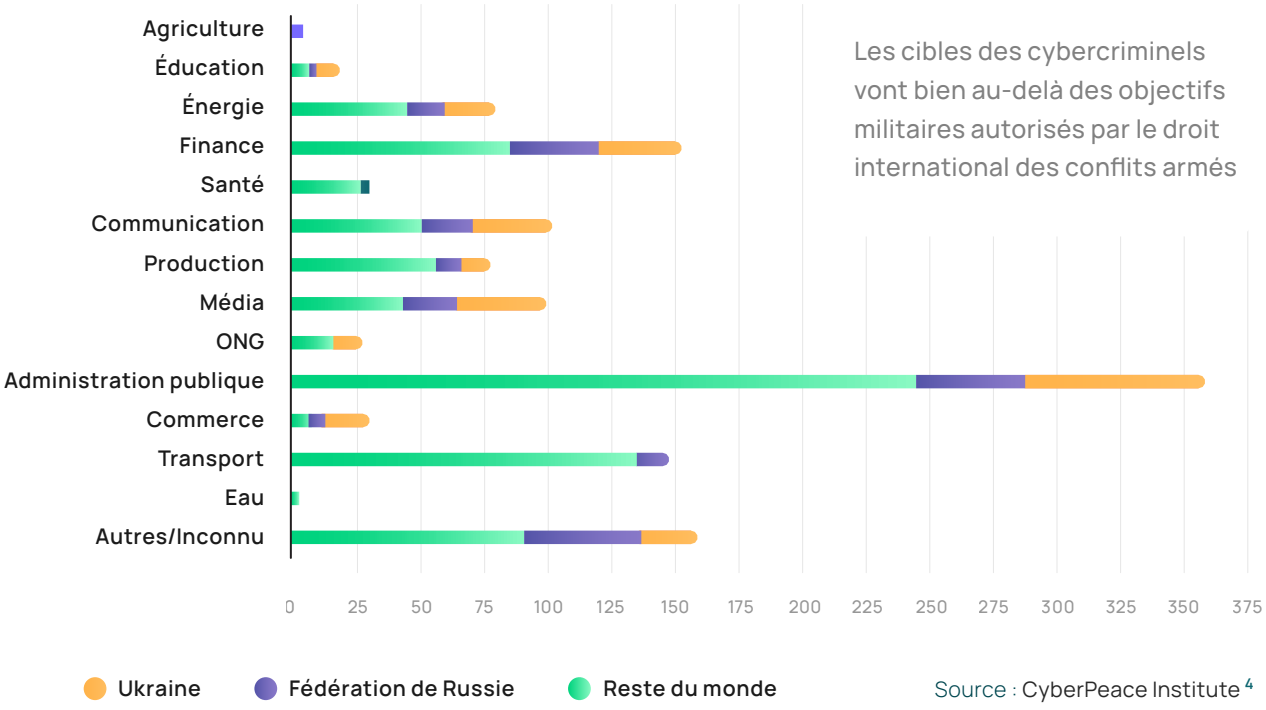
À votre avis, quelles sont les causes de cette évolution ?

En premier lieu, le contexte politique tendu. Au CHU Uniklinik Münster, nous avons noté que ces « rumeurs » d'attaques ont augmenté d'environ 8 000 %, depuis février, par rapport à l'année dernière. Les e-mails malveillants, qu'il s'agisse de phishing ou de rançongiciel, sont de plus en plus fréquents, et chaque « vague » d'attaque est plus forte que la précédente.

Avez-vous remarqué, de manière générale, un changement d'état d'esprit par rapport à la sécurité informatique ?

Je trouve que le sujet est davantage présent dans les esprits depuis qu'il est médiatisé. Mais il faut encore amener les gens à prendre conscience de leurs propres responsabilités et à avoir envie de se former davantage. À partir du moment où les collaborateurs cessent de penser que la cybersécurité « leur met des bâtons dans les roues » et commencent au contraire à y voir une clé pour réussir, la partie est gagnée. Au début, nous avons regroupé ce sujet avec d'autres thématiques en lien avec la sécurité au sens large, par exemple la protection contre les incendies. Nous veillons aussi à soumettre les employés à une simulation d'attaque : ils peuvent ainsi se rendre compte par eux-mêmes qu'un incident est très vite arrivé et que les conséquences peuvent être considérables. L'objectif est de remodeler leur conception de la cybersécurité. Le facteur humain n'est pas une simple ligne de défense : c'est la ligne de défense la plus importante.

Nombre de cyberattaques par secteur et par localisation géographique dans le contexte du conflit armé russo-ukrainien



Source : CyberPeace Institute [4]

Les défis auxquels sont confrontées les entreprises

«

Les criminels savent bien, depuis longtemps, que les attaques perpétrées dans le cyberespace peuvent être très lucratives. Il serait presque naïf de penser le contraire.

Stefan Lüders, PhD
Responsable de la sécurité informatique au CERN

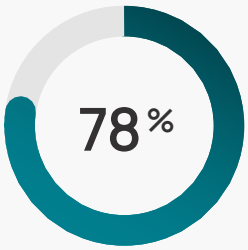
Le fait que les crises géopolitiques et la cybersécurité sont aujourd'hui inextricablement liées n'affecte pas uniquement les gouvernements et les services essentiels, mais aussi les entreprises du monde entier. Ces dernières années, les exemples de cyberattaques menées contre des sociétés en marge de tensions géopolitiques se sont multipliés.

Les gouvernements américain et britannique ont, par exemple, accusé la Corée du Nord d'être à l'origine de WannaCry, une cyberattaque qui a touché plus de 300 000 ordinateurs dans quelque 150 pays, affectant notamment des hôpitaux, des entreprises et des banques, et provoquant plusieurs milliards de dollars de dégâts.[5]

4 **Cyberpeace Institute (2023).** Impact & Harm. How do cyberattacks and operations impact civilians?

5 **Le Parisien (2018).** Cyberattaque mondiale Wannacry : les États-Unis accusent la Corée du Nord.

En 2021, le piratage de Microsoft Exchange qui avait affecté plus de 30 000 sociétés dans le monde entier a, quant à lui, été attribué au gouvernement chinois.[6] Ces différentes attaques montrent bien que les conflits internationaux peuvent avoir des répercussions sur les entreprises et compromettre leur sécurité.



des professionnels de la cybersécurité estiment que la situation géopolitique a entraîné une augmentation des risques cyber pour leur société.

En outre, les tensions géopolitiques sont loin d'être les seuls événements mondiaux exploités par les cybercriminels pour parvenir à leurs fins. Quelques heures à peine après l'effondrement de la SVB (Silicon Valley Bank), en mars de cette année, des pirates commençaient déjà à enregistrer des domaines suspects, à créer des sites de phishing et à préparer des attaques BEC (Business Email Compromise).[7] Les attaquants profitent de l'instabilité croissante à l'échelle mondiale pour affiner leurs stratégies et cibler principalement les secteurs et les régions les plus vulnérables à un instant.

Crises géopolitiques armées : quand les hackers s'en prennent aux particuliers

«

En cas de crise ou de conflit spécifique, les civils se retrouvent impliqués dans des cyberattaques de grande ampleur. C'est particulièrement inquiétant, car il en résulte des cyberattaques qui ratissent large et ne distinguent plus entre civils et militaires.

Stéphane Duguin
PDG de CyberPeace Institute

Dans ce contexte de tensions géopolitiques, les particuliers tendent à être **émotionnellement surchargés, avec des points de vue polarisés**, ce qui les rend encore plus vulnérables à l'ingénierie sociale. Les cybercriminels en sont bien conscients et exploitent ces faiblesses en répandant de fausses informations, en manipulant l'opinion publique ou même en incitant à la violence. Ils mènent des attaques de phishing en surfant sur plusieurs canaux à la fois pour accroître le sentiment d'urgence et effrayer les gens, les poussant ainsi à prendre des décisions sans réfléchir ni s'informer auparavant.

6 **Siecle Digital (2021).** Piratage de Microsoft Exchange : l'UE, l'OTAN, et les États-Unis désignent la Chine.

7 **Le Monde Infomatique (2023).** Les cybercriminels ciblent les clients de la Sillicon Valley Bank.

La guerre menée par la Russie contre l'Ukraine s'est ainsi doublée de cyberattaques massives et coordonnées visant des entreprises et des particuliers, aussi bien dans ces deux pays que dans le monde entier. Aujourd'hui encore, plus d'un an après le début du conflit, on apprend que des escrocs continuent d'exploiter des centaines de sites Internet de fausses associations caritatives afin de détourner des dons pour l'Ukraine.[8]

Sachant l'impact considérable que les événements géopolitiques peuvent avoir sur le paysage des menaces cyber, il est essentiel de nous tenir informés et de mettre en place les mesures de sécurité nécessaires pour déjouer les tentatives d'une cybercriminalité complexe et en perpétuelle évolution.

« La guerre s'organise sur un mode hybride, et nombreux sont ceux qui ont versé dans la cybercriminalité pour soutenir l'un ou l'autre des belligérants. Une fois le conflit terminé, une grande partie de ces attaquants se retrouvera désœuvrée. Ces cybercriminels « au chômage » se mettront alors en quête d'un nouveau défi.

Tobias Ludwichowski
RSSI chez Signal Iduna

8 **Actu.fr. (2022).** Guerre en Ukraine : attention aux arnaques aux dons sur les réseaux sociaux.

« La sensibilisation cyber doit devenir une routine quotidienne rodée, comme le port de la ceinture de sécurité avant de prendre le volant.

Major General Jürgen Setzer
RSSI Bundeswehr

Le général de division Jürgen Setzer est entré dans la Bundeswehr en 1980 en tant qu'élève officier de l'armée de terre. La formation d'officier de l'infanterie a été suivie d'études d'informatique à l'Université de la Bundeswehr à Munich. Depuis avril 2018, le général de division Jürgen Setzer est l'adjoint du chef d'état-major du service Cyber et information, Chief Information Security Officer de la Bundeswehr (CISOBw) et chargé de l'espace de l'état-major du service Cyber et information. Le général de division Jürgen Setzer (né en 1960) est marié et père de deux enfants.

L'état-major du « service Cyber et information » allemand a été créé en 2017. Quel était le facteur déterminant pour sa création ?

Pour relever le plus efficacement possible les défis dans le domaine de l'espace cyber et information, outre la mise en place d'une direction générale Cyber et technologies de l'information au sein du ministère de la Défense, il a été ordonné de regrouper les capacités dans un nouvel élément organisationnel supérieur militaire, le service Cyber et information. Ce service regroupe les forces et les moyens de la Bundeswehr dans le domaine cyber et information.

Quelles sont les missions du service cyber et information de la Bundeswehr ?

Les membres du service Cyber et information sont globalement responsables du domaine cyber et information. Ils assurent la protection et le fonctionnement du système informatique de la Bundeswehr sur le territoire national comme en opération. En outre, ils mettent à disposition et développent les capacités de reconnaissance et d'action dans l'espace cyber et information.

Par ailleurs, ils soutiennent tous les domaines de la Bundeswehr dans l'accomplissement de leur mission en mettant à leur disposition des données géospatiales et contribuent à la prévention sécuritaire à l'échelle nationale en échangeant et coopérant avec d'autres institutions.

À combien et à quels types de cyberattaques la Bundeswehr est-elle soumise chaque jour ?

Les cyberattaques font aujourd'hui partie des risques généraux d'un monde de plus en plus numérisé et n'épargnent pas non plus la Bundeswehr. Elles sont à l'ordre du jour et se produisent des millions de fois par an. Toutefois, l'analyse purement quantitative des tentatives d'attaque ou

d'accès n'est pas très pertinente, même pour la Bundeswehr, car elle ne permet pas de conclure sur les menaces concrètes.

Et comment la menace a-t-elle changée au cours de l'année dernière ?

En règle générale, le potentiel de menace dans l'espace cyber est en hausse en raison des attaques de logiciels malveillants, tels que les chantages numériques avec des rançongiciels, l'espionnage et les tentatives d'extraction de données et d'informations. Depuis des années, on peut observer une tendance progressive à des cyberattaques de plus en plus ciblées et techniquement sophistiquées contre les systèmes informatiques des organisations gouvernementales, des infrastructures critiques, de l'industrie et des institutions scientifiques. En tant que cible potentielle de grande valeur, la Bundeswehr est confrontée aux mêmes menaces que toute autre organisation, mais doit en outre se prémunir des cyberattaques sur mesure de grande complexité. A ces menaces s'est ajoutée l'année dernière une nette augmentation des attaques techniquement moins sophistiquées ayant pour objectif le sabotage par déni de service et présentant un rapport évident avec l'attaque de la Russie sur l'Ukraine. Il semble que des acteurs non étatiques veulent ainsi placer des messages politiques dans l'espace cyber.

Le rapport entre la menace physique et la menace numérique a-t-il changé ?

L'espace cyber offre aux adversaires potentiels la possibilité de provoquer des dommages parfois importants dans l'espace physique, aussi et surtout en dessous du seuil d'un conflit conventionnel. Par exemple, le chantage d'un hôpital en utilisant un rançongiciel pourrait rendre inutilisable des équipements médicaux en soutien de fonctions vitales et donc mettre en péril des vies humaines. Ceci inclut expressément les acteurs étatiques et non étatiques. C'est surtout la possibilité de pouvoir dissimuler sa propre position géographique et frapper sous couvert qui rend l'espace cyber intéressant pour les adversaires potentiels. Ainsi, il s'agit d'une menace permanente, présente bien avant une menace physique et classique potentielle.

Comment cette évolution a- t-elle été influencée par le début de la guerre en Ukraine ?

Avant le début de la guerre d'agression russe en février 2022, de nombreux experts pensaient que le prochain conflit se déroulerait en grande partie dans l'espace cyber et information. On s'attendait à des cyberattaques ainsi qu'à de la désinformation, de la propagande et de petites opérations militaires menées par des forces opérant sous couvert. Des batailles impliquant des forces armées conventionnelles en masse étaient presque inimaginables. Cependant, nous assistons justement à ce type de guerre. Elle est accompagnée d'un nombre inédit d'activités dans l'espace cyber et information, qui ne constituent toutefois pas l'effort principal. Apparemment, on a constaté qu'il est toujours plus facile, moins cher et plus rapide de mettre une centrale électrique hors service par un missile que par une cyberattaque. Nous devons en prendre note et en tirer des conclusions. Néanmoins, il ne faut surtout pas commettre l'erreur de croire qu'il s'agit là du modèle des conflits futurs.

Avez-vous observé des éléments de conduite d'une guerre hybride ?

Oui. Ceux qui suivent les médias ont pu voir comment la Russie a, par exemple, déployé de gros efforts pour diffuser des désinformations sur une opération militaire spéciale visant à protéger la sécurité nationale de la Russie ainsi que d'une partie de la population ukrainienne. L'attaque contre le système de communication par satellite utilisé par l'Ukraine, avec des répercussions sur le fonctionnement des éoliennes allemandes, représente un exemple parfait d'une cyberattaque. Et avec les attaques militaires classiques, nous avons trois éléments marquant une stratégie hybride offensive.

« La guerre d'agression russe est accompagnée d'un nombre inédit d'activités dans l'espace cyber et information.

Diriez-vous que l'Allemagne devrait accorder la même priorité à la cybersécurité quelle accorde aux autres armées ? Ou est-ce déjà le cas ?

Le ministère fédéral de l'Intérieur, de la Construction et du Territoire et ses autorités subordonnées ainsi que les services de police des Länder sont en principe compétents en matière de cyberdéfense (prévention de dangers).

La Bundeswehr travaille en étroite coopération interministérielle avec les autorités de sécurité intérieure (notamment via le Centre national de cyberdéfense). En cas de défense du territoire ou de défense collective, elle dispose de capacités défensives et offensives qui, par-delà la reconnaissance et l'action dans l'espace cyber, servent à prévenir, à détecter et à gérer les cyberattaques contre la TI de la Bundeswehr en Allemagne et à l'étranger.

Au sein de la Bundeswehr, la cybersécurité joue donc un rôle important qui est soulignée par la création d'un élément organisationnel supérieur militaire propre, le service Cyber et information. Ce service se trouve sur un pied d'égalité avec les trois armées classiques que sont l'armée de terre, l'armée de l'air et la marine.

Quelles sont, à votre avis, les trois grandes tendances du côté des attaquants ?

Tendance 1 - Ingénierie sociale.

Tendance 2 - Attaques de logiciels malveillants, notamment avec des rançongiciels.

Tendance 3 - Déni ou déni de service distribué.

Quel est le rôle du facteur humain dans une stratégie de (cyber)défense ? Comment ce sujet est-il abordé au sein de la Bundeswehr ?

Aujourd'hui, les mesures techniques de protection des réseaux sont d'un niveau si élevé que les attaques directes ne dépassent guère la protection du périmètre. Par conséquent, les cyberattaques visent souvent l'utilisateur final de l'informatique et atteignent leur objectif de l'intérieur. L'attention des utilisateurs finals revêt une importance primordiale pour réagir rapidement et correctement. Pour moi, en tant que Chief Information Security Officer, il est donc essentiel de former les membres de la Bundeswehr aux enjeux de la cybersécurité et de développer des résiliences.

L'efficacité des mesures de cybersécurité est régulièrement vérifiée au sein de la Bundeswehr, par exemple par notre campagne de sécurité interne « Phishing as a Service in der Bundeswehr) » (le phishing en tant que service dans la Bundeswehr). Nos militaires et notre personnel civil constituent, pour ainsi dire, la dernière ligne de défense (« The last Line of Defense »). Il s'agit de les sensibiliser et de durcir cette ligne de défense. En effet, la sensibilisation cyber doit devenir une routine quotidienne rodée, comme le port de la ceinture de sécurité avant de prendre le volant.

La cybersécurité ne fonctionne qu'à l'échelle nationale et exige une coopération au niveau interministériel. C'est dans cet esprit que de nombreux services de la Bundeswehr participent chaque année au mois européen de la cybersécurité (organisé en octobre) en apportant des contributions et des mesures de sensibilisation afin de sensibiliser l'ensemble du personnel aux risques liés à l'utilisation des technologies de l'information. Cette participation a pour objectif de renforcer la sensibilisation contre les adversaires potentiels utilisant les innovations numériques également pour attaquer la Bundeswehr et ses alliés.

Comment gérez-vous le changement pour faire de la sécurité de l'information un sujet central dans la culture de la Bundeswehr et, le cas échéant, établir une culture de sécurité ?

La sécurité de l'information est aujourd'hui perçue comme une fonction de commandement importante au sein de la Bundeswehr. C'est déjà un pas important. Pour une culture de sécurité réussie, l'interaction de tous les acteurs au sein du système de la Bundeswehr – à l'échelon des cadres jusqu'à chaque membre individuel de la Bundeswehr - est déterminante. Depuis 2020, nous incitons les chercheurs externes en sécurité de l'information, les « white hat hackers », à trouver des failles dans les systèmes/portails web de la Bundeswehr et à nous les signaler.

Avec la « Vulnerability Disclosure Policy » (politique de divulgation de failles) de la Bundeswehr, nous avons créé un cadre juridique pour les professionnels de la sécurité de l'information leurs permettant d'identifier et de communiquer ces failles et de protéger les systèmes contre les abus accidentels ou intentionnels. Grâce au soutien des personnes qui ont signalé des failles et à leurs documentations détaillées, le niveau de la sécurité de l'information de la Bundeswehr a pu être amélioré. La Bundeswehr a donc joué un rôle de pionnier dans la production d'une telle directive de signalement de failles parmi les autorités publiques.

100 milliards d'euros mobilisés dans un fonds spécial pour la Bundeswehr : comment cela a-t-il influencé votre travail ? Quelles sont les répercussions sur la cyberdéfense, où investissez-vous ?

Il n'y a pas un seul grand projet de cybersécurité. La cybersécurité joue plutôt un rôle important dans chaque projet d'armement et est prise en compte dès le début.

L'ingénierie sociale: la poule aux œufs d'or

Top 3 des stratégies de cyberattaques qui réussissent le mieux

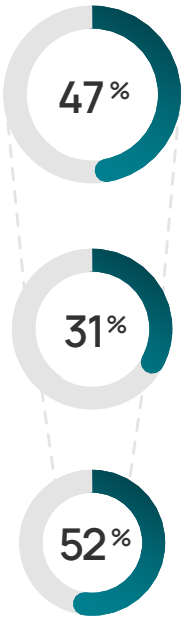
1. Logiciel malveillant
2. Phishing
3. Rançongiciel

> Les points d'accès utilisés lors des cyberattaques ne semblent pas varier beaucoup : infiltration par un logiciel malveillant ou vol de données sensibles par phishing, par exemple.
>
> **Stefan Lüders, PhD**
> responsable de la sécurité informatique au CERN

Dans un contexte où les bouleversements géopolitiques et les crises mondiales élargissent le périmètre de frappe des cybercriminels, et où les progrès de la technologie les aident à perfectionner leurs modèles commerciaux, les stratégies d'attaques sophistiquées gagnent du terrain (plus d'informations à ce sujet au chapitre suivant). Pourtant, les cybercriminels restent fidèles à leur tactique de prédilection : l'ingénierie sociale, qui prend généralement la forme de phishing. Notre enquête a révélé qu'elle arrivait toujours dans le top 3 des stratégies de cyberattaques les plus fructueuses, se classant même au deuxième rang, aux côtés des logiciels malveillants et des rançongiciels. Il est d'ailleurs intéressant de souligner que ces deux autres modes d'attaque commencent eux-mêmes souvent par du phishing ou de la manipulation psychologique. Le fait est que plus de 61 % des professionnels de la cybersécurité affirment que leurs sociétés ont été la cible d'e-mails envoyés par des cybercriminels et que la tendance semble s'accélérer encore.

> Nous recevons de plus en plus souvent des e-mails malveillants. Chaque nouvelle vague est plus forte que la précédente.
>
> **Sascha Czech**
> RSI au CHU Uniklinikum de Münster

Les hackers ont de bonnes raisons pour continuer à faire aussi intensément usage du phishing : selon les données recueillies sur notre plateforme, le phishing reste un outil efficace pour leur permettre d'obtenir des données sensibles et/ou un accès aux systèmes des entreprises. Les statistiques prouvent, en effet, qu'un utilisateur sur trois clique sur le contenu des e-mails de phishing.



Taux d'ouverture

Près d'1 utilisateur sur 2 ouvre les e-mails de phishing…

+2 par rapport à 2022

Taux de clics

un tiers de ces utilisateurs clique sur le contenu malveillant de ces e-mails…

+1 par rapport à 2022

Taux d'interaction

et la moitié d'entre eux continue d'interagir avec leurs contenus.

-6 par rapport à 2022

Bien que les utilisateurs soient un peu plus prudents qu'en 2022, dans leurs interactions avec les contenus malveillants (le taux est passé de 58 à 52 %), les statistiques restent anormalement élevées. Nous constatons encore que, lorsqu'un e-mail de phishing a réussi à déclencher un clic chez le destinataire, il parvient aussi, dans la moitié des cas, à l'entraîner plus loin dans l'interaction en l'amenant, par exemple, à saisir des données sur de faux écrans de connexion. **Les récentes avancées technologiques, notamment l'IA générative, vont très probablement augmenter encore ces ICP.** Elles offrent, en effet, aux criminels de nouvelles opportunités pour améliorer leur contenu de phishing et obtenir davantage de résultats (plus d'informations à ce sujet au chapitre suivant).

Pour quelle raison l'ingénierie sociale est-elle si efficace ? Pour parvenir à leurs fins, les cybercriminels exploitent différents vecteurs qu'ils adaptent constamment aux tendances du moment afin de décupler l'impact de leurs attaques. Si l'on analyse ces vecteurs en détail, on comprend assez vite pourquoi la manipulation psychologique reste au cœur de leurs stratégies : elle continue à atteindre son but, quelles que soient les précautions prises par les sociétés sur le plan technique.

Des ajustements techniques pour remporter la partie

L'une des méthodes utilisées par les cybercriminels pour concevoir des campagnes de phishing encore plus percutantes consiste à apporter des modifications techniques au format de leurs e-mails : ajout d'une pièce jointe ou d'un lien, référence à un masque de saisie ou imitation d'une conversation. Toutes ces variantes continuent de très bien fonctionner, bien qu'elles enregistrent un taux de réussite global nettement moins élevé que les années précédentes. De toute évidence, les **utilisateurs sont plus prudents avec les pièces jointes** et le taux de clics a, à cet égard, diminué de 8 % par rapport à 2022.

Taux de clics par type d'attaque
(comparativement à 2022)

Pièces jointes	Liens
32% -8	25% -1
Masques de saisie	**Conversations**
27% -2	34% -5

Les cybercriminels ont également à leur disposition toute une panoplie de techniques pour manipuler les adresses. Si les modifications simples du nom de domaine ciblé ne génèrent de clics que chez une personne sur cinq ou sur six, **le squat de sous-domaine et l'usurpation d'adresse e-mail trompent davantage** et obtiennent des taux de clics de 26 % et 29 % respectivement.

Les chiffres montrent que les utilisateurs sont de plus en plus conscients des techniques de manipulation utilisées. Dans la mesure où les méthodes traditionnelles, telles que l'ajout d'une pièce jointe malveillante, commencent à perdre de leur efficacité, il faut s'attendre à ce que les attaquants se détournent des techniques de manipulation de masse et adoptent des modes d'action plus sophistiqués.

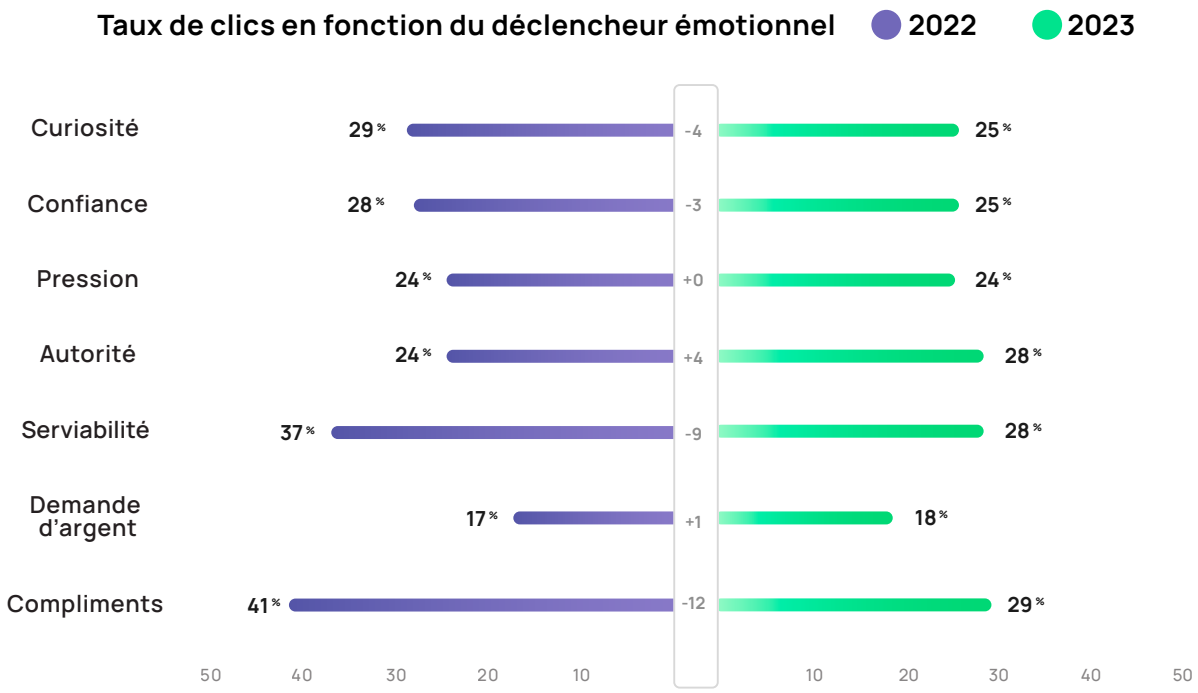
Taux de clics par mode d'attaque

Typosquat	Squat de sous-domaine
17%	26%
Usurpation d'adresse e-mail	Squat de nom de domaine
29%	20%

L'aspect psychologique : jouer sur les émotions

Ce qui fait la force de l'ingénierie sociale, c'est sa capacité d'adaptation. Elle prospère en surfant sur les actualités sociétales ou politiques pour jouer sur les émotions humaines. C'est ce qu'a montré une étude approfondie des vecteurs psychologiques utilisés dans les campagnes de phishing. La force de conviction d'un e-mail de phishing et sa capacité à toucher la corde sensible déterminent de manière décisive le nombre de personnes qui finiront par cliquer sur son contenu malveillant.

Il semble que les émotions susceptibles d'être les plus lucratives pour les cybercriminels ont évolué par rapport à 2022. Bien que les émotions positives provoquées par les compliments ou une attitude serviable continuent généralement à susciter des taux de clics élevés, le succès remporté par les tactiques générant des émotions négatives (ton autoritaire, pression et demandes d'argent) a légèrement augmenté. Il semble donc que les utilisateurs soient devenus plus sensibles à ce type de manipulation psychologique. Cette tendance pourrait s'expliquer par le fait que l'année écoulée a été marquée par de nombreuses crises et conflits qui ont déstabilisé nos contemporains et accru l'anxiété ambiante. Les pirates ont, dans ce contexte, plus de facilité à générer des réactions négatives.



Les intitulés des e-mails sont également révélateurs : ils montrent que les campagnes de phishing qui jouent sur les émotions négatives sont celles qui obtiennent le plus de résultats. Dans le top 5 des tentatives de phishing ayant fait le plus de victimes parmi les employés, quatre jouaient sur un sentiment d'urgence ou de pression.

Top 5 des objets d'e-mails de phishing en 2022

1. **Véhicule accidenté**
   Pression/Curiosité
2. **Invitation sur Teams**
   Curiosité
3. **Erreur sur le salaire**
   Pression/Curiosité
4. **Votre mot de passe Office expire aujourd'hui**
   Pression
5. **Vous avez manqué une conversation sur Teams**
   Pression/Curiosité

Le rôle majeur des formations de sensibilisation à la cybersécurité dans la prévention du phishing

La bonne nouvelle, c'est que les méthodes de formation modernes permettent de sensibiliser durablement les employés aux différentes tactiques d'ingénierie sociale. Les données recueillies sur la plateforme de sensibilisation SoSafe le prouvent : en associant une formation en ligne gamifiée, des simulations de phishing et des outils de signalement contextuels, il est possible d'augmenter jusqu'à 80 % les taux d'alerte phishing. Cette combinaison gagnante contribue fortement à protéger les sociétés des cyberattaques et à accroître leur rapidité de réaction en cas de menace (plus d'informations au chapitre Perspectives). Il est essentiel que ces formations mettent l'accent sur l'humain : les sciences comportementales permettent, en effet, de trouver les méthodes les plus efficaces pour développer, chez les collaborateurs, des habitudes de vigilance. Les professionnels de la sécurité informatique peuvent, par exemple, s'inspirer d'approches telles que le modèle de sécurité comportementale qui met à jour les synergies entre le contexte, les connaissances, la motivation et les comportements au sein des sociétés (voir également le rapport Human Risk Review 2022).

« On pense à tort qu'il n'y a aucune règle dans le cyberespace. Or, c'est faux. De nombreuses lois régissent la cybersécurité, mais elles sont mal appliquées.

Stéphane Duguin
PDG de CyberPeace Institute

Stéphane Duguin est PDG du CyberPeace Institute. Depuis vingt ans, il analyse la façon dont la technologie est détournée et utilisée comme une arme contre les communautés vulnérables. Expert en transformation numérique et en convergence des technologies disruptives, il siège au conseil d'administration de l'Initiative Datasphere et est membre du comité consultatif du Global Forum on Cybercrime Expertise (GFCE). Avant de diriger le Cyberpeace Institute, Stéphane Duguin travaillait comme cadre supérieur chez Europol où il a mené des opérations clés contre le cybercrime et le terrorisme en ligne.

Le CyberPeace Institute a adopté une approche axée sur l'humain. D'après l'expérience que vous en avez, comment les cyberattaques peuvent-elles affecter des particuliers ?

Il ne faut pas oublier que, dans la plupart des cas, l'objectif des cyberattaquants est de jouer sur la psychologie de la victime : il y a donc une dimension de manipulation. Les attaques par rançongiciel, par exemple, sont l'un des rares cybercrimes nécessitant la complicité de la victime. Une personne frappée par ce type de logiciel malveillant se retrouve contrainte de prendre des décisions difficiles avec un profond impact psychologique : faut-il payer ou non la rançon ? Faut-il signaler l'attaque ?

Dans un deuxième temps, les malfrats cherchent à susciter un sentiment de culpabilité chez leur victime. Les ONG sont énormément ciblées par des fraudes au président. En cas d'attaque réussie, la personne qui s'est laissée piéger va souvent être montrée du doigt au sein de l'organisation.

Ces atteintes psychologiques ont une autre conséquence, plus généralisée : elles ont des répercussions sur les bénéficiaires des services de l'entité victime de l'attaque. C'est assez manifeste dans le secteur dans la santé, par exemple. Une étude de Vanderbilt a montré que, lorsqu'un hôpital a subi une cyberattaque, les séquelles restent présentes plusieurs mois, voire un an après. Les patients souffrant de pathologies graves sont moins bien pris en charge qu'avant l'attaque et sont davantage susceptibles de connaître une issue fatale.

Il ne faut pas sous-estimer les retombées psychologiques à long terme de ces événements sur les victimes. Il existe un exemple très parlant, à ce sujet : c'est celui de l'attaque par rançongiciel dont a été victime la clinique Vastaamo, en Finlande. Lorsque cette dernière a refusé de payer la somme exigée, les criminels ont décidé de rançonner, un à un, tous les patients de cette clinique, en les menaçant de divulguer des informations privées sur leur santé psychique. Pour gérer cette crise, la Finlande a dû mettre sur pied une unité de soutien adaptée qui a pris en charge plus de 25 000 victimes.

Dans le contexte actuel des menaces cyber, qu'est-ce qui, selon vous, a changé au cours de l'année écoulée ?

Avant tout, l'évolution de la cybercriminalité vers un modèle commercial. Nous avons constaté une **augmentation très rapide du nombre de groupes criminels utilisant des technologies révolutionnaires**. Les cybercriminels savent collaborer avec beaucoup d'efficacité et exploitent désormais les nouvelles technologies comme des vecteurs d'attaque. On le voit aujourd'hui avec ChatGPT, mais c'était déjà le cas, il y a plusieurs années, lorsque les deepfakes ont fait leur apparition.

Le deuxième point qui me vient à l'esprit est la protection qu'offrent les États contre les menaces cyber. Ils doivent, en effet, veiller à ce que les lois, les normes et les réglementations soient correctement appliquées dans le cyberspace, mais la situation ne va pas en s'améliorant. On pense à tort qu'il n'y a aucune règle dans le cyberespace. Or, c'est faux. De nombreuses loi régissent la cybersécurité, mais elles sont mal appliquées. Les forces de l'ordre n'ont tout simplement pas assez de ressources pour apporter une réponse systématique au problème. Les États contribuent également à envenimer la situation en menant des attaques à des fins de renseignement. Tant qu'ils persistent à utiliser leurs ressources pour des cyberattaques d'espionnage, ils participent à l'insécurité générale dans le cyberespace. En effet, pour que ces opérations de renseignement soient efficaces, ils doivent veiller à entretenir certaines vulnérabilités.

Il y a enfin un troisième aspect, qui a émergé depuis quelque temps déjà, mais semble malheureusement se développer plus que jamais dans le contexte de la guerre en Ukraine, c'est l'enrôlement de civils dans les cyberattaques. Dans un contexte de crise ou de conflit spécifique, les civils se retrouvent impliqués dans des piratages de grande ampleur. Nous avons vu, par exemple, des groupes de hackers russes s'en prendre à tous ceux qui s'opposaient aux intérêts de la Russie et des pirates bénévoles rejoindre les rangs de la cyberarmée ukrainienne. C'est particulièrement inquiétant, car il en résulte des cyberattaques qui ratissent large et ne distinguent plus entre civils et militaires.

Avec l'émergence de nouveaux outils comme ChatGPT, l'intelligence artificielle connaît un essor sans précédent. Selon vous, quel impact aura ce phénomène sur le paysage des menaces cyber ?

Tout ce que nous avons vu en matière de deepfake depuis 2017 a constitué une véritable révolution dans l'univers de l'intelligence artificielle. Quelques années se sont écoulées depuis, et aujourd'hui, certains groupements criminels parviennent à générer des contenus très réalistes et convaincants pour manipuler les gens : une voix ou un visage connu, des e-mails bien rédigés, etc. Par ailleurs, l'intelligence artificielle est une technologie qui permet de mieux analyser l'écosystème social des personnes de façon à élaborer des attaques d'ingénierie sociale très bien pensées.

Nous assistons également à la montée en puissance d'une nouvelle stratégie des cybercriminels : les attaques générées ou assistées par IA. Elles sont mieux automatisées et dévoilent plus facilement l'infrastructure. Pour contrer ces évolutions, il faut donc que nous mettions en œuvre, du côté de la défense, des outils d'intelligence artificielle qui nous protègent mieux.

« Or, à l'heure actuelle, le problème numéro 1, dans le secteur de la cybersécurité, est le burnout : il y a trop de données, trop de dossiers et pas assez de temps.

Vous venez de parler des avantages de l'intelligence artificielle dans le cadre de notre cybersécurité. Selon vous, quels nouveaux défis allons-nous rencontrer en utilisant l'IA dans cette optique de défense ?

Le principal risque est que l'IA va générer une quantité importante de données qu'il nous faudra traiter en tant qu'humains. Or, à l'heure actuelle, le problème numéro 1, dans le secteur de la cybersécurité, est le burnout : il y a trop de données, trop de dossiers et pas assez de temps. L'intelligence artificielle ne va malheureusement faire qu'amplifier ce problème en multipliant encore le nombre de données. C'est assez inquiétant.

Les vecteurs démographiques favorisant le succès de l'ingénierie sociale

Au-delà des facteurs sur lesquels les cybercriminels jouent en déployant leurs modèles d'attaques, d'autres variables démographiques semblent influer sur leur taux de réussite. Assez étonnamment, l'âge a toujours été un facteur déterminant pour le taux de clics : **les natifs du numérique sont ainsi 65 % plus susceptibles de cliquer sur des e-mails de phishing que les utilisateurs plus âgés**. Cette disparité pourrait s'expliquer par le fait que les utilisateurs plus âgés, de par leur expérience de la vie et leur plus grande prudence en ligne, sont mieux armés pour identifier et éviter les éventuelles menaces. Les natifs du numérique (c'est-à-dire, pour ce rapport, les personnes âgées de 18 à 40 ans) ont, en revanche, davantage confiance dans la communication numérique puisqu'ils ont grandi avec. Contrairement à leurs aînés (les personnes âgées de 41 à 60 ans), ils ont tendance à ne pas remettre en question la légitimité de ce que le numérique leur présente.

Les utilisateurs jeunes (18 à 40 ans) sont

↗ 65 %

plus susceptibles de cliquer sur des e-mails de phishing que les utilisateurs plus âgés (41-60).

«

Il faut, dès le départ, intégrer la probabilité d'une cyberattaque dans notre culture et nos tâches quotidiennes.

Thomas Schumacher
Directeur général d'Accenture Security

Les secteurs en ligne de mire

Le succès de l'ingénierie sociale et du phishing varie également d'un secteur à l'autre. Certains secteurs, comme la logistique, l'énergie et le tourisme, ont été fortement impactés par les récents événements sociétaux et affichent des taux de clics record en cas de phishing. En revanche, parmi les secteurs enregistrant les taux de clics les plus bas, certains comptent un fort pourcentage de travailleurs de première ligne : agriculture, construction, matières premières et substances chimiques, par exemple.

Secteur	Taux de clics
Transport et logistique	38%
Énergie et environnement	35%
Tourisme et gastronomie	35%
Pharmacie et santé	33%
E-commerce	32%
Éducation	31%
Services et artisanat	29%
Finance, assurance et immobilier	28%
Technologie et télécommunications	27%
Métal et électronique	26%
Média et marketing	25%
Consommateurs et produits de grande consommation	25%
Commerce	24%
Société	24%
Administration et défense	24%
Internet	23%
Loisirs	23%
Agriculture	20%
Construction	20%
Économie et politique	20%
Produits chimiques et matières premières	16%

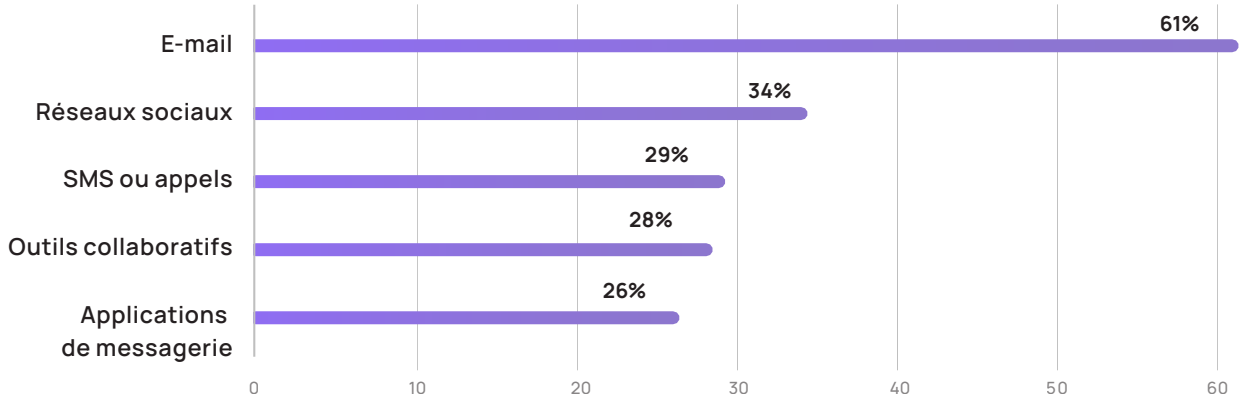
L'avenir du phishing : des e-mails aux outils collaboratifs et aux réseaux sociaux Quelle sera la prochaine étape ?

L'innovation est le propre des cybercriminels : ils ne se contentent pas d'identifier les vecteurs techniques, psychologiques ou démographiques qui leur permettront de perfectionner leurs attaques, mais ils exploitent aussi de nouveaux outils pour les déployer. Si les e-mails restent le moyen par excellence, d'autres canaux gagnent du terrain, lentement mais sûrement.

Peu à peu, les sociétés cessent de communiquer exclusivement par e-mails et il est probable que l'on assiste, dans les années qui viennent, à une diversification des outils de collaboration et de communication. Les cybercriminels sauront en tirer profit.

De fait, les premières attaques menées sur plusieurs canaux ont déjà causé des pertes considérables, dans l'affaire Uber notamment.[1] Dans un message WhatsApp, les attaquants se sont fait passer pour le service informatique et ont poussé un employé à accepter une notification MFA. La société a alors été contrainte d'arrêter une grande partie de ses systèmes afin de limiter l'accès des criminels aux données sensibles.

Canaux utilisés pour cibler les sociétés en 2022



> **Quand nous commençons à introduire de nouvelles technologies dans notre environnement de travail, nous devons prendre en compte les risques dès le départ. Sinon, nous courons à la catastrophe.**
>
> **Thomas Tschersich**
> RSI chez Deutsche Telekom

À l'heure actuelle, les sociétés ne sont pas suffisamment protégées contre les méthodes d'ingénierie sociale. Or, étant donné les progrès fulgurants de la technologie, celles-ci vont indubitablement se perfectionner. L'IA générative en est, d'ores et déjà, un exemple criant. C'est la raison pour laquelle de nombreuses sociétés ont commencé à investir davantage dans leur culture de la sécurité et à placer l'humain au cœur de leurs stratégies.

1 **Le Monde (2022).** Uber victime d'un important piratage informatique.

« Pour être complète, une stratégie de cybersécurité doit intégrer trois grands piliers : la technologie, l'humain et les processus.

Thomas Schumacher
Directeur général chez Accenture Security

Thomas Schumacher dirige le secteur Sécurité chez Accenture pour la région Autriche, Suisse et Allemagne (ASG). Il est également membre de l'ASG Leadership Team et de l'Accenture Security Leadership Team. M. Schumacher a conseillé, pendant plus de 20 ans, de grandes sociétés allemandes en matière de sécurité informatique et d'exploitation des infrastructures informatiques. Il est spécialisé dans les projets de transformation complexes pour différents secteurs, notamment dans le cadre de transitions numériques, d'intégrations consécutives à des fusions et du renforcement de l'efficacité informatique.

Selon vous, quel point essentiel les sociétés doivent-elles toujours garder à l'esprit en matière de stratégie de cybersécurité ?

D'après moi, il faut aborder la cybersécurité et la cyber-résilience, comme nous l'appelons chez Accenture, de façon stratégique. Pour être complète, une stratégie de cybersécurité doit intégrer trois grands piliers : la technologie, l'humain et les processus. Chaque société doit pouvoir répondre aux questions suivantes : « Quel est mon ADN ? », « Que dois-je faire pour être en mesure de maintenir mon activité et mes processus quoi qu'il arrive ? » et « Quels sont les éléments à protéger en priorité ? » Ceci fait, vous pouvez commencer à réfléchir au meilleur moyen pour y parvenir. Beaucoup d'entreprises continuent à se lancer dans cette démarche à l'aveuglette et le manque de préparation finit toujours par les rattraper, notamment en cas d'attaque.

Vous venez de dire que le facteur humain était l'un des aspects à prendre en compte dans les stratégies de cybersécurité. Quel est précisément le rôle des employés ?

On peut toujours avancer que, tôt ou tard, les collaborateurs finiront par cliquer sur quelque chose. C'est probablement vrai : on ne peut pas se protéger de tout. Mais le plus important est de savoir combien de temps vos lignes de défense peuvent résister. C'est la raison pour laquelle il faut synchroniser les trois dimensions : la technologie, l'humain et les processus. Selon moi, c'est une mauvaise idée de tout miser sur la technologie, car on augmente considérablement les coûts. Tout ce qu'une entreprise peut protéger en sensibilisant et en formant ses employés, à l'aide de la technologie appropriée, la rend plus résiliente. En effet, les lignes de défense humaines vont protéger les sociétés quelle que soit la technique d'attaque utilisée, et non se limiter à un cas de figure donné. L'entreprise économise ainsi de l'argent, gagne du temps et s'épargne bien du stress en évitant d'amplifier les risques.

En ce qui concerne la gestion du facteur humain, quelle est la plus grande difficulté ?

Je crois que le principal obstacle à surmonter, c'est notre culture de l'erreur. L'objectif est d'éviter que, la première pensée des gens, lorsqu'ils réalisent qu'ils ont cliqué sur un e-mail de phishing soit : « Il ne faut surtout pas que j'en parle. » Ce qui importe réellement, dans ce cas, c'est la rapidité avec laquelle nous réagissons, en signalant immédiatement l'incident, en comprenant ce qui vient de se produire et en prenant en main la situation

La culture interne d'une entreprise peut-elle avoir une influence sur ce facteur ?

Oui, c'est plus ou moins comparable à l'éducation d'un enfant. Personnellement, j'ai un grand frère et, avec lui, j'ai appris assez vite à me défiler, lorsque j'avais fait des bêtises. Pourtant, à long terme, je me suis rendu compte que ce n'était pas une attitude intelligente, parce que le problème resurgirait probablement plus tard, de manière amplifiée. De même, il est extrêmement important de développer, au sein d'une entreprise, une culture du signalement. Il faut dire aux personnes qui sont à l'origine d'un incident et qui le signalent rapidement : « Ne t'inquiète pas, tu as bien fait d'en parler ». Malheureusement, cette attitude n'est pas encore monnaie courante, notamment dans les PME et en particulier lorsqu'il y a de l'argent en jeu.

Comment impulser des changements positifs dans cette culture d'entreprise ?

Je crois qu'en premier lieu, il faut insister sur le fait qu'on ne peut empêcher ni les cyberattaques ni les erreurs humaines. Il faut, dès le départ, intégrer la probabilité d'une cyberattaque dans notre culture et nos tâches quotidiennes. Par ailleurs, il est important de mettre en place des chaînes de signalement rapides, voire anonymes, pour être sûr que personne, en particulier, ne « porte le chapeau ». Ce principe est plus facile à mettre en œuvre dans les grandes sociétés, où il y a moins de lien avec la perte et l'investissement que chez un particulier.

Parlons plus spécifiquement de la sensibilisation à la cybersécurité : constatez-vous une tendance générale à se détacher des obligations en matière de formations et de politiques pour adopter une approche continue ?

Je vois encore beaucoup d'entreprises s'en tenir aux obligations de conformité. Cependant, il est vrai que de plus en plus de sociétés ressentent la nécessité de former leurs employés, en particulier ceux qui sont en télétravail : des connaissances de base en cybersécurité apportent une réelle valeur ajoutée. Je constate aussi que certaines entreprises éprouvent le besoin de développer leur propre solution de sensibilisation, alors qu'il existe aujourd'hui de nombreux outils spécialement conçus à cet effet.

Les PME ont-elles tendance à aborder différemment la question de la sensibilisation à la sécurité informatique ?

À mon avis, le principal problème des grands groupes est qu'ils pensent tout avoir sous contrôle. Là encore, beaucoup d'entreprises sont concernées, car la cyber-résilience est un sujet très complexe.

Peut-être faut-il élargir un peu la perspective : nous traversons une période où nous devons nous protéger des cyberattaques, des menaces physiques, d'une pandémie et de catastrophes naturelles. Cela fait beaucoup de risques d'un coup. La difficulté réside dans la nécessité d'apporter une réponse qui dépasse le « simple » cercle des menaces cyber.

Or, cette complexité donne justement une dimension totalement différente à la cybersécurité : je dois préparer mes équipes à des scénarios totalement inédits, par exemple à être soudainement dans l'impossibilité de travailler dans les filiales de la société. Il faut associer plus étroitement la cyber-résilience et la résilience d'entreprise.

« Il est extrêmement important de développer, au sein d'une entreprise, une culture du signalement. Il faut dire aux personnes qui sont à l'origine d'un incident et qu'elles le signalent rapidement : « Ne t'inquiète pas, tu as bien fait d'en parler. »

Le contexte actuel tendu accentue-t-il encore la nécessité d'une formation de sensibilisation continue ?

La technologie progresse, les cyberattaques aussi. Il faut donc que les gens adaptent, dans une certaine mesure, leurs habitudes quotidiennes à cette nouvelle situation. C'est un schéma comportemental classique : j'ai conscience que les temps changent et que la technologie évolue, mais je continue à agir comme je le faisais, il y a 20 ans. Personnellement, je pense qu'il faut arrêter de dire aux gens ce qu'ils doivent faire et les amener à s'approprier les réflexes de sécurité comme de nouvelles compétences qui vont s'exercer même au-delà du cadre professionnel. Si j'achète une voiture dotée de la technologie « keyless go », je devrai aussi intégrer le fait que les éléments sont interconnectés et j'adapterai mon comportement en conséquence. Il faut donc insister sur l'idée que la sécurité concerne également nos vies privées et l'incorporer de façon permanente dans notre quotidien de façon que chacun soit constamment en mesure d'ajuster son comportement.

L'innovation technologique dont vous parlez est à la disposition des cyberattaquants depuis longtemps, mais ceux-ci ne semblent pas pressés de sauter le pas. Est-ce aussi votre point de vue ?

Oui, les attaques ont beau être souvent assez simples, elles atteignent malgré tout leur but. Mais on assiste aussi à des cyberattaques destructrices menées par des criminels disposant de ressources financières importantes qui leur ouvrent des perspectives monstrueuses. Je suis quasiment sûr que dès qu'un attaquant mettra la main sur un ordinateur quantique, il l'utilisera pour casser les procédés de chiffrement. Il faut bien comprendre que certains criminels disposent de ressources immenses et nous préparer en conséquence.

Tout cela est assez angoissant. Peut-être est-il aussi nécessaire de dissiper les craintes à ce sujet ?

La peur est toujours mauvaise conseillère. La véritable question est : Que peut-on faire ? Où peut-on aider ? La situation n'est pas désespérée. Il faut juste établir quelques règles de base.

Comment les budgets dédiés à la sécurité ont-ils évolué ? S'adaptent-ils au nouveau contexte ?

MLà encore, il y a de nettes différences entre les grandes sociétés et les PME, et d'un secteur à l'autre. Depuis 2014, les autorités de contrôle poussent tout le secteur financier, notamment les banques et les assurances, à prendre des initiatives en matière de sécurité. Elles ont dépassé l'étape où la « culture de la peur » incite à débloquer des budgets. Ces sociétés font l'objet d'une surveillance étroite et restreignent leurs investissements parce qu'elles ont appris à gérer ce genre de problèmes. Une question reste cependant en suspens : ces secteurs investissent-ils à bon escient ? Personnellement, j'en doute : ils continuent d'investir à l'excès dans des outils et pensent que l'installation d'un nouveau logiciel suffira à dissiper tous les risques.

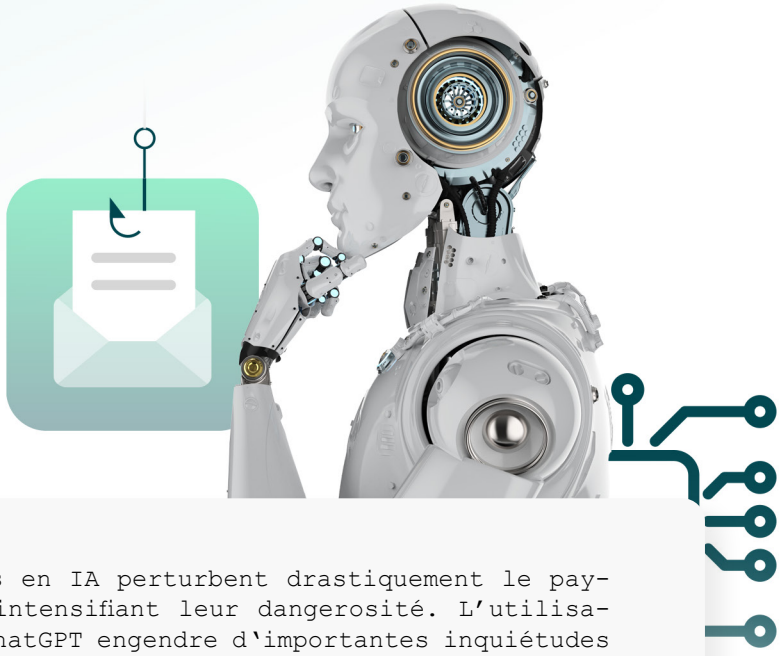
Je pense que, de manière générale, il n'est plus aussi facile de débloquer des budgets. De nombreuses entreprises de taille moyenne ont longtemps pensé que la cyber-résilience ne les concernait pas. Les cyberattaques leur ont prouvé le contraire. En réalité, le plus grand danger est de se lancer à l'aveuglette dans cette démarche et de penser que tout peut être réglé avec la technologie. Bien souvent, ces sociétés n'ont même pas de service informatique en interne. Il nous faut donc une nouvelle génération d'entreprises qui sache évaluer les risques cyber aussi bien que ceux liés au marché.

Quel message aimeriez-vous faire passer aux autres responsables de la cybersécurité ?

Tout d'abord que la cyber-résilience est un problème de société qu'il faut impérativement régler. Nous devons unir nos forces pour parvenir à une solution : plus nous collaborons étroitement dans ce domaine, mieux nous réussirons.

Ensuite, je tiens à rappeler qu'il ne s'agit pas de remporter la médaille d'or de « la société qui gère les risques mieux que tout le monde ». Nous parlons de survie. Ça semble un peu apocalyptique, mais c'est pourtant assez fidèle à la réalité. Le danger est bien réel, il faut en parler davantage sans pour autant semer la panique.

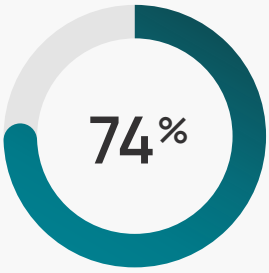
L'IA au service du cybercrime : de l'innovation technologique au cocktail explosif



Les récentes innovations en IA perturbent drastiquement le paysage des cybermenaces, intensifiant leur dangerosité. L'utilisation d'outils tels que ChatGPT engendre d'importantes inquiétudes concernant la protection des données. Ces outils permettent non seulement d'accentuer le phishing, arme privilégiée des pirates, mais aussi de générer de nouvelles formes d'attaques, tels que les deepfakes et le clonage vocal.

Dans cette ère numérique, l'IA démocratise la cybercriminalité en simplifiant la création de menaces pour les pirates. Elle sert aussi à la manipulation sociale, exacerbant ainsi les tensions mondiales. De plus, la possibilité d'utiliser ces outils pour contourner l'authentification biométrique ajoute une dimension supplémentaire à la complexité du combat contre la cybercriminalité. Face à cette évolution, la course entre la protection des données et les cybercriminels s'intensifie de jour en jour.

Ces paragraphes ont été rédigés par ChatGPT-4



des professionnels de la cybersécurité pensent que l'intelligence artificielle va aggraver les menaces cyber

Deepfakes et clonage vocal : quand l'ingénierie sociale est alimentée par l'IA

Si les deepfakes ne datent pas de 2023, ils sont aujourd'hui dans tous les esprits, et pour cause : les pirates s'en servent pour manipuler les masses et exacerber les tensions sur la scène internationale. La vidéo hypertruquée de Zelensky annonçant la capitulation de l'Ukraine en 2022 en a été un exemple marquant.[1]

Mais cette technologie n'est pas uniquement utilisée à des fins politiques. Les cybercriminels élaborent aussi des attaques sophistiquées, associant le vishing au clonage vocal, afin de dérober des données ou de l'argent. Récemment, en Arizona, des malfaiteurs ont tenté de faire croire à une mère que sa fille de 15 ans avait été kidnappée : dans un appel téléphonique, elle a entendu la voix de sa fille appelant désespérément à l'aide. La mère de famille a fini par savoir que sa fille n'était pas en danger et que sa voix avait été clonée grâce à l'intelligence artificielle, mais elle a affirmé qu'elle n'avait, à aucun moment, douté qu'il s'agissait bien de la voix de sa fille.[2] Dans le cadre d'une autre affaire, les criminels se sont fait passer pour le PDG d'une entreprise à l'aide d'un hypertrucage audio et ont convaincu un employé de transférer 35 millions de dollars sur leur compte.[3] Et cette technologie est en train de se perfectionner encore avec des outils comme VALL-E de Microsoft. Celui-ci peut générer un discours en simulant n'importe quelle voix, à partir d'un échantillon audio de seulement 3 secondes.[4]

Alors que les entreprises du monde entier adoptent progressivement l'authentification biométrique, pensant y trouver une alternative plus sécurisée que les mots de passe et les codes pin, il est à craindre que les clonages vocaux et les vidéos hypertruquées permettent de contourner ces nouvelles méthodes de protection. Aux États-Unis, déjà, certaines régions ont interdit l'utilisation de la reconnaissance faciale par les instances gouvernementales.[5] À mesure que la technologie du deepfake va progresser et que de nouvelles utilisations en seront faites, les secteurs public et privé devront joindre leurs efforts pour sensibiliser davantage à son potentiel et à ses limites.

L'IA générative et son exploitation : les attaques menées par ChatGPT

L'avènement de nouveaux outils d'IA a placé entre les mains des cybercriminels des moyens puissants qu'ils apprennent à manier pour perfectionner encore leurs stratégies d'attaque les plus

1 **Siecle Digital (2022).** Un deepfake du président ukrainien rendant les armes diffusé sur la toile.

2 **CNET France (2023).** Des malfaiteurs utilisent une voix générée par l'IA pour simuler une tentative d'enlèvement.

3 **CNews (2021).** Deepfake : Ils dérobent 35 millions de dollars grâce à un appel téléphonique.

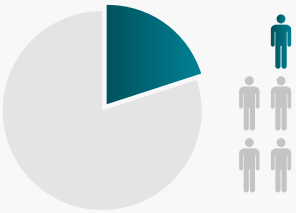
4 **L'Usine Digitale (2023).** VALL-E : l'IA qui imite une voix à partir de 3 secondes d'enregistrement.

5 **La Tribune (2019).** Etats-Unis : les villes s'attaquent à la régulation de la reconnaissance faciale.

efficaces, à commencer par l'ingénierie sociale. Bien que les applications d'IA générative comme ChatGPT interdisent expressément toute utilisation frauduleuse, les hackers ont trouvé de nombreuses façons de les contourner.

Les e-mails de phishing créés par ChatGPT ou d'autres outils similaires sont habilement conçus et bien rédigés, de sorte qu'ils éveillent moins les soupçons que les messages de masse traditionnels. Il va donc être de plus en plus difficile de les détecter, tant pour les filtres anti-spams que pour les destinataires.

Une récente étude réalisée par l'équipe d'ingénierie sociale de SoSafe a révélé que les outils d'IA générative pouvaient aider les groupes criminels à rédiger des e-mails de phishing au moins 40 % plus vite. Plus inquiétant encore : les données recueillies par la plateforme de sensibilisation de SoSafe lors d'une évaluation anonyme de quelque 1 500 simulations d'attaques de phishing en mars 2023 ont montré que les e-mails ayant été rédigés par l'IA étaient ouverts par 78 % des destinataires. Parmi eux, une personne sur cinq est allée jusqu'à cliquer sur le contenu malveillant, lien ou pièce jointe, associé au message.[6] Et ce n'est que le début : le test avait, en effet, été réalisé au moyen d'e-mails de phishing non personnalisés rédigés par ChatGPT-3.5. Or, de nouveaux outils d'IA basés sur des modèles de langage améliorés apparaissent presque chaque jour. Le passage de ChatGPT-3 à ChatGPT-4 a déjà permis de franchir une étape décisive en matière de personnalisation.



1 personne sur 5

clique sur les e-mails de phishing générés par l'IA

Pourtant, le phishing n'est pas la seule stratégie que les hackers ont réussi à perfectionner grâce à l'IA. Cette technologie permet en effet à toute personne possédant un minimum de connaissances techniques de générer un code de logiciel malveillant « polymorphe », capable de changer de forme pour contourner les mécanismes de sécurité traditionnels.[7] Il est à craindre que ces outils ne soient détournés et ne deviennent des armes redoutables entre les mains de n'importe qui, démocratisant ainsi la cybercriminalité.

« Les garde-fous qui ont été posés pour éviter que ChatGPT ne génère du code potentiellement malveillant ne fonctionnent que si le système comprend ce qu'il est en train de faire. Si les invites sont décomposées étape par étape, il est assez facile de contourner les mesures de sécurité.

EUROPOL[8]

6 **SoSafe (2023).** Une personne sur cinq se fait piéger par des emails de phishing générés par l'IA.

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

8 **EUROPOL (2023).** ChatGPT The impact of Large Language Models on Law Enforcement.

9 **Journal du Geek (2023).** L'historique des utilisateurs de ChatGPT fuite à cause d'un bug.

10 **Étudestech.com (2023).** ChatGPT est interdit en Italie.

11 **LINC (2022).** Sécurité des systèmes d'IA, les gestes qui sauvent.

12 **European Commission (2023).** Intellectual Property in ChatGPT.

ChatGPT : vos données sont-elles en sécurité ?

Pour fonctionner efficacement, l'intelligence artificielle a besoin de volumes de données considérables. La question de la confidentialité et de la sécurité des informations fournies par les particuliers et les entreprises pour pouvoir utiliser l'outil se pose alors inévitablement.

Quels sont les risques ?

Le stockage d'énormes quantités de données sur de vastes serveurs ne va pas sans risques. Au début de l'année, un bug relativement simple de ChatGPT a permis à certains utilisateurs d'accéder aux questions posées par d'autres, voire à leurs e-mails de connexion et numéros de téléphone.[9] Cet incident n'a fait que mettre en lumière les faiblesses existantes au niveau du stockage et de l'utilisation des données sensibles par OpenAI. L'Italie a même pris la décision d'interdire temporairement l'utilisation de ChatGPT sur son territoire au motif que l'entreprise ne disposait d'aucune base légale justifiant la collecte massive de ces données sensibles pour entraîner ses algorithmes. Le pays pointe également du doigt des défauts de conformité au RGPD.[10] D'autres attaques, utilisant, par exemple, la rétro-ingénierie pour obtenir les informations sensibles des utilisateurs à partir des conversations, pourraient avoir des conséquences désastreuses et entraîner des violations de données massives.[11] Les experts sont également préoccupés par l'éventualité que ces outils puissent être piratés. Les criminels pourraient, en effet, en compromettre les résultats à des fins de désinformation ou de manipulation, en particulier dans le contexte des grandes crises qui frappent actuellement le monde. Les réponses de ChatGPT posent aussi la question troublante des éventuelles atteintes à la propriété intellectuelle et aux droits d'auteur. Bien que les conditions générales d'utilisation d'OpenAI transfèrent à l'utilisateur tous les droits sur le contenu généré et affirment son caractère original (mais pas nécessairement unique), les réponses fournies par le chatbot proviennent de sources pouvant être soumises à des droits d'auteur.[12]

Que peut-on faire ?

Bien qu'il s'agisse d'une technologie récente, des organismes tels que l'Union européenne promulguent de nouvelles lois visant à réglementer, sur le plan légal, l'utilisation des outils d'IA. Cependant, les utilisateurs peuvent aussi se protéger eux-mêmes en prenant certaines précautions :

- **Ne saisissez jamais d'informations personnelles ou professionnelles sensibles.** Vos données peuvent être collectées à des fins d'analyse ou d'entraînement de l'outil, mais elles risquent aussi d'être exposées en cas de violation de données.
- **Vérifiez toujours les informations fournies à l'aide d'autres sources.** L'intelligence artificielle n'est pas parfaite. Elle peut faire des déclarations qui sont fausses ou avoir été entraînée à partir de sources erronées.
- **Demandez conseil à un juriste avant d'utiliser les résultats fournis à des fins commerciales.** Assurez-vous que vous n'enfreignez aucune loi et ne portez pas atteinte à la propriété intellectuelle.

Des possibilités encore inexploitées

La technologie progresse à une vitesse vertigineuse et, avec elle, les risques de voir l'intelligence artificielle utilisée pour des cyberattaques. Pourtant, malgré quelques cas isolés d'attaques spectaculaires, les hackers n'ont pas encore exploité tout le potentiel de ces outils.

Tant que les méthodes traditionnelles, telles que le phishing de masse ou le spear phishing, restent efficaces pour ouvrir une brèche dans les lignes de défense humaine et s'infiltrer dans les systèmes, il est peu probable que les cybercriminels consacrent le temps et les ressources nécessaires à l'élaboration d'attaques plus sophistiquées. Pourtant, dans la mesure où les outils d'IA sont continuellement améliorés et ouvrent la voie à une véritable démocratisation de la cybercriminalité tout en augmentant les chances de succès et la portée des cyberattaques les plus communes, le risque d'être piégé n'a jamais été aussi grand, tant pour les particuliers que pour les entreprises.

Depuis quelque temps déjà, les cybercriminels ont une technologie extrêmement perfectionnée à leur disposition, notamment le clonage vocal. Pourtant, nous n'avons pas encore vu surgir d'attaques à grande échelle utilisant ces techniques sophistiquées d'ingénierie sociale. C'est donc que les procédés les plus simples continuent de fonctionner. Cependant, avec le partage illégal des accès à de grands modèles de langage et l'explosion de l'IA générative dans tous les domaines, la situation va très certainement évoluer.

Niklas Hellemann, PhD
PDG de SoSafe

Armer les lignes de défense humaines pour résister aux cyberattaques assistées par IA

Depuis longtemps déjà, les professionnels de la sécurité utilisent l'intelligence artificielle pour les assister dans de nombreuses tâches : prédiction et détection d'attaques, réponses automatisées en cas d'incident, entre autres. Or, les récentes avancées de l'IA générative ont mis cette même technologie à la disposition d'attaquants susceptibles de la détourner à des fins malhonnêtes, modifiant de ce fait le paysage des menaces cyber et démocratisant la cybercriminalité. Dans un contexte où l'on continue à découvrir de nouveaux emplois potentiels de l'intelligence artificielle, les forces de l'ordre, les institutions internationales et les fournisseurs d'outils d'IA redoublent d'efforts pour empêcher que cette technologie ne devienne un vecteur d'attaque entre les mains des hackers. Mais aucune loi n'est infaillible et les cybercriminels trouvent sans cesse de nouveaux moyens pour atteindre leurs victimes. Afin d'éviter d'éventuels dommages de grande ampleur, les équipes de sécurité doivent mettre au point de nouvelles stratégies pour s'adapter à ce paysage de menaces en constante évolution, et aujourd'hui assisté par l'intelligence artificielle. Alors que les outils de contrôle de sécurité ont de plus en plus de mal à déceler les menaces, il devient essentiel de développer une solide culture de la sécurité qui sensibilise les humains et les arme contre ces éventualités.

Même si la technologie évolue constamment et nous soulage en grande partie des questions de sécurité, le risque humain reste présent et nous devons nous assurer que notre pare-feu humain fonctionne bien.

Stefanie Boem
Déléguée à la protection des données chez Sport-Thieme

Une nouvelle ère s'ouvre avec la professionnalisation de la cybercriminalité

L'essor de l'IA générative n'a pas seulement contribué à démocratiser la cybercriminalité : elle **favorise aussi, de plus en plus, sa professionnalisation.** Cherchant à organiser davantage leurs activités sur le modèle des entreprises, les cybercriminels versent dans la commercialisation du « cybercrime-as-a-service » (CaaS). La conjonction de différents facteurs leur offre, en effet, un terreau fertile pour organiser leurs collaborations, innover et attaquer des sociétés vulnérables.

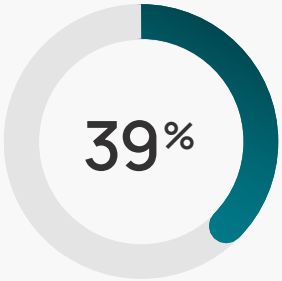
Les rançongiciels, notamment, semblent être les principaux ingrédients de cette tendance au CaaS. Depuis leur lancement à la fin des années 1980, **ils sont restés l'une des formes de cyberattaques les plus fréquentes**, faisant trembler entreprises et particuliers.

Notre enquête souligne bien cette triste réalité : les rançongiciels continuent de compter parmi les types de piratages les plus fréquents et, sur l'ensemble des sociétés ayant subi une cyberattaque au cours des 3 dernières années, une sur trois a été victime d'un rançongiciel. En outre, un pourcentage alarmant (39 %) de ces entreprises a admis avoir payé la rançon exigée. Dans le cas des petites entreprises, c'est même la moitié d'entre elles qui ont été contraintes de payer.

> **Les attaques par rançongiciel sont l'un des rares cybercrimes nécessitant la complicité de la victime. Une personne frappée par ce type de logiciel malveillant se retrouve contrainte de prendre des décisions difficiles avec un profond impact psychologique : faut-il payer ou non la rançon ? Faut-il signaler l'attaque ?**
>
> **Stéphane Duguin**
> PDG de CyberPeace Institute

31%

des sociétés victimes de cyberattaque au cours des 3 dernières années ont été la cible d'un rançongiciel, et



ont admis avoir payé la rançon

La plus grande évolution de l'histoire du rançongiciel est pourtant toute récente : la naissance du rançongiciel-as-a-service (RaaS), au cours des dix dernières années et l'essor qu'il connaît aujourd'hui illustrent bien la capacité des cybercriminels à s'adapter et à diversifier leurs stratégies pour intensifier encore leurs activités illégales.

Le rançongiciel-as-a-service est une véritable pandémie qui affecte les entreprises du monde entier

Aujourd'hui, les cybercriminels n'ont plus besoin de grandes compétences en informatique ou en piratage pour mener des attaques par rançongiciel. Il suffit d'une simple recherche sur le dark web et d'un paiement en cryptomonnaie pour accéder à des plateformes de rançongiciel-as-a-service (RaaS) sur lesquelles les utilisateurs peuvent s'inscrire et même bénéficier d'un service client, comme nous l'ont appris les fuites sur le rançongiciel Conti.[1] Un récent rapport d'IBM a révélé qu'une attaque par rançongiciel coûtait en moyenne aux entreprises, la somme exorbitante de 4,54 millions de dollars (hors rançon).[2] Sur le plan économique, cette méthode continue à faire des ravages parmi les sociétés, et la facilité d'accès aux plateformes de RaaS augmente aujourd'hui, de manière exponentielle, le nombre de cybercriminels en puissance

4,54 M$

Coût moyen d'une attaque par rançongiciel, hors rançon

Source : IBM [2]

L'attaque tristement célèbre de REvil a, par exemple, ébranlé le marché mondial en 2021. Cette attaque de masse perpétrée sur la chaîne d'approvisionnement de l'éditeur de logiciel Kaseya a, en effet, affecté des milliers de sociétés dans le monde entier. L'incident a marqué un nouveau record avec un montant de rançon sans précédent : 70 millions de dollars.[3] Bien que Kaseya ait refusé de la payer, d'autres victimes d'attaques par RaaS, telles que la compagnie d'assurance CNA Financial et le producteur brésilien de viande JBS, ont défrayé la chronique en réglant certaines des rançons les plus fortes jamais payées, à savoir 40 millions et 11 millions de dollars respectivement.[4]

1 **Risk Insight (2022).** Ransomware : Immersion au sein de l'ancien groupe CONTI.

2 **IBM (2022).** Coût d'une violation de données en 2022. Détecter et répondre aux menaces: la course qui valait des milions.

3 **Le Monde Informatique (2021).** Cyberattaque via Kaseya : REvil réclame une rançon de 70 M$.

4 **Hiscox (2022).** Top 10 des cyberattaques qui ont marqué 2021.

Top 10 des rançons payées par les sociétés

Projet	Rançon payée	Franchise de rançongiciel	Origine
CNA Financial	$40.000.000	Phoenix	Russie
JBS	$11.000.000	REvil/Sodinokibi	Russie
CWT	$4.500.000	Ragnar Locker	N/A
Brenntag	$4.400.000	Darkside	Europe de l'Est
Colonial Pipeline	$4.400.000	Darkside	Europe de l'Est
Travelex	$2.300.000	REvil/Sodinokibi	Russie
UCSF	$1.140.895	Netwalker Ransomware	N/A
BRB Bank	$957.245	LockBit	Europe de l'Est
Jackson County, Georgia	$400.000	Sam Sam	Iran
University of Maastricht	$218.000	Ciop Ransomware	Russie

Source : Immunefi [5]

Les cyberattaques de grande envergure menées par le groupe de RaaS HIVE ont également fait la une de l'actualité, l'an dernier. HIVE ne s'est pas contenté de cibler de grandes multinationales des secteurs informatiques et pétroliers, mais s'en est aussi pris aux données et aux systèmes d'organismes publics et sanitaires. Depuis juin 2021, les attaques de ce groupement criminel ont touché plus de 1 500 sociétés dans 80 pays et poussé les victimes à payer près de 100 millions d'euros de rançon.[6]

Nouvel acteur sur le marché du cybercrime, le rançongiciel Sugar a été détecté pour la première fois par l'équipe de sécurité de Walmart en novembre 2021 et concentre actuellement son activité sur les ordinateurs individuels plutôt que sur les grands réseaux d'entreprise.[7] En renonçant à pêcher de gros poissons pour orienter leur action vers les particuliers ou les petites entreprises, avec des demandes de rançons plus faibles, ces cybercriminels élargissent leur base de victimes potentielles, tout en réduisant le risque d'attirer l'attention des forces de l'ordre. Les cybercriminels montrent ainsi leur capacité à nouer des alliances, à mettre en commun des ressources et à apprendre les uns des autres pour ouvrir la voie à des **attaques redoutablement bien coordonnées**.

Avancer en terrain miné : la question des partenariats au sein d'un réseau mondial complexe

L'attaque de Kaseya ne prouve pas uniquement le grand pouvoir des rançongiciels-as-a-service, mais montre bien que la cybercriminalité s'est professionnalisée, **augmentant de façon dramatique l'ampleur, l'impact et la complexité des**

5 **Immunefi (2023).** Top Crypto Ransomware Payments Report.

6 **Numerama (2022).** 1300 victimes, 100 millions de dollars, l'impressionnant butin des hackers de Hive.

7 **Le MagIT (2022).** Sugar, une nouvelle franchise de ransomware.

attaques de la chaîne d'approvisionnement. Face à cette évolution, les sociétés, dépendantes d'un paysage numérique où tout est interconnecté, se retrouvent en position de vulnérabilité. Lors de la cyberattaque, les pirates avaient ciblé le logiciel VSA de la société, un outil de gestion permettant de superviser des services à distance pour les clients.[8] En infiltrant ce logiciel, les criminels ont pu compromettre simultanément les systèmes de milliers de sociétés clientes de Kaseya : de quoi nous rappeler que **notre sécurité dépend de celle des autres**.

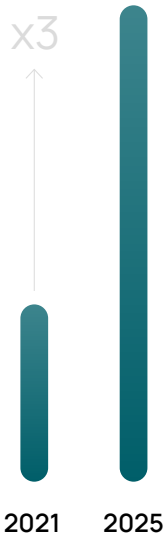
8 professionnels de la sécurité sur **10**

trouvent que la sécurité de leur société dépend de plus en plus de celle de ses partenaires et fournisseurs.

Lors d'attaques de la chaîne d'approvisionnement, les attaquants passent généralement par les maillons les plus faibles, comme de petits fournisseurs ou prestataires moins bien protégés, pour nuire à leur cible principale. Ce mode opératoire a été clairement illustré par la violation de données qu'a subie, cette année, un éditeur de logiciel sous-traitant de la filiale nord-américaine de Nissan. Celle-ci a exposé les noms et les dates de naissance de milliers de clients de Nissan.[9]

Une récente attaque perpétrée sur les applications de VoIP 3CX DesktopApp est également représentative de l'ampleur que peuvent prendre les atteintes sur la chaîne d'approvisionnement numérique. Le système téléphonique logiciel de 3CX est utilisé par plus de 600 000 sociétés dans le monde, dont BMW et McDonald's.[10] À l'instar de celle qui a frappé SolarWinds, cette compromission a infiltré un cheval de Troie dans des programmes d'installation de 3CX DesktopApp pour introduire, au sein des réseaux des entreprises, un logiciel malveillant qui dérobe des informations système et des données depuis les principaux navigateurs Web.

Et cette tendance ne semble pas près de reculer. Gartner prédit, en effet, que d'ici 2025, 45 % des entreprises dans le monde auront été victimes d'attaques contre leurs chaînes d'approvisionnement numérique, soit trois fois plus qu'en 2021.



45 %

des entreprises auront subi des attaques sur leur chaîne d'approvisionnement numérique d'ici 2025

Source : Gartner [11]

Alors que les sociétés d'aujourd'hui dépendent de plus en plus de sous-traitants et de logiciels externalisés pour pouvoir suivre le rythme effréné de notre monde numérique, il est essentiel qu'elles renforcent leurs stratégies de cybersécurité afin de se protéger dans le labyrinthe des chaînes d'approvisionnement numérique.

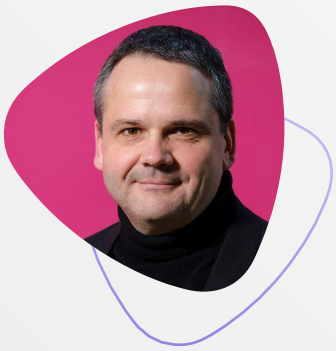
8 **L'Usine Digitale (2021).** Une cyberattaque utilisant Kaseya VSA menace des milliers d'entreprises à travers le monde.

9 **SecNews (2023).** Nissan North America : Violation des données client révélée.

10 **Le Monde Informatique (2023).** L'offre VoIP de 3CX victime d'une attaque supply chain redoutable.

11 **Gartner (2022).** Gartner Identifies Top Security and Risk Management Trends for 2022.

« Quand nous commençons à introduire de nouvelles technologies dans notre environnement de travail, nous devons prendre en compte les risques dès le départ. Sinon, nous courons à la catastrophe.



Thomas Tschersich
RSI chez Deutsche Telekom et PDG de Telekom Security

Responsable de la sécurité informatique (RSI) chez Deutsche Telekom AG et PDG de Deutsche Telekom Security, Thomas Tschersich gère la cybersécurité et la sécurité opérationnelle au sein du groupe. Titulaire d'un diplôme d'ingénieur en électricité, il préside le conseil d'administration de l'initiative « Deutschland sicher im Netz » et est également membre du Conseil de sécurité allemand en cybernétique, ainsi que du comité consultatif d'UP KRITIS.

Pensez-vous que la façon dont les entreprises appréhendent la sécurité informatique et mettent au point leurs stratégies soit problématique ?

La sécurité est en grande partie une affaire de comportement. Souvent, les équipes de cybersécurité ont tendance à totalement interdire certaines choses ou à compliquer inutilement les procédures. Moi, je pense qu'il faut trouver le bon compromis entre la sécurité et un certain côté pratique au quotidien. Si vous négligez le côté pratique, les utilisateurs finiront par trouver un moyen pour contourner les mesures de sécurité.

Avez-vous des exemples ?

C'est une attitude que l'on retrouve à bien des niveaux. Si vous forcez les gens à modifier constamment leurs mots de passe, au fil du temps, les mots de passe deviendront de plus en plus vulnérables. Si les collaborateurs doivent se soumettre à des authentifications multifacteur complexes, vous ne tarderez pas à voir surgir des problèmes de type « Fatigue MFA » : les cybercriminels vont bombarder les utilisateurs de demandes d'authentifications pour les pousser à bout et les faire céder. Si vous interdisez les clés USB, les gens vont probablement envoyer les fichiers sensibles sur leurs boîtes mail personnelles pour en faire des copies. Reste à savoir s'il est préférable de conserver un fichier sur une clé USB protégée et surveillée ou sur un compte personnel.

Je suis convaincu que les mesures de sécurité doivent être transparentes et faciles à comprendre. Si les gens comprennent pourquoi certaines mesures et procédures sont mises en place, ils seront plus disposés à s'y conformer. S'ils ne les comprennent pas, ces règles deviendront vite rébarbatives et ils chercheront à les contourner. .

Pendant longtemps, de nombreuses sociétés ont géré leur politique de cybersécurité comme une liste de tâches à accomplir. Pensez-vous que ce soit toujours pertinent d'agir ainsi aujourd'hui ?

Quand j'ai pris mon poste chez Deutsche Telekom, j'étais également responsable des politiques de sécurité. Aujourd'hui, je plaisante en disant que j'écrivais des politiques que 200 000 collaborateurs s'ingéniaient à ignorer. Bien entendu, il faut mettre certaines choses par écrit, ne serait-ce que pour des raisons de conformité et ce n'est pas un problème. Mais je n'ai jamais obtenu aucun résultat en me contentant d'écrire des politiques. Et je n'ai jamais entendu dire qu'un hacker ait renoncé à ses projets parce qu'il avait lu la politique de cybersécurité d'une société.

Je pense qu'une des erreurs les plus graves que l'on puisse faire en matière de sécurité, c'est justement se contenter des formalités. La certification ISO-27001 ne garantit pas non plus notre sécurité : elle prouve juste que j'ai toutes les clés en main pour me protéger. On ne peut pas se cacher derrière ces réglementations et ces certifications.

Quels sont vos points d'appui, dans ce cas ?

Il est important de pratiquer pour palier rapidement d'éventuelles vulnérabilités comme la gestion des correctifs, par exemple. Nous limitons les politiques au minimum : elles servent juste à définir nos exigences générales en matière de cybersécurité. L'objectif est de se ménager un maximum de temps pour mettre en place des mesures effectives. Nous procédons à une analyse de sécurité et de confidentialité qui nous permet d'identifier nos besoins en matière de cybersécurité, puis nous y remédions immédiatement par des mesures organisationnelles et techniques adaptées. À mon avis, c'est beaucoup plus efficace et cela nous permet de tuer dans l'œuf toute éventuelle faille de sécurité.

Quel conseil donneriez-vous à des entreprises qui cherchent à concevoir une bonne stratégie de sécurité ?

Bien des entreprises renoncent à mettre en place une stratégie de sécurité informatique parce que la complexité de ces procédures leur fait peur. Je suis un fervent défenseur des solutions simples. Nous cherchons à montrer qu'une stratégie de cybersécurité est le fruit de nombreuses petites étapes individuelles. Commencez par mettre à jour les logiciels. Ensuite, on peut investir dans des technologies de défense, tels que des antivirus et des outils EDR pour renforcer encore la protection. L'étape suivante consiste à sensibiliser les employés, et c'est un processus sans fin.

Comment les entreprises peuvent-elles sensibiliser davantage leurs équipes aux problèmes de cybersécurité ?

On confond souvent sensibilisation à la cybersécurité et formation en ligne. Et quand je pense « formation en ligne », je visualise une série de pages qu'on parcourt très rapidement, suivies d'un test avec quelques questions. Ces formations véhiculent une image assez négative et les employés les trouvent plus ennuyeuses qu'enrichissantes.

Comment les rendre plus efficaces ?

Il faut présenter la sensibilisation à la cybersécurité de manière divertissante et faire en sorte que cette formation soit doublement utile, en prodiguant des conseils que les collaborateurs pourront aussi utiliser dans leur sphère privée. Ils verront alors la cybersécurité comme une alliée et seront disposés à modifier leurs habitudes. Il est important que les personnes qui apprennent bénéficient d'un retour d'information. En effet, lorsque nous simulons des attaques de phishing, l'intérêt est minime si les participants ne découvrent les faits que plusieurs semaines après. Les utilisateurs ont besoin qu'on leur donne une appréciation dès qu'ils commettent une erreur. C'est le moment où leur attention est au maximum et où les enseignements auront le plus de poids.

« Les attaques sont devenues extrêmement sophistiquées et c'est dangereux.

Nous assistons actuellement à l'émergence de nouveaux modes d'attaque et de nouvelles tendances en matière de cybersécurité. Quel regard portez-vous sur ces évolutions ?

Je me méfie toujours du mot « tendance ». Il y a quelque temps, le mot à la mode, c'était « chaînes de blocs » et, encore avant, c'était le « cloud ». Nous ne devrions pas toujours nous laisser guider par ces termes. À mon avis, le principal problème est que nous négligeons les bases.

Cependant, je constate que de nombreuses évolutions ont des répercussions sur la sécurité informatique : l'usurpation d'identité (via le phishing ou les fraudes au président), les attaques DDoS et les rançongiciels. À l'heure actuelle, c'est principalement sur ces sujets qu'il faut insister. Or, souvent, la cause première de ces attaques est un manquement au niveau de la mise à jour des logiciels. Il y a également la question de la sensibilisation : vous cliquez sur les fichiers par curiosité, ou parce que vous souhaitez aider quelqu'un, et vous ouvrez la boîte de Pandore. Les attaques sont devenues extrêmement sophistiquées et c'est dangereux. Autrefois, un message qui contenait des fautes d'orthographe ou qui avait visiblement été rédigé par une machine nous mettait la puce à l'oreille. Mais nous avons depuis longtemps dépassé cette étape : aujourd'hui, il n'est plus possible de reconnaître les e-mails de phishing du premier coup d'œil.

Le Machine learning est utilisé, depuis longtemps, pour la cybersécurité. Aujourd'hui, nous assistons à l'essor de l'IA générative qui facilite la tâche des pirates, notamment pour mettre sur pied des attaques par clonage vocal. Avez-vous connu ce type d'attaques dans votre pratique ?

Nous avons vu des fraudes au président sous forme d'arnaques vocales, mais avec des artéfacts. La difficulté, c'est que nous sommes habitués aux visioconférences. Il est donc plus facile, pour de faux participants, de s'immiscer dans ces appels. Il va donc falloir concevoir les « identités numériques » différemment, à l'avenir. Nous devons créer une « identité pour tout », pour ainsi dire : pour les services, les machines, etc.

Voyez-vous une évolution dans le regard que portent les directeurs exécutifs sur la cybersécurité ?

Une évolution dans le regard qu'ils portent, oui, mais pas dans leur manière d'agir. La sécurité informatique est un sujet important qui revient dans tous les échanges avec les clients. Mais j'entends souvent le même refrain : « Pourquoi changer ce qui fonctionne bien ? » Pourtant, en cas d'attaque, les conséquences peuvent être désastreuses.

En fin de compte, la meilleure protection reste la prévention. Est-ce encore plus vrai pour les sociétés qui ont déjà fait l'objet d'attaques par le passé ?

Malheureusement, le fait d'avoir été victime d'une cyberattaque ne provoque généralement qu'un sursaut de vigilance assez passager. Souvent, après une attaque, les différents services mènent des analyses et conçoivent des plans de défense. Mais lorsqu'on rentre dans les détails et qu'il apparaît que ces mesures pourraient coûter quelques millions d'euros, l'attaque est déjà loin et les conséquences se sont estompées au point qu'on n'est pas prêt à investir de telles sommes dans la cybersécurité. C'est un revirement fréquent, surtout dans les petites entreprises. Au sein des grands groupes, la question de la sensibilisation est abordée différemment, mais ils ont des équipes entières qui s'y consacrent.

On considère souvent la sécurité comme un poste de dépenses indirectes, qui ne contribue pas à la productivité. Pourtant, en cas de faille de sécurité, les dépenses peuvent très rapidement devenir directes. Les dommages sur le long terme peuvent être considérables.

Quelles technologies de pointe recommanderiez-vous à d'autres RSI/RSSI ?

Le cloud a révolutionné notre monde. Autrefois, la cybersécurité était assurée par l'intégrité du réseau, mais ce n'est plus le cas. D'ailleurs, Amazon et Microsoft fournissent des pare-feux. Par conséquent, il faut concentrer nos efforts au niveau des applications, sur la gestion de l'identité, le cryptage de données et la gestion des droits. Avec la nouvelle tendance au télétravail, les terminaux prennent également de plus en plus d'importance. Il faut que je sois toujours en mesure de contrôler la fiabilité d'un périphérique à un instant. Pour ce faire, il faut associer les solutions EDR et les accès conditionnels. Enfin et surtout, il faut surveiller régulièrement l'infrastructure et y appliquer des correctifs lorsque c'est nécessaire. Les mesures de sensibilisation permettent aux entreprises de s'acquitter de ces nécessités techniques pour se concentrer sur des problèmes précis, tout en proposant aux collaborateurs une formation continue et adaptée.

> « J'entends souvent le même refrain : « Pourquoi changer ce qui fonctionne bien ? » Pourtant, en cas d'attaque, les conséquences peuvent être désastreuses.

Thomas Tschersich
RSI chez Deutsche Telekom et PDG de Telekom Security

Burn-out et pénurie de talents : les plus grandes craintes du secteur face à l'intensification des menaces cyber

Alors que le monde de la cybercriminalité se professionnalise et innove constamment, la surcharge de travail et le burn-out poussent, sans grande surprise, de nombreux professionnels de la sécurité informatique à démissionner. 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 principaux motifs de démission.[1] Une pénurie de talents dans le secteur de la sécurité informatique, estimée à 3,5 millions de postes vacants, vient encore aggraver la situation.[2]

3,5 millions

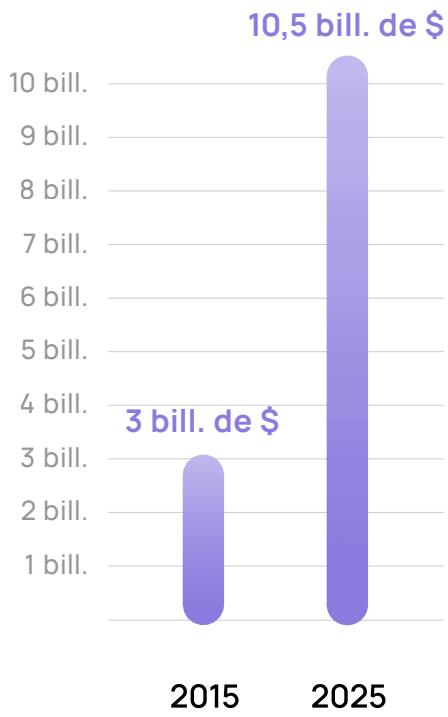
de postes vacants dans le secteur de la cybersécurité

Source : Chartered Institute of Information Security [2]

1 **ISACA (2022).** State of cybersecurity 2022: cyber workforce challenges.

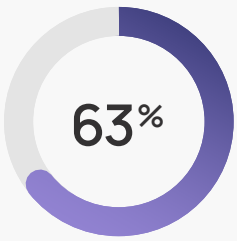
2 **Chartered Institute of Information Security (2022).** The security profession 2021/2022.

Les professionnels de la cybersécurité restants ont donc de plus en plus de mal à suivre les avancées fulgurantes de la cybercriminalité, un secteur qui devrait entraîner des coûts d'environ 10,5 billions de dollars par an à l'échelle mondiale d'ici 2025, contre 3 billions en 2015.[3]



Source : Security Magazine[3]

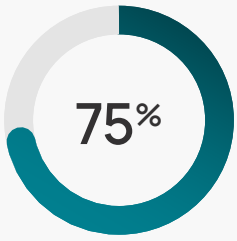
Nous avons montré, dans les chapitres précédents, toute l'inventivité dont les cybercriminels peuvent faire preuve : ils développent de nouvelles stratégies et exploitent les technologies émergentes, mettant à rude épreuve les ressources limitées d'équipes de sécurité déjà surmenées. Un cercle vicieux est en train de s'installer : le sous-effectif alimente le burn-out, et celui-ci vient, à son tour, entraver les efforts de ces professionnels pour ne pas perdre pied face à l'évolution des menaces cyber.



des experts en cybersécurité affirment que l'intensification des menaces cyber les met sous pression

Le travail hybride met les stratégies de cybersécurité à rude épreuve

Bien que certains employés commencent à retrouver leurs bureaux après deux années en télétravail, le travail hybride est en plein essor, de nombreuses entreprises optant pour ce modèle plus flexible. Or, bien que rentable et pratique, cette nouvelle forme de travail s'accompagne de risques accrus en matière de cybersécurité.



des experts en cybersécurité pensent que le télétravail/travail hybride augmente les risques de cyberattaques

3 **Security Magazine (2023).** One of the biggest threats of a cybersecurity team? Employee burnout.

Plusieurs facteurs clés contribuent à augmenter ces risques, notamment :

- **Les vulnérabilités des réseaux privés :**

  les réseaux Wi-Fi privés sont souvent moins sécurisés que ceux des entreprises en raison, notamment, d'un chiffrement plus faible, de paramètres par défaut et de négligences au niveau des mises à jour. L'accès des cybercriminels aux données sensibles s'en trouve alors facilité.

- **Le recours à des connexions sans fil :**

  les collaborateurs en télétravail sont davantage susceptibles de travailler pendant des déplacements. Ils passent, par exemple, leurs derniers appels de la journée dans le train en utilisant des réseaux publics : ces comportements augmentent les risques cyber de manière significative.

- **La surcharge cognitive :**

  les interactions virtuelles sollicitent énormément nos cerveaux, entraînant une baisse de concentration qui ouvre la porte aux attaques de phishing. Les cybercriminels ciblent les personnes au moment où elles sont susceptibles de baisser la garde, à la fin de leur journée de travail, par exemple[4].

- **L'essor des outils collaboratifs :**

  le télétravail va souvent de pair avec une utilisation plus intensive d'outils comme Microsoft Teams, qui deviennent, de ce fait, de nouveaux canaux exploitables par les cybercriminels.

- **Le manque de formation des collaborateurs :**

  la transition vers le travail hybride s'est faite si rapidement que certains employés n'ont pas été suffisamment formés à la cybersécurité.

> Beaucoup d'utilisateurs relâchent leur vigilance lorsqu'ils travaillent de chez eux, dans un cadre moins formel. Ils intègrent beaucoup d'activités privées dans leur flux de travail et sont donc moins attentifs.

Stefan Lüders, PhD
Responsable de la sécurité informatique au CERN

Conclusion : le burn-out, un nouveau vecteur d'attaque

Stress, sous-effectif et nouvelles formes de travail qui augmentent la surface de frappe : la conjoncture est idéale pour les cybercriminels. Ils **profitent de l'épuisement des experts en cybersécurité**, et de ce qu'ils ont, dans ce contexte, davantage tendance à commettre des erreurs d'inattention et plus de mal à trouver des solutions efficaces aux problèmes qui surgissent.[5]

> 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

En outre, les équipes de sécurité ne doivent pas seulement assurer la protection des autres services et réagir rapidement lorsqu'ils sont attaqués, mais elles doivent aussi se protéger elles-mêmes : d'après notre enquête, leur secteur est en effet l'un des plus ciblés par les cyberattaques.

Top 3 des services risquant le plus d'être ciblés par des cyberattaques

1. Informatique
2. Finance
3. Sécurité

Sachant bien que le stress affaiblit les équipes de sécurité informatique, les cybercriminels exploitent le burn-out comme un nouveau vecteur d'attaque. Ils **ciblent plus spécifiquement des entreprises dont les équipes semblent plus vulnérables** vues de l'extérieur.

Il est donc nécessaire que les entreprises investissent, en particulier sur le plan financier, pour retenir les collaborateurs, mettre à leur disposition des ressources adaptées et les former en continu. Elles développeront ainsi des équipes de professionnels solides et une culture de la résilience qui leur permettront de tirer leur épingle du jeu dans le contexte actuel, si complexe.

4 **VentureBeat (2022).** Why hybrid work is leading to cybersecurity mistakes.

5 **ZDNet (2022).** Cybersécurité : le burn-out guette, et cela va devenir un problème pour nous tous.

« Il est important de toujours aborder les stratégies cyber et informatique selon trois perspectives : l'humain, la technologie et le processus.

Tobias Ludwichowski
RSSI chez Signal Iduna

SIGNAL IDUNA

Après un cursus en ingénierie industrielle, Tobias Ludwichowski a occupé différents rôles au sein du groupe allemand SIGNAL IDUNA, depuis 2015 : cadre dans le service de gestion des risques et de gouvernance informatique, responsable du département de sécurité de l'information depuis 2022 et RSSI pour les compagnies d'assurances de la société.

Le regard posé par la direction et les comités consultatifs des sociétés sur la sécurité de l'information a-t-il évolué au cours des années ?

La réglementation qui s'applique à la sécurité de l'information pour les prestataires en assurances se développe rapidement : de plus en plus de lois sont adoptées. Depuis quelques années déjà, l'Autorité allemande de supervision financière travaille beaucoup sur cette question.

De manière générale, les instances de direction ont énormément de pression sur leurs épaules, car ce sujet est associé à la complexité des menaces qui nous entourent. De ce fait, les cadres supérieurs se sont beaucoup sensibilisés aux problèmes de cybersécurité, ces dernières années. Heureusement, il existe aujourd'hui davantage de ressources dans lesquelles nous pouvons investir.

Intéressons-nous plus précisément au monde de l'assurance dans le cyberespace : quelles nouvelles tendances avez-vous remarquées, en tant que professionnel de ce secteur, sur le marché actuel ?

Nous constatons que la cyberassurance se centralise autour des quelques compagnies qui se sont préparées à intégrer ces risques dans la couverture qu'elles proposent. Si l'offre est si limitée, c'est principalement parce qu'il est difficile d'évaluer et d'appréhender les risques cyber d'une entreprise, sur un marché où les menaces changent constamment. Définir, de manière objective, l'efficacité d'une couverture contre les risques cyber actuels et futurs est extrêmement délicat.

D'autant que l'assurance doit être attractive pour le client. Par exemple, des sociétés de taille moyenne n'auront aucun intérêt à souscrire à un contrat qui ne les couvre qu'à hauteur de 200 000

euros. Nous devons aussi garantir que, même assurées contre les risques cyber, les sociétés ne se reposent pas sur leurs lauriers et continuent de se protéger activement. À l'heure actuelle, la cyberassurance est un réel défi.

Comment peut-on faire en sorte que la sécurité de l'information cesse d'être considérée comme un domaine réservé aux initiés et devienne une sorte de projet commun auquel, dans l'idéal, tous aient envie de participer ?

Il faudrait adopter une double approche : d'abord, mettre en place une communication et des formations en continu, pour donner de la visibilité aux éventuels effets des incidents de sécurité. C'est, par exemple, une bonne idée de présenter activement aux collaborateurs les menaces actuelles et les bons gestes à connaître. Cela peut leur être utile même en dehors de la sphère professionnelle et on peut donc rendre les choses plus concrètes en leur expliquant qu'ils doivent aussi protéger leurs comptes personnels.

Dans un second temps, il faut intégrer ces principes dans le flux de travail de telle sorte que les collaborateurs adoptent des comportements sécurisés sans même s'en rendre compte. Il faut concevoir les processus de façon que les employés respectent automatiquement les normes de sécurité : à long terme, ils auront moins l'impression que la cybersécurité leur donne plus de travail. Si vous envoyez des directives et vous attendez à ce que tout le monde les lise, les comprenne et adopte les comportements attendus, ça ne marchera jamais.

> « Les meilleurs outils ne serviront à rien si vos processus ne sont pas adaptés et si vos employés ne sont pas capables d'identifier les risques.

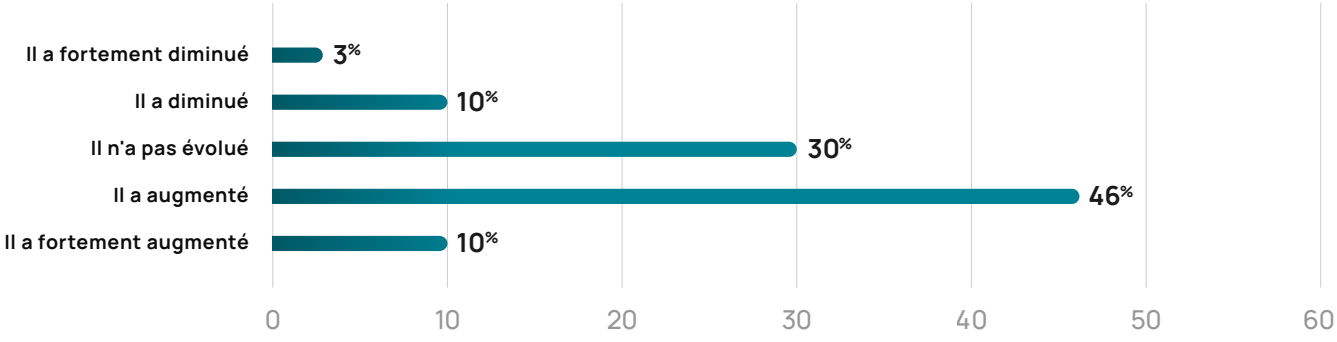
Tobias Ludwichowski
RSSI chez Signal Iduna

La sécurité, une priorité pour les cadres supérieurs : pourquoi la cybersécurité arrive-t-elle à l'ordre du jour au sein des comités exécutifs ?

Face au contexte actuel, les sociétés commencent à faire de la cybersécurité l'une de leurs principales priorités. Cette année, **56 % des professionnels de la sécurité ont, en effet, rapporté que leur direction mettait davantage l'accent sur la sécurité informatique** que l'année précédente.

Ce nouvel état d'esprit et cette volonté de considérer la cybersécurité comme une composante majeure de la stratégie commerciale, de la gestion des risques et de la réussite à long terme de la société, plutôt que comme un simple problème informatique, sont à l'origine de **changements importants au sein des entreprises**. En intégrant cet aspect dans leur conception des choses, les hauts responsables sont en mesure d'harmoniser les stratégies de défense en fonction des objectifs commerciaux, de prévoir les ressources nécessaires, d'initier les changements requis et de définir clairement les responsabilités. Notre enquête met également en lumière les avantages de cette prise de conscience au niveau de la direction.

Le cas échéant, l'intérêt de votre direction pour la cybersécurité a-t-il augmenté ou diminué au cours de l'année écoulée ?



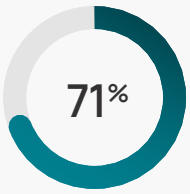
Les sociétés dont les cadres dirigeants sont conscients des risques cyber sont

↗ 67 %

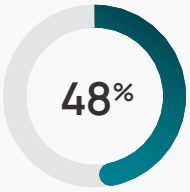
plus susceptibles d'avoir les ressources suffisantes pour couvrir leurs besoins en cybersécurité que celles où la direction n'est pas sensibilisée

Gartner prédit aussi que, d'ici 2026, le contrat de travail **des cadres supérieurs inclura des exigences de performance liées au risque dans 50 % des cas**.[1] Cette évolution aura des répercussions certaines sur la rapidité et la qualité des décisions en matière de cybersécurité, dans la mesure où celles-ci seront de plus en plus prises par des personnes extérieures au service informatique. Les responsabilités seront alors officiellement transférées à d'autres cadres supérieurs. Dans cette optique, certains pays comme les États-Unis commencent à instaurer des réglementations de cybersécurité s'appliquant aux membres des comités directeurs. La SEC (Security and Exchange Commission) a ainsi proposé, en mars 2022, de soumettre les entreprises publiques à de nouvelles obligations de divulgation : elles devraient notamment indiquer si certains membres de leur conseil d'administration possèdent une expertise en cybersécurité, dans la mesure où cela pourrait peser sur les décisions des investisseurs et sur le choix des directeurs.[2]

Niveau ressenti de sensibilisation à la cybersécurité en fonction du degré de sensibilisation au sein de la direction



des experts estiment que le niveau général de sensibilisation au sein de leur entreprise est élevé si la prise de conscience est forte au niveau de la direction



d'entre eux estiment que le niveau général de sensibilisation est élevé si la prise de conscience est faible au sein de la direction

L'attention que les hauts dirigeants portent à la cybersécurité a un impact considérable sur la cyber-résilience au sein des sociétés, y compris **parmi le personnel**. Selon notre enquête, le niveau ressenti de sensibilisation à la cybersécurité dans une entreprise dépend grandement du degré de prise de conscience des dirigeants : 71 % des professionnels de la sécurité informatique estimant que leur direction est bien au fait des risques cyber pensent que leur société est très vigilante à ce sujet, contre 48 % chez les professionnels qui ressentent des lacunes en la matière parmi leurs cadres dirigeants.

1 **Gartner (2022).** Gartner Says the Cybersecurity Leader's Role Needs to Be Reframed.

2 **Security and Exchange Commission (2022).** SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies.

Survivre dans la jungle des menaces cyber : la nécessité de savoir s'adapter au sein des comités directeurs

«

La cybersécurité est une véritable course de vitesse : tout change très vite, il faut constamment se former et se tenir à jour. Il est donc essentiel de développer de nouveaux modèles, en investissant plus massivement dans les formations, par exemple, ou en intégrant, au sein des comités consultatifs, des personnes plus jeunes, disposant d'une expertise spécifique, même si elles n'ont pas d'expérience en direction d'entreprise.

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

Tenter de suivre le rythme effréné du cyberespace en constante évolution peut s'apparenter à une course sans fin où il faut sans cesse accélérer. Les dirigeants d'entreprise commencent à considérer la cybersécurité comme une priorité. Cependant, alors qu'ils ont l'habitude de s'appuyer sur leurs acquis pour gérer les difficultés, ils n'ont pas tous une grande expérience du numérique et des questions de sécurité informatique. Il devient donc essentiel d'aborder ce problème avec un regard neuf, à la fois en **formant les hauts responsables en continu**, mais aussi en **modifiant la composition des comités** pour intégrer, par exemple, des personnes dotées de compétences spécifiques, mais peut-être moins chevronnées en matière de management.

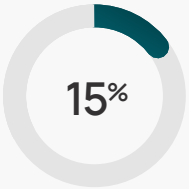
Une autre option serait d'inviter régulièrement l'équipe de sécurité informatique aux réunions du conseil d'administration, afin de discuter ouvertement de la position de la société en matière de cybersécurité et de son exposition aux risques, de manière générale. La capacité d'adaptation et la collaboration peuvent renforcer considérablement la cyber-résilience en permettant d'identifier les domaines à haut risque et de fixer des objectifs de sécurité qui limitent les dangers.

Les budgets dédiés à la cybersécurité augmentent, mais restent insuffisants

Ces dernières années, les sociétés tendent à augmenter leurs investissements en cybersécurité. D'après le pronostic de Gartner, **les dépenses globales en matière de sécurité et de gestion des risques devraient augmenter de plus de 11 % en 2023**, pour atteindre 188 milliards de dollars, contre 158 en 2021.[3] Cette évolution s'accompagne d'une volonté de traiter la cybersécurité comme une priorité en l'inscrivant à l'ordre du jour des conseils d'administration. Notre enquête révèle ainsi que la culture de la sécurité est une priorité dans seulement 15 % des sociétés manquant de ressources en la matière, contre 94 % chez celles qui ont des ressources suffisantes.

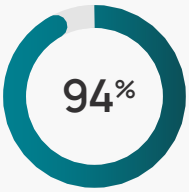
Quoi qu'il en soit, pour développer une cybersécurité efficace, il est impératif d'adopter une approche qui ne se limite pas exclusivement à la technologie et aux outils. Déployer des efforts de sécurité qui soient en phase avec les objectifs commerciaux et promouvoir la cybersécurité au rang de priorité pour les cadres dirigeants sont certes des initiatives utiles, mais il faut les intégrer à une stratégie plus globale.

Parmi les entreprises qui manquent de ressources adaptées en cybersécurité seulment



font de leur culture de la sécurité une priorité

contre



des sociétés ayant les ressources nécessaires

La fréquence des cyberattaques augmente plus vite que les budgets alloués à la cybersécurité et les attaquants savent qu'ils ont de grandes chances de réussir en ciblant le facteur humain, puisque 82 % des violations de données exploitent ce vecteur.[4] Il est donc aujourd'hui plus important que jamais de prendre des mesures efficaces de sensibilisation à la cybersécurité pour ancrer en chaque collaborateur des réflexes de sécurité.

3 **Gartner (2022).** Gartner Identifies Three Factors Influencing Growth in Security Spending.

4 **Verizon (2022).** 2022 Data Breach Investigations Report.

« On entend souvent dire que l'informatique coûte trop cher, mais les investissements réalisés dans ce domaine sont des leviers qui permettent la croissance de l'entreprise, qui améliorent la qualité des services et qui, grâce à l'automatisation, garantissent des économies à tous les niveaux.

Jens Becker
Directeur des systèmes d'information (DSI),
Zurich Gruppe Deutschland

Jens Becker est DSI et responsable du service numérique au sein de la filiale allemande du groupe Zurich depuis janvier 2021. À ce titre, il gère l'initiative « Accelerated Evolution » du service informatique. Il a travaillé auparavant en tant que consultant chez KPMG et a assuré diverses fonctions de direction au sein des services informatiques d'AXA pendant plus de 12 ans. Il a mené à bien plusieurs projets de transition numérique : c'est notamment lui qui a instauré le modèle DevOps lorsqu'il dirigeait le service des opérations informatiques et a initié la migration sur le cloud chez AXA.

À votre avis, que faudrait-il pour pousser les dirigeants à s'impliquer davantage dans la sensibilisation à la cybersécurité ?

La plupart des cadres supérieurs comprennent, intellectuellement parlant, que la cybersécurité est ou doit être une priorité. La vraie question est de savoir si cette prise de conscience aboutit à des actes, si elle déclenche une vigilance durable ou si l'on continue de considérer que, dans certaines circonstances, c'est plus pratique de ne pas verrouiller l'écran ou chiffrer les données.

Si l'on veut renforcer la vigilance et faire prendre conscience aux gens de la réalité des menaces qui nous entourent, de la nécessité de développer la cyber-résilience, et de la manière dont il faut traiter les données sensibles, je crois qu'il ne faut pas uniquement se concentrer sur le monde de l'entreprise. Il faudrait rendre obligatoire l'acquisition de ces compétences dès l'âge scolaire. Les élèves doivent savoir que l'on peut dérober leurs mots de passe et usurper leur identité. Il faut les y sensibiliser sans pour autant leur faire peur, pour qu'ils sachent gérer correctement d'éventuelles attaques.

Au niveau d'une entreprise ou d'une société, le degré d'exigences est naturellement plus élevé. Les employés sont tenus de traiter les données des clients en toute confidentialité et doivent être conscients de leur responsabilité à cet égard. Ce point doit également être abordé en conseil d'administration, en insistant sur le fait que chaque service

est responsable des concepts d'autorisation, doit assurer la continuité de l'activité et sécuriser le traitement des données personnelles.

Récemment, lors d'un événement, vous avez souligné que les sociétés devaient faire des économies grâce à l'informatique, et non en informatique. Pourriez-vous préciser votre pensée à ce sujet ?

Absolument. On entend souvent dire que l'informatique coûte trop cher, mais les investissements réalisés dans ce domaine sont des leviers qui permettent la croissance de l'entreprise, qui améliorent la qualité des services et qui, grâce à l'automatisation, garantissent des économies à tous les niveaux.

Les tâches simples devraient être automatisées pour que les équipes d'assistance puissent se concentrer sur des points plus importants. Les chatbots offrent des solutions économiques pour prendre les appels, trier les demandes des clients et en vérifier le bien-fondé. Ils soulagent ainsi les collaborateurs et leur permettent de se concentrer sur les vrais besoins. L'automatisation aide également à adapter les temps de réponse aux attentes des clients. Lorsque nous correspondions par courrier postal, nous avions l'habitude de patienter deux semaines avant de recevoir la réponse. Aujourd'hui, avec les e-mails, nous nous attendons à obtenir un retour dans les deux jours. Une prise en charge rapide des demandes, selon le principe du « first time right », augmente la satisfaction des clients et réduit les frais de traitement.

Et puisque nous parlons de transition numérique, nous devons aussi faire des efforts pour numériser des éléments physiques comme notre courrier. Notre secteur a encore de gros progrès à faire dans ce domaine et les investissements faits en ce sens auront de nombreuses retombées positives, comme la réduction des frais d'affranchissement et des dépenses en papier ou la diminution des émissions en CO2.

Il est donc préférable d'investir aujourd'hui pour limiter les risques ?

C'est une évidence. Il vaut mieux installer des coupe-feu aujourd'hui que d'avoir à éteindre l'incendie et à financer les réparations demain. Il faut juste trouver le bon équilibre. Selon certaines directives officielles, les sociétés devraient investir 7 % de leur budget informatique dans la cybersécurité. Pourtant, vous pourriez investir tout votre budget dans la cybersécurité et rester exposé. Il est donc nécessaire d'adopter une approche appropriée, qui cible les principaux risques. Les normes NIST et ISO, entre autres, fournissent de bons repères à cet égard. Dans le cadre de partenariats, elles prouvent aussi que vous avez atteint un certain niveau de sécurité. De manière générale, il est important de continuer à investir et de ne jamais se reposer sur ses lauriers.

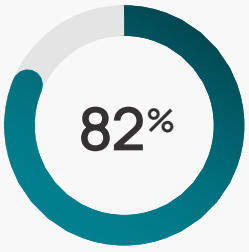
En règle générale, les sociétés investissent-elles suffisamment ? Ou considèrent-elles toujours la cybersécurité comme un dossier qui sera refermé un jour ?

Oui et non. Pour répondre à la première question : je pense qu'elles investissent beaucoup, mais jamais assez. C'est la raison pour laquelle Zurich a adopté une « approche par classement forcé » : nous avons créé une matrice dans laquelle nous saisissons les différents risques. Nous les traitons ensuite pas à pas, en suivant cette matrice.

Pour ce qui est de la seconde question : cela fait maintenant plusieurs années que nous procédons ainsi et il n'est pas question de relâcher nos efforts à l'avenir.

Perspectives : pourquoi faut-il intégrer la cybersécurité dans notre quotidien

Les chapitres précédents nous ont montré que la cybercriminalité a pris une ampleur considérable et s'est beaucoup professionnalisée. Devenus experts en stratégies innovantes et sophistiquées, les attaquants s'engouffrent dans la moindre faille. Ce contexte en constante évolution représente un défi de taille pour les entreprises, les gouvernements et les particuliers qui luttent pour préserver leurs actifs dans un monde où tout est de plus en plus interconnecté. Le plus inquiétant est que **cette situation ne va probablement pas aller en s'améliorant** : selon notre enquête, 8 professionnels de la cybersécurité sur 10 pensent que les menaces vont perdurer au cours des 12 prochains mois.



des experts en cybersécurité prédisent que les tensions actuelles vont persister au cours des 12 prochains mois

Un examen plus approfondi des données a également montré que l'ingénierie sociale restait au cœur des cyberattaques et parvenait à contourner les nombreuses mesures techniques prises par les sociétés. Alors que les attaques par e-mail restent très répandues et que les hackers gagnent peu à peu du terrain sur d'autres canaux, tels que les réseaux sociaux et les outils collaboratifs, les entreprises commencent à prendre conscience de l'importance d'une solide culture de la sécurité qui place le facteur humain au centre de sa stratégie.

«

Nous recevons sans cesse, dans nos boîtes de réception, des milliers de spams inoffensifs. Malheureusement, il s'y mêle aussi des e-mails de phishing dangereux et ce, malgré de nombreux contrôles de sécurité. Nos collaborateurs doivent apprendre à ne pas tomber dans ces pièges. C'est la raison pour laquelle nous tenons autant à ce qu'ils suivent une formation de sensibilisation.

Frank Heymann
Senior IT Team Manager chez Buhlmann

Pour y voir clair dans ce paysage de menaces de plus en plus complexe, les sociétés ont grand besoin de formations efficaces qui sensibilisent leurs collaborateurs à la cybersécurité et leur apprennent à protéger l'entreprise de manière proactive, sur tous les fronts : au niveau des e-mails, mais aussi sur tous les nouveaux canaux de communication.

« Ces 10 dernières années, les entreprises ont davantage investi dans la technologie que dans les personnes. Elles commencent à comprendre que la technologie ne fait pas tout et que l'ingénierie sociale, en particulier le phishing, pose un réel problème. Beaucoup de ces entreprises sont aujourd'hui en bonne voie, mais ont encore du chemin à parcourir.

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

Les formations de sensibilisation à la cybersécurité sont notre plus grand espoir...

« Les êtres humains ont toujours plus de facilité à comprendre les comportements d'autres êtres humains. Si vous ne comptez que sur la technologie en pensant qu'elle interceptera tout, vous faites erreur.

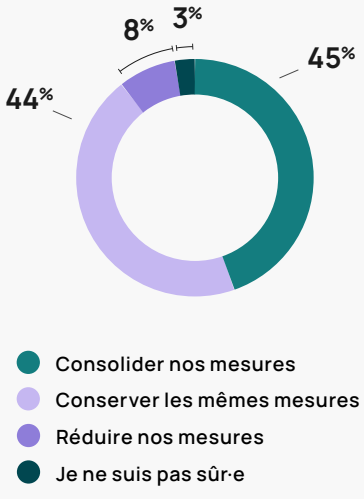
Tobias Ludwichowski
RSSI chez Signal Iduna

Fort heureusement, de nombreux services d'informatique et de cybersécurité ont aujourd'hui conscience du rôle majeur que joue le facteur humain dans leur entreprise. Notre enquête montre que la priorité numéro 1 des professionnels de la sécurité informatique est de mieux sensibiliser les employés. Ce point arrive en tête de liste, devant la gestion des identités et des accès, et la sécurisation du travail hybride ou des processus existants. Par ailleurs, 9 experts sur 10 ont affirmé que leur société allait maintenir ou renforcer les mesures de sensibilisation à la sécurité informatique.

Principales priorités des services d'informatique et de sécurité

1. Sensibiliser davantage les employés à la cybersécurité
2. Renforcer la gestion des identités et des accès
3. Sécuriser le travail hybride
4. Sécuriser les processus existants

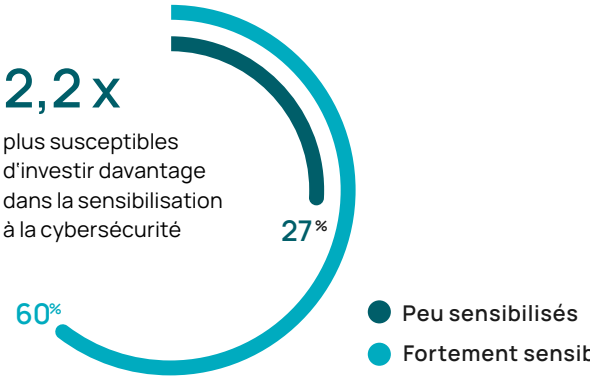
Quels sont vos objectifs en matière de consolidation ou de réduction des mesures de sensibilisation à la cybersécurité en 2023 ?



... mais il faut le soutien de la direction

Nous avons vu, dans la dernière section, combien il est important que les directions d'entreprise comprennent les défis liés à la sécurité informatique et y réfléchissent. Les conclusions de notre enquête abondent dans ce sens : la conscience qu'ont les cadres dirigeants des risques cyber a un impact direct sur la priorité accordée aux investissements pour promouvoir la sensibilisation à la cybersécurité.

Conséquences du niveau de sensibilisation aux risques cyber chez les cadres dirigeants



Notre enquête révèle également que **94 % des sociétés disposant de ressources adaptées en matière de cybersécurité considèrent le développement d'une culture de la sécurité comme une priorité**. En revanche, parmi les sociétés manquant de ressources dans ce domaine, seules 15 % estiment qu'il est prioritaire de construire une culture de la sécurité. Cette disparité ne fait que souligner à quel point l'engagement d'une société en matière de cybersécurité dépend des ressources dont elle dispose et du degré de conscience de ses dirigeants.

Il est donc essentiel que les professionnels de l'informatique et de la sécurité communiquent en continu avec les cadres supérieurs et soient en mesure de produire des chiffres et des ICP qui étayent leurs explications. En cherchant non seulement à quantifier les performances, à l'aide de mesures comme les taux de clics, mais aussi à présenter l'évolution des comportements au fil du temps et les résultats en termes de sécurité de manière générale (par exemple, l'impact du bouton d'alerte phishing sur le taux de signalement dans le temps), il est possible d'inscrire durablement la cybersécurité au nombre des priorités de l'entreprise.

Sciences comportementales : le présent et l'avenir de la sensibilisation à la cybersécurité

Si la sensibilisation à la cybersécurité n'est pas une nouveauté dans le monde de l'entreprise, elle connaît aujourd'hui une mutation profonde afin de pouvoir répondre efficacement à tous les défis qui émergent. Les schémas de formation traditionnels, dont l'objectif premier est de remplir les obligations de conformité, sont insuffisants pour capter l'attention des employés et les pousser à s'impliquer dans la lutte contre les menaces cyber. Les conclusions de notre étude soulignent ces limites :

Top 3 des raisons pour lesquelles les utilisateurs ont du mal avec les formations de sensibilisation à la cybersécurité :

1. **Elles prennent trop de temps**
2. **Les informations sont trop génériques**
3. **La formation est trop répétitive**

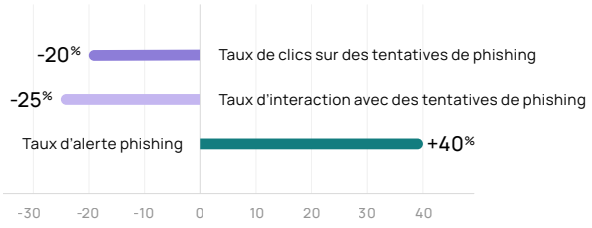
De toute évidence, les sociétés doivent donc aller au-delà du simple respect des normes et établir une solide culture de la cybersécurité : il faut développer activement des réflexes de défense chez les employés, tout en proposant des sessions pédagogiques adaptées à leurs modes de travail et à leurs

emplois du temps chargés. Pour y parvenir, **il est essentiel d'axer les programmes de sensibilisation sur le facteur humain et d'y intégrer des méthodes inspirées des sciences comportementales**, comme le micro-apprentissage, la gamification et les rappels automatisés. C'est ce type de formation qui fournira aux employés les clés pour prendre des décisions éclairées, que ce soit dans leur quotidien professionnel ou dans leurs vies personnelles.

Mettre la cybersécurité à la portée de tous, l'intégrer de manière fluide dans les activités de chaque jour, c'est garantir une prise de conscience généralisée à tous les niveaux de l'entreprise et créer une véritable synergie entre cybersécurité et production. Il nous faut agir de manière proactive et stratégique, afin de lutter contre le fléau d'une cybercriminalité implacable, dont les conséquences se chiffrent aujourd'hui à plus d'un milliard de dollars. Pour tirer notre épingle du jeu, il est crucial de savoir s'adapter et évoluer avec la même rapidité que ceux qui nous menacent.

On constate que, grâce à ces méthodes inspirées des sciences comportementales, un plus grand nombre de personnes suit la formation jusqu'au bout. Au niveau des indicateurs, cela se traduit par une baisse des taux de clics et d'interaction avec les e-mails de phishing et par une hausse du taux de signalement. C'est un grand pas en avant dans la stratégie de défense des entreprises qui ont ainsi toutes les clés en main pour repousser les éventuelles attaques.

UTILISATION DU PRODUIT
Résultats provenant des utilisateurs avec des taux élevés d'achèvement des modules



Développer de nouveaux réflexes ancrés dans la durée

Différentes approches et méthodes permettent de tirer le meilleur parti de ces formations de sensibilisation et de les intégrer aux contextes dans lesquels évoluent les collaborateurs. La **répétition espacée**, par exemple, consiste à revenir régulièrement sur les informations, par le biais de différents canaux. Elle rappelle aux utilisateurs ce qu'ils ont appris afin que les effets perdurent sur le long terme. Pour alimenter le côté interactif et stimuler la vigilance, on peut y ajouter des **rappels automatisés**, notamment sous la forme d'e-mails envoyés à intervalles réguliers. Le **micro-apprentissage** permet, quant à lui, de consolider les acquis et de favoriser la rétention des connaissances. Sur la plateforme de SoSafe, nous avons ainsi opté pour des formats courts, faciles à assimiler, avec une approche narrative qui favorise l'engagement.

Être arnaqué ou ne pas être arnaqué

Pour garantir l'efficacité d'une formation à la cybersécurité, il est également essentiel de l'adapter au contexte des utilisateurs. Les simulations de phishing, par exemple, sont des mesures contextuelles qui ont fait leurs preuves. Elles consistent à tester les connaissances acquises de manière théorique par une mise en situation pratique. Intuitif et réaliste, ce mode d'apprentissage simule des attaques envoyées de manière inattendue, dans le flot des activités quotidiennes. Il permet d'ancrer, chez l'utilisateur, des habitudes durables. De nombreux experts s'accordent à dire qu'en associant ce type de simulations avec des contenus pédagogiques correspondants, il est possible de limiter efficacement les risques cyber :

«

Dans un monde où nous sommes tous submergés d'informations et n'avons pas le temps d'apprendre, il est essentiel de dispenser les unités d'apprentissage aux employés sous un format très court et de les leur présenter au point de rupture, lorsque la motivation pour apprendre est très forte. C'est ce qui se passe par exemple, lorsqu'une page de formation apparaît après que l'utilisateur a cliqué sur un faux e-mail de phishing. Répartie en tranches de 5 minutes, la formation de sensibilisation à la cybersécurité s'intègre parfaitement dans une journée de travail très chargée.

Martin Schmidt
Directeur général de la consultance numérique, chez Freudenberg Home and Cleaning Solutions

«

Il est très important que les personnes qui apprennent bénéficient d'un retour d'information. Lors des simulations de phishing, les utilisateurs ont besoin qu'on leur donne une appréciation à la fin du test. C'est le moment où leur attention est au maximum et où les enseignements auront le plus de poids.

Thomas Tschersich
RSI chez Deutsche Telekom

«

L'interaction avec une simulation de phishing est toujours suivie d'un moment de « révélation » où l'utilisateur comprend son erreur et découvre comment il aurait dû réagir. Il ressort généralement de cette expérience mieux armé, avec une meilleure compréhension des risques.

Stefan Lüders, PhD
Responsable de la sécurité informatique au CERN

Il s'agit d'incorporer, dans l'infrastructure existante, **des composants et des outils contextuels** qui permettent aux employés de prendre une part active à la stratégie de défense contre les cyberattaques. Les statistiques montrent, par exemple, que le **bouton d'alerte phishing** de SoSafe réduit de 30 % les interactions des collaborateurs avec les e-mails de phishing. Cette fonctionnalité limite ainsi les chances de succès d'éventuelles attaques et présente des avantages évidents :

Impact du bouton d'alerte phishing

↗ 38 %
Taux d'adhésion à la formation en ligne

↗ 25 %
Pourcentage de personnes ayant terminé le module

Les besoins en innovation : quelle est la demande, au sein des entreprises, en matière de fonctionnalités

Dans notre enquête, nous avons demandé aux professionnels européens de la cybersécurité quelles autres fonctionnalités pourraient, à leur avis, avoir un impact majeur sur leur formation de sensibilisation. Voici ce qu'ils ont répondu :

Ces résultats montrent bien que les experts en sécurité de l'information ressentent le besoin de formations qui mettent la cybersécurité à la portée de tous. La **sensibilisation multicanal**, par exemple, est une solution intéressante, dans la mesure où elle propose une approche plus conversationnelle. Les fonctionnalités de sensibilisation rapide, qui alertent sur les nouvelles stratégies d'attaques par le biais d'outils de communication comme Microsoft Teams, sont un bon moyen pour intégrer la cybersécurité au flux de travail quotidien. Une des méthodes de sensibilisation les plus efficaces reste également la **formation personnalisée** qui s'adapte aux besoins de chaque employé, selon ses fonctions et ses responsabilités. On ne le dira jamais assez : il y a autant de besoins en cybersécurité qu'il y a de personnes.

Enfin, proposer un **programme sur mesure** avec des fonctionnalités qui permettent, par exemple, d'appliquer la charte graphique de l'entreprise au contenu ou d'y inclure les politiques de confidentialité qui lui sont propres, est probablement l'un des moyens les plus sûrs pour garantir le succès de la formation. En résumé : en cybersécurité, il n'y a pas de modèle unique. Le succès ne sera au rendez-vous que si la démarche est adaptée, au cas par cas, aux personnes et à l'entreprise.

Les meilleures méthodes pour garantir un réel impact des formations de sensibilisation selon les professionnels du secteur

1. Sensibilisation via les applications de messagerie
2. Formations personnalisées
3. Personnalisation des programmes

Actions recommandées

Le cœur du problème : adapter les mesures de sécurité au fur et à mesure que les comportements évoluent

1 La sécurité doit passer avant tout

S'il y a une chose à retenir de cette étude, c'est que nous sommes tous concernés. La transition numérique et les progrès de la technologie nous exposent aujourd'hui indéniablement à toutes sortes de menaces en ligne, que ce soit dans notre vie privée ou professionnelle. Pour nous protéger efficacement contre des attaques de plus en plus subtiles, nous devons intégrer les bonnes pratiques de sécurité au cœur même de notre quotidien. À l'échelle des sociétés, il faut soumettre les questions de cybersécurité aux instances dirigeantes, afin de trouver des solutions qui permettront de mener de front les activités commerciales et la stratégie de défense de l'entreprise. Les mesures de sécurité ne peuvent, en effet, déployer tout leur potentiel que si elles sont traitées comme des priorités. Si l'on parvient, dans les sociétés, à faire comprendre aux gens que la cybercriminalité ne frappe pas uniquement des personnes, mais affecte toute la croissance de l'entreprise, la bataille pour trouver des ressources sera gagnée.

2 L'évolution des comportements est la clé de la réussite à long terme

Les mesures comportementales sont des outils tangibles et clairs qui permettent de communiquer les résultats obtenus en matière de sécurité et de sensibilisation à tous les acteurs au sein de l'entreprise. Jusqu'à récemment, les sociétés se contentaient souvent des indicateurs de performance, avec notamment les taux de clics sur les tentatives de phishing et le pourcentage de personnes ayant terminé la formation en ligne. S'il s'agit certes d'un bon début pour se faire une idée de la vigilance des employés, ce qui va réellement convaincre les décideurs de la nécessité d'une formation, c'est la capacité des mesures de sécurité à mettre fin au statu quo. En matière de sensibilisation, les mesures comportementales, telles que le taux d'alerte phishing et l'évolution des scores de risque, sont des indices de premier ordre. Les résultats de notre enquête montrent qu'une société sur deux continue à s'appuyer sur des indicateurs traditionnels, mais que les mesures comportementales gagnent du terrain et sont déjà exploitées dans un tiers des entreprises. Alors que les cybercriminels misent de plus en plus sur l'ingénierie sociale, les mesures comportementales et les scores de risques humains sont des points de repère fiables permettant d'établir l'efficacité de la protection mise en place par les entreprises face à d'éventuelles attaques sophistiquées

3 S'adapter, s'adapter et encore s'adapter

La cybersécurité est probablement l'un des domaines ayant connu l'évolution la plus impressionnante au cours des années et des décennies écoulées. Et pour cause : les progrès de la technologie ne nous permettent pas de nous reposer sur nos lauriers. Tout va de plus en plus vite. Par conséquent, les entreprises doivent développer des facultés d'adaptation encore plus rapides pour ajuster leurs stratégies actuelles au nouveau contexte, caractérisé notamment par la professionnalisation de la cybercriminalité et des menaces d'une complexité croissante. Il n'est plus question aujourd'hui de se contenter de répondre aux exigences de conformité : il faut aller plus loin et faire de la cybersécurité une partie intégrante de la stratégie commerciale, tout en veillant à ce que les mesures prises restent en phase avec le vécu et le contexte des personnes qui composent l'entreprise. S'il peut paraître difficile d'adapter continuellement les méthodes de sensibilisation alors même que les ressources en cybersécurité se raréfient et que les équipes sont au bord de l'épuisement, ce défi peut être relevé en choisissant les bons partenaires.

4 Mettre l'humain au cœur de la démarche

Si la tâche semble aujourd'hui colossale, les circonstances nous appellent à recentrer notre attention sur le facteur humain en le plaçant au cœur de la cybersécurité. La cible des attaques, c'est l'humain. La victime, qui paye les conséquences, c'est encore l'humain. Le meilleur pare-feu pour empêcher les attaques, c'est donc toujours l'humain. Pour prévenir les effets dévastateurs d'une cybercriminalité qui se professionnalise, nous avons tous intérêt à développer, au sein de nos entreprises, de solides cultures de la cybersécurité et, dans nos vies privées, des réflexes aiguisés. Notre meilleure défense sera d'adapter les stratégies de protection aux besoins de chacun et de mettre en place des formations s'inspirant des sciences comportementales. Car nous pouvons être sûrs d'une chose : les cybercriminels n'ont pas fini d'innover. Restons vigilants, en phase avec la réalité, et prenons les devants pour préparer chacun aux défis qui nous attendent.

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 »

Remerciements

Merci à tous ceux qui ont apporté leur contribution à ce rapport, et tout particulièrement aux experts qui ont donné de leur temps pour se prêter au jeu de l'interview.

Jens Becker
DSI et responsable du service numérique de la filiale allemande du groupe Zurich

Stefanie Boem
Déléguée à la protection des données chez Sport-Thieme

Sascha Czech
Responsable de la sécurité informatique au CHU de Münster (Uniklinik Münster), Allemagne

Stéphane Duguin
PDG de CyberPeace Institute

Frank Heymann
Senior IT Team Manager chez Buhlmann

Tobias Ludwichowski
Responsable du département de sécurité de l'information chez Signal Iduna

Stefan Lüders, PhD
Responsable de la sécurité informatique au CERN

Martin Schmidt
Directeur général de la consultance numérique, chez Freudenberg Home and Cleaning Solutions

Thomas Schumacher
Directeur général d'Accenture Security

Major Général Jürgen Setzer
RSSI Bundeswehr

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

Thomas Tschersich
Responsable de la sécurité informatique (RSI) chez Deutsche Telekom et PDG de Telekom Security

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

Clause de non-responsabilité :

Tous les efforts ont été déployés pour garantir l'exactitude du contenu de ce document. Cependant, nous n'acceptons aucune responsabilité quant à l'exhaustivité et la précision de son contenu. En l'espèce, SoSafe rejette toute responsabilité en cas de dommage direct ou indirect résultant de son utilisation.

(ISC)² | CPE SUBMITTER

Gagnez des crédits CPE (ISC)² avec ce rapport :

SoSafe offre aux membres de (ISC)² la possibilité d'obtenir des crédits de formation professionnelle continue (CPE). Les certifications de cybersécurité (ISC)² sont reconnues dans le monde entier comme le plus haut niveau d'excellence en matière de cybersécurité.

Si vous souhaitez obtenir des points CPE après avoir lu ce rapport, il vous suffit de scanner le QR code pour savoir comment procéder. Gagnez des crédits CPE (ISC)² avec ce rapport.

SoSafe GmbH
Lichtstraße 25a
50825 Köln
Allemagne

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