HORNETSECURITY

CYBERSECURITY REPORT 2025

Une analyse approfondie du paysage des menaces de Microsoft 365 sur la base d'informations provenant de plus de

55,6 milliards d'emails

hornetsecurity.com

HORNETSECURITY
CSR2025

À PROPOS D'HORNETSECURITY

Hornetsecurity permet aux entreprises de toutes tailles de se concentrer sur leur cœur de métier tout en protégeant les charges de travail M365, les communications par email, en sécurisant les données et en assurant la continuité des activités et la conformité grâce à des solutions nouvelle génération basées sur l'informatique dans le Cloud.

Notre produit phare, 365 Total Protection, est la solution de sécurité dans le Cloud la plus aboutie du marché pour Microsoft 365, comprenant la sécurité de la messagerie, la conformité, la gouvernance et la sauvegarde.

QU'EST-CE QUE LE CYBERSECURITY REPORT ?

Le Cybersecurity Report publié par Hornetsecurity est une analyse annuelle basée sur des données réelles collectées et étudiées par l'équipe dédiée du laboratoire de sécurité du groupe Hornetsecurity alias Security Lab du paysage des menaces pour Microsoft 365. Les solutions de cybersécurité déployées par Hornetsecurity traitent plus de 4 milliards et demi d'e-mails chaque mois. En analysant les menaces identifiées dans ces communications, combinées à une connaissance approfondie du paysage des menaces au sens large, le Security Lab révèle les principales tendances en matière de sécurité, les actions des auteurs de menaces et peut faire des projections éclairées sur l'avenir des menaces de sécurité pour Microsoft 365, ce qui permet aux entreprises d'agir en conséquence. Ces conclusions et ces données sont présentées dans ce rapport.

QU'EST-CE QUE LE SECURITY LAB ?

Le Security Lab est un département d'Hornetsecurity qui conduit des analyses approfondies sur les menaces de sécurité actuelles et critiques, en se spécialisant dans la sécurité des emails dans l'écosystème Microsoft 365. Notre équipe multinationale de spécialistes de la sécurité possède une vaste expérience dans la recherche en sécurité, l'ingénierie logicielle et la science des données.

Une compréhension approfondie du paysage des menaces, établie grâce à un examen pratique des attaques de phishing, des logiciels malveillants, des gangs de ransomwares et autres, est essentielle pour développer des contre-mesures efficaces. Les informations détaillées recueillies par le Security Lab servent de base aux solutions de cybersécurité nouvelle génération d'Hornetsecurity.

TABLE DES MATIÈRES

CYBERSECURITY REPORT 2025

CHAPITRE 1
RÉSUMÉ

CHAPITRE 1 – RÉSUMÉ

En tirant parti de son vaste ensemble de données sur les utilisateurs, Hornetsecurity est particulièrement bien placé pour procéder à un examen détaillé des menaces basées sur l'email ainsi que des menaces ciblant l'ensemble de l'écosystème Microsoft 365. Cela permet aux spécialistes de la sécurité d'Hornetsecurity de distiller ces données en informations indispensables pour les équipes informatiques et les professionnels de la sécurité. L'email reste un canal de communication majeur, en particulier pour les entreprises. Dans notre analyse de plus de 55,6 milliards d'emails en 2024, 36,9 % sont classés comme « indésirables ». 97,8 % des emails indésirables sont des spams ou sont rejetés d'emblée en raison d'indicateurs externes et 2,3 % des emails indésirables ont été signalés comme étant malveillants.

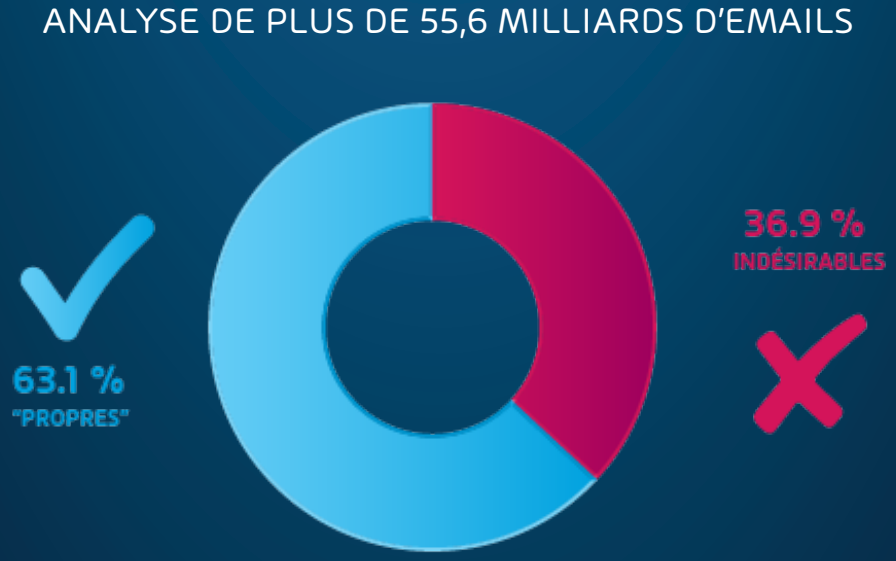


FIG 1. CLASSIFICATION DES EMAILS ANALYSÉS PAR HORNETSECURITY

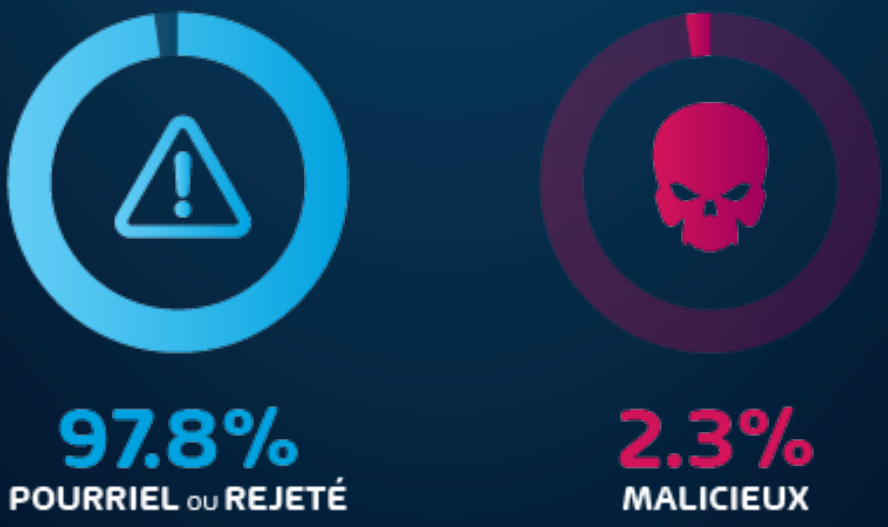


FIG 2. CLASSIFICATION DES COURRIELS INDÉSIRABLES

“HAMEÇONNAGE 33,3 % DES ATTAQUES”

En examinant les types d'attaques utilisés dans les attaques par e-mail, l'hameçonnage reste la méthode d'attaque la plus répandue, représentant 33,3 % des attaques. Il est suivi de près par les URL malveillantes, qui représentent 22,7 % des cas. Ces chiffres correspondent aux types d'attaques qui ont gagné en popularité parmi les acteurs de menace au cours de l'année écoulée - principalement les attaques de vol d'informations d'identification de type reverse-proxy qui reposent fortement sur l'ingénierie sociale et les liens malveillants.

Le regain d'intérêt pour l'ingénierie sociale et le vol d'identifiants de sécurité / d'informations d'identification est également perceptible dans nos données concernant les types de fichiers malveillants. Nous effectuons un suivi des types de fichiers utilisés pour la livraison de charges utiles malveillantes dans les attaques par e-mail et notons une diminution de l'utilisation des pièces jointes malveillantes pendant la période considérée. Presque tous les types de fichiers malveillants ont diminué par rapport à l'année dernière. Cela dit, les fichiers HTML, les fichiers PDF et les fichiers d'archive restent dans le trio de tête, comme l'année précédente.

Les acteurs de la menace ont exploité un volume légèrement plus important d'attaques par e-mail plus faciles à détecter (et finalement « rejetées ») au cours de la période couverte par les données. C'est ce qu'indique la légère diminution du nombre d'e-mails malveillants classés dans les catégories « Menaces » et « Menaces Avancées». Par conséquent, l'indice de menace de presque tous les secteurs d'activité a baissé au cours de la période de référence.

En effet, notre indice de menace sectoriel compare le nombre d'e-mails propres au volume de « menaces » et de “ menaces avancées ”. Il convient également de noter qu'il y a peu de variations d'un secteur à l'autre. Certes, certains sont plus élevés que d'autres, mais les données recueillies ne cessent de montrer, année après année, que TOUS les secteurs subissent des attaques.

En ce qui concerne les tentatives d'usurpation d'identité des marques au cours de l'année écoulée, nous avons constaté que, bien que la marque DHL soit restée en tête des marques les plus usurpées, le nombre de tentatives d'usurpation d'identité a fortement diminué. Cela dit, le nombre de tentatives d'usurpation d'identité de FedEx a triplé, celui de Docusign et de Facebook a plus que doublé, tandis que Mastercard et Netflix ont également connu des augmentations notables.

Enfin, dans le cadre de notre discussion annuelle sur la sécurité des données dans le Cloud, l'un des principaux thèmes abordés par les attaquants cette année est, une fois encore, l'utilisation croissante de kits d'outils de vol d'informations d'identification/d'identifiants par le biais d'une attaque Adversary-in-the-Middle. Par rapport aux années précédentes, ces attaques sont devenues populaires auprès des acteurs de la menace. Cela s'explique par la facilité avec laquelle ils peuvent cibler un grand nombre de victimes avec des pages d'accueil TRÈS convaincantes, sans trop d'efforts. Ces boîtes à outils sont également conçues pour prendre en compte l'authentification multifactorielle (MFA), ce qui permet à de nombreuses entreprises de penser (à tort) qu'elles sont totalement à l'abri de ces attaques. Le secteur de la cybersécurité continue de s'attaquer à ce problème en proposant de meilleurs mécanismes d'analyse, des formations de sensibilisation à la sécurité et des technologies de connexion résistantes au phishing, comme les passkeys. Toutefois, ces mesures d'atténuation prennent du temps et, par conséquent, certaines entreprises en ont été victimes, ce qui a entraîné la perte ou la fuite de données sensibles.

Étant donné que ce schéma d'attaque fait encore largement usage des communications par e-mail ainsi que de l'utilisation croissante des communications par chat tel que Microsoft Teams, une stratégie robuste de sécurité de la messagerie et de Microsoft 365 est essentielle pour opérer en toute sécurité dans l'écosystème numérique d'aujourd'hui.

CYBERSECURITY
REPORT 2025

CHAPITRE 2

LE PAYSAGE ACTUEL DES MENACES DE MICROSOFT 365

CHAPITRE 2 - LE PAYSAGE ACTUEL DES MENACES DE MICROSOFT 365

Chaque année, le Security Lab d'Hornetsecurity examine l'ensemble des données de l'entreprise et analyse l'état des menaces mondiales liées à la messagerie électronique et les statistiques de communication. En outre, l'équipe effectue régulièrement des exercices de réflexion prospective et donne un aperçu des menaces potentielles futures. Ce chapitre se concentre sur l'examen des points de données de la période définie du 1er novembre 2023 au 31 octobre 2024, qui constitue la base des projections de l'évolution du paysage des menaces présentées au chapitre 4.

TENDANCES EN MATIÈRE DE SÉCURITÉ DE L'E-MAIL

Malgré l'utilisation croissante de logiciels de collaboration et de messagerie instantanée, tels que Microsoft Teams, l'e-mail occupe toujours une place prépondérante dans les cyberattaques. Nous avons observé une diminution continue du nombre d'e-mails classés dans la catégorie Menaces/Menaces Avancées de 2,3 % cette année, contre 3,7 % l'année dernière et 5,5 % l'année précédente (si l'on considère les e-mails « indésirables »). Cela dit, le risque pour les entreprises du monde entier reste toutefois élevé. Cela est principalement dû à l'utilisation accrue de techniques d'ingénierie sociale par le biais d'attaques par e-mail de type « spray » à faible effort qui cherchent à amener l'utilisateur cible à s'engager d'une manière ou d'une autre.

En examinant plus de 55,6 milliards d'e-mails collectés au cours de la période de reporting actuelle (1er novembre 2023 - 31 octobre 2024), le Security Lab a fait les calculs suivants :

SPAM, LOGICIELS MALVEILLANTS, MÉTRIQUES DE MENACES AVANCÉES

Comme nous l'avons vu au cours de la dernière décennie, l'e-mail continue d'être l'un des principales méthodes utilisées par les acteurs de la menace pour lancer des attaques. Les données de ce rapport classent 36,9 % de tous les e-mails comme « indésirables », soit une augmentation de 0,6 point de pourcentage par rapport à 2023. La définition du terme « indésirable » fait référence aux e-mails qui ne sont pas des communications authentiques souhaitées par le destinataire. Le graphique ci-dessous montre la répartition des e-mails indésirables et des e-mails propres.

FIG 3. 2024 : E-MAILS INDÉSIRABLES PAR CATÉGORIE, Y COMPRIS LES E-MAILS PROPRES

Ce chiffre est à comparer à celui de l'année dernière, où 36,3 % de tous les e-mails étaient classés comme « indésirables », ce qui indique une légère augmentation du nombre d'mails indésirables d'une année sur l'autre.

Si l'on considère que nous avons traité 55,6 milliards d'e-mails en 2024, le nombre d'e-mails indésirables représente environ 20,5 milliards d'e-mails « indésirables » envoyés aux entreprises au cours de la période considérée.

Pour une répartition concise des pourcentages qui composent les emails « indésirables », nous les avons classés comme suit :

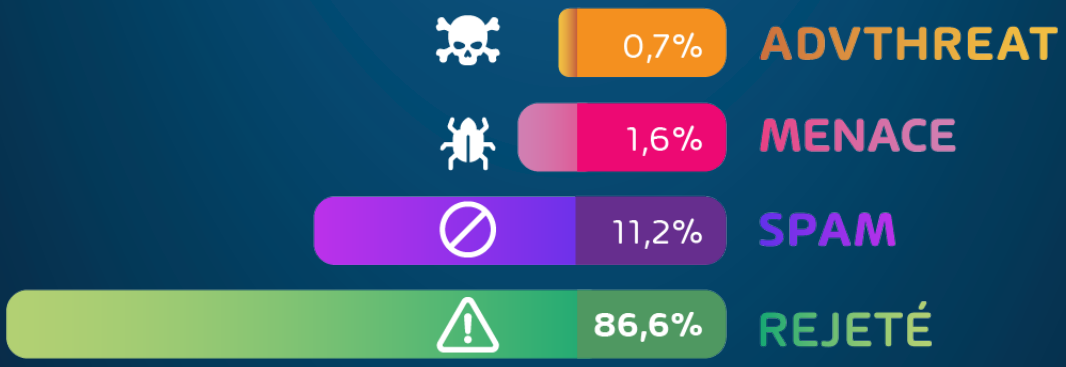


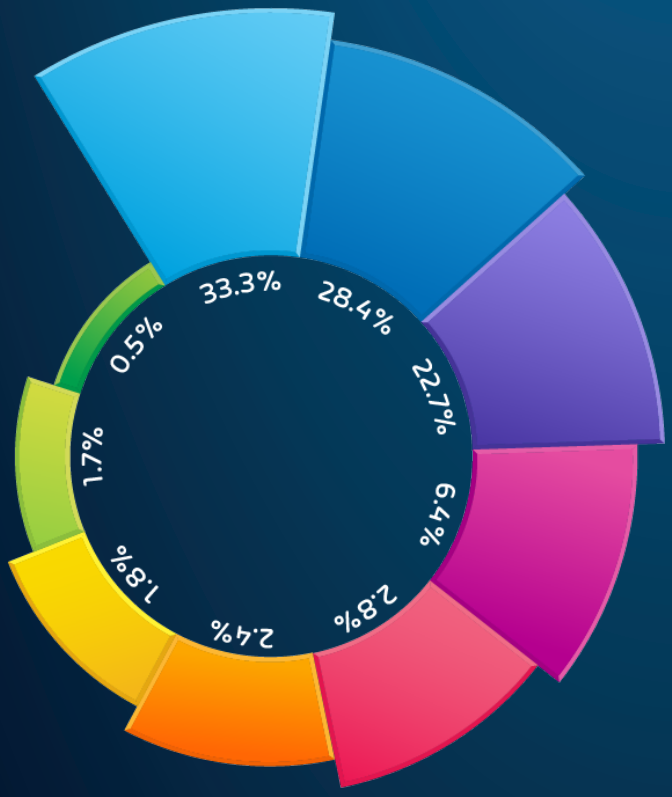
FIG 4. 2024 EMAILS INDÉSIRABLES PAR CATÉGORIE

CATÉGORIE	DESCRIPTION
Spam	Ces e-mails sont indésirables et sont souvent de nature promotionnelle ou frauduleuse. Ils sont envoyés simultanément à un grand nombre de destinataires.
Menace	Ces e-mails contiennent des contenus préjudiciables, tels que des pièces jointes ou des liens malveillants, ou sont envoyés à des fins criminelles, comme l'hameçonnage (phishing).
AdvThreat	Advanced Threat Protection a détecté une menace dans ces e-mails. Les e-mails sont utilisés à des fins illégales et font appel à des moyens techniques sophistiqués qui ne peuvent être contrés qu'à l'aide de procédures dynamiques avancées.
Rejeté	Notre serveur de messagerie rejette ces e-mails directement lors de la connexion initiale du serveur de messagerie émetteur en raison de caractéristiques externes, telles que l'identité de l'expéditeur, et les e-mails ne sont pas davantage analysés.

REMARQUE : Pour plus de détails, la catégorie « Rejeté » se réfère aux e-mails que les services d'Hornetsecurity ont rejeté au cours du dialogue SMTP en raison de caractéristiques externes, telles que l'identité ou l'adresse IP de l'expéditeur. Si un expéditeur est déjà identifié comme compromis, le système ne poursuit pas l'analyse. Le serveur SMTP refuse le transfert d'e-mail dès le point de connexion initial en raison de la réputation négative de l'adresse IP et de l'identité de l'expéditeur.

TECHNIQUES D'ATTAQUE UTILISÉES DANS LES ATTAQUES PAR COURRIER ÉLECTRONIQUE EN 2024

Notre analyse des e-mails de la période considérée a révélé la répartition suivante des types d'attaques utilisés dans les attaques par e-mails :



TECHNIQUES D'ATTAQUE	
HAMEÇONNAGE	33.3%
"OTHER"	28.4%
URL	22.7%
ARNAQUE DES AVANCES DE FRAIS	6.4%
EXTORSION	2.8%
ARCHIVES/IMAGES DISQUES	2.4%
IMPERSONATION	1.8%
HTML	1.7%
MALDOC	0.5%

FIG 5. TECHNIQUES D'ATTAQUE PAR E-MAIL UTILISÉES EN 2024

REMARQUE : Les années précédentes, nous avons été en mesure de suivre l'évolution des types d'attaques d'une année à l'autre. Toutefois, en raison des changements intervenus dans la manière dont nous identifions les éléments malveillants et les e-mails indésirables, il existe un sous-ensemble d'occurrences qui sont marquées comme « Autres ». Cette catégorie comprend diverses méthodes d'attaque qui ne rentrent pas parfaitement dans l'une des catégories principales que nous avons affichées les années précédentes. Bien que nous puissions fournir une ventilation des types d'attaques pour cette période de données, la comparaison directe de ces données avec celles de l'année dernière ne donnerait pas une représentation exacte.

Ce que nos données nous montrent pour cette période, c'est que le phishing reste le type d'attaque le plus utilisé dans les attaques par e-mail, suivi par les URL malveillantes. La popularité croissante des URL malveillantes parmi les attaquants s'explique en grande partie par leur utilisation dans les attaques de collecte d'informations d'identification par proxy inverse, à l'aide d'outils tels qu'Evilginx.

En dehors de cela, les escroqueries à l'avance de frais restent très populaires parmi les acteurs de la menace, suivies par l'extorsion en quatrième position. L'extorsion est notable car nous continuons à voir des cas où les acteurs de la menace exfiltrent d'abord des données avant de mettre en place un ransomware dans un environnement donné. Si la cible refuse de payer (en raison de la récupération de la sauvegarde), l'auteur de la cybermenace menace de divulguer les données au public.

UTILISATION DES PIÈCES JOINTES ET TYPES D'ATTAQUES

Les pièces jointes aux e-mails continuent d'être utilisées par les acteurs de la menace pour la livraison de charges utiles malveillantes en 2024. Les acteurs de la menace utilisent les pièces jointes pour dissimuler des logiciels malveillants et ajouter un air d'authenticité à leurs communications malveillantes, en fonction du type de fichier joint utilisé.

En outre, certains filtres anti-spam et anti-programmes malveillants rudimentaires peuvent être incapables d'analyser certains types de fichiers, ce qui entraîne une infection par des attaques plus complexes telles que le trafic d'HTML. En fait, l'utilisation de fichiers **HTML malveillants** reste en tête des types de fichiers les plus utilisés dans les e-mails malveillants, comme le montre le tableau ci-dessous.

La répartition des types de fichiers utilisés pour la livraison de charges utiles malveillantes au cours de la période de référence est présentée ci-dessous :

FILE TYPE	2023	2024
HTML	37.5%	20.4%
PDF	22.8%	19.2%
ARCHIVE	19.4%	17.6%
EXECUTABLE	3.5%	3.2%
EXCEL	3.2%	3.0%
WORD	3.0%	2.5%
DISK IMAGE FILES	2.2%	2.2%

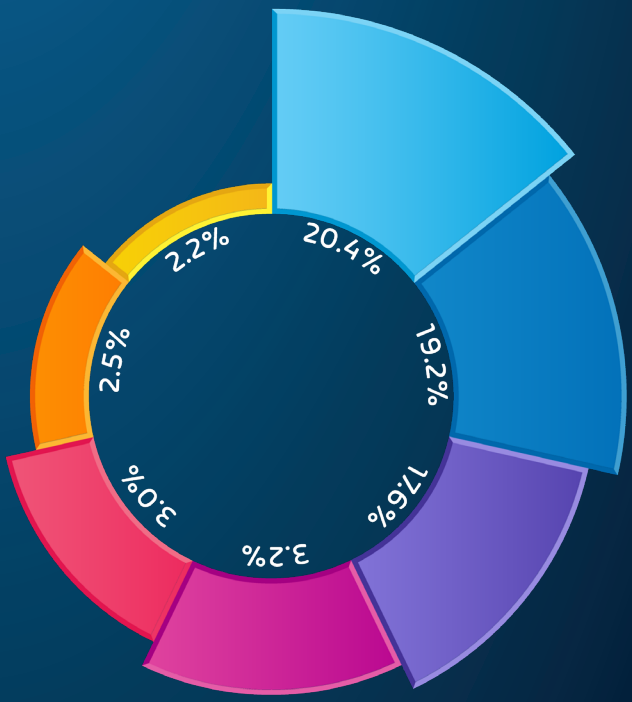


FIG 6. TYPES DE FICHIERS POUR LES CHARGES UTILES MALVEILLANTES 2024

> **L'UTILISATION DES FICHIERS HTML A BAISSÉ**
> DE 17,1 POINTS DE POURCENTAGE EN 2024 PAR RAPPORT À 2023

- L'utilisation des **fichiers PDF** a diminué de 3,6 points de pourcentage en 2024
- Les **fichiers d'archive** ont connu une tendance similaire avec une baisse de 1,8 point de pourcentage en 2024
- Nous avons observé une diminution quasi universelle de tous les types de **fichiers malveillants** au fur et à mesure que les auteurs d'attaques se tournent vers d'autres styles d'attaques

Au cours de l'année écoulée, l'utilisation de pièces jointes malveillantes n'a pas été aussi utile que par le passé pour les acteurs de la menace. Nous avons donc constaté que les auteurs d'attaques se tournent davantage vers l'ingénierie sociale dans le but d'amener la cible à faire autre chose que d'ouvrir une pièce jointe. Par exemple, l'utilisation de kits d'outils reverse-proxy adversary-in-the-middle a été très répandue au cours de la période couverte par les données. Cela s'explique par le fait qu'avec l'adoption croissante de l'authentification multifactorielle (MFA), les auteurs d'attaques utilisent plus fréquemment le vol d'identifiants via des outils tels qu'Evilginx et PyPhisher. Il est plus facile de se procurer les authentifiants que d'accéder à la méthode d'authentification multifactorielle de la cible.

INDEX DES MENACES PAR E-MAIL POUR LES SECTEURS D'ACTIVITÉ

L'un des domaines clés que nous examinons chaque année (et chaque mois) est le nombre de menaces qui pèsent sur les différents secteurs d'activité. Cela nous permet de déterminer s'il existe des campagnes dédiées ou des attaques ciblées sur des secteurs spécifiques. Les chefs d'entreprise peuvent également s'en inspirer pour déterminer s'ils sont exposés à un risque accru d'attaque ou non.

Le plus remarquable dans les données de cette année est le fait que TOUS les secteurs d'activité ont vu leur indice de menace par e-mail diminuer. Cela correspond à nos données ci-dessus qui montrent que le nombre d'e-mails classés comme « Menaces » et « Menaces Avancées » a diminué par rapport à l'année dernière.

Cela dit, certains secteurs ont été un peu plus ciblés que d'autres.

- **Industrie minière** - La plupart des entreprises minières ont les mêmes types de problèmes et de défis qu'une entreprise manufacturière. En outre, elles vendent généralement des métaux précieux, ce qui en fait une cible de choix pour les acteurs de la menace qui cherchent à utiliser des ransomware pour soutirer de l'argent à l'entreprise.
- **Industrie du divertissement** - Les entreprises de ce type relèvent généralement du secteur des jeux d'argent, de la vente de billets, etc. Ces entreprises sont devenues une cible en raison des importantes sommes d'argent en jeu. Regardez l'attaque de 2023 contre MGM et Caesars Entertainment que nous abordons plus en détail ci-dessous.
- **Industrie manufacturière** - L'industrie manufacturière a l'habitude d'être fréquemment ciblée par les acteurs de la menace. Beaucoup considèrent ce secteur comme une cible facile pour une **double extorsion** et une perturbation de la production en raison de la nature de la sécurité de leur réseau et du fait qu'ils utilisent souvent un grand nombre d'appareils non sécurisés de l'Internet des objets (IoT) et des contrôleurs logiques programmables (PLC).

FIG 7. INDICE ANNUEL DE MENACE POUR L'INDUSTRIE

REMARQUE : La valeur de l'indice de menace est déterminée par le calcul suivant :

Pourcentage de l'indice de menace = nombre d'emails malveillants (Menace+AdvThreat) / (nombre d'emails malveillants (Menace+Menace Avancée) + nombre d'emails propres) multiplié par 100 - Ceci exclut les spams et newsletters.

Note sur la méthodologie

Chaque entreprise (de taille différente) reçoit un nombre absolu d'e-mails différent. Nous déterminons donc le pourcentage d'e-mails à caractère menaçant dans les e-mails suspects et non suspects de chaque entreprise, afin de comparer les entreprises entre elles. Nous calculons ensuite la médiane de ces pourcentages pour toutes les entreprises d'un même secteur afin d'obtenir le score final de menace du secteur.

USURPATION D'IDENTITÉ DE MARQUE

L'usurpation d'identité de marque reste une technique majeure d'attaque par e-mail ciblant les utilisateurs finaux et les entreprises en 2024.

La société d'expédition DHL a peut-être connu l'évolution la plus fulgurante en matière de tentatives d'usurpation d'identité. La marque n'a vu qu'une fraction des tentatives d'usurpation d'identité en 2024 par rapport à 2023. Cela dit, elle reste en tête de notre liste des marques les plus usurpées, suivie de près par FedEx.

Les marques d'expédition continuent d'être populaires car elles peuvent être facilement intégrées dans des attaques de type ingénierie sociale par le biais du phishing et du **smishing**. Ces deux types d'attaques présentent un degré élevé de similitude avec les communications réelles de ces entreprises et incitent facilement les utilisateurs moins expérimentés à divulguer des informations personnelles et/ou des informations de paiement.

Autres données notables dans ce domaine :

- Le nombre d'usurpations d'identité des marques FedEx et Facebook a triplé au cours de l'année écoulée
- Le nombre d'usurpations d'identité de la marque Docusign a doublé au cours de la période de référence
- Mastercard et Netflix sont deux autres marques notables qui ont également connu des augmentations notables

Nos données complètes sur la période de référence ont révélé les marques les plus usurpées, comme suit :

FIG 8. LES 10 MARQUES LES PLUS USURPÉES

REMARQUE : Les données relatives à l'usurpation d'identité des marques sont fortement influencées par les variations régionales. Plusieurs marques allemandes sont répertoriées ici en raison de l'importance de notre clientèle en Allemagne.

Notre analyse de 10 743 561 domaines actifs d'envoi d'e-mails en 2024 révèle des lacunes dans la mise en œuvre de l'authentification du courrier électronique, ce qui rend de nombreuses entreprises vulnérables aux attaques consistant à usurper l'identité d'une marque et à usurper le nom d'un destinataire.

> **SEULS 35,4 %**
> ONT MIS EN ŒUVRE LES PROTOCOLES DMARC

Seuls 35,4 % des domaines analysés ont mis en œuvre les protocoles **DMARC** (Domain-based Message Authentication, Reporting, and Conformance), ce qui signifie que près des deux tiers des domaines ne disposent pas de cette mesure de sécurité essentielle. Seuls 16,6 % des domaines utilisent les fonctionnalités RUA (Aggregate Reporting URI), qui offrent une visibilité essentielle sur les résultats de l'authentification de l'e-mail.

Les enregistrements RUA (Aggregate Reporting URI) sont un élément essentiel du DMARC qui permet aux propriétaires de domaines de recevoir des rapports détaillés sur les e-mails envoyés à partir de leur domaine. Ces rapports comprennent :

- Volume des messages reçus
- Adresses IP envoyant des emails au nom du domaine
- Taux de réussite/échec de l'authentification
- Sources d'envoi et leur conformité avec les politiques du domaine

Parmi les domaines qui ont mis en œuvre **DMARC**, 47 % exploitent les capacités RUA, ce qui montre que de nombreuses entreprises qui adoptent DMARC comprennent la valeur du suivi et de la visibilité.

Grâce au suivi des RUA, les entreprises sont en mesure d'observer des vagues d'e-mails usurpés provenant d'adresses IP précédemment inconnues, ce qui leur permet d'alerter leurs clients au sujet d'une campagne d'hameçonnage spécifique. Les institutions financières utilisent souvent le suivi des RUA pour lancer des procédures de démantèlement dans les heures qui suivent le lancement d'une campagne d'hameçonnage.

SÉCURITÉ DES DONNÉES DANS L'INFORMATIQUE DÉMATÉRIALISÉE (LE CLOUD)

Le Cloud existe depuis plus de dix ans maintenant, mais nous commençons tout juste à voir les entreprises migrer en masse vers les services Cloud ou s'établir en tant qu'entreprises entièrement hébergées dans le cloud. Prenons l'exemple du stockage des données d'entreprise. Il y a dix ans, la plupart des entreprises possédaient encore un serveur de fichiers sur site hébergeant les données essentielles de l'entreprise. Aujourd'hui, il est de plus en plus courant d'exploiter le stockage cloud à cette fin. SharePoint Online et OneDrive for Business deviennent de plus en plus le lieu où les données sont conservées et sécurisées grâce à des services tels que Microsoft Entra. La sécurité des données dans le cloud devient donc un sujet de discussion important, non seulement pour le cloud M365, mais aussi pour les services cloud en général. Bien que nous portions notre attention sur Microsoft 365 et l'écosystème cloud de Microsoft tout au long de ce rapport, une grande partie de ce qui est discuté ici s'applique également à d'autres fournisseurs de cloud.
Les défenses de base dans le cloud Microsoft se sont améliorées au fil des ans, mais elles sont encore loin d'être parfaites. De plus en plus d'entreprises utilisent les nouvelles fonctionnalités de sécurité, telles que l'authentification multifactorielle (MFA) et la sécurité de base des e-mails grâce à des services tels qu'Exchange Online Protection, mais cela reste souvent insuffisant. Les cybercriminels sont en constante évolution, comme en témoignent les attaques de type « Adversary-in-the-Middle ».

Attaques de type Passkeys et Adversary in the Middle (AitM)

Là où vont les défenseurs, les attaquants suivent. Depuis plusieurs années, nous chez Hornetsecurity, ainsi que toutes les personnes et entreprises soucieuses de la sécurité, avons préconisé l'utilisation de l'authentification multi facteur (MFA) comme une alternative plus sécurisée aux traditionnels noms d'utilisateur et mot de passe pour se connecter aux systèmes. L'adoption de diverses formes de MFA a augmenté lentement mais sûrement, allant des messages SMS aux clés de sécurité matérielles. Cependant, les criminels ne vont certainement pas abandonner leur «business» lucratif et se sont plutôt adaptés.

Leur approche principale a été d'utiliser des kits d'hameçonnage de type reverse-proxy, qu'ils soient open source ou des packages « commerciaux » qui aident à créer des e-mails d'hameçonnage convaincants pour tromper les utilisateurs afin qu'ils cliquent sur un lien, et mettent également en place des services proxy avec des pages de connexion d'apparence légitime. Lorsqu'un utilisateur clique sur le lien et est dirigé vers une fausse page de connexion pour entrer son nom d'utilisateur et son mot de passe, ces informations d'identification sont alors transmises au site réel (et capturées par l'attaquant). Lorsque la demande MFA est ensuite activée, ces kits reverse-proxy permettent à l'utilisateur final d'entrer son code MFA ou d'approuver la demande comme d'habitude, et cela aussi est transmis à la véritable page de connexion en coulisses. Pendant ce temps, l'attaquant vole l'identifiant généré par le service d'identité cible (comme Entra ID par exemple) et peut maintenant l'utiliser pour se connecter en tant qu'utilisateur, d'où le nom d'attaque Adversary in the Middle (AitM).

Pour contrer ces attaques plus sophistiquées, il vous faut une méthode MFA résistante à l'hameçonnage. Ces méthodes sont plus récentes et ne sont pas encore très largement adoptées dans l'industrie. Parmi elles, on trouve **Windows Hello for Business**, les clés USB matérielles FIDO2 et, plus récemment, les **Passkeys**. Ces méthodes MFA verrouillent l'authentification à l'URL du site légitime uniquement, donc même si l'utilisateur est trompé en visitant une page de connexion qui semble légitime, la technologie elle-même refuse de fonctionner parce qu'elle voit que l'adresse du site ne correspond pas.

Le problème est que Windows Hello for Business nécessite du matériel spécialisé (et ne fonctionne que pour Windows), tandis que les clés matérielles FIDO2 sont coûteuses, ce qui a malheureusement apporté des limites à leur adoption. Cela dit, une Passkey utilise les mêmes technologies qu'une clé FIDO2 mais repose sur la puce de sécurité de votre iPhone ou téléphone Android, éliminant ainsi le besoin de matériel supplémentaire. Ici encore, l'adoption a été lente, mais de plus en plus de services la prennent en charge, et si vous êtes responsable de la sécurité dans votre organisation, vous devriez certainement commencer à la piloter dès aujourd'hui. Nous prévoyons que maintenant qu'Entra ID de Microsoft, Google Workspace, AWS ainsi que Facebook et bien d'autres prennent en charge les Passkeys, l'adoption augmentera considérablement au cours des 12 prochains mois.

Les préoccupations concernant la dépendance aux fournisseurs s'intensifient en matière de sécurité des données dans le Cloud

La dépendance aux fournisseurs consiste à confier de nombreux processus et procédures commerciaux, voire presque tous, à un partenaire fournisseur. Le problème avec cet arrangement est que si le fournisseur rencontre des problèmes (liés à la sécurité ou autres), l'entreprise en pâtit.

Nous avons longuement discuté du problème potentiel de la dépendance aux fournisseurs que certaines entreprises pourraient rencontrer avec Microsoft, notamment via nos rapports de menaces mensuels et notre podcast « **The Security Swarm** ». Il va sans dire que ce problème persiste et risque de s'aggraver à mesure que Microsoft continue à gagner des parts de marché dans différents domaines.

Cela dit, de nouvelles préoccupations ont émergé au cours de l'année écoulée, mettant encore plus en lumière cette question. Dans la série continue de violations réussies chez Microsoft, un **article intéressant** est apparu en juin 2024.

En résumé, Andrew Harris, qui travaillait chez Microsoft à l'époque, a identifié une faille sérieuse dans les services de fédération Active Directory (AD FS) et a tenté désespérément de la corriger. Ses craintes ont été minimisées et, alors que le gouvernement fédéral américain était sur le point de signer un accord de plusieurs milliards de dollars avec Microsoft pour ses services Cloud, le problème a été mis sous le tapis. Après son départ de Microsoft en 2020, l'attaque SolarWinds, probablement la plus grande attaque de la chaîne d'approvisionnement jamais réalisée, a été révélée - et alors que l'attention se concentrait sur SolarWinds et son produit Orion compromis, les attaquants russes se sont répandus dans les réseaux en utilisant la faille ADFS après leur attaque initiale. Bien sûr, cela s'est produit bien avant le rapport du **Cyber Safety Review Board (CSRB)** mentionné plus loin, et bien avant que l'Initiative pour un **Futur Sécurisé (SFI)** de Microsoft ne commence sérieusement, mais le temps nous dira si le « nouveau » Microsoft mettra effectivement la sécurité au-dessus des nouvelles fonctionnalités, ce qui incarne le vrai défi pour chaque entreprise commerciale.

Encore une fois, chaque organisation doit prendre sa propre décision en ce qui concerne la dépendance aux fournisseurs, mais si l'on prend en compte des années de préoccupations diverses en matière de sécurité à de multiples niveaux, et le fait de savoir où s'arrête la responsabilité de Microsoft en ce qui concerne vos données, le choix devient clair.

De quoi Microsoft est-il responsable ?

Nombreux sont ceux qui se demandent : « Si Microsoft ne s'occupe pas de mes données et de ma sécurité, de quoi est-elle vraiment responsable ? » La position actuelle de Microsoft sur cette question n'a pas changé en 2024. Pour bien comprendre, il faut connaître le modèle de responsabilité partagée de Microsoft.

Le point important est que le modèle de responsabilité partagée stipule que

> **LA RESPONSABILITÉ EST TOUJOURS CONSERVÉE PAR LE CLIENT POUR :**

- Informations et données
- Appareils (mobiles et PC)
- Comptes et identifiants

En substance, le client est responsable de la sécurisation et de la protection de ses informations et de ses données. Microsoft ne l'est pas. À mesure que les entreprises adoptent la technologie cloud, elles sont de plus en plus confrontées à des problèmes de sécurité et d'intégrité.

Un autre point qui mérite d'être mentionné est un élément que nous avons inclus dans ce rapport l'année dernière. De nombreux clients de M365 en sont encore surpris et il convient donc de le mentionner également dans ce rapport annuel. Microsoft a modifié en 2023 sa position de longue date sur l'utilisation d'applications de sauvegarde avec M365. Lors d'une conférence Microsoft l'année dernière, **Microsoft a annoncé Microsoft 365 Backup**. Un service a été exposé dans le but de fournir des capacités de sauvegarde de base pour M365. L'élément important de cette annonce n'est pas le service en lui-même, mais le changement de la position de longue date de Microsoft, à savoir que « vous n'avez pas besoin de sauvegarder vos données dans M365 ». De nombreux acteurs du secteur considèrent que ce changement est motivé par l'une des deux raisons suivantes :

1. **Microsoft a finalement capitulé et admet désormais que l'accent mis sur la conservation des données n'est PAS suffisant dans le cadre de M365**
2. **Microsoft veut simplement s'approprier une part du marché de la sauvegarde M365, maintenant qu'il a constaté l'existence d'un vaste marché pour ce type de service.**

Les deux options semblent probables, l'option 2 étant renforcée par le fait que Microsoft a également publié une API de sauvegarde que les fournisseurs peuvent également utiliser, moyennant paiement. Quoi qu'il en soit, le message est plus clair que jamais. Les entreprises SONT responsables de la protection de toutes les données qu'elles placent dans les services Microsoft Cloud.

Les difficultés posées par les multiples tenants dans le Cloud Microsoft

Alors que les principaux services cloud de Microsoft sont disponibles depuis une dizaine d'années ou plus, de nombreuses entreprises se retrouvent dans une situation où elles doivent gérer et maintenir plusieurs environnements Microsoft 365. Il peut s'agir d'une entreprise qui a procédé à plusieurs fusions et acquisitions, ou d'un fournisseur de services gérés (MSP) qui fournit des services informatiques à plusieurs clients. Dans les deux cas, beaucoup de ces entreprises se rendent compte des difficultés liées à la gestion de plusieurs environnements M365.

Lorsqu'on parle des ressources humaines nécessaires à cette charge de gestion accrue, il peut y avoir des répercussions directes sur la sécurité des données dans le cloud. En tant qu'entreprise, des normes pour les meilleures pratiques de sécurité et l'activation des fonctionnalités au sein des environnements M365 sous gestion ont probablement été définies. De nombreux administrateurs trouvent qu'il est très difficile d'appliquer ces normes et de limiter les divergences de configuration ou les erreurs dans plusieurs tenants M365 disparates. Avec la nature des services cloud, une mauvaise configuration peut faire la différence entre une entreprise sécurisée et une grave violation de données.

La gestion des environnements devient de plus en plus importante pour les entreprises qui cherchent à sécuriser leurs données M365. Bien que Microsoft fournisse un utilitaire appelé Lighthouse, il présente certaines limites et de nombreux MSP trouvent qu'il manque de fonctionnalités et d'échelle. Certains éditeurs de logiciels ont conçu des solutions pour répondre à ce besoin de gestion pour les MSP, comme **365 Multi-Tenant Manager pour les MSPs d'Hornetsecurity**. Une gestion et une gouvernance adéquates deviennent d'une importance cruciale dans le monde d'aujourd'hui où l'informatique dématérialisée est reine, et les équipes dirigeantes doivent être conscientes des dangers que ces défis posent pour la sécurité des données dans l'informatique du Cloud.

CYBERSECURITY
REPORT 2025

CHAPITRE 3

UNE ANALYSE DES PRINCIPAUX INCIDENTS DE SÉCURITÉ ET DE L'ACTUALITÉ DE LA CYBERSÉCURITÉ EN 2024

CHAPITRE 3 – UNE ANALYSE DES PRINCIPAUX INCIDENTS DE SÉCURITÉ ET DE L'ACTUALITÉ DE LA CYBERSÉCURITÉ EN 2024

Les douze derniers mois ont été une succession de péripéties en ce qui concerne les cyber événements dans le monde entier. Nous allons donc nous concentrer sur les plus importants, soit en raison de leur impact sur la société, soit parce qu'ils nous donnent un bon aperçu que nous pouvons tous utiliser pour améliorer la position de nos entreprises en matière de cybersécurité.

L'INCIDENT CROWDSTRIKE

Le 19 juillet 2024 s'est produite la plus grande panne informatique de tous les temps. En l'espace de quelques minutes, environ 8,5 millions de systèmes Windows utilisant l'agent Crowdstrike Falcon se sont bloqués ou ont eu un écran bleu et ont continué à redémarrer puis à se bloquer jusqu'à ce qu'ils soient réparés manuellement. Cet outil Endpoint Detection and Response (EDR) repose (comme tous les outils Windows) sur un pilote de noyau et une mise à jour particulière de la signature comportait une faille logique qui a provoqué le crash du système après l'écriture de données dans une partie de la mémoire qui n'était pas censée le faire. Le coût estimé pour les entreprises du classement Fortune 500 touchées est de plus de 5,4 milliards de dollars américains.

En septembre, Microsoft a organisé un sommet pour tous les fournisseurs de cybersécurité produisant des agents pour Windows afin de discuter de la voie à suivre et de s'assurer qu'une telle panne ne se reproduise jamais. Beaucoup ont suggéré que Microsoft adopte l'approche de macOS, qui consiste à ne permettre aucun accès au noyau pour les agents EDR et à ne fournir qu'un accès API. De nombreux experts, y compris chez Hornetsecurity, pensent que c'est trop radical et que cela freine également l'innovation, et Microsoft semble être d'accord. Il semble que les futures versions de Windows auront plus de garde-fous contre ce type de risques, tout en évitant de bloquer totalement l'accès au noyau.

CHANGE HEALTHCARE

En février 2024, Change Healthcare, une filiale de UnitedHealth, a subi une attaque massive de **ransomware** qui a compromis les dossiers personnels, financiers et médicaux d'environ 100 millions d'Américains. Cette violation a été attribuée au gang de **ransomware BlackCat, basé en Russie**, et est considérée comme la plus grande violation connue d'informations de santé protégées aux États-Unis. Les auteurs de l'attaque ont exploité les vulnérabilités du réseau de l'entreprise, accédant ainsi à des données sensibles, y compris les antécédents médicaux des patients, les détails de l'assurance et les informations relatives aux paiements.

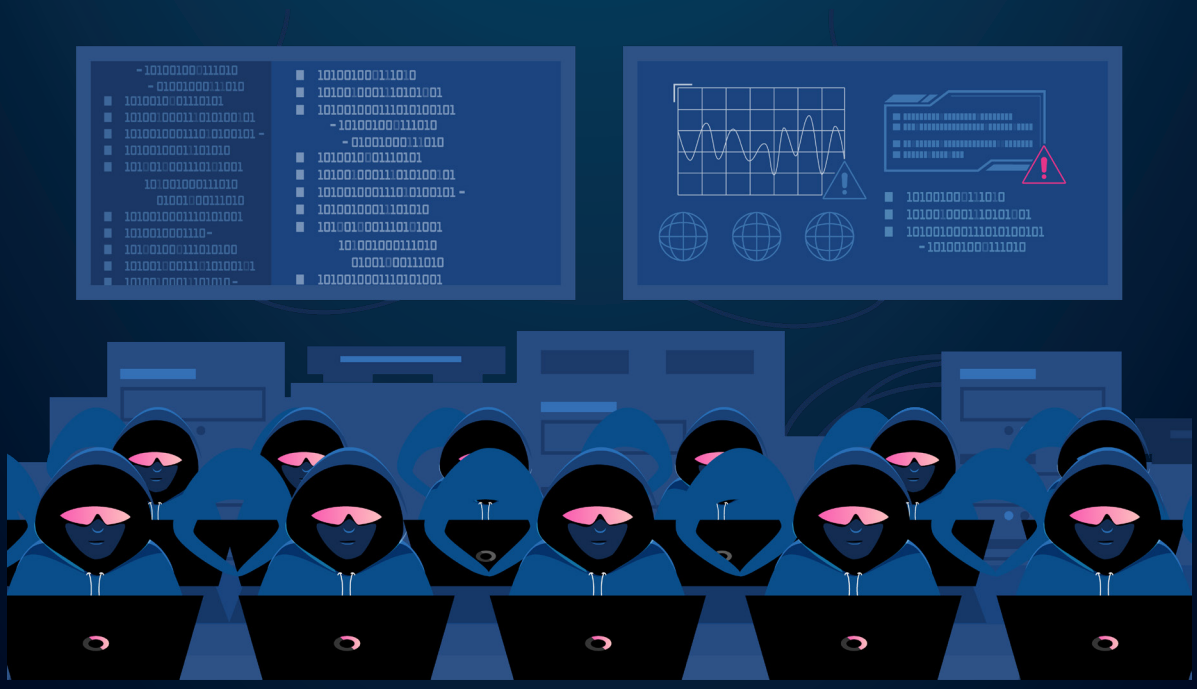
Cette violation a non seulement révélé les insuffisances des défenses de Change Healthcare en matière de cybersécurité, mais elle a également mis en évidence les vulnérabilités plus générales du secteur des soins de santé aux États-Unis.

À la suite de cette violation, Change Healthcare s'est efforcé de limiter les dégâts et a travaillé en étroite collaboration avec les autorités fédérales pour enquêter sur l'incident. L'entreprise a dû faire face à une levée de boucliers de la part du public et des organismes de réglementation, ce qui a conduit à des appels en faveur d'une réglementation plus stricte en matière de protection des données dans le secteur des soins de santé.

L'autre fait marquant de cette attaque est qu'elle fait partie d'un nombre croissant de cas où le bilan humain d'une cyber-attaque est très **VRAI**. En l'occurrence, des patients américains n'ont pas pu obtenir des médicaments essentiels en temps voulu. Un autre exemple d'attaque ayant un coût humain très réel est une violation similaire du **NHS (National Health Service)** britannique. Ces attaques montrent que les auteurs des attaques sont de plus en plus attentifs aux personnes qu'ils ciblent et qu'ils peuvent même choisir des cibles dans le secteur de la santé afin d'augmenter la probabilité d'un gros paiement.

DONNÉES PUBLIQUES NATIONALES

La violation de **National Public Data (NPD)**, qui s'est produite au début de l'année 2024, est l'une des plus importantes violations de données de l'histoire, exposant jusqu'à 2,9 milliards de dossiers. Cette violation a affecté environ 170 millions de personnes aux États-Unis, au Royaume-Uni et au Canada. Les données compromises comprenaient des informations personnelles très sensibles telles que les noms et prénoms, les numéros de sécurité sociale, les adresses postales, les adresses électroniques et les numéros de téléphone. La faille a été découverte lorsqu'un acteur malveillant a accédé aux systèmes de l'entreprise en décembre 2023 et a divulgué les données sur le dark web d'avril à l'été 2024.



Les risques associés à cette violation sont importants, car les données exposées peuvent être exploitées pour diverses activités cybercriminelles et frauduleuses. Les personnes touchées par la violation sont confrontées aux risques habituels d'usurpation d'identité, d'activités financières non autorisées et d'attaques ciblées par hameçonnage. Ce qui est particulièrement notable à propos de cette masse de données, c'est que les acteurs de la menace peuvent l'utiliser pour faire des liens croisés entre les individus. Cela leur permet de créer des attaques d'ingénierie sociale de plus en plus convaincantes ciblant de futures victimes.

VIOLATION DES CASINOS MGM ET CAESAR'S

Cette attaque s'est produite fin octobre 2023, alors que nous étions en train de finaliser le rapport de l'année dernière. Elle mérite du coup d'être mentionnée ici, car ses répercussions tombent dans la période de données de ce rapport. De plus, il s'agit de l'une des attaques les plus importantes des 12 derniers mois, principalement en raison de la taille des entreprises touchées.

En octobre 2023, les casinos et centres de villégiature MGM et Caesar's ont tous deux été touchés par un ransomware. MGM n'a pas payé la rançon et estime que son rétablissement coûtera 100 millions de dollars, tandis que Caesar's a payé, environ 15 millions de dollars. La leçon à tirer n'est pas de payer la rançon, mais de savoir **comment ils sont entrés en premier lieu**, avec une ingénierie sociale implacable contre le personnel du service d'assistance, y compris en offrant des pots-de-vin.

VIOLATION DU SERVICE DE TESTS ADN 23ANDME

L'entreprise a minimisé pendant plusieurs mois l'ampleur de la violation du **service de test ADN 23andMe**, jusqu'à ce qu'il apparaisse clairement, en décembre 2023, que les données de 6,9 millions de clients ont été volées (mais n'ont pas été divulguées publiquement), tandis qu'un million de clients d'origine juive ont vu leurs données divulguées sur BreachForums, un forum de piratage informatique populaire maintenant disparu. La MFA n'était pas appliquée mais est désormais obligatoire pour tous les utilisateurs et 23andMe fait actuellement face à de graves problèmes financiers, en partie à cause de la violation.

DÉMASQUAGE DU LEADER DE LOCKBIT

En février 2024, les leaders derrière LockBit, autrefois l'un des plus grands gangs criminels de rançongiciels, **ont eux-mêmes été piratés, dirigés par l'Agence nationale britannique de lutte contre la criminalité**, et leur leader identifié sous le nom de Dmitry Yuryevich Khorosev. Cette affaire s'inscrit dans une tendance intéressante : où les forces de l'ordre ne peuvent pas extrader ou arrêter des criminels identifiés parce qu'ils sont en Russie, ou dans d'autres pays où les autorités n'ont aucun problème à abriter des criminels (tant qu'ils n'attaquent pas des cibles nationales), donc doxer ou révéler l'identité de quelqu'un est une façon de rendre leur vie difficile indirectement. Après tout, si d'autres criminels savent qui vous êtes et où vous vivez, ils pourraient venir vous rendre visite pour obtenir une part de votre trésor de crypto-monnaie.

XZ UTILS BACKDOOR

La porte dérobée **XZ Utils** a constitué une saga intéressante, révélée en mars 2024. De faux personnages y ont établi une relation avec le responsable du logiciel Open-Source (OSS) XZ Utils pendant plusieurs années. Ils ont participé à la mise à jour du code et à la rédaction de la documentation dans le but ultime de prendre la place du responsable, puis ont injecté une charge utile malveillante permettant de déverrouiller toute connexion Secure SHell (SSH) si l'on possède la clé spéciale.

Le paquet empoisonné n'a été introduit que dans les versions alpha et les versions de test de diverses distros Linux et a été découvert par Andres Freund (Microsoft) qui a remarqué des pics étranges au niveau du processeur lors du test d'un pack de base de données open-source. Si elle avait été introduite dans le système Linux classique (et dans d'autres systèmes reposant sur SSH), cela aurait pu avoir un impact énorme. Cette attaque n'a pas été officiellement attribuée, mais la plupart des experts s'accordent à dire qu'il s'agissait d'espions russes. La leçon à en tirer est que si vous créez des logiciels internes qui s'appuient sur des composants OSS (ils le font presque toujours), vous devez prendre en compte leur posture de sécurité (et celle de leurs blocs de construction aussi) comme un risque.

UNE ANNÉE DE DRAME DE SÉCURITÉ CHEZ MICROSOFT

En juin 2023, le groupe chinois (Storm-0558) a compromis les messageries électroniques de 22 entreprises dans le monde, dont le département d'État américain (60 000 e-mails volés). En janvier 2024, Midnight Blizzard (Russie) s'est introduit dans les messageries de Microsoft, en devinant des mots de passe pour accéder à un environnement de test, qui disposait d'une application OAuth donnant accès à l'environnement de production. Cette attaque faisait suite à celle de Midnight Blizzard en 2020 (SolarWinds) et à celle de juillet 2021, au cours de laquelle les pirates avaient volé des informations sur un nombre limité de clients. En mars 2024, ils ont lancé une nouvelle attaque, accédant à certains systèmes internes et à des référentiels de code source en utilisant des documents d'authentification volés lors de l'attaque de janvier.

En avril 2024, le Comité d'examen de la cybersécurité (CSRB) a publié son **troisième rapport**, consacré cette fois au piratage chinois de 2023 mentionné ci-dessus. Le rapport est cinglant dans son évaluation des raisons de la compromission de Microsoft, décrivant une série de défaillances qui ont conduit à la violation et formulant 25 recommandations d'amélioration.

Ce rapport et les attaques ont conduit Microsoft à adopter l'initiative Secure Future (SFI), qui ressemblait à l'origine plutôt à un flyer marketing. Mais désormais, tous les employés de Microsoft verront leur impact sur la sécurité mesuré chaque année, et le nouveau mantra de Satya Nadella est de « mettre la sécurité au premier plan ». Nous verrons ce qu'il en est au cours de l'année ou des deux années à venir.

CYBERSECURITY
REPORT 2025

CHAPITRE 4
PRÉVISION DU PAYSAGE DES MENACES EN 2024

CHAPITRE 4 – PRÉVISION DU PAYSAGE DES MENACES EN 2024

AVONS-NOUS BIEN PRÉDIT LES MENACES DE L'ANNÉE DERNIÈRE ?

Il est assez curieux de revenir sur les différentes prédictions que nous avons faites dans l'édition 2023 du rapport sur la cybersécurité. Prédire l'avenir s'avère toujours difficile, mais il est certain que nous avons vu juste et que certaines choses ne se sont pas déroulées comme nous l'espérions.

459 MILLIONS
DE DOLLARS AMÉRICAINS
RANÇONS PAYÉES POUR
LA PREMIÈRE MOITIÉ DE 2024

Il y a plus de groupes de rançongiciels en 2024 qu'en 2023, et plus de publications sur les sites de fuite, ce qui indique que les ransomwares sont toujours d'actualité avec plus d'entreprises compromises que l'année dernière. Le montant approximatif des rançons payées en 2023 était de 1,1 milliard de dollars américains, tandis **que les statistiques pour la première moitié de 2024 s'élèvent à 459 millions de dollars américains**, bien que la prédiction soit que 2024 sera une année plus « fructueuse » que 2023. Cela est en partie dû à des paiements plus importants pour des violations plus graves, avec la plus grande rançon connue de 75 millions de dollars américains (par une entreprise du Fortune 50 inconnue).

Nous nous attendions à ce que les attaques de fatigue MFA et de contournement MFA augmentent, et cela a certainement été le cas. Le nombre et la prolifération des kits open source et « commerciaux » pour à la fois créer les leurres par email et configurer les services proxy qui prétendent être un site de connexion réel ont pris un envol fulgurant, en réponse à une adoption plus large des options de notification push MFA. Pour combattre cela dans votre organisation, recherchez des MFA résistantes à l'hameçonnage, telles que Windows Hello for Business, les clés matérielles FIDO2 ou les Passkeys, qui utilisent un smartphone comme clé FIDO2, évitant ainsi le besoin d'achats supplémentaires de matériel. Ces technologies sont « verrouillées » sur la page de connexion légitime, donc même si l'utilisateur est amené à visiter un faux site, la technologie d'ouverture de session ne fonctionnera pas, d'où leur nom de « résistantes à l' hameçonnage». Nos recommandations pour une sécurité sans mot de passe dans le rapport 2023 sur la cybersécurité sont toujours d'actualité, avec l'ajout des Passkeys, qui sont également sans mot de passe et résistants à l'hameçonnage.

Nous avons constaté certains risques liés à l'ancien client Microsoft Teams, construit sur la plateforme electron. Heureusement, il a été remplacé par le nouveau client Teams, qui ne semble pas présenter autant de vulnérabilités. Teams reste néanmoins un vecteur d'attaque pour les tentatives d'hameçonnage, même si, depuis que Microsoft a modifié les options par défaut pour l'acceptation des communications provenant de parties externes et l'affichage d'avertissements lorsqu'un nouveau contact tente de vous joindre, la popularité de ce type d'attaques n'a pas vraiment connu d'essor.

Les logiciels espions et les malwares sur les smartphones sont des problèmes persistants avec des actions en cours de la part de **l'UE** et des **États-Unis** pour contenir la prolifération des fournisseurs et leur utilisation dans les sociétés démocratiques, comme nous l'avions prédit.

Comme nous l'avons mentionné, les attaques contre les interfaces de programmation d'applications (API) ont augmenté en 2024 par rapport à 2023 (diverses sources estiment qu'elles se situent entre 20 et 29 %). Il s'agit souvent d'un vecteur d'attaque « caché », et donc populaire auprès des criminels, car la surveillance et l'alerte sur les API ne sont pas aussi robustes que pour d'autres systèmes. Si votre entreprise publie des API pour vos applications web, assurez-vous d'avoir un modèle de sécurité robuste pour l'accès et surveillez les utilisations malveillantes, y compris les attaques DDOS.

La gestion de la posture de cybersécurité des tenants de Microsoft 365 continue de constituer un défi, comme nous l'avions prédit, bien que nous voulions attirer l'attention sur un nouvel outil, actuellement en avant-première publique et disponible pour tous les environnements M365 - **Exposure Management** (Gestion de l'exposition). Cet outil vous donne un aperçu de la configuration et de la posture de sécurité de votre environnement, ainsi que des initiatives sur lesquelles vous pouvez vous concentrer pour améliorer des domaines particuliers tels que la défense contre les BEC ou les ransomwares.

Le temps d'exploitation (le temps entre la divulgation publique d'une vulnérabilité et la disponibilité d'un exploit fonctionnel pour celle-ci) est passé de 63 jours en 2018/2019, 32 jours en 2021/2022, à cinq jours en 2023. Bien que nous n'ayons pas encore vu les statistiques pour 2024, nous avons vu plusieurs attaques réussies dans les jours suivant la divulgation d'une vulnérabilité.

Cela met encore plus de pression sur les défenseurs, car la correction des failles est un travail de longue haleine, et il est impossible de tout corriger partout en même temps, ce qui nécessite une priorisation, en veillant à ce que les dispositifs exposés à Internet soient maintenus à jour.

Nous avons examiné les dispositifs IoT comme vecteurs d'attaques dans les réseaux d'entreprise et au cours des **cinq premiers mois de 2024**, ils ont augmenté de 107 % par rapport à la même période en 2023.

Bien que nous ayons certainement vu des deep fakes convaincants en 2024, même avec le soutien des outils d'IA pour générer des images, des audios et des vidéos, nous n'avons pas encore vu de violations majeures causées par ceux-ci. Nous pensons néanmoins qu'à mesure que ces outils deviendront plus faciles à utiliser et plus performants, nous verrons plus d'attaques et de campagnes de désinformation s'appuyant sur eux.

PRÉDICTIONS DU SECURITY LAB

Chaque année, dans le cadre de ce rapport, l'équipe du **Security Lab** d'Hornetsecurity examine l'état de l'industrie, nos données, les tendances des attaques, et plus encore pour faire une série de prédictions pour l'année à venir. Cela sert à informer les entreprises des menaces potentielles qu'elles pourraient rencontrer dans l'année à venir, ainsi que des évolutions de l'industrie. Voici les prédictions du Security Lab pour l'année 2025.

Il n'est pas surprenant qu'un grand nombre de nos prédictions dans ce rapport concernent l'IA. Bien que certaines de ces prédictions puissent facilement être regroupées, d'autres sont plus spécifiques. Nous avons ventilé ces prédictions en fonction des besoins tout au long de cette section.

Les LLM entre les mains des attaquants

L'année dernière, nous avons examiné la montée de ChatGPT et d'autres modèles de langage de grande taille (LLMs) et leur impact sur la cybersécurité, tant pour les attaquants que pour les défenseurs. Les craintes initiales des LLMs écrivant des codes malveillants parfaits ne se sont pas matérialisées et, de manière discutable, l'inclusion d'interfaces de chat d'IA et d'autres automatisations dans les solutions de sécurité a été plus réussie pour aider les défenseurs.

Nous avons vu des données réelles sur l'utilisation des LLM par des attaquants de **Microsoft**, où Forest Blizzard, un acteur de menace parrainé par l'État russe, les a utilisés pour faire des recherches sur les technologies de satellite et de radar, probablement pour soutenir la guerre en Ukraine, ainsi que pour aider à des tâches de script, y compris la manipulation de fichiers. Emerald Sleet, de Corée du Nord, utilise quant à lui largement l'hameçonnage pour attirer ses cibles et a utilisé les LLM pour comprendre les vulnérabilités connues et améliorer le langage et le ton des messages d'hameçonnage. Enfin, Crimson Sandstorm (Iran, lié au Corps des gardiens de la révolution islamique) a utilisé les LLM pour l'assistance à l'ingénierie sociale, le dépannage des erreurs et l'assistance au développement .NET. Il est à noter que presque tous ces cas d'utilisation auraient pu être réalisés à l'aide de requêtes de moteurs de recherche ordinaires qui n'auraient pas permis à Microsoft de recueillir ces informations. On peut donc dire qu'en tant qu'attaquant, vous avez échoué dans votre sécurité opérationnelle (OpSec) si vous utilisez un LLM public pour faire vos recherches.

Les attaques contre les LLM eux-mêmes continuent de proliférer et MITRE a créé **ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems)** pour suivre les différents types, d'une manière similaire à la matrice **ATT&CK de l'entreprise**.

Compte tenu de ce qui précède, il est probable que l'IA et les LLM feront l'objet de discussions sur la cybersécurité au cours de l'année à venir, et ce pour un certain nombre de raisons :

1. **L'IA sera de plus en plus utilisée pour la reconnaissance et la collecte d'informations**
2. **L'IA sera utilisée pour aider les attaquants à comprendre le meilleur moment pour lancer des attaques sur la base des données fournies**
3. **L'IA continuera d'être utilisée pour améliorer presque tous les vecteurs d'attaque des acteurs de menaces, y compris le courrier électronique, la voix, l'ingénierie sociale, etc.**
4. **L'IA sera de plus en plus utilisée pour identifier rapidement les objets facilement exploitables dans les infrastructures faibles**
5. **Les outils fondés sur l'IA continueront d'évoluer pour aider les défenseurs**

Les deepfakes basés sur l'IA utilisés pour le spear-phishing et pour influencer le public

L'utilisation de la technologie deepfake dans les attaques de spear-phishing est de plus en plus préoccupante et il est probable que nous assistions à cette combinaison en 2025. Les deepfakes permettent de créer des vidéos et des enregistrements audio très réalistes qui imitent l'apparence et la voix de personnes réelles. Cette technologie peut être utilisée pour créer des messages d'hameçonnage convaincants qui incitent les destinataires à révéler des informations sensibles ou à effectuer des actions qui compromettent la sécurité.

L'essor de la technologie deepfake constitue également une menace potentielle pour l'opinion publique et la confiance. Les « deepfakes » sont à même de créer des vidéos et des enregistrements audio très réalistes qu'il est difficile de distinguer d'un contenu authentique. Cette technologie a déjà été utilisée pour diffuser des informations erronées et continuera d'être de plus en plus utilisée par les acteurs de la menace. En fin de compte, cela entraînera une érosion de la confiance dans les médias numériques.

Nous allons commencer à assister à des attaques notables sur les produits LLM

Les grands modèles de langage (LLM) sont de plus en plus populaires, mais ils sont également vulnérables à divers types d'attaques. Il s'agit notamment d'attaques par injection, d'exfiltration de données et de jailbreaks, où des acteurs malveillants manipulent les données d'entrée pour tromper le modèle ou extraire des informations sensibles. Ces vulnérabilités peuvent compromettre l'intégrité, la sécurité et, en fin de compte, la confiance dans les systèmes basés sur le LLM. Compte tenu de la dépendance accrue à l'égard de ces systèmes, les acteurs de la menace (en particulier les États-nations) n'aimeraient rien de plus que d'utiliser un LLM courant à leur avantage. Qu'il s'agisse de désinformation, de diffusion de liens malveillants ou d'autre chose, l'avenir nous le dira.

L'utilisation de l'IA donnera lieu à des affaires juridiques et conduira à une réglementation

Cette question a été longuement débattue depuis que ChatGPT a fait ses premiers pas sur le marché. Les questions de légalité, de droits d'auteur et de propriété ont sous-tendu le contenu généré par l'IA à presque tous les stades de son évolution. Cela dit, il est probable que nous arrivions à un point où nous verrons des litiges plus fréquents et plus importants à la suite de l'utilisation des LLM.

Il est également probable que nous assistions à une forme de réglementation gouvernementale de l'utilisation de l'IA par les principaux États-nations. Cette réglementation sera probablement axée sur la confidentialité des données, en particulier dans des pays comme l'Union européenne, qui a déjà ouvert la voie avec sa loi sur **l'IA**. Ces nouvelles réglementations ne nécessiteront pas seulement l'attention des créateurs de LLM eux-mêmes, mais aussi celle des organisations qui cherchent à utiliser l'IA générative dans leurs propres organisations.

Nouveaux cadres réglementaires et défis

En ce qui concerne la réglementation, l'introduction de nouveaux cadres réglementaires tels que NIS2, DORA, CRA et KRITIS (Allemagne uniquement) représentera un défi de taille pour les organisations. Ces nouveaux cadres visent à renforcer la cybersécurité et la protection des données et sont plus que nécessaires, mais il sera difficile pour de nombreuses organisations de s'y conformer et cela nécessitera beaucoup de ressources. En outre, la place du responsable de la conformité au sein de nombreuses organisations continuera d'évoluer et deviendra de plus en plus importante.

Par ailleurs, le nombre d'organisations exigeant un certain type d'adhésion à la conformité pour pouvoir faire des affaires avec elles augmentera également. Les attaques contre la chaîne d'approvisionnement sont de plus en plus fréquentes et préjudiciables, et plutôt que de faire explicitement confiance aux organisations partenaires comme autrefois, de nombreuses organisations exigent que leurs clients et/ou leurs fournisseurs se conforment à certains des mêmes cadres réglementaires qu'elles doivent elles-mêmes respecter.

Corruption de la communauté Open Source

Pendant de nombreuses années, les logiciels libres ont été considérés comme une sorte d'oasis dans un écosystème logiciel perçu comme peu sûr. Avec l'incident XZ Utils que nous avons évoqué plus haut dans ce rapport, ainsi que plusieurs autres failles de sécurité très médiatisées, ce sentiment n'est plus de mise. Dans le cas de XZ Utils, un acteur très déterminé a tenté de s'emparer d'un logiciel libre très populaire et de l'utiliser pour créer une attaque généralisée de la chaîne d'approvisionnement.

Avec un tel succès (ou presque), les attaquants sont susceptibles de tenter quelque chose de similaire avec d'autres paquets open-source critiques pour l'industrie. **Le nombre de logiciels libres malveillants a déjà augmenté, et ce qui s'est passé récemment avec le dépôt de logiciels PyPi** n'est probablement qu'un avant-goût de ce qui nous attend.

Poursuite des prévisions concernant l'informatique quantique

Dans les rapports précédents, nous avons évoqué la menace qui n'est pas encore imminente, mais qui se profile néanmoins à l'horizon, à savoir l'informatique quantique. Bien que nous soyons encore à quelques années d'un ordinateur quantique cryptographique (CRQC), certains experts l'estiment à 2037, soit moins 5 à plus 20 ans, et le développement se poursuit rapidement. Le jour où ces ordinateurs arriveront est connu sous le nom de « jour Q ». Si votre entreprise stocke aujourd'hui des données sensibles sous forme cryptée auxquelles vous pensez avoir encore besoin d'accéder dans dix ans, vous devez vous pencher sur la question dès maintenant. En effet, la NSA, et probablement ses homologues dans d'autres pays, saisissent de grandes quantités de données qu'ils ne peuvent pas décrypter aujourd'hui, mais qu'ils pourront peut-être décrypter à l'avenir.

Le NIST, aux États-Unis, partage cet avis et a **normalisé trois algorithmes de chiffrement post-quantique :**

- ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism)
- ML-DSA (algorithme de signature numérique basé sur des modules en treillis)
- SLH-DSA (Stateless Hash-Based Digital Signature Algorithm - Algorithme de signature numérique sans hachage)

Un quatrième standard est également prévu. Les anciens noms inspirés du cristal kyber étaient nettement plus ringards. Les nouveaux noms indiquent dans quel domaine de la cryptographie ils doivent être utilisés.

Microsoft prend également cette menace au sérieux dans le cadre de son programme **Quantum Safe** et a récemment **annoncé** que sa bibliothèque cryptographique open-source **SymCrypt**, utilisée dans Windows 10 et 11, Windows Server, Azure et Microsoft 365, prend désormais en charge le ML-KEM, et bientôt le ML-DSA et le SLH-DSA.

Le défi des ordinateurs quantiques est leur mise à l'échelle, tant en ce qui concerne le nombre de qubits physiques (un CRQC aura besoin de plusieurs milliers) que la correction d'erreurs nécessaire pour produire un qubit logique fiable contre lequel programmer. Nous recommandons toujours que si votre entreprise détient des données sensibles, que vous prévoyez / avez l'obligation réglementaire de conserver pendant plus de 10 ans, de trouver un moyen de les recrypter avec un algorithme quantique sûr, en particulier maintenant que les normes ont été ratifiées.

Adoption accrue de langages « sans mémoire »

Les logiciels sont depuis longtemps confrontés à des problèmes de sécurité résultant de problèmes de gestion de la mémoire. Il s'agit notamment de débordements de mémoire tampon et d'erreurs de type « **use-after-free** ». En conséquence, l'industrie a commencé à s'orienter vers des langages « sans risque pour la mémoire » comme Rust et/ou Swift. Ces langages disposent de protections intégrées contre de nombreuses vulnérabilités courantes liées à la mémoire, ce qui allège le fardeau des développeurs de logiciels lorsqu'il s'agit d'écrire du code sécurisé.

Compte tenu de la perspective croissante d'une **réglementation imminente** sur l'industrie du logiciel, les développeurs sont susceptibles d'adopter davantage ces langages non seulement pour rendre leurs logiciels plus sûrs, mais aussi pour se préparer à l'avance aux réglementations susmentionnées.

QUEL SERA LE NIVEAU DE RISQUE POUR MON ENTREPRISE EN 2025 ?

Notre réponse à cette question reste la même que les années précédentes : si votre entreprise est capable de payer une rançon ou si vous détenez des informations ou des éléments de propriété intellectuelle susceptibles d'être vendus à des fins lucratives, vous **ÊTES** une cible. C'est ce que démontrent nos données relatives à l'indice de menace par courriel de l'industrie, qui montrent que les cybercriminels continuent de cibler tous les secteurs de l'industrie. Cela dit, si votre entreprise traite des données sensibles, est impliquée dans le secteur de la défense ou de l'infrastructure critique, ou détient une propriété intellectuelle de grande valeur, vous êtes une cible encore plus importante.

CE QUE LES ENTREPRISES DOIVENT FAIRE POUR SE DÉFENDRE

Commencer par les bases

Les entreprises ont tendance à réagir à des menaces spécifiques et à acquérir des solutions de sécurité ponctuelles pour chaque domaine, et donc à se concentrer sur les solutions technologiques, au lieu de commencer par les principes de base de l'hygiène de sécurité. La grande majorité des entreprises victimes d'une intrusion ne le sont pas à cause d'un obscur exploit de type « zero-day » ou d'une technique de piratage avancée. Leurs défenses échouent parce qu'elles n'ont pas mis en œuvre une authentification forte (MFA, de préférence du matériel résistant aux hameçonnages), autorisé des mots de passe simples, configuré les utilisateurs en tant qu'administrateurs locaux sur leurs appareils ou n'ont pas formé les utilisateurs à être prudents lorsqu'ils cliquent sur des liens dans des courriels. Ne pas valider les sauvegardes en testant les procédures de restauration peut conduire à un sal quart d'heure en cas d'attaque de ransomware, tout comme une politique laxiste en matière de correctifs.

En d'autres termes, il faut d'abord s'occuper de l'hygiène de base en matière de sécurité, ce qui inclut la technologie, les processus et les personnes. Commencez par adopter une attitude "confiance zero" :

- **Vérifier chaque connexion** - ce n'est pas parce qu'un appareil est géré qu'il est automatiquement sûr, et ce n'est pas parce qu'un utilisateur se connecte à partir d'un réseau connu qu'il ne s'agit pas d'un pirate utilisant des informations d'identification volées.
- **Utiliser le moindre privilège** - ne donner aux utilisateurs et aux identités de charge de travail que les **autorisations** dont ils ont besoin pour remplir leur rôle et procéder à des examens réguliers pour s'assurer que les autorisations données ne s'accumulent pas.
- **Supposez une violation** - construisez vos défenses aussi solidement que votre budget le permet, mais travaillez également sur les scénarios possibles en cas d'échec. Si un attaquant compromet un utilisateur, comment le détecterez-vous ? Comment pouvez-vous limiter la capacité d'un attaquant à se déplacer latéralement dans votre environnement ?

Une liste plus exhaustive est disponible dans les commandements **ZT d'Open Groups.**

La culture dévore la stratégie au petit déjeuner

Transformer votre entreprise en une entreprise cyber-résiliente exigera bien sûr du temps, des efforts et de la persévérance. Vous ne pouvez pas transformer votre entreprise en une cyberforteresse bien défendue sans impliquer tout le monde et sans les aider à comprendre comment le problème les affecte et pourquoi ils doivent faire partie de la solution.

Lorsqu'il s'agit de déployer le MFA, il faut s'assurer que les dirigeants montrent l'exemple et qu'ils comprennent (ainsi que le conseil d'administration) la raison de l'ajout d'une friction supplémentaire pour l'authentification. Une partie de ce changement de culture consiste à comprendre que la cyber-résilience n'est pas le travail du département informatique ou du département de la sécurité. Le service informatique ne peut pas sécuriser des charges de travail dont il n'a pas connaissance, et si le service marketing met en place un site web et une solution SaaS de suivi des prospects sans impliquer le service informatique et le service de sécurité, le risque que cela introduit appartient au service marketing. Chaque choix technologique ou décision de processus qui définit le fonctionnement d'une entreprise comporte des risques, et la manière dont ces risques seront gérés doit être transparente pour l'entreprise afin qu'elle puisse prendre les bonnes décisions.

Une leçon importante pour les services informatiques et de sécurité est de parler le bon langage, celui de la gestion des risques. Si vous commencez à parler de détails techniques et de leur fonctionnement, vous perdrez tous les autres acteurs de l'entreprise, mais si vous traduisez les changements de technologie et de processus en termes de risques (ou d'opportunités) pour l'entreprise, tout le monde devrait y trouver son compte.

Et cette cyber-résilience n'est pas statique, tout comme d'autres risques pour les entreprises (géopolitiques, économiques, concurrents), elle est en constante évolution et l'entreprise doit apprendre et s'adapter en permanence. Parmi les exemples récents, on peut citer la manière dont les attaquants contournent ou déjouent les formes « plus faibles » de MFA, avec des boîtes à outils « Attacker in the Middle » (attaquant au milieu) ou des attaques de fatigue de MFA. L'ingénierie sociale est un risque omniprésent - votre service d'assistance aurait-il mieux réussi à défendre votre entreprise que ceux de Caesar's ou de MGM's ?

Une stratégie de sécurité équilibrée

Pour relever les défis de l'écosystème de sécurité actuel, les entreprises doivent envisager de mettre en œuvre une approche équilibrée de la sécurité - une approche qui s'attaque aux menaces avancées spécifiques à leur secteur d'activité tout en veillant à ce que les mesures de sécurité fondamentales soient fermement en place.

Se reposer sur un seul outil ou une seule solution de sécurité n'est plus suffisant. Les organisations doivent mettre en œuvre une stratégie multicouche qui les protège contre les vecteurs d'attaque courants tout en s'attaquant aux menaces propres à leur secteur d'activité. Cette stratégie doit inclure

- **La détection des spams et des logiciels malveillants de nouvelle génération avec ATP** pour l'analyse comportementale afin de se protéger contre le barrage continu de menaces basées sur l'email que nous observons dans ce secteur
- **Une formation de sensibilisation à la sécurité pour les utilisateurs finaux** afin de les former à repérer les attaques d'ingénierie sociale et les attaques de spear-phishing
- **Des capacités de sauvegarde et de récupération** pour les données sur site et les données hébergées dans des services en Cloud tels que M365 à des fins de récupération en cas d'attaque par ransomware.
- **Des fonctionnalités de conformité et de gouvernance** qui aident à protéger contre les fuites accidentelles de données et à garantir que les contrôles de conformité sont respectées.

En savoir plus

Les méthodes mentionnées ici pour assurer la sécurité de votre entreprise ne sont qu'un début. La gestion des risques, l'évaluation des fournisseurs et la formation s'accompagnent de réglementations et d'exigences de sécurité en constante évolution. Toutes les entreprises ne peuvent pas être des experts en matière de sécurité. Veillez à faire appel à des fournisseurs de confiance qui vous permettent non seulement d'assurer la sécurité de votre entreprise, mais aussi de tirer parti de leurs connaissances approfondies en matière de cybersécurité. Par exemple, votre personnel de sécurité possède peut-être des connaissances approfondies en matière de prévention des pertes de données, mais pas en ce qui concerne les attaques avancées par e-mail. En vous associant à un fournisseur de sécurité de confiance comme Hornetsecurity, vous pourrez tirer parti de ses connaissances et des vôtres. Collectivement, nous pouvons tous travailler ensemble pour améliorer la sécurité, alors n'oubliez pas de contacter vos fournisseurs de sécurité pour en savoir plus et voir comment vous pouvez collaborer plus étroitement.

HORNETSECURITY

CSR2025

365 TOTAL PROTECTION

NEXT-GEN MICROSOFT 365 SECURITY

BUSINESS

PLAN 1

- SPAM & MALWARE PROTECTION
- EMAIL ENCRYPTION
- EMAIL SIGNATURES & DISCLAIMERS

ENTERPRISE

PLAN 2

INCLUDES ALL BENEFITS OF PLAN 1

- ADVANCED THREAT PROTECTION
- EMAIL ARCHIVING
- EMAIL CONTINUITY

ENTERPRISE BACKUP

PLAN 3

INCLUDES ALL BENEFITS OF PLAN 1 + 2

- AUTOMATIC BACKUP OF M365 DATA
- GRANULAR RECOVERY WITH END USER SELF SERVICE
- UNLIMITED STORAGE IN ONE ALL-INCLUSIVE FEE

COMPLIANCE & AWARENESS

PLAN 4

INCLUDES ALL BENEFITS OF PLAN 1 + 2 + 3

- SECURITY AWARENESS
- PHISHING & ATTACK SIMULATION
- ESI® REPORTING
- PERMISSION MANAGEMENT
- PERMISSION ALERTS
- PERMISSION AUDIT
- DMARC REPORTING & MANAGEMENT
- ENHANCED EMAIL REPUTATION & DELIVERY
- EASY DNS MANAGEMENT & OPTIMISATION
- AI RECIPIENT VALIDATION
- COMMUNICATION PATTERN ANALYSIS
- SENSITIVE DATA CHECK

LIEN VERS L'ESSAI GRATUIT

HORNETSECURITY
CSR2025

À PROPOS DES AUTEURS

ECRIT PAR

Andy Syrewicze

Andy a plus de 20 ans d'expérience dans la fourniture de solutions technologiques dans plusieurs secteurs verticaux. Il est spécialisé dans l'infrastructure, le cloud et la suite Microsoft 365.

Andy est titulaire du prix Microsoft MVP en Cloud et Datacenter Management et est l'un des rares à être également un expert VMware.

Paul Schnackenburg

Paul Schnackenburg a débuté dans l'informatique à l'époque où DOS et les processeurs 286 étaient à la pointe de la technologie. Il dirige Expert IT Solutions, une société de conseil en informatique pour petites entreprises située sur la Sunshine Coast, en Australie. Il est également professeur d'informatique à la Microsoft IT Academy.

Paul est un auteur technologique très respecté et actif dans la communauté, rédigeant des articles techniques approfondis, axés sur Hyper-V, System Center, le cloud privé et hybride et les technologies de cloud public Office 365 et Azure.

Il est titulaire des certifications MCSE, MCSA et MCT.

HORNETSECURITY
CSR2025

CHAPITRE 5
RESSOURCES

- https://attack.mitre.org/techniques/T1027/006/
- https://github.com/kgretzky/evilginx2
- https://www.techtarget.com/searchSecurity/definition/double-extortion-ransomware
- https://www.csoonline.com/article/569273/what-is-smishing-how-phishing-via-text-message-works.html
- https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/
- https://youtu.be/SScaV2PjFcg?si=Ivjyfnk7YmwUUnVh
- https://www.hornetsecurity.com/en/blog/category/threat-reports/
- https://www.youtube.com/watch?v=o3JFNaNES0Q&list=PLyKOQIbp_zWzsfkSUQ0F-Ved_0bZXts70W&index=13
- https://www.propublica.org/article/microsoft-solarwinds-golden-saml-data-breach-russian-hackers
- https://www.cisa.gov/resources-tools/groups/cyber-safety-review-board-csrb
- https://www.microsoft.com/en-us/trust-center/security/secure-future-initiative?msocki=35a127b0490c698b23e234bd4819680d
- https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
- https://techcommunity.microsoft.com/t5/microsoft-syntex-blog/welcome-to-microsoft-inspire-2023-introducing-microsoft-365/ba-p/3874887
- https://www.hornetsecurity.com/fr/services/365-multi-tenant-manager/
- https://techcrunch.com/2024/02/29/unitedhealth-change-healthcare-ransomware-alphv-blackcat-pharmacy-outages/
- https://en.wikipedia.org/wiki/2024_National_Public_Data_breach
- https://cybernews.com/security/mgm-caesars-ransomware-attack-timeline/
- https://www.theverge.com/2024/9/13/24243986/23andme-settlement-dna-data-breach-lawsuit
- https://www.nationalcrimeagency.gov.uk/news/lockbit-leader-unmasked-and-sanctioned
- https://en.wikipedia.org/wiki/XZ_Utils_backdoor
- https://www.cisa.gov/resources-tools/resources/CSRB-Review-Summer-2023-MEO-Intrusion
- https://www.bleepingcomputer.com/news/security/ransomware-rakes-in-record-breaking-450-million-in-first-half-of-2024/
- https://www.politico.eu/article/eu-commission-national-security-does-not-justify-spying-document/

- https://home.treasury.gov/news/press-releases/jy2581
- https://virtualizationreview.com/Articles/2024/03/25/exposure-management.aspx
- https://wca.org/security-attacks-on-iot-devices-surge-by-107-in-early-2024/
- https://atlas.mitre.org/matrices/ATLAS
- https://attack.mitre.org/matrices/enterprise/
- https://www.infosecurity-magazine.com/news/156-increase-in-oss-malicious/
- https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
- https://www.microsoft.com/en-us/security/blog/2023/11/01/starting-your-journey-to-become-quantum-safe
- https://techcommunity.microsoft.com/t5/security-compliance-and-identity/microsoft-s-quantum-resistant-cryptography-is-here/ba-p/4238780
- https://github.com/microsoft/SymCrypt
- https://fr.wikipedia.org/wiki/depassement_de_tampon
- https://fr.wikipedia.org/wiki/Dangling_pointer
- https://securityboulevard.com/2024/10/eu-cra-good-intentions-impossible-requirements/
- https://pubs.opengroup.org/security/zero-trust-commandments/