RAPPORT SUR LA CYBERSÉCURITÉ 2026

LES ATTAQUES SONT À NOUVEAU EN HAUSSE – CE QUE VOUS DEVEZ SAVOIR

À PROPOS DE HORNETSECURITY

Hornetsecurity permet aux entreprises et aux organisations de toutes les tailles de se concentrer sur leur cœur de métier en protégeant le cloud M365, les communications par e-mail, en sécurisant les données et en garantissant la continuité des activités et la conformité grâce à des solutions cloud de nouvelle génération.

Notre produit phare, 365 Total Protection, est la solution de sécurité cloud la plus complète du marché pour Microsoft 365. Elle inclut notamment la sécurité des e-mails, la conformité, la gouvernance et la sauvegarde.

QU'EST-CE QUE LE RAPPORT SUR LA CYBERSÉCURITÉ ?

Le rapport sur la cybersécurité d'Hornetsecurity est une analyse annuelle du paysage actuel des menaces, basée sur des données réelles collectées et étudiées par l'équipe dédiée du Security Lab Hornetsecurity. L'entreprise traite plus de 6 milliards e-mails chaque mois. En analysant les menaces identifiées dans ces communications, combinées à une connaissance approfondie du paysage global des menaces, notre laboratoire révèle les principales tendances en matière de sécurité, les campagnes des acteurs malveillants et formule des projections éclairées sur l'avenir des menaces de sécurité Microsoft 365, permettant ainsi aux entreprises d'agir en conséquence. Les conclusions et les données de 2025 ainsi que les projections pour 2026 sont contenues dans ce rapport.

QU'EST-CE QUE LE LABORATOIRE DE SÉCURITÉ ?

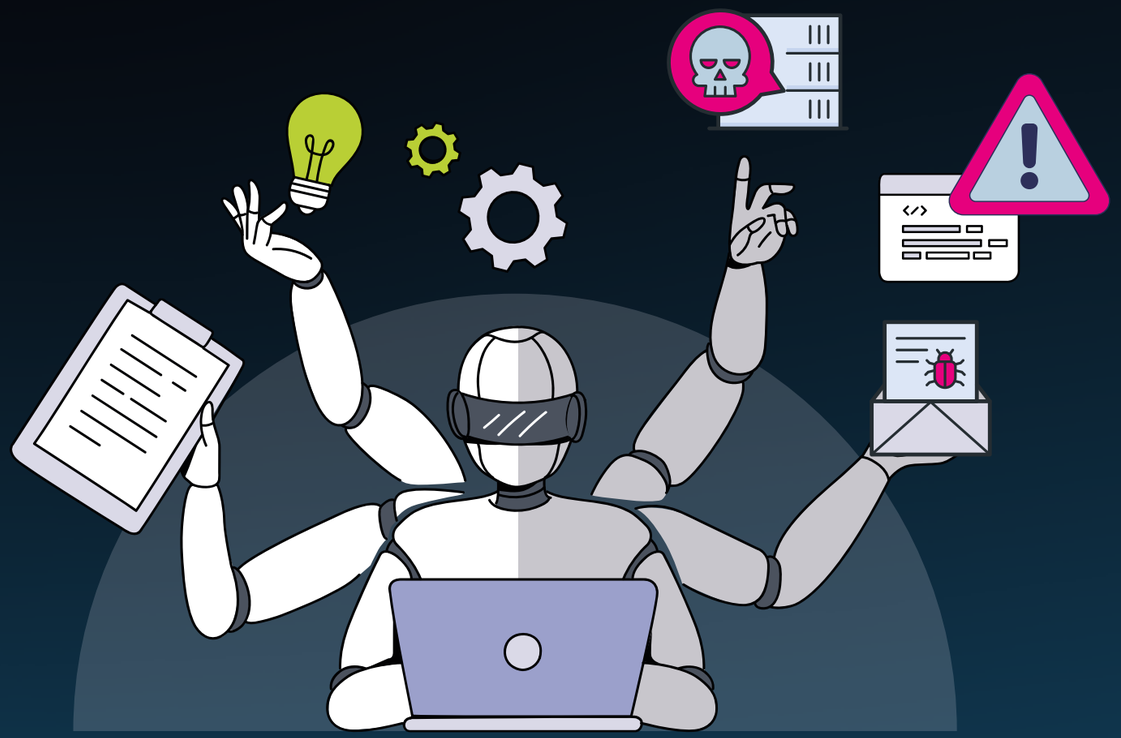
Le Security Lab est une division de Hornetsecurity qui effectue des analyses numériques des menaces de sécurité les plus récentes et les plus critiques, spécialisée dans la sécurité des e-mails et l'écosystème Microsoft 365. Cette équipe multinationale de spécialistes en sécurité possède une vaste expérience dans la recherche en sécurité, l'ingénierie logicielle et la science des données.

Une compréhension approfondie du paysage des menaces, établie grâce à l'examen pratique d'attaques de phishing, de logiciels malveillants, de gangs de ransomware et plus encore, est essentielle pour développer des mesures de sécurité efficaces. Les informations détaillées révélées par notre Security Lab constituent la base des solutions de cybersécurité de nouvelle génération de Hornetsecurity.

COMMENT UTILISER CE RAPPORT

Ce rapport comprend cinq sections principales :

- Le chapitre 1 est le résumé exécutif.
- Le chapitre 2 se concentre sur le paysage actuel des menaces pesant sur la plateforme Microsoft 365.
- Le chapitre 3 traite des préoccupations et des discussions actuelles concernant les menaces et les tendances les plus importantes de 2025.
- Le chapitre 4 contient les prévisions du Security Lab concernant les menaces de cybersécurité en 2026, ainsi que des conseils et des lignes directrices pour vous aider à protéger votre entreprise.
- Le chapitre 5 répertorie toutes les références, les liens et les ensembles de données utilisés dans ce rapport.



ÉQUILIBRE ENTRE INNOVATION ET MENACE :

LA DOUBLE NATURE DE L'IA

CHAPITRE 1

RÉSUMÉ

L'année 2025 a été marquée par une accélération. Les acteurs malveillants ont adopté l'automatisation, l'intelligence artificielle et l'ingénierie sociale à une vitesse sans précédent, tandis que les défenseurs se sont empressés d'adapter leurs programmes de gouvernance, de résilience et de sensibilisation en conséquence. Ce que nous avons observé dans l'écosystème Hornetsecurity, grâce à notre analyse de plus de **6 milliards d'e-mails traités chaque mois**, confirme une vérité simple : la surface d'attaque s'étend plus rapidement que la plupart des organisations ne peuvent la sécuriser.

Le courrier électronique reste le vecteur de transmission le plus courant pour les cybermenaces, mais les tactiques ont évolué. Les courriels contenant des **logiciels malveillants ont augmenté de 130 %** d'une année sur l'autre, accompagnés d'une **hausse des escroqueries (+34,7 %)** et du **phishing (+21 %)**. Les attaquants ont troqué la force brute contre la précision, en tirant parti d'infrastructures légitimes, d'URL obscurcies et de techniques HTML furtives pour contourner les filtres et échapper à la vigilance humaine. Parallèlement, les pièces jointes TXT et DOC malveillantes, autrefois considérées comme largement inoffensives ou obsolètes, ont refait surface en tant que principaux vecteurs d'infection, soulignant ainsi que même les types de fichiers « à faible risque » ne peuvent plus être ignorés.

Les ransomwares ont également fait un retour en force en 2025. Après plusieurs années de déclin relatif, **24 % des organisations ont déclaré en avoir été victimes**. Cela représente une augmentation de **29 % par rapport à l'année précédente**. Si les sauvegardes immuables et l'amélioration des plans de reprise après sinistre ont permis de **réduire le taux de paiement des rançons à seulement 13 % des cas**, les attaquants ont réagi en diversifiant leurs points d'entrée et leurs objectifs. Le phishing, les identifiants compromis et l'exploitation des terminaux sont désormais autant de voies d'infiltration, et les **nouvelles variantes du « ransomware 3.0 »** commencent à se concentrer moins sur le chiffrement et davantage sur la manipulation de l'intégrité des données, corrompant ainsi la confiance elle-même plutôt que simplement la disponibilité.

L'intelligence artificielle a bouleversé les deux aspects de l'équation en matière de sécurité. Les RSSI sont optimistes mais prudents : 61 % d'entre eux estiment que l'IA a directement **accru le risque de ransomware**. Les préoccupations des RSSI concernant l'IA sont nombreuses. Elles vont de l'automatisation du phishing à l'usurpation d'identité par deepfake, en passant par le "model poisoning". Le potentiel d'utilisation abusive de l'IA est devenu une caractéristique déterminante du paysage des menaces. Cependant, le camp défensif rattrape son retard, **68 % des entreprises investissent dans la détection et l'analyse basées sur l'IA**. En 2026, le défi pour les organisations et les équipes de sécurité consistera à mettre en place une gouvernance et à exploiter les capacités de l'IA sans amplifier les risques.

Le Hornetsecurity Security Lab prévoit que l'année à venir verra la poursuite de l'adoption incontrôlée des outils d'IA dans les entreprises, souvent à un rythme plus rapide que celui auquel les équipes juridiques ou de sécurité peuvent les évaluer. Cette situation, associée à l'utilisation de l'IA agentielle à des fins malveillantes, amplifiera les vulnérabilités existantes tout en en introduisant de nouvelles qui défient les modèles de confinement traditionnels. L'identité reste également le principal champ de bataille : **les kits d'attaque de type « man-in-the-middle »**, les extensions de navigateur compromises et les abus "OAuth" montrent que les identifiants et l'identité continuent d'être le maillon faible des écosystèmes cloud modernes.

Malgré cette complexité croissante, il y a des raisons d'être optimiste. Les organisations gagnent progressivement en maturité. L'adoption des principes Zero Trust, des technologies de sauvegarde immuables et de l'authentification multifactorielle (MFA) résistante au phishing devient une attente de base plutôt qu'un objectif ambitieux. La sensibilisation à la sécurité, qui était autrefois une simple case à cocher en matière de conformité, s'intègre de plus en plus dans la culture d'entreprise. La voie à suivre est claire : la résilience, et non la perfection, est le nouveau critère de réussite. Ceux qui considèrent la cybersécurité comme un élément central de la continuité des activités et non comme un simple problème informatique seront les mieux placés pour prospérer dans le paysage des menaces en constante évolution de 2026.

SMART DEFENSE :

COMMENT L'IA PROTÈGE VOTRE BOÎTE DE RÉCEPTION

CHAPITRE 2

L'ÉTAT DE LA SÉCURITÉ DANS LE SECTEUR

TENDANCES EN MATIÈRE DE SÉCURITÉ DES E-MAILS

Les e-mails restent la colonne vertébrale de la communication d'entreprise et, comme le montrent nos données, ils continuent également d'être le principal champ de bataille des attaquants. Les changements dans la classification et les types de menaces en 2025 révèlent deux réalités simultanées : les hackers expérimentent de nouveaux types de fichiers et des méthodes de livraison peu coûteuses (augmentation des fichiers TXT et DOC hérités), tandis que l'ingénierie sociale reste un levier constant pour compromettre les systèmes. En termes simples : la quantité et la qualité changent. Alors que les volumes de spam classiques se sont stabilisés après normalisation, les catégories à fort impact (malwares, escroqueries, hameçonnage, etc.) connaissent une croissance substantielle. Cette combinaison (contenu plus dangereux diffusé à grande échelle) augmente la probabilité que même les organisations bien protégées soient confrontées à des incidents, à moins qu'elles n'adaptent leurs pratiques en matière de détection, de sensibilisation des utilisateurs et de récupération.

Spam, logiciels malveillants et mesures des menaces avancées

Les chiffres clés sont sans ambiguïté : les logiciels malveillants ont connu **la plus forte augmentation relative (+130,92 %)**, suivis par **les escroqueries (+34,70 %)** et **le phishing (+20,97 %)**. Ces trois catégories représentent la majeure partie du risque qui a un impact opérationnel (vol de données, cryptage, perturbation des activités). Parallèlement, les catégories qui représentaient traditionnellement un risque moindre pour les entreprises, à savoir les messages légitimes, les e-mails transactionnels et commerciaux, n'ont connu qu'une évolution modeste, ce qui indique que les acteurs malveillants concentrent leurs efforts sur des types d'attaques à plus forte valeur ajoutée.

Principales implications:

- **Prolifération des charges utiles** malveillantes. Une augmentation de **131 % dans la classification des logiciels malveillants** signifie que davantage d'e-mails contiennent des charges utiles actives (ou au moins des indicateurs de charge utile) plutôt que de simples nuisances. Les stratégies de détection doivent dans tous les cas partir du principe qu'il s'agit d'actes malveillants.
- **Les escroqueries et les techniques avancées d'ingénierie sociale sont en hausse. Les scams (+34,7 %) associées au phishing (+21,0 %)** indiquent que les hackers affinent leurs techniques et leur retour sur investissement. Ils mettent en place des fraudes plus convaincantes et des messages plus personnalisés, probablement grâce aux technologies d'IA générative.
- **La croissance des « publicités malveillantes » sape les filtres heuristiques. L'augmentation des e-mails publicitaires malveillants (+17,72 %)** suggère que les hackers informatiques pourraient utiliser des modèles marketing de moindre qualité pour contourner les filtres de contenu simples et se fondre dans le trafic marketing légitime.
- **La part du spear phishing ciblé est en baisse, mais n'a pas disparu. Le spear phishing suspect est en baisse (-9,75 %),** ce qui reflète prosbablement une évolution vers un phishing plus automatisé/standardisé et vers des approches de vol d'identifiants qui contournent la détection classique du spear phishing. Ne vous laissez pas bercer par un faux sentiment de sécurité : les attaques ciblées restent très efficaces, même si leur volume est moindre.

CATÉGORIES DE CLASSIFICATION DES E-MAILS

Catégorie	Variation annuelle ajustée 2025 par rapport à 2024
Malware	+130.92 %
Scam / Escroquerie	+34.70 %
Phishing	+20.97 %
E-mails commerciaux indésirables	+17.72 %
Emails commerciaux	+2.37 %
Messages légitimes	+3.38 %
Transactionnels	+3.19 %
Spam	+0.03 %
Réseaux sociaux	-8.05 %
Suspects / Spear Phishing	-9.75 %
E-mails commerciaux professionnels	-13.73 %
Rebonds (bounce)	-18.69 %

Remarque : Les calculs tiennent compte des variations de la taille de l'échantillon d'une année à l'autre et sont ajustés en conséquence.

DESCRIPTIONS DES CATÉGORIES

Spam
Messages électroniques non sollicités envoyés en masse à un grand nombre de destinataires, généralement à des fins publicitaires ou malveillantes.

Hameçonnage/phishing
Messages électroniques frauduleux conçus pour inciter les destinataires à révéler des informations sensibles telles que des mots de passe, des numéros de carte de crédit ou des données personnelles.

E-mails commerciaux
E-mails marketing ou promotionnels légitimes envoyés par des entreprises à leurs clients ou prospects, souvent pour annoncer des produits ou proposer des offres.

Messages légitimes
Courriels authentiques et non promotionnels échangés entre des individus ou des organisations à des fins de communication normale.

E-mails commerciaux professionnels
E-mails marketing de qualité professionnelle, souvent très ciblés et personnalisés, généralement utilisés dans les campagnes B2B. .

Transactionnels
E-mails déclenchés par des actions de l'utilisateur ou des événements système, tels que des confirmations de commande, des réinitialisations de mot de passe ou des notifications de compte.

Réseaux sociaux
E-mails provenant de plateformes de réseaux sociaux, y compris les notifications, les demandes d'ajout à la liste d'amis et les alertes d'activité.

Rebonds/bounce
E-mails qui ne parviennent pas à la boîte de réception du destinataire en raison d'adresses invalides, de boîtes aux lettres pleines ou de problèmes de serveur.

E-mails commerciaux indésirables
E-mails marketing qui enfreignent les normes de conformité ou les bonnes pratiques, souvent mal formatés ou trompeurs.

Escroquerie/scam
E-mails destinés à frauder les destinataires, impliquant souvent de fausses offres, des gains de loterie ou des stratagèmes d'usurpation d'identité.

Malware
E-mails contenant des pièces jointes ou des liens malveillants conçus pour installer des logiciels nuisibles sur l'appareil du destinataire. .

Suspect/Spear Phishing
Tentatives de phishing très ciblées visant des personnes ou des organisations spécifiques, utilisant souvent des informations personnalisées pour paraître crédibles.

TECHNIQUES UTILISÉES DANS LES ATTAQUES PAR E-MAIL EN 2025

Le paysage des techniques d'attaque en 2025 montre une nette préférence pour les tactiques axées sur l'évasion : les attaquants se concentrent moins sur des charges utiles spectaculaires et plus sur la manière de contourner les filtres et la méfiance humaine. Les principales techniques utilisées (falsification d'en-têtes, astuces HTML subtiles, utilisation d'hébergements légitimes et obscurcissement d'URL) sont toutes optimisées pour dissimuler les intentions malveillantes dans des e-mails d'apparence anodine. **Cette évolution explique pourquoi nous observons moins d'exemples évidents de spear phishing, mais davantage de vols d'identifiants et d'intrusions en plusieurs étapes réussis : l'e-mail n'est que la première étape, et non la conclusion.**

Principales observations :

- **La manipulation des en-têtes et des métadonnées domine**. Les en-têtes falsifiées et manipulées liées au spam arrivent en tête de liste, ce qui démontre que l'usurpation d'identité et la falsification des métadonnées restent des méthodes peu coûteuses et très efficaces pour contourner les filtres naïfs et susciter la confiance des utilisateurs.
- **L'abus d'infrastructures légitimes est en augmentation.** L'envoi de campagnes via des plateformes d'hébergement réputées donne l'impression que les e-mails malveillants proviennent de sources fiables. Cette tactique augmente la délivrabilité et réduit la suspicion immédiate des filtres.
- **L'obfuscation des URL est omniprésente**. Le raccourcissement des URL, les caractères non ASCII, les TLD (domaines de premier niveau) exotiques et le fuzzing de domaine sont autant de moyens simples de masquer l'intention de la destination et de contourner les listes de blocage ou l'inspection visuelle.
- **Les astuces HTML/MIME visent à semer la confusion chez les détecteurs, pas chez les lecteurs**. Les balises <a> vides, les messages en plusieurs parties et l'insertion de polices de taille nulle sont conçus pour tromper les moteurs d'analyse basés sur les signatures et les mots-clés tout en préservant la lisibilité pour les destinataires.
- Les techniques d'évasion automatisées et à grand volume sont plus efficaces que les attaques ciblées à petite échelle. Ces techniques sont évolutives : les attaquants peuvent lancer de nombreuses campagnes qui semblent inoffensives individuellement, mais qui, collectivement, permettent de capturer des identifiants, de compromettre des comptes ou d'effectuer des téléchargements en chaîne.

LES 10 PRINCIPALES TECHNIQUES UTILISÉES DANS LES ATTAQUES PAR E-MAIL EN 2025

Classement	Technique
1	Fausse modification de l'en-tête « From »
2	Fausse modification de l'en-tête « Spamcause »
3	Utilisation d'une plateforme d'hébergement légitime pour envoyer la campagne
4	Utilisation de TLD exotiques ou inexistants
5	Raccourcissement d'URL
6	Balise HTML <a> vide
7	E-mails en plusieurs parties
8	URL avec des caractères non ASCII
9	Domaines aléatoires/Fuzzing d'URL
10	Technique ZeroFont

DESCRIPTIONS DES TECHNIQUES

1. ***Falsification de l'en-tête « From »***
   Les pirates falsifient l'en-tête « From» dans les e-mails afin d'usurper l'identité d'expéditeurs de confiance, incitant ainsi les destinataires à croire que l'e-mail est légitime.
2. ***Falsification de l'en-tête « Spamcause »***
   Manipulation des en-têtes liés au spam afin de contourner les filtres anti-spam et de donner l'impression que les e-mails malveillants sont sûrs.
3. ***.Utilisation d'une plateforme d'hébergement légitime pour envoyer des campagnes*** Utilisation de services d'hébergement ou de messagerie électronique réputés (par exemple, des plateformes cloud) pour diffuser des campagnes de phishing ou malveillantes, rendant leur détection plus difficile.
4. ***Utilisation de TLD exotiques ou inexistants***
   Utilisation de domaines de premier niveau inhabituels ou faux (par exemple, .xyz, .club) pour créer des URL trompeuses qui semblent légitimes.
5. ***Raccourcissement d'URL***
   Utilisation de raccourcisseurs d'URL (par exemple, bit.ly) pour masquer la véritable destination des liens malveillants, ce qui les rend plus difficiles à détecter.
6. ***Balise HTML <a> vide***
   Intégration de balises d'ancrage vides dans les e-mails HTML pour semer la confusion dans les filtres anti-spam ou masquer des liens malveillants.
7. ***E-mails en plusieurs parties***
   Envoi d'e-mails comportant plusieurs parties MIME (par exemple, texte et HTML) afin d'échapper à la détection par les outils de sécurité.
8. ***.URL avec des caractères non ASCII***
   Inclusion de caractères spéciaux ou Unicode dans les URL afin de créer des liens trompeurs visuellement (par exemple, attaques par homoglyphes). .
9. ***Domaines aléatoires/Fuzzing d'URL***
   Génération de domaines aléatoires ou légèrement modifiés pour contourner les systèmes de filtrage et de détection basés sur les domaines.
10. ***Technique ZeroFont***
    Insertion de texte en police de taille zéro dans les e-mails afin de manipuler les filtres basés sur des mots-clés tout en conservant la lisibilité du message pour les humains.

UTILISATION ET TYPES DE PIÈCES JOINTES DANS LES ATTAQUES

Les tendances en matière de pièces jointes en 2025 montrent un changement radical dans la stratégie de diffusion des logiciels malveillants. Les formats de fichiers qui connaissent la plus forte croissance sont **TXT** (**+181,39 %**) **et DOC** (**+118,25 %**), tandis que les formats ZIP et Office modernes (DOCX, XLSX) sont également présents, mais connaissent une croissance plus modeste. **Les vecteurs hérités ou autrefois populaires (HTML, RAR, HTM, XLS)** ont décliné, tandis que **ICS et SHTML font leur apparition dans notre top 10**. Cela indique que les hackers recherchent des types de fichiers négligés ou peu contrôlés, ainsi que des fichiers de calendrier ou des vecteurs d'inclusion côté serveur.

Points clés à retenir :

- Les fichiers TXT et DOC hérités sont des signaux d'alarme. Les fichiers TXT, largement considérés comme « à faible risque », sont utilisés comme artefacts de préparation (contenant des URL ou des scripts obscurcis). Les anciens fichiers DOC (avec prise en charge des macros) restent attractifs, car de nombreux environnements autorisent encore ou ne parviennent pas à inspecter de manière approfondie les macros Office.
- Les archives restent importantes. Les fichiers ZIP (+29,82 %) restent un vecteur de regroupement et de contournement des charges utiles ; les archives compressées continuent d'être une tactique fiable pour les hackers.
- L'émergence des formats ICS et SHTML est remarquable. Les invitations de calendrier (ICS) et les variantes d'inclusion de serveur (SHTML) représentent des vecteurs non traditionnels qui peuvent contourner certains filtres de messagerie et les attentes des utilisateurs. Cela est particulièrement vrai pour les destinataires qui acceptent les éléments de calendrier ou prévisualisent le contenu HTML.
- Le déclin des formats HTML/HTM/RAR/XLS reflète probablement un renforcement des mesures de défense, mais les hackers redirigent leurs attaques vers des canaux moins surveillés plutôt que d'abandonner complètement le courrier électronique comme vecteur.

TYPES DE FICHIERS UTILISÉS POUR LES CHARGES UTILES MALVEILLANTES EN 2025

Type de fichier	Variation annuelle ajustée 2025 par rapport à 2024
TXT	+181.39%
DOC	+118.25%
ZIP	+29.82%
DOCX	+11.69%
XLSX	+7.85%
PDF	-3.32%
HTML	-27.44%
RAR	-36.93%
HTM	Sorti du top 10
XLS	Sorti du top 10
ICS	Nouvelle entrée dans la liste en 2025
SHTML	Nouvelle entrée dans la liste en 2025

Remarque : les calculs tiennent compte et s'ajustent en fonction des variations de la taille de l'échantillon d'une année à l'autre.

DÉFINITIONS DES TYPES DE FICHIERS

PDF
Portable Document Format – Couramment utilisé pour les documents ; les hackers intègrent souvent des liens ou des scripts malveillants dans les fichiers PDF.

DOC
Document Microsoft Word (ancien) – Ancien format de fichier Word ; peut contenir des macros qui exécutent du code malveillant.

DOCX
Document Microsoft Word (moderne) – Format Word actuel ; prend en charge les macros et scripts intégrés qui peuvent être exploités.

XLS
Feuille de calcul Microsoft Excel (ancienne) – Ancien format Excel ; souvent ciblé par des attaques basées sur des macros.

XLSX
Feuille de calcul Microsoft Excel (moderne) – Format Excel actuel ; peut inclure des macros ou des liens malveillants.

TXT
Fichier texte brut – Fichiers texte simples ; les hackers peuvent les utiliser pour diffuser du contenu de phishing ou des scripts déguisés en texte.

HTML
Fichier HyperText Markup Language – Format de page Web ; souvent utilisé dans les e-mails de phishing avec des liens malveillants intégrés.

HTM
Fichier HTML (variante) – Similaire au HTML. Ancienne extension de fichier pour les fichiers HTML ; utilisé pour le contenu Web et les charges utiles de phishing.

SHTML
Fichier HTML sécurisé – Variante HTML prenant en charge les inclusions côté serveur ; peut être exploité pour des redirections malveillantes.

ZIP
Fichier d'archive compressé – Couramment utilisé pour regrouper des fichiers ; les attaquants cachent des logiciels malveillants dans des archives compressées.

RAR
Fichier d'archive compressé (alternative) – Similaire au ZIP, mais utilise un algorithme de compression différent ; souvent utilisé pour la diffusion de logiciels malveillants.

ICS
Fichier calendrier – format iCalendar ; les hackers utilisent des invitations de calendrier malveillantes pour diffuser des liens de phishing ou des charges utiles.

LA RÉSURGENCE DES RANSOMWARES EN 2025

Après trois années consécutives de déclin, les ransomwares sont revenus au premier plan des préoccupations en matière de cybersécurité. Les données de Hornetsecurity montrent qu'en 2025, **24 % des organisations ont déclaré avoir été victimes d'une attaque par ransomware, soit une forte augmentation par rapport aux 18,6 % enregistrés en 2024**. Ce revirement est un signal d'alarme dans le paysage des menaces post-pandémique et un avertissement que les attaquants évoluent de plus en plus rapidement.

Malgré des années de campagnes de sensibilisation et de programmes de formation, les ransomwares restent un risque critique pour les entreprises, précisément parce qu'ils s'adaptent à nos défenses. Les acteurs malveillants combinent désormais l'automatisation améliorée par l'IA avec des techniques d'ingénierie sociale éprouvées pour atteindre une plus grande portée, une plus grande précision et une plus grande persistance.

AUTOMATISATION, IA ET NOUVEAU MANUEL DES RANSOMWARES

Les attaquants exploitent de plus en plus l'IA générative et l'automatisation pour identifier les vulnérabilités, créer des leurres de phishing plus convaincants et orchestrer des intrusions en plusieurs étapes avec un minimum de supervision humaine.

Malheureusement, cela rend les opérations de ransomware plus évolutives et plus personnelles.

Quelques données clés :

- **61 % des RSSI** estiment que l'IA a directement accru le risque d'attaques par ransomware.
- **77 % identifient le phishing généré par l'IA** comme **une menace émergente** et **grave**.
- **68 % investissent désormais dans des capacités de détection** et de protection basées sur l'IA.

Il en résulte une course à l'armement où les deux camps utilisent l'apprentissage automatique. Pour l'un, l'objectif est de tromper, pour l'autre, de se défendre.

POINTS D'ENTRÉE : LE PHISHING PERD DU TERRAIN, LES TERMINAUX GAGNENT DU TERRAIN

Si le phishing reste le principal vecteur d'infection pour **46 % des personnes interrogées**, sa domination s'estompe. Les attaquants se diversifient :

Vecteur	2024	2025	Δ
Phishing	52.3 %	46 %	-6,3 pp
Identifiants compromis	~20 %	~25 %	+5 pp
Vulnérabilités exploitées	–	12 %	n/a
Compromission des terminaux	–	26 %	n/a

pp = « point de pourcentage »

Les données montrent une nette évolution vers le vol d'identifiants et la compromission des terminaux, en particulier dans les environnements de travail hybrides et à distance où la politique *BYOD* (*Bring Your Own Device*) et les lacunes en matière de correctifs restent très répandus. Les ransomwares ne sont plus seulement un problème lié aux e-mails, mais un problème lié à l'écosystème.

LA FATIGUE LIÉE À LA FORMATION ET LE PIÈGE DE LA « FAUSSE CONFORMITÉ

Les organisations continuent d'investir massivement dans la formation à la sensibilisation. **74 % d'entre elles la proposent, mais 42 % estiment qu'elle est insuffisante**.

De nombreux programmes restent des exercices de routine : annuels, peu engageants et rapidement oubliés. Il en résulte ce que Hornetsecurity appelle la « *fausse conformité* ». Il s'agit de l'illusion d'une préparation sans changement comportemental significatif.

Les petites et moyennes entreprises (PME) sont les plus touchées. Beaucoup fonctionnent avec un personnel informatique minimal et une infrastructure obsolète, en s'appuyant sur des prestataires externes ou des locataires cloud non patchés. Si de plus en plus de PME déclarent disposer d'un plan de reprise après sinistre, la préparation sur le papier ne se traduit pas toujours par une résilience dans la pratique.

RÉCUPÉRATION ET RÉSILIENCE : LE BON CÔTÉ DES CHOSES

Cela dit, même si les attaques se multiplient, les capacités de récupération s'améliorent discrètement :

- **62 % des organisations utilisent désormais des technologies de sauvegarde immuables**. Il s'agit de systèmes dans lesquels les données ne peuvent être ni modifiées ni cryptées une fois qu'elles ont été écrites. Même les administrateurs ou un compte administrateur compromis lors d'une attaque n'y ont pas accès.
- **82 % ont mis en place un plan de reprise après sinistre**, qui devient rapidement la nouvelle norme en matière de résilience opérationnelle.
- **Autre bonne nouvelle** : seulement **13 % des victimes ont payé la rançon** en 2025, contre **16,3 % en 2024**.

Le message est clair : les organisations apprennent à se remettre d'une attaque sans négocier.

L'assurance, cependant, raconte une autre histoire. **La couverture d'assurance contre les ransomwares est passée de 54,6 % en 2024 à 46 % cette année, en raison de l'augmentation des primes et des exclusions et de la baisse de confiance dans les indemnisations**. Cette correction du marché suggère que les organisations ne peuvent plus externaliser les risques. Elles doivent intégrer la sécurité dans leurs systèmes et renforcer leur résilience en interne.

GOUVERNANCE : LA STRATÉGIE RESTE À LA TRAÎNE PAR RAPPORT À LA RÉALITÉ DES MENACES

La cybersécurité est désormais une préoccupation au niveau du conseil d'administration, mais de nombreuses organisations ont encore du retard à rattraper pour répondre aux exigences opérationnelles de la gouvernance à l'ère des ransomwares. Peu de conseils d'administration organisent des **simulations de crises cybernétiques**, et les manuels interfonctionnels restent l'exception plutôt que la règle.

À mesure que la **désinformation alimentée par l'IA et l'extorsion par deepfake deviennent plus plausibles**, la préparation à la communication fait désormais partie de la cybersécurité et, heureusement, n'est plus une réflexion après coup en matière de relations publiques.

PERSPECTIVES : LA RÉSILIENCE AUGMENTE, MAIS LES MENACES AUSSI

Les données pour 2025 brossent un tableau nuancé : les attaques par ransomware augmentent, mais notre capacité à nous en remettre aussi. Les organisations qui résisteront à cette **nouvelle vague sont celles qui considèrent la résilience comme une stratégie et non comme une simple conformité**.

Les sauvegardes immuables, les plans de reprise bien testés et la formation significative des utilisateurs ne sont plus facultatifs, ils constituent la défense minimale viable.

Les attaquants ne restent pas inactifs, et les défenseurs ne peuvent pas non plus se permettre de rester les bras croisés. Le défi pour 2026 ne sera pas d'empêcher complètement les ransomwares, mais de s'assurer que, lorsqu'ils frappent, la continuité des activités ne soit pas compromise.

PERSPECTIVES DES RSSI : TROUVER L'ÉQUILIBRE ENTRE LES PROMESSES ET LES DANGERS DE L'IA

L'intelligence artificielle est en train de redéfinir la cybersécurité, non seulement en tant qu'outil défensif, mais aussi en tant que question stratégique. Le **sondage 2025 "Perspective et réflexions des RSSI"** a cherché à comprendre comment les responsables de la sécurité dans le monde réel abordent l'IA : où elle fonctionne, où elle présente des risques et quels sont les défis qui entravent son adoption responsable.

Les résultats révèlent une situation complexe. Les RSSI sont enthousiastes, prudents et, dans de nombreux cas, encore en phase d'expérimentation. L'IA est omniprésente, mais la confiance, la gouvernance et la compréhension ne sont malheureusement pas encore au rendez-vous.

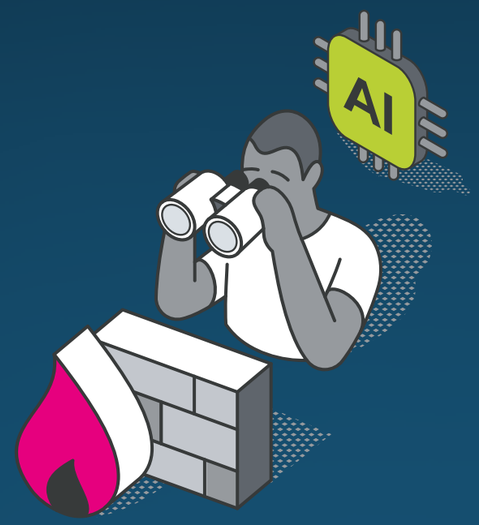
ADOPTION : CROISSANCE RAPIDE, GOUVERNANCE INÉGALE

La plupart des RSSI interrogés font état d'une **expérimentation importante de l'IA**, mais son adoption structurée reste rare. Certaines organisations intègrent l'IA dans des flux de travail tels que le triage, l'enrichissement et la gestion des tickets, tandis que d'autres en limitent totalement l'utilisation.

Le RSSI d'une société financière internationale a déclaré : « *Nous constatons un taux d'adoption supérieur à 75 % au sein de notre organisation au cours des deux dernières années.* » À l'inverse, un RSSI virtuel a fait remarquer : « *Il y a deux ans, tous les services d'IA étaient accessibles librement. Au cours de l'année écoulée, nous avons commencé à mettre en place davantage de processus et de LLM internes.* »

Cette variabilité met en évidence le défi principal : l'adoption de l'IA progresse plus rapidement que sa gouvernance, à l'instar des précédentes tendances innovantes dans le domaine technologique. De nombreux dirigeants ont commencé à centraliser le contrôle et à développer des outils internes, mais d'autres restent dans une posture réactive et cherchent à se conformer aux normes plutôt qu'à mener l'innovation.

Le **Shadow IT**, autrefois considéré comme une source d'irritation, a été redéfini par l'IA en **Shadow AI**. Les outils non approuvés, les extensions de navigateur et les intégrations SaaS créent de nouveaux risques opaques. Comme l'a résumé un RSSI, « les préoccupations liées à la sécurité de l'IA ont amplifié les dangers du Shadow IT ».



SENSIBILISATION DES UTILISATEURS FINAUX : LE NOUVEAU FACTEUR DE RISQUE HUMAIN

Si la force d'une entreprise dépend de son employé le moins préparé, l'IA a abaissé la barre.

Les RSSI s'accordent à dire que la sensibilisation des **utilisateurs finaux aux risques liés à l'IA est dangereusement faible**.

Si quelques organisations se vantent d'avoir une culture de conformité forte, certaines s'attribuant même une note de « 5 sur 5 », la plupart des RSSI estiment que le niveau de sensibilisation est plutôt de « 1 ou 2 sur 5 ».

Le principal problème ? Les employés utilisent avec enthousiasme les outils d'IA publics sans se rendre compte des implications en matière de sécurité ou de conformité. Comme l'a dit un RSSI virtuel, « les gens n'ont pas compris les enjeux, en particulier lorsqu'ils partagent des informations sur leur entreprise dans une IA publique ».

Le consensus : les efforts de sensibilisation à la sécurité en interne n'ont pas évolué au même rythme que l'adoption de l'IA. Une formation ciblée et basée sur des scénarios est désormais aussi importante que les pares-feux et les filtres.

COMPRÉHENSION DU LEADERSHIP : LE FOSSÉ DE SENSIBILISATION AU SOMMET

Les RSSI soulignent également une grande disparité dans la compréhension des risques liés à l'IA par les dirigeants.

Notre sondage a révélé la plus grande dispersion des réponses à cette question, allant d'une « profonde sensibilisation » à une « absence de compréhension réelle ». La réponse médiane était un « le leadership connaît quelque peu les risques » plutôt tiède. Il est clair que les progrès sont inégaux et varient considérablement d'une entreprise à l'autre.

Certaines organisations avancent de manière collaborative. Un RSSI du secteur technologique allemand a attribué les progrès réalisés à des initiatives conjointes des services juridiques et de sécurité : « La direction commence à comprendre les enjeux liés à la sécurité de l'IA. » D'autres, cependant, font état du contraire. « La direction voit les gains de productivité, mais pas les risques », a déclaré un RSSI virtuel.

Cette prise de conscience inégale confère aux RSSI une double responsabilité : se défendre contre les menaces externes tout en sensibilisant la direction en interne.

MENACES ÉMERGENTES : DEEPFAKES, EMPOISONNEMENT DES MODÈLES ET FUITES DE DONNÉES

Presque tous les RSSI interrogés s'accordent à dire que l'utilisation abusive de l'IA sera **une source majeure de cyber risques au cours des 12 prochains mois.**

Les préoccupations les plus pressantes sont les suivantes :

- **La fraude à l'identité synthétique** à l'aide de documents ou d'identifiants générés par l'IA,
- **Le clonage vocal et les vidéos deepfake** utilisés à des fins d'usurpation d'identité et de fraude,
- **L'empoisonnement des modèles**, où des données malveillantes corrompent les systèmes d'IA internes,
- **La fuite de données sensibles** due à l'utilisation abusive d'outils d'IA publics par les employés.

Un RSSI a lancé cette mise en garde : « *Nous sommes particulièrement préoccupés par les attaques par empoisonnement des modèles, car nous utilisons nos propres modèles en interne.* » Un autre a souligné que « *le risque numéro un lié à l'IA est la fuite volontaire de données d'entreprise vers des systèmes publics.* »

L'IA est devenue à la fois un outil et une cible, et la surface d'attaque s'étend clairement plus rapidement que beaucoup ne le pensent.

ADOPTION PAR LES ÉQUIPES DE SÉCURITÉ : PRUDENTE, CONTRÔLÉE ET TACTIQUE

Dans le domaine des opérations de sécurité, l'adoption de l'IA est mesurée, mais en pleine croissance. Les RSSI décrivent des déploiements limités axés sur des tâches spécifiques à faible risque. Par exemple, la classification des tickets ou l'enrichissement des données sur les menaces. Un RSSI du secteur financier a partagé une expérience pratique réussie : « *L'IA s'est avérée très efficace pour les notes de tickets destinées aux clients. Elles sont concises et exemptes de tout parti pris.* »

Cet « optimisme prudent » est caractéristique de 2025. Les équipes de sécurité adoptent l'automatisation, mais restent méfiantes à l'égard d'une dépendance excessive à des systèmes opaques ou à des modèles immatures.

DÉFIS LIÉS À LA MISE EN ŒUVRE : LES OBSTACLES PRATIQUES

Le chemin vers une adoption responsable de l'IA est loin d'être sans embûches. Notre sondage auprès des RSSI a révélé que les principaux obstacles sont les suivants :

- **Incertitude quant aux risques liés à l'IA** et à son utilisation abusive potentielle
- **Conformité et contraintes juridiques**
- **Justification budgétaire et démonstration du retour sur investissement**
- **Difficultés d'intégration** avec les outils existants
- **Pénurie de talents** dans le domaine de l'IA et de la science des données
- **Adhésion de la direction**

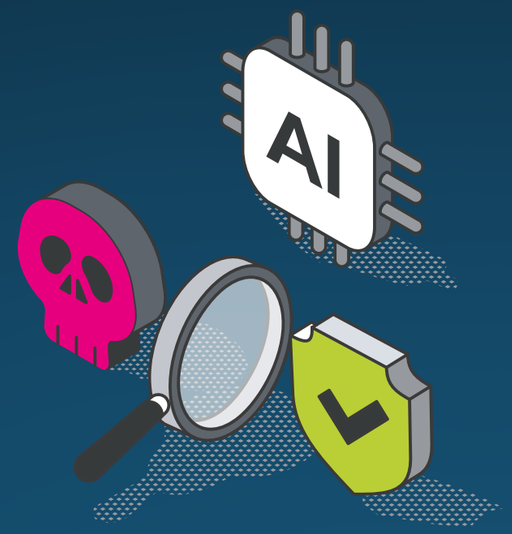
Comme l'a résumé un RSSI, « *nous manquons encore de compétences et d'experts spécialisés en IA* ». Un autre a ajouté : « *Détecter un scan de port en lisant dix lignes de journaux n'apporte pas grand-chose* ».

Malgré les obstacles, les RSSI restent pragmatiques : l'IA n'est pas un effet de mode, c'est une évolution inévitable. Mais son adoption restera au cas par cas jusqu'à ce que la transparence, les compétences et la gouvernance rattrapent l'ambition.

DE LA CURIOSITÉ À LA CAPACITÉ

L'IA dans le domaine de la cybersécurité n'est plus expérimentale, mais elle n'est pas encore tout à fait mature. Dans tous les secteurs, l'accent est passé de « *Que peut faire l'IA ?* » à « *Comment la gouverner ?* ».

L'année à venir déterminera si les équipes de sécurité peuvent transformer l'IA d'un risque en un allié fiable.



PERSONNE N'EST À L'ABRI :

LES MENACES VISENT TOUTES LES ORGANISATIONS

CHAPITRE 3

ANALYSE DES PRINCIPAUX INCIDENTS DE SÉCURITÉ ET ACTUALITÉS EN MATIÈRE DE CYBERSÉCURITÉ EN 2025

Il est important d'utiliser les incidents majeurs de cybersécurité dont sont victimes les organisations comme outil d'apprentissage, en examinant comment votre entreprise aurait géré une attaque similaire et comment améliorer votre résilience à l'avenir. Les exemples ne manquent pas depuis notre rapport de fin 2024/début 2025. Voici les dix onze que nous avons sélectionnés.

OCTOBRE 2024 – VIOLATION DE LA SÉCURITÉ D'INTERNET ARCHIVE ET ATTAQUE DDOS

Début octobre 2024, l'organisation à but non lucratif Internet Archive (connue pour Wayback Machine) a subi une importante violation de données affectant plus de **31 millions de comptes d'utilisateurs**. Les attaquants ont eu accès à une **base de données de 6,4 Go** contenant les adresses e-mail, les noms d'utilisateur et les mots de passe hachés Bcrypt des utilisateurs, entre autres informations. À peu près au même moment, un groupe de hacktivistes baptisé BlackMeta a lancé une **série d'attaques par déni de service distribué (DDoS)** contre les sites web des Archives, les mettant temporairement hors ligne. Cet incident a mis en évidence **les vulnérabilités de la gestion de la configuration des Archives** (un fichier de configuration GitLab exposé aurait été le vecteur de l'attaque).

Deux enseignements peuvent être tirés de cet incident. Même si vous êtes une organisation à but non lucratif ou « *trop insignifiante pour être vulnérable* », vous êtes toujours une cible. De plus, vous devez toujours vérifier la configuration de vos développeurs pour leurs référentiels de code, car une configuration insuffisante pourrait avoir des répercussions négatives sur vous à l'avenir.

DÉCEMBRE 2024 – PIRATAGE DU TRÉSOR AMÉRICAIN PAR UN GROUPE APT CHINOIS

Fin décembre 2024, le département du Trésor américain a révélé avoir été **victime d'une cyberattaque commanditée par l'État** et attribuée au gouvernement chinois. Des **hackers liés à un groupe APT (Advanced Persistent Threat)** chinois ont exploité une faille dans la chaîne d'approvisionnement en compromettant une plateforme d'identité et **d'assistance à distance de BeyondTrust, un fournisseur utilisé par le Trésor**. En obtenant une clé d'administration BeyondTrust, les hackers ont pu accéder à distance aux postes de travail de plusieurs employés du Trésor et voler des documents non classifiés. Les responsables du Trésor ont qualifié cet incident de « *grave incident de cybersécurité* » et ont averti les autorités américaines chargées de la cybersécurité (CISA) le 8 décembre 2024, peu après que BeyondTrust les ait alertés de l'intrusion. Cette violation, qui fait suite à d'autres attaques liées à la Chine contre des cibles américaines, a exacerbé les tensions et a conduit à un examen urgent de la sécurité des accès tiers et des cyberdéfenses du gouvernement.

La principale leçon à tirer ici est de comprendre votre modèle de menace et les risques liés à la dépendance. Si vous avez mis en place une solution de sécurité, où se trouve la « *clé principale* » de cette solution ? Que se passe-t-il si elle est compromise, et comment le détecter avant qu'il ne soit trop tard ?

JANVIER 2025 – EXPLOITS CRITIQUES DE TYPE « ZERO DAY » SUR LES VPN (IVANTI ET SONICWALL)

En janvier 2025, des hackers ont activement exploité **des vulnérabilités critiques de type « zero day »** dans deux produits d'accès à distance très utilisés par les entreprises, ce qui a déclenché des alertes de sécurité d'urgence dans le monde entier. **Ivanti (Pulse Secure) a révélé que son appliance Connect Secure VPN** contenait une faille critique permettant de contourner l'authentification, qui était exploitée dans la nature. Cette faille zero-day, qui permettait l'exécution de code à distance sans connexion, a été utilisée pour infiltrer au moins **17 organisations (dont Nominet, le registre de noms de domaine britannique) dès décembre 2024**. Les chercheurs de Mandiant ont établi un lien entre les exploits VPN d'Ivanti et un acteur malveillant basé en Chine, compte tenu des outils et des logiciels malveillants utilisés.

À peu près à la même époque, SonicWall a averti qu'une faille zero-day dans son **VPN Secure Mobile Access (SMA) série 1000** était également **exploitée de manière similaire par des attaquants**. **Microsoft et la CISA ont confirmé que la faille SonicWall, qui permettait également l'exécution de code à distance sans authentification, avait été utilisée dans des attaques, avec des incidents survenus également en juillet**. Ces défaillances successives de **la sécurité VPN** ont révélé le potentiel alarmant d'abus des systèmes d'accès à distance fiables par des adversaires, ce qui a conduit les organisations du monde entier à publier en urgence des correctifs et des mesures d'atténuation critiques.

Ce ne sont là que deux exemples d'une tendance observée ces dernières années, où les technologies que vous avez déployées pour protéger votre réseau (pare-feu, appareils VPN) sont si mal conçues et entretenues qu'elles constituent au contraire un point d'accès facile pour les hackers informatiques qui souhaitent s'introduire dans votre environnement. Quelle que soit la taille de votre fournisseur, vous devez exiger de lui qu'il fasse mieux. **Il est tout simplement inacceptable d'acheter des technologies de sécurité censées vous protéger, mais qui vous rendent en réalité plus vulnérable**.

MARS 2025 – CAMPAGNE D'ESPIONNAGE DES ROUTEURS JUNIPER NETWORKS

En mars 2025, la société de **cybersécurité Mandiant** a révélé une campagne d'espionnage en cours visant les infrastructures réseau. Un **groupe APT lié à la Chine (UNC3886)** exploitait une vulnérabilité récemment découverte dans le système d'exploitation **Junos de Juniper Networks**, le système d'exploitation des routeurs Juniper. **À partir de la mi-2024**, les attaquants ont utilisé cette faille zero-day pour accéder aux routeurs d'entreprises et peut-être même d'administrations, puis ont implanté des logiciels malveillants de type « *backdoor* » sur les appareils. Ces portes dérobées furtives ont permis aux hackers de **surveiller le trafic réseau et de s'introduire plus profondément dans les réseaux sans être détectés**. Juniper a corrigé la faille dès sa découverte, mais cet incident a été comparé à des attaques passées visant **la chaîne d'approvisionnement et les infrastructures**. Il a mis en évidence le fait que les acteurs malveillants avancés ciblent désormais directement les routeurs réseau et les pares-feux pour mener des activités d'espionnage à long terme, contournant ainsi la sécurité traditionnelle des terminaux.

Cet incident peut être signalé directement à votre équipe réseau. Les routeurs et les commutateurs font partie de la « *plomberie* » de votre infrastructure et, une fois déployés, ils ont tendance à être oubliés tant qu'ils fonctionnent. Cela en fait également un excellent endroit où les hackers peuvent se cacher, d'autant plus que vous ne pouvez pas y exécuter de solution EDR (Endpoint Detection and Response). Veillez donc à surveiller les changements de configuration et à les maintenir à jour.

JUIN 2025 – UNE ATTAQUE PAR RANSOMWARE CONTRE UNFI PERTURBE LA CHAÎNE D'APPROVISIONNEMENT ALIMENTAIRE

En juin 2025, une attaque par ransomware contre United Natural Foods, Inc. (UNFI), une importante entreprise de distribution alimentaire, a démontré l'impact réel des cyberattaques sur les chaînes d'approvisionnement. UNFI, connu pour être le principal distributeur de Whole Foods et d'autres épiceries, a détecté **une activité non autorisée sur ses systèmes informatiques le 5 juin**. Afin de contenir la menace, l'entreprise a mis hors ligne les systèmes affectés, ce qui a temporairement paralysé sa capacité à traiter les commandes et à effectuer les livraisons. En conséquence, certains détaillants alimentaires ont connu des pénuries de produits et des retards de livraison. La perturbation a duré plusieurs jours et UNFI a déclaré que l'incident entraînerait **des retards opérationnels et des coûts supplémentaires**. L'impact sur la chaîne d'approvisionnement alimentaire a attiré l'attention des régulateurs et a mis en évidence la nécessité de renforcer les cyberdéfenses dans les secteurs de la distribution et de la fabrication, car même de brèves interruptions peuvent avoir des effets en cascade sur les consommateurs.

Si votre entreprise fournit un service qui fait partie d'un réseau plus large d'entreprises où une interruption peut avoir un effet domino, touchant le public ou des infrastructures critiques, votre modélisation des risques doit en tenir compte, et pas seulement l'effet immédiat qu'une cyberattaque peut avoir sur vos propres opérations. En effet, aux yeux du public (et des régulateurs), vous serez tenu responsable de ces répercussions plus larges.

JUILLET 2025 – SCATTERED SPIDER HACKS (COMPAGNIES AÉRIENNES ET COMMERCE DE DÉTAIL – VIOLATION DE QANTAS)

Dans certains rapports sur divers incidents survenus au cours des dernières années, « Scattered Spider » a été qualifié de groupe de hackers informatiques. Ce n'est pas tout à fait exact, car il s'agit plutôt d'une affiliation lâche de nombreux acteurs différents, utilisant des tactiques similaires. Il est donc plus juste de parler de techniques « *de type Scattered Spider* ». Leur approche repose largement sur l'ingénierie sociale, consistant à tromper le personnel du service d'assistance (souvent externalisé) pour qu'il réinitialise les identifiants. Il s'agit moins de pirater des ordinateurs que de pirater des personnes. Une autre différence notable par rapport à de nombreux autres acteurs malveillants est qu'ils sont jeunes, vivent dans des pays occidentaux et sont de langue maternelle anglaise, ce qui a conduit, comme on pouvait s'y attendre, à l'arrestation de nombre d'entre eux au cours des deux dernières années.

Plus tôt en 2025, Scattered Spider avait été impliqué dans des attaques contre de grands détaillants britanniques (Marks & Spencer, Co-op, Harrods) et des compagnies d'assurance comme Aflac. **En juillet 2025**, le groupe s'est tourné vers le secteur aérien. Qantas Airways, la compagnie aérienne nationale australienne, a annoncé qu'une plateforme de centre de contact tierce qu'elle utilise avait été compromise, exposant les dossiers d'**environ 6 millions de clients**. Les données volées comprenaient les noms, les coordonnées, les dates de naissance et les numéros de voyageur fréquent, mais pas les informations financières. Qantas a confirmé avoir été victime d'une tentative d'extorsion liée à cette violation, et les cyberenquêteurs ont noté que l'attaque portait la marque des tactiques de Scattered Spider. À peu près à la même époque, WestJet (Canada) et Hawaiian Airlines (États-Unis) auraient également été touchées par des incidents similaires.

La principale leçon à tirer de ces attaques est de revoir vos procédures d'assistance, en particulier pour la réinitialisation des identifiants (« *J'ai perdu mon téléphone* »), surtout pour les comptes à privilèges élevés. Toutes les informations habituelles utilisées pour la vérification (numéro d'employé, nom du responsable, nom de jeune fille de la mère, etc.) peuvent être trouvées sur LinkedIn et d'autres réseaux sociaux et ne sont pas suffisamment sécurisées. Dans un premier temps, exigez que toute personne souhaitant récupérer un compte privilégié le fasse en personne dans les locaux de l'entreprise.

JUILLET 2025 – ATTAQUE PAR RANSOMWARE CONTRE INGRAM MICRO

Au cours de la première semaine de juillet 2025, Ingram Micro, l'une des plus grandes sociétés de distribution informatique au monde, a été mise hors ligne par une attaque critique par ransomware. Le 4 juillet, des informations ont fait état d'une panne majeure des systèmes d'Ingram Micro ; la société a rapidement confirmé qu'elle avait été victime d'une attaque par ransomware et qu'elle avait proactivement mis hors ligne de nombreux systèmes afin de la contenir. L'attaque a perturbé les activités d'Ingram à l'échelle mondiale, paralysant ses systèmes de commande en ligne et de logistique pendant près d'une semaine. Le 10 juillet, le distributeur avait rétabli toutes ses activités commerciales, mais pas avant d'avoir eu un impact significatif sur les revendeurs et les partenaires qui dépendent des services de la chaîne d'approvisionnement d'Ingram. Les journalistes spécialisés dans la cybersécurité ont identifié un groupe de ransomware relativement nouveau, appelé SafePay, comme étant le responsable.

Contrairement à UNFI ci-dessus, Ingram Micro n'a pas de présence publique, mais la leçon à tirer ici est que si votre entreprise est essentielle au bon fonctionnement de nombreuses autres, une interruption (dans ce cas pendant plus d'une semaine) aura un impact considérable sur les autres et entraînera une pression accrue pour payer, ce que vous devez inclure dans votre évaluation des menaces.

JUILLET 2025 – ATTAQUES « TOOLSHELL » ZERO DAY CONTRE MICROSOFT SHAREPOINT

En juillet 2025, des chercheurs en sécurité ont mis en garde contre une vague continue de cyberattaques exploitant de nouvelles vulnérabilités zéro-day dans les serveurs Microsoft SharePoint sur site, collectivement baptisées « ToolShell ». Au 23 juillet, plus de 400 serveurs SharePoint dans le monde avaient été compromis via cette chaîne d'exploits. Nous avons publié un article de blog contenant plus de détails sur cette attaque ici. Les attaques ont permis un accès non autorisé et l'exécution de code sur les hôtes SharePoint, donnant ainsi aux attaquants un pied dans les réseaux d'entreprise des victimes. Diverses victimes ont été signalées, notamment des entreprises du secteur privé et au moins quelques agences gouvernementales américaines ; même le ministère américain de l'Énergie a confirmé avoir été « très peu affecté » par les violations de SharePoint. Les équipes de veille stratégique de Microsoft ont attribué cette activité à plusieurs groupes chinois soutenus par l'État (nommés Linen Typhoon, Violet Typhoon et Storm-2603) qui ont rapidement adopté ces exploits dès qu'ils ont été connus. Par ailleurs, des criminels liés à un nouveau ransomware appelé Warlock ont également utilisé ToolShell pour infiltrer des organisations et déployer des logiciels malveillants. Microsoft a publié des correctifs pour les failles SharePoint et, en collaboration avec des agences telles que la CISA, a exhorté toutes les organisations à effectuer immédiatement la mise à jour.

Il convient donc d'évaluer soigneusement si vous souhaitez continuer à utiliser des logiciels sur site (quel que soit le fournisseur), car ceux-ci ne sont souvent pas la priorité des fournisseurs, qui privilégient leurs offres SaaS. Si vous devez absolument les utiliser.

AOÛT 2025 – SALESLOFT+DRIFT

À la fin du mois d'août 2025, il est apparu clairement que Salesloft, une intégration pour Salesforce (et Slack / Pardot), **avait été compromise**, et Salesforce a désactivé l'intégration de Drift à ces systèmes. **L'attaque a en fait commencé en juin 2025**, avec le piratage du compte GitHub de Salesloft, suivi de l'accès à leur environnement AWS, où les auteurs de la menace ont obtenu des jetons OAuth pour accéder aux environnements des clients de Drift. Ce type d'attaque de la chaîne d'approvisionnement, où le piratage d'un seul fournisseur peut potentiellement donner aux attaquants l'accès à des centaines d'organisations victimes, est particulièrement dangereux. Les jetons OAuth sont extrêmement puissants, et une fois qu'ils sont en possession des criminels, seule leur révocation et celle de l'intégration elle-même peuvent vous protéger, et non l'authentification multifactorielle (MFA) ou la réinitialisation des identifiants (contrairement aux identifiants utilisateur compromis). **La liste des victimes est longue et comprend BeyondTrust, CloudFlare, CyberArk, Nutanix, Palo Alto Networks, Qualys, Rubrik, Tenable et Zscaler.**

La réponse à l'incident est difficile, car si vous êtes touché, vous devez déterminer à quelles données l'intégration avait accès, quelles informations d'identification supplémentaires pour d'autres systèmes pourraient être disponibles dans ces données (et ainsi de suite), puis réinitialiser toutes ces informations d'identification. **Il existe également un risque d'exposition ou d'amendes, selon le contenu des données qui ont été exfiltrées**.

La leçon à tirer ici est exactement celle que nous avons soulignée dans notre rapport de l'année dernière : les identités non humaines et **les intégrations via les API et OAuth dans le cloud et chez vos différents fournisseurs SaaS doivent faire l'objet d'une surveillance afin de détecter toute activité anormale**. Cela fait partie de la structure d'identité, n'est pas supervisé et est donc extrêmement attractif pour les pirates.

SEPTEMBRE 2025 - JAGUAR LAND ROVER

Le lundi 1er septembre 2025, la production de Jaguar Land Rover (JLR) s'est arrêtée dans ses usines du Royaume-Uni, de Slovaquie, du Brésil et d'Inde. Comme cette situation perdure et que seule une production limitée a repris au moment de la rédaction de cet article, quatre semaines plus tard, **cette attaque par ransomware a eu un impact considérable sur JLR et ses fournisseurs**. Les détails techniques ne sont pas encore disponibles, mais la plupart des systèmes informatiques de JLR étaient externalisés à Tata Consultancy Services (TCS), qui fait partie du groupe Tata, propriétaire de JLR depuis 2008.

De nombreuses industries manufacturières, y compris l'industrie automobile, s'orientent vers des chaînes d'approvisionnement entièrement automatisées, avec des pièces arrivant « juste à temps » et des processus de conception et de fabrication entièrement numériques. Cela peut bien sûr être très efficace, mais il est essentiel de **comprendre le réseau complexe d'interdépendances d'un système aussi vaste et de veiller à ce que la cybersécurité soit intégrée à chaque point faible**. Bien que JLR dispose d'énormes réserves de trésorerie (les estimations pour le seul mois de septembre prévoient **une dépense de 900 millions de livres sterling)**, le gouvernement britannique a garanti un prêt de **1,5 milliard de livres sterling** pour l'aider à faire face aux conséquences. L'impact financier global devrait s'élever à **1,9 milliard de livres sterling, avec plus de 5 000 organisations touchées par l'attaque**. JLR emploie **plus de 34 000 personnes**, **dont 120 000 dans sa chaîne d'approvisionnement**, et certains de ces fournisseurs devraient faire faillite. Il semble également que JLR n'ait pas souscrit d'assurance contre les cyberattaques et ait donc dû prendre en charge l'intégralité des coûts liés à cette catastrophe.

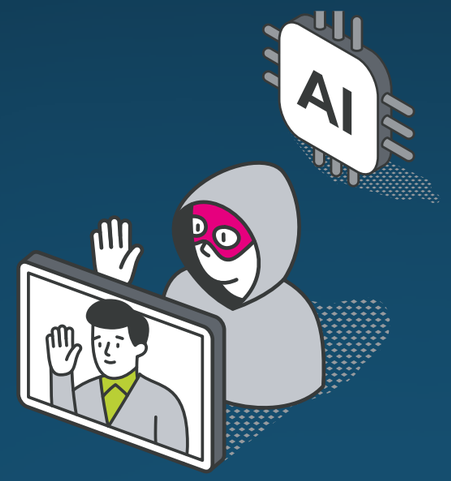
La leçon à tirer est claire : depuis une dizaine d'années, tous les secteurs d'activité réclament à grands cris une transformation numérique. Si celle-ci est importante pour toute entreprise, ne pas prendre les mesures appropriées pour atténuer les faiblesses en matière de cybersécurité dans chaque partie du système global comporte des risques énormes. **Assurez-vous également de disposer d'une assurance cybersécurité adaptée à votre profil de risque**. La dernière conclusion qui donne à réfléchir est qu'avec le plan de sauvetage du gouvernement, il est probable que les futures attaques cibleront les entreprises britanniques, **car elles sont plus susceptibles de payer.**

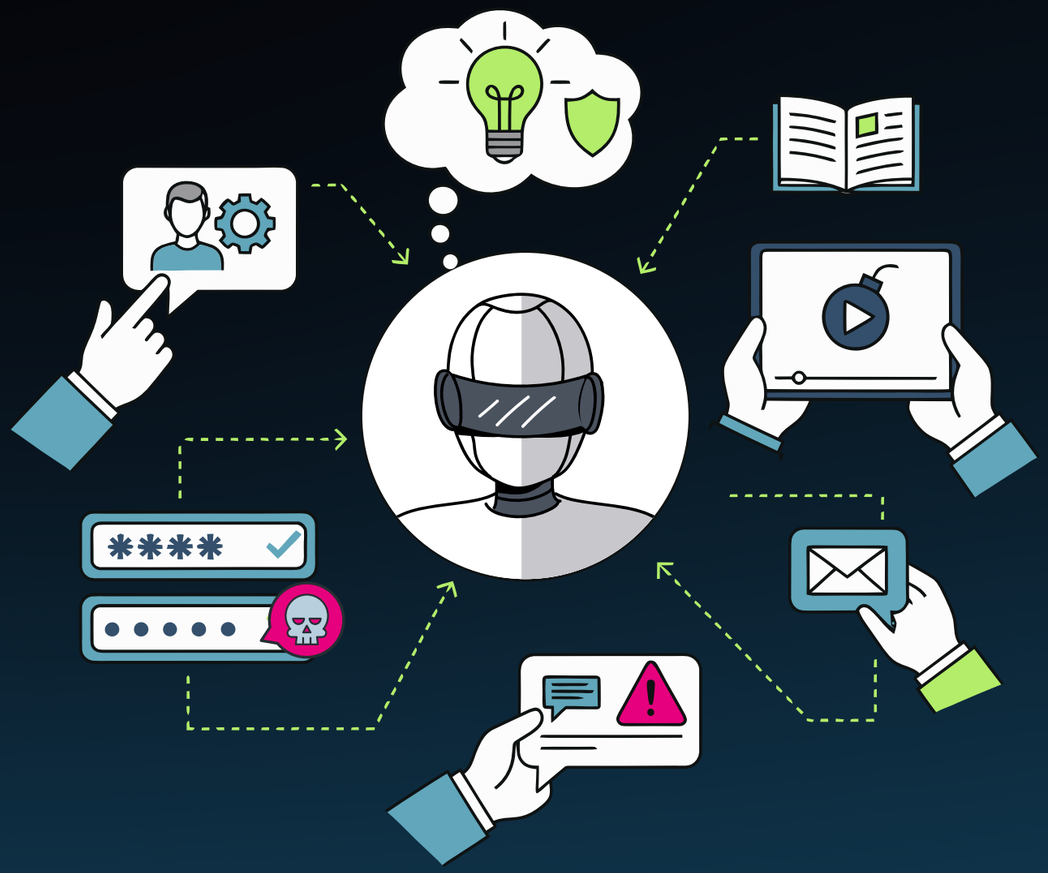
OCTOBRE 2025 – COMPROMISSION TOTALE DE F5

En octobre 2025, F5 Networks (un important fournisseur de contrôleurs de livraison d'applications et d'équipements de sécurité réseau) a révélé avoir été victime d'une **attaque très sophistiquée** menée par un acteur étatique. L'enquête qui a suivi a révélé que les attaquants avaient probablement obtenu un accès initial fin 2023 en exploitant un système F5 qui avait été laissé par erreur exposé en ligne, contournant ainsi les politiques de sécurité internes. Cette faille a permis aux pirates informatiques de **s'implanter et de maintenir un accès furtif à long terme au réseau interne de F5 pendant au moins 12 mois sans être détectés**. La faille n'a été découverte qu'en août 2025, après quoi F5 l'a rendue publique à la mi-octobre, soulignant de graves préoccupations en matière de sécurité de la chaîne d'approvisionnement, étant donné que les produits F5 sont **profondément intégrés dans l'infrastructure de nombreuses organisations**.

Une fois à l'intérieur, les intrus ont utilisé une porte dérobée malveillante personnalisée (baptisée « *BRICKSTORM* ») pour se déplacer latéralement dans l'environnement virtualisé de F5 tout en contournant les contrôles de sécurité. **BRICKSTORM, attribué à un groupe d'espionnage lié à la Chine connu sous le nom d'UNC5221, a permis aux attaquants de rester pratiquement invisibles**. À un moment donné, ils sont même restés inactifs pendant plus d'un an, probablement pour dépasser la période de conservation des journaux de F5 et effacer toute trace de la compromission initiale. Lorsqu'ils se sont réactivés, les pirates ont exfiltré des fichiers extrêmement sensibles, notamment des parties du code source propriétaire BIG-IP et des rapports internes sur des vulnérabilités non divulguées (zero-day) dans les produits F5. **Ces données volées ont permis aux pirates de découvrir des failles de sécurité qui n'avaient pas encore été corrigées ou rendues publiques, une mine d'informations que les experts ont comparée à une « clé passe-partout » pour de futures attaques potentielles contre les appareils F5 dans le monde entier**. Cet incident a mis en évidence à quel point une seule violation bien exécutée d'un fournisseur de technologies de base peut présenter des risques importants, car les plateformes de F5 sont utilisées pour protéger et équilibrer la charge des applications critiques sur les réseaux gouvernementaux et d'entreprise à l'échelle mondiale.

La leçon à tirer ici est dérangeante et fait écho à la violation de SolarWinds en 2020 : même le plus grand fournisseur de cybersécurité peut être compromis par un attaquant déterminé, et sans surveillance et journalisation adéquates, cela peut rester indétectable pendant très longtemps. Cette affaire est en cours et, bien que nous ne disposions pas encore de suffisamment de détails techniques pour prédire l'issue finale dans les mois à venir, si votre réseau repose sur des équipements F5, vous devez tout mettre à jour, y compris toutes les informations d'identification.





CHAPITRE 4

PRÉVISIONS CONCERNANT
LE PAYSAGE DES MENACES EN 2026

MENACES LIÉES À L'IA : QUAND L'INNOVATION DEVIENT EXPLOITATION

NOS PRÉVISIONS DE L'ANNÉE DERNIÈRE SE SONT-ELLES AVÉRÉES EXACTES ?

Dans le rapport de l'année dernière, nous avions fait quelques prévisions concernant l'avenir de la cybersécurité en 2025, et dans l'ensemble, nous avions vu juste. Sans surprise, nous avions évoqué le risque que représentent les modèles d'apprentissage automatique à grande échelle (LLM) basés sur l'IA générative (GenAI) entre les mains de pirates informatiques. Bien que nous ne puissions pas affirmer avec certitude qu'un e-mail de phishing ou une autre arnaque a été facilité par des pirates informatiques qui ont affiné leur leurre pour le rendre aussi attrayant que possible, OpenAI et Anthropic ont continué à publier des rapports sur des cas où ils ont repéré une utilisation malveillante de leurs outils (et ont par la suite bloqué ces comptes).

Parmi les utilisations novatrices, on peut citer l'utilisation de Claude Code pour automatiser la reconnaissance, la collecte d'identifiants et la pénétration des réseaux. Les données financières exfiltrées ont également été analysées par l'IA afin de déterminer le montant des rançons.

Les informaticiens nord-coréens constituent désormais une menace généralisée. **Ils ont utilisé Claude et ChatGPT pour créer de faux profils, automatiser la génération de CV, passer des évaluations techniques et de codage pendant le processus de recrutement, ainsi que pour livrer leur travail une fois embauchés**. Même si cette prédiction était facile à faire et que nous l'avons vue juste, il est intéressant de voir comment les attaquants expérimentent différentes utilisations de l'IA au cours des différentes phases de leurs attaques.

Nous avions également prédit l'utilisation de deepfakes plus convaincants pour le spear-phishing et les opérations d'influence (IO), ce qui s'est également confirmé au cours des 12 derniers mois. Les nouvelles versions des outils de création vidéo ont entraîné un déluge d'IA « *médiocre* » qui brouille la capacité des utilisateurs ordinaires à distinguer la réalité de la fiction, une réalité à laquelle les sociétés (et les entreprises) du monde entier sont déjà confrontées.

Le rapport de l'année dernière prévoyait également des affaires judiciaires liées à l'IA, et là encore, nous avons vu juste, avec notamment le recours collectif de 1,5 milliard de dollars contre Anthropic. En raison des changements politiques, les États-Unis ne sont pas susceptibles de freiner les pires excès des entreprises d'IA sur leur territoire, mais l'UE a adopté la loi sur l'IA.

La mise en place incessante de nouveaux cadres réglementaires et de mises à jour se poursuit dans la plupart des pays du monde. **Notre prédiction selon laquelle cela augmenterait la charge de travail et les défis pour les entreprises (et leurs fournisseurs) s'est également avérée exacte, avec la directive NIS2, qui prélève des fonds sur le budget consacré au recrutement et aux réserves d'urgence, tandis que la loi sur la résilience opérationnelle numérique (DORA) et la Prudential Regulation Authority (PRA) du Royaume-Uni coûtent plus d'un million d'euros aux entreprises en frais de mise en conformité**.

Notre analyse de l'écosystème des logiciels libres et open source (FOSS) s'est également révélée assez prémonitoire, avec des rapports réguliers faisant état de centaines ou de milliers de paquets malveillants signalés sur NuGet, PyPI, RubyGems et npm (**35 000 paquets malveillants dans npm en août 2025 occupant la première place**) au cours de l'année dernière. Cette tendance semble s'aggraver et si votre entreprise développe des logiciels en interne, vous devez suivre ces paquets malveillants avant qu'ils ne soient inclus dans vos applications. L'époque où les geeks du monde entier contribuaient volontairement au code des FOSS pour le bien de l'humanité tout entière touche peut-être à sa fin.

Notre dernière prédiction concernant l'adoption de langages sécurisés en mémoire (Rust / Swift) semble également se vérifier, **même si elle est plus lente à se concrétiser**. Rust apparaît dans les pilotes tiers Windows, dans le noyau du **système d'exploitation (où environ 70 % de tous les CVE proviennent de problèmes de sécurité de la mémoire)**, ainsi que dans Hyper-V, Azure et Microsoft 365. Linux intègre également Rust, tout comme Android, où cela a conduit à une réduction de **52 % des vulnérabilités de la mémoire au cours des six dernières années**.

Apple, quant à lui, suit une voie légèrement différente, car il contrôle l'ensemble du matériel et des logiciels grâce à son système Memory Integrity Enforcement, mais le résultat est le même : éviter les problèmes de mémoire exploitables.

Dans l'ensemble, toutes nos prévisions se sont réalisées, ce qui en dit plus long sur la prévisibilité des cybercriminels que sur notre capacité à prophétiser.

LES PRÉVISIONS DU SECURITY LAB POUR 2026

ADOPTION INCONTRÔLÉE DES OUTILS D'IA

À mesure que **les outils d'IA continuent de mûrir**, leur adoption par les organisations s'accélère, souvent plus rapidement que ne peuvent s'adapter les cadres de gouvernance ou de sécurité. Cette accélération est menée à la fois par des initiatives prises par la direction et par des expérimentations menées à la base par les employés, et de nouvelles solutions d'IA sont déployées quotidiennement dans certains cas. Le rythme de l'innovation a dépassé la capacité des équipes juridiques, informatiques et de sécurité à évaluer chaque mise en œuvre, laissant ainsi des lacunes critiques en matière de visibilité.

Une adoption incontrôlée élargit effectivement la surface d'attaque de l'organisation. De nombreux outils d'IA, en particulier ceux qui sont alimentés par des modèles linguistiques de grande taille (LLM), ne permettent pas la séparation entre le code et les données inhérente aux applications plus traditionnelles. Cela introduit de nouveaux vecteurs pour l'injection rapide, la fuite de données et la divulgation involontaire de données sensibles de l'entreprise. L'essor de l'IA agentique aggrave ce risque, car des actions autonomes peuvent se produire sans supervision humaine ni chaînes d'approbation établies.

Les récentes vulnérabilités telles que **Echoleak dans M365 Copilot (Aim Labs)** montrent bien la gravité de ces risques. Contrairement aux débordements de mémoire tampon ou aux injections de code, les exploits basés sur les LLM ne peuvent pas être facilement atténués. Même en suivant les meilleures pratiques recommandées dans le guide OWASP LLM01:2025 Prompt Injection, les organisations restent exposées à des risques résiduels en raison du comportement imprévisible des modèles d'IA. Des rapports tels que « Detecting and Countering Misuse of AI » (août 2025, Anthropic) confirment en outre que même les modèles de pointe restent vulnérables à la manipulation et aux abus.

MILITARISATION DE L'IA AGENTIQUE

Il n'est donc pas surprenant que les systèmes d'IA agentique (modèles autonomes capables d'exécuter des objectifs en plusieurs étapes) soient déjà militarisés. La frontière entre automatisation et orchestration est devenue floue. Les attaquants peuvent désormais créer des scripts, adapter et lancer des campagnes multivectorielles avec un minimum d'expertise, ce qui réduit les barrières à l'entrée. Ces modèles peuvent prendre en charge toutes les étapes du cycle de vie d'une attaque, de la reconnaissance à l'exploitation en passant par l'impact, en suivant le cadre MITRE ATT&CK de bout en bout.

Il n'est pas nécessaire de chercher très loin dans les résultats de recherche en ligne pour trouver des cas où l'IA agentique a commencé à avoir un impact sur les opérations des acteurs malveillants. Ces cas impliquent des techniques telles que la création d'appâts de phishing, le contournement des CAPTCHA ou l'usurpation d'identité humaine à l'aide de deepfakes vocaux et vidéo. Ces conclusions confirment ce que de nombreux défenseurs soupçonnent déjà : l'IA amplifie à la fois l'accessibilité et la vitesse de la cybercriminalité.

Malgré les promesses de sécurité des principaux fournisseurs, les abus persistent. Le rapport sur les menaces publié par Anthropic en août 2025 (mentionné ci-dessus) reconnaît que les modèles continuent d'être utilisés à des fins de reconnaissance et de génération de charges utiles, confirmant ainsi la crainte que les systèmes d'IA agentielle continuent de devancer les mesures de protection. Avec les LLM capables de « coder » de manière autonome des chaînes d'attaque entières, les obstacles à l'exploitation complexe ont pratiquement disparu.

RANSOMWARE 3.0 : BASÉ SUR LES LLM ET AXÉ SUR L'INTÉGRITÉ

Comme nous l'avons vu plus haut dans les résultats de **notre enquête sur les ransomwares en 2025**, les opérations de ransomware entrent dans une nouvelle phase d'évolution. Cette phase se caractérise par l'automatisation, l'autonomie et la corruption des données. En 2026, nous prévoyons l'émergence d'une orchestration pilotée par les LLM, dans laquelle de grands modèles linguistiques coordonneront la reconnaissance, la génération de charges utiles et l'évasion adaptative. Parallèlement, les attaquants passent du chiffrement ou de l'exfiltration à la manipulation de l'intégrité des données : ils modifient, corrompent ou falsifient subtilement les enregistrements afin de semer le doute sur la fiabilité des données elles-mêmes.

Historiquement, les ransomwares ont évolué en réponse à la résilience des défenseurs. Pensez aux attaques par cryptage seul (Ransomware 1.0) et à la double extorsion (Ransomware 2.0). Avec l'adoption généralisée des sauvegardes immuables et des cyberassurances, les attaques par cryptage direct ont un rendement décroissant. La prochaine étape logique pour les cybercriminels consiste à compromettre la confiance plutôt que l'accès. La manipulation des données dans les systèmes financiers, les dossiers médicaux ou les contrôles industriels entraîne un chaos prolongé, une exposition réglementaire et une atteinte à la réputation.

Des recherches universitaires ont déjà démontré la faisabilité de campagnes de ransomware orchestrées de manière autonome par l'IA. Une étude réalisée en 2025 par la NYU Tandon School of Engineering a montré que les LLM pouvaient exécuter de manière autonome des chaînes d'attaques complètes. Cela comprenait la reconnaissance, l'exfiltration, le chiffrement et l'adaptation, le tout sans intervention humaine. L'ajout de la corruption des données à ce processus est une évolution naturelle et dangereuse.

L'ATTAQUE DE TYPE « MAN-IN-THE-MIDDLE » RENDRA OBLIGATOIRE L'AUTHENTIFICATION MULTIFACTORIELLE (MFA) RÉSISTANTE AU PHISHING

Le passage à la MFA pour une authentification plus forte au cours de la dernière décennie a été une bonne chose, mais les attaquants ont évolué parallèlement à nos défenses. Les attaquants utilisent des kits de phishing, notamment l'open source **Evilginx**, pour créer de fausses pages de connexion, imitant celles de Microsoft, Google ou Okta, puis incitent les utilisateurs, via des e-mails de **phishing** ou **des messages Teams**, à cliquer sur un lien vers ces pages. Les utilisateurs se connectent à la fausse page, et leur nom d'utilisateur, leur mot de passe et leurs invites MFA sont transmis à la page de connexion légitime en arrière-plan, tandis que le pirate vole le jeton résultant et peut alors accéder à tout ce dont dispose l'utilisateur, ce que l'on appelle l'attaque de l'homme du milieu (AiTM).

La possibilité de gérer l'invite MFA est désormais une « fonctionnalité standard » de ces kits de phishing. La seule bonne défense consiste à utiliser des technologies MFA résistantes au phishing, telles que les clés matérielles FIDO2, Windows Hello for Business, l'authentification basée sur un certificat (CBA) et les clés d'accès, car celles-ci sont liées à la page de connexion légitime et ne fonctionnent pas sur la page factice, même si l'utilisateur a été piégé. Cependant, non seulement vous devez déployer une authentification multifactorielle résistante au phishing, mais vous devez également l'imposer comme seule méthode de connexion, car la plupart des kits de phishing forcent désormais le passage d'une méthode d'authentification multifactorielle plus forte à **une méthode moins sécurisée**.

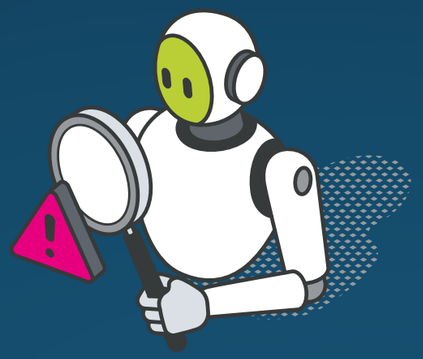
L'ADOPTION DES CLÉS D'ACCÈS SERA RALENTIE PAR DES EXPÉRIENCES UTILISATEUR DÉROUTANTES

Si les clés matérielles FIDO constituent une excellente option pour une authentification multifactorielle résistante au phishing, elles représentent un coût supplémentaire à prendre en compte dans le budget de chaque utilisateur. Les clés d'accès, qui utilisent à la place la puce de sécurité de votre smartphone moderne, constituent une alternative. Nous avions prévu que leur adoption s'accélérerait cette année, ce qui a été le cas, mais pas dans la mesure où nous l'avions prévu. La raison principale en est une expérience utilisateur fragmentée, qui diffère selon qu'il s'agit d'un iPhone, d'un téléphone Android ou d'un ordinateur portable Windows/MacOS. De plus, il existe deux types de clés : celles destinées aux consommateurs sont « synchronisables », ce qui signifie qu'elles sont stockées dans votre compte Apple ou Google afin que vous puissiez les utiliser sur différents appareils. Le stockage des identifiants d'entreprise dans les comptes cloud personnels des utilisateurs finaux n'est pas acceptable pour la plupart des entreprises, qui imposent donc généralement des clés d'accès non synchronisables. Celles-ci sont verrouillées sur le smartphone où elles ont été créées et, dans le cas de Microsoft 365, la seule application acceptée est Microsoft Authenticator. À cela s'ajoute une expérience déroutante où vous vous connectez à un service sur votre ordinateur portable, puis devez scanner un code QR avec votre téléphone, avant de terminer la procédure de connexion sur votre téléphone.

Les clés d'accès sont l'avenir de l'authentification multifactorielle résistante au phishing, mais les géants de la technologie doivent se réunir et harmoniser l'expérience globale pour les utilisateurs grand public et professionnels.

LES PROCESSUS DE VÉRIFICATION ET DE RÉINITIALISATION D'IDENTITÉ CONTINUERONT DE COMPROMETTRE LES ORGANISATIONS

Plusieurs des violations très importantes que nous avons observées récemment étaient dues au fait que le personnel du service d'assistance (souvent externalisé) avait été trompé et avait réinitialisé des comptes d'utilisateurs administratifs. N'oubliez pas que la force de votre authentification ne se mesure pas à la technologie que vous utilisez lorsque tout fonctionne normalement, mais à la difficulté de contourner vos processus d'inscription et de récupération. Comment vous assurez-vous que les nouvelles recrues sont bien les personnes que vous attendez (et non des infiltrés nord-coréens) dans le monde actuel du télétravail ? Quel est votre processus de récupération des comptes pour les utilisateurs qui ont perdu leur téléphone, leur clé FIDO, oublié leur mot de passe ou dont l'ordinateur portable vient de tomber en panne ? Disposez-vous d'un processus plus sécurisé pour les comptes à privilèges élevés ? (Y compris l'obligation d'une validation en personne dans les locaux de l'entreprise). L'identité est le nouveau pare-feu, mais vous devez envisager de manière holistique l'atténuation des risques dans l'ensemble de votre flux de travail lié à l'identité, depuis l'offre d'emploi jusqu'au dernier jour de travail.



LES APPLICATIONS SAAS CONSTITUENT LA NOUVELLE SURFACE D'ATTAQUE

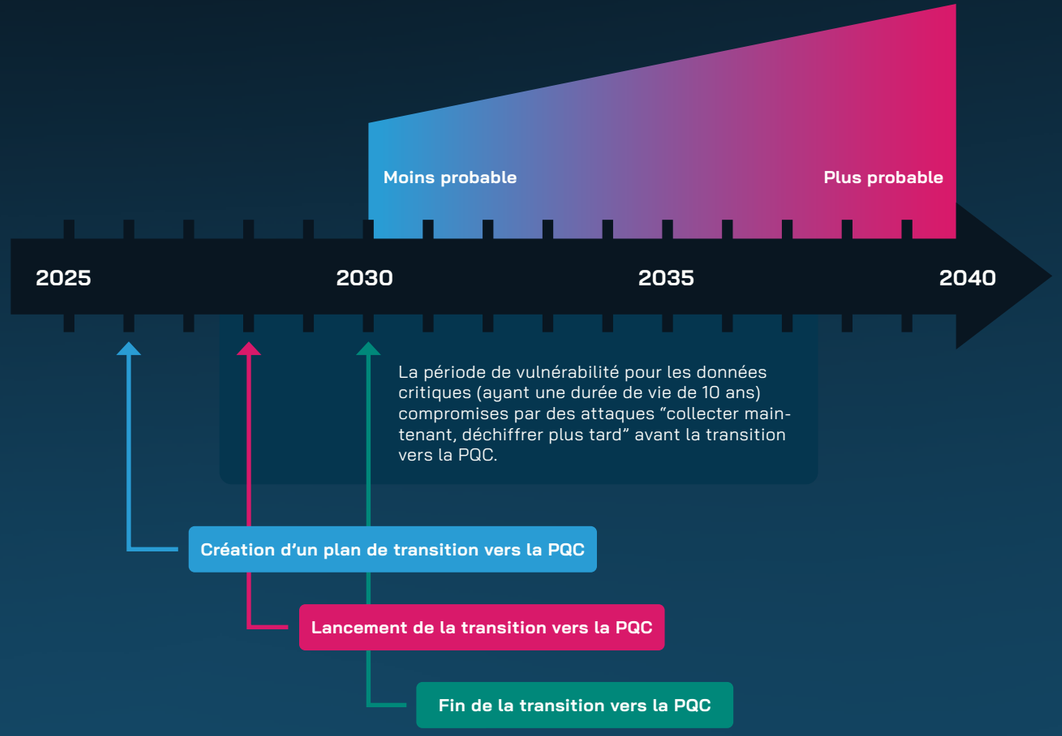
Certaines compromissions d'entreprises au cours des dernières années sont intéressantes, car elles contournent complètement le schéma traditionnel « compromettre un utilisateur normal, pivoter dans le réseau interne, compromettre les comptes administrateur ». À mesure que les entreprises dépendent de plus en plus des services SaaS, de nouveaux types d'attaques qui compromettent uniquement les données et les identités dans le cloud deviennent plus courants. Les défenses normales telles que l'EDR sont pour la plupart aveugles à ces attaques, car bien qu'elles se produisent dans le navigateur, il n'y a pas de fichiers ou d'activités malveillants que la protection des terminaux puisse détecter. En fait, une grande partie de l'informatique moderne des entreprises se fait désormais dans un navigateur, qui est opaque à l'EDR, c'est pourquoi nous recommandons vivement d'utiliser un navigateur d'entreprise et/ou un logiciel spécialisé pour la protection dans le navigateur. Mitre dispose même d'une MATRICE ATT&CK pour les différentes attaques SaaS.

LES EXTENSIONS DE NAVIGATEUR COMPROMETTRONT DAVANTAGE D'ENTREPRISES AU COURS DE L'ANNÉE À VENIR

Les navigateurs modernes sont des applications complexes, presque comme des systèmes d'exploitation à part entière, et dotés de protections qui nous protègent en grande partie des dangers d'Internet, tant dans notre vie personnelle que professionnelle. Mais la plupart d'entre nous utilisons également des extensions de navigateur, souvent pour des raisons de productivité ou de commodité, mais celles-ci comportent parfois des risques cachés.

Dans certains cas, elles sont vulnérables d'une manière ou d'une autre, ce qui dégrade la protection du navigateur lui-même, dans d'autres cas, elles sont intentionnellement malveillantes. Cela peut se traduire par un nom similaire à celui d'un complément populaire, ou par l'achat par des criminels d'une extension auparavant inoffensive, qu'ils transforment ensuite en arme. Assurez-vous que votre entreprise dispose d'un moyen de suivre les extensions installées dans les navigateurs de vos utilisateurs, de bloquer facilement celles qui s'avèrent malveillantes (Intune ou AD GPOs peuvent le faire) et d'informer vos utilisateurs des risques.

Probabilité estimée d'atteindre le CRQC



HORNETSECURITY

PRÉVISIONS CONCERNANT L'INFORMATIQUE QUANTIQUE

La plupart des menaces que nous examinons dans ce rapport sont actuelles, tandis que l'avènement d'un ordinateur quantique pertinent sur le plan cryptographique (**CRQC**) n'est pas prévu avant plusieurs années. Ce jour, connu sous le nom de Q-Day, correspond au moment où ces types d'ordinateurs auront une taille suffisante (nombre de qubits, l'équivalent des bits dans un ordinateur classique) et un coût suffisamment bas pour pouvoir utiliser **l'algorithme de Shor** afin de briser les cryptages asymétriques tels que RSA et Diffie-Hellman. Ou **l'algorithme de Grover** pour réduire de moitié la puissance de la cryptographie symétrique (AES-128 devient AES-64).

De nombreuses entreprises technologiques, dont les habituelles (Google, IBM, Microsoft), investissent des millions dans différents types d'ordinateurs quantiques afin de déterminer quelle approche technologique permettra d'obtenir des qubits suffisamment stables. Le problème réside dans le bruit : si vous disposez de nombreux qubits, mais que vous en utilisez la plupart pour la correction d'erreurs, le nombre total de qubits logiques disponibles pour effectuer vos calculs est réduit au minimum. Les ordinateurs quantiques ne remplaceront pas nos ordinateurs actuels, mais seront utilisés pour des types de calculs très spécifiques, notamment pour déchiffrer nos algorithmes de cryptage actuels.

Même si les CRCQ ne seront pas disponibles avant 5 à 15 ans, vous ne pouvez pas attendre leur arrivée. Votre organisation doit commencer à planifier dès maintenant. Si vous stockez des informations personnelles identifiables (PII) ou des informations médicales personnelles (PHI) et que vous avez l'intention (ou que vous êtes obligé par la réglementation) de les conserver pendant plus de cinq ans, vous devez commencer dès maintenant à utiliser des algorithmes résistants à la cryptographie quantique pour le chiffrement. En effet, plusieurs agences à travers le monde utilisent la méthode « Harvest Now, Decrypt Later » (HDNL) pour stocker des données qu'elles ne peuvent pas déchiffrer aujourd'hui, mais qu'elles pourront déchiffrer avec les CRCQ. De plus, il s'agit d'un projet de grande envergure : vous devez identifier tous les systèmes, appareils et éléments de votre réseau qui utilisent le chiffrement, déterminer quel algorithme est utilisé et quel type de données est stocké ou transmis.

Dans certains cas, il sera facile d'ajouter des algorithmes résistants aux attaques quantiques, tandis que dans d'autres, vous devrez remplacer entièrement le système ou repenser l'architecture de vos processus.

Le NIST a normalisé trois algorithmes résistants aux attaques quantiques :

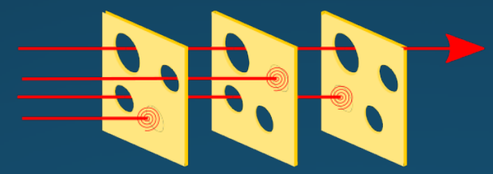
- La norme FIPS 203 définit un schéma cryptographique appelé « Module-Lattice-Based Key-Encapsulation Mechanism » (ML-KEM), dérivé de la proposition CRYSTALS-KYBER.
- La norme FIPS 204 est l'algorithme de signature numérique basé sur un module-réseau (ML-DSA), basé sur la proposition CRYSTAL-Dilithium.
- La norme FIPS 205 spécifie l'algorithme de signature numérique sans état basé sur un hachage (SLH-DSA), dérivé de la proposition SPHINCS+.

Ils s'appuient sur la sécurité de la couche transport (TLS) version 1.3, alors commencez par la déployer partout où vous le pouvez dans votre environnement.

En ce qui concerne les systèmes d'exploitation, les versions préliminaires de Windows 11 et Windows Server ont mis à jour SymCrypt, la même bibliothèque que celle utilisée dans Azure et Microsoft 365. ML-KEM et ML-DSA sont déjà disponibles dans SymCrypt, à la fois sur Windows et Linux. **SymCrypt-OpenSSL** offre également la même prise en charge pour OpenSSL. Apple inclut également le **PQC dans son CryptoKit** pour les développeurs, et iMessage dans iOS et TLS 1.3 dans iOS26 intègrent déjà le PQC. Si vous écrivez vos propres applications en interne, visez l'agilité cryptographique afin de pouvoir remplacer des suites de chiffrement ou des algorithmes entiers à mesure que les mises à jour sont livrées.

RISKS FOR ORGANIZATIONS IN 2026

La cybersécurité n'est pas un problème technologique, c'est un problème lié aux personnes et aux processus. Comme cela arrive souvent lorsque l'on est plongé dans les dernières technologies et que l'on assiste à des développements rapides dans le domaine de l'IA générique, de l'apprentissage automatique ou de l'IA agentique, les solutions que l'on envisage sont basées sur la technologie (« quand on n'a qu'un marteau, tous les problèmes ressemblent à des clous »). Mais les organisations sont rarement victimes de violations dues uniquement à des défaillances technologiques, il s'agit plutôt d'une combinaison de défaillances humaines, procédurales et technologiques. Le modèle du **fromage suisse** illustre clairement ce principe :



En d'autres termes, si vous intégrez la cyber-résilience dans votre organisation, grâce à des couches de protection et des processus, vous aurez plus de chances d'éviter une violation dévastatrice.

Quelle que soit la taille de votre entreprise, vous serez la cible d'attaques de cybersécurité en 2026. Comme vous pouvez le constater dans nos données, le fait d'être une petite organisation, une organisation à but non lucratif ou de « ne rien avoir qui vaille la peine d'être attaqué » ne constitue pas une protection contre les criminels. Si votre entreprise détient des données sensibles et des réserves de liquidités, vous êtes une cible. Mettez en place un programme de cyber-résilience basé sur les principes du Zero Trust :

- **Disposez-vous de réseaux isolés et n'attribuez-vous que les autorisations nécessaires afin de minimiser l'impact d'une attaque ?** Disposez-vous du personnel et des processus nécessaires pour réagir aux alertes et expulser rapidement les attaquants avant qu'ils ne causent des dommages importants ?
- **Privilège minimal :** c'est sans doute la chose la plus difficile à mettre en place. Ne donnez aux employés que **les autorisations dont ils ont besoin pour faire leur travail et revoyez-les régulièrement** afin qu'elles ne s'accumulent pas au fil du temps.
- **Vérifiez chaque connexion :** mettez en place un moteur de politiques solide (accès conditionnel dans Entra ID) qui vérifie chaque connexion et chaque accès aux applications, fichiers et autres ressources afin de garantir que l'accès n'est pas autorisé par défaut, mais uniquement lorsque les conditions requises sont remplies.

Avant d'investir dans des outils de sécurité avancés qui résolvent des problèmes spécifiques, commencez par vous occuper des bases de la sécurité en vous basant sur les principes ci-dessus :

- **Mettez en place l'authentification multifactorielle (MFA) pour tout le monde**. Compte tenu de l'augmentation considérable du nombre de kits AiTM (Attacker-in-The-Middle) intégrant un contournement de l'authentification multifactorielle, vous devez passer à une authentification multifactorielle résistante au phishing. Cela inclut les clés OAuth matérielles, Windows Hello for Business, l'authentification basée sur des certificats et les clés d'accès, qui ne permettent pas l'authentification sur de fausses pages de connexion, même si l'utilisateur lui-même a été trompé.
- **Disposez d'une solution de protection des terminaux robuste** sur tous les appareils où cela est possible, et intégrez-la à une solution d'identité, d'applications cloud et d'hygiène des e-mails pour une détection et une réponse étendues (XDR) complètes.
- **Formez vos utilisateurs à repérer les tentatives d'hameçonnage**, que ce soit dans les e-mails, Teams, Zoom ou WhatsApp, mais surtout, instaurez une culture de la sécurité. Partir du principe que le service informatique ou l'équipe de sécurité s'occupe de toute la cybersécurité et que les autres membres de l'entreprise n'ont donc pas à s'en soucier revient à dire que « seul le personnel chargé de la santé et de la sécurité au travail doit se préoccuper des accidents ». Non, tout le monde doit signaler tout ce qui lui semble dangereux, qu'il s'agisse d'une chaise branlante sur laquelle quelqu'un s'équilibre pour remplacer une ampoule ou d'une personne sur le point de cliquer sur un lien qu'elle ne devrait pas.
- **Mettez à jour vos logiciels**, mais à moins que vous ne souhaitiez doubler la taille de votre service informatique, faites-le de manière intelligente. Appliquez les principes de la gestion continue de l'exposition aux menaces (CTEM) pour protéger en priorité les systèmes critiques de votre entreprise qui présentent des vulnérabilités exploitables, plutôt que d'essayer de tout mettre à jour partout, ce qui est impossible.
- **Examinez votre chaîne d'approvisionnement**. Plusieurs violations importantes au cours des derniers mois ont été causées par des organisations d'assistance externalisées victimes d'ingénierie sociale (piratage des personnes plutôt que des systèmes informatiques). Comprenez tous vos processus externalisés, en gardant à l'esprit que vous pouvez externaliser une fonction, mais pas le risque qui y est associé. Et examinez toutes les chaînes d'approvisionnement qui permettent à votre entreprise de fonctionner, et renforcez votre résilience en cas de perturbation, que ce soit à cause d'attaques de cybersécurité ou pour d'autres raisons.

UNE ORGANISATION CYBER-RÉSILIENTE

La cybersécurité étant un problème lié aux personnes et aux processus, la solution ne réside pas dans davantage de technologie, mais dans un changement de culture au sein de votre entreprise.

Nous pouvons tirer de nombreux enseignements de l'industrie aéronautique, où chaque incident et accident fait l'objet d'une enquête approfondie, non pas pour attribuer des responsabilités, mais pour identifier tous les facteurs humains, technologiques et liés aux processus qui y ont contribué. Ces enseignements sont ensuite intégrés à des formations supplémentaires ou différentes, et les processus et technologies sont modifiés afin d'éviter que cela ne se reproduise.

Cela commence par la promotion d'une culture de la sécurité dans laquelle chacun se sent libre de s'exprimer lorsqu'il constate un problème. Cela n'est possible que si les personnes ne sont pas blâmées individuellement lorsqu'un incident se produit. Il s'agit d'améliorer les processus afin que les personnes soient moins susceptibles de commettre ces erreurs. En retour, cela signifie que la cybersécurité est la responsabilité de tous, et pas seulement du service informatique ou de sécurité, car différentes parties de l'entreprise prennent des décisions technologiques qui entraînent des risques que tout le monde, et pas seulement le service informatique, doit gérer. Nous, les professionnels de la cybersécurité, devons également améliorer notre communication avec les autres parties prenantes, en traduisant le « jargon technique » en langage commercial.
À mesure que vous renforcez la résilience de chaque partie de votre entreprise, restez à l'affût des changements dans le paysage des menaces, car les pirates informatiques ne cessent d'innover pour trouver des failles à exploiter dans nos systèmes.

UNE STRATÉGIE DE SÉCURITÉ HOLISTIQUE

Nous l'avons déjà mentionné, mais cela mérite d'être répété : commencez par les bases. Les processus et technologies fondamentaux en matière de cybersécurité seront bien plus efficaces pour défendre votre organisation que les dernières solutions ponctuelles en matière de cybersécurité. Vous avez besoin de plusieurs niveaux de protection (rappelez-vous le modèle du fromage suisse) :

Détection de spam/malware de nouvelle génération avec ATP pour l'analyse comportementale afin de vous protéger contre le flot continu de menaces par e-mail que nous observons dans ce secteur.

Formation de sensibilisation à la sécurité des utilisateurs finaux afin de leur apprendre à repérer les attaques d'ingénierie sociale et les attaques de spear-phishing.

Capacités de sauvegarde et de restauration pour **les données sur site** ET les données stockées dans des services cloud tels que M365 à des fins de restauration en cas d'attaque par ransomware.

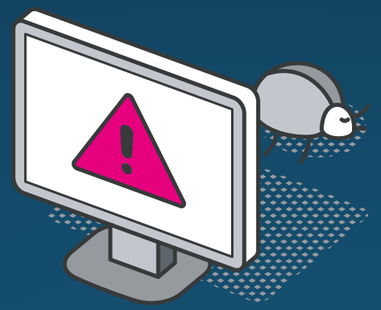
Fonctionnalités de conformité et de gouvernance qui contribuent à protéger contre les fuites accidentelles de données et à garantir le respect des contrôles de conformité.

Contrôle des privilèges et du partage pour vos données d'entreprise sensibles stockées dans SharePoint et OneDrive for Business.

Assistant cybernétique alimenté par l'IA pour la protection des e-mails et des équipes, aidant chaque utilisateur à rester en sécurité.

EN SAVOIR PLUS
La cybersécurité n'est qu'un des nombreux défis auxquels les entreprises sont confrontées aujourd'hui, mais ne pas lui accorder suffisamment d'importance peut avoir des conséquences catastrophiques (il suffit de demander à Jaguar Land Rover).

Tout comme de nombreuses entreprises externalisent certaines parties de leurs activités à des spécialistes dans ce domaine, profitez des connaissances approfondies et des compétences que Hornetsecurity a développées depuis 2007. **Collaborez avec nous pour assurer la sécurité de votre entreprise**.



365 TOTAL PROTECTION

AI-POWERED, ALL IN ONE M365 SECURITY, BACKUP & GRC

PLAN 1
- SPAM & MALWARE PROTECTION
- EMAIL ENCRYPTION
- EMAIL SIGNATURES & DISCLAMER

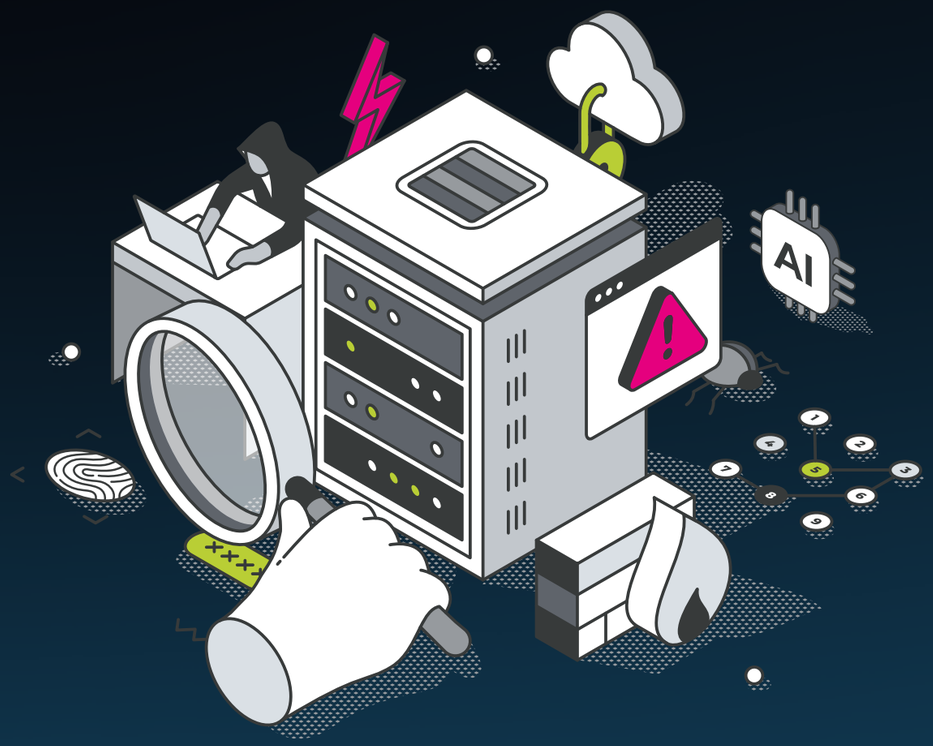
PLAN 2
INCLUDES 1
- ADVANCED THREAT PROTECTION
- EMAIL ARCHIVING
- EMAIL CONTINUITY

PLAN 3
INCLUDES 1 + 2
- AUTOMATIC BACKUP O M365 DATA
- GRANULAR RECOVERY WITH END USER SELF SERVICE
- UNLIMITED STORAGE IN ONE ALL-INCLUSIVE FEE

PLAN 4
INCLUDES 1 + 2 + 3
- SECURITY AWARENESS
- PERMISSION MANAGEMENT
- DMARC REPORTING & MANAGEMENT

POWERED BY AI CYBER ASSISTANT
- AI RECIPIENT VALIDATION
- TEAMS PROTECTION
- AI EMAIL SECURITY ANALYST

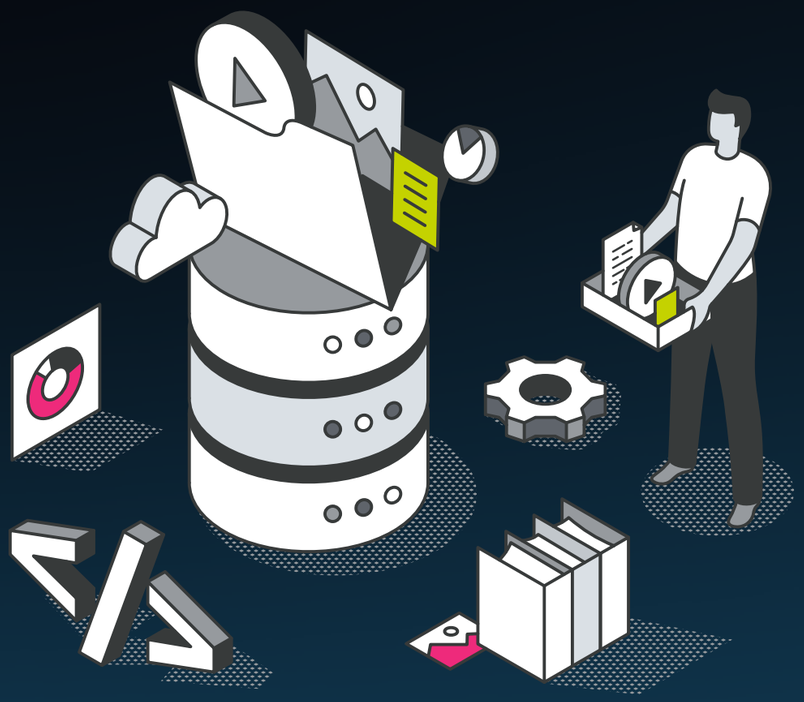
COMMENCEZ VOTRE ESSAI GRATUIT



CHAPITRE 5

RESSOURCEN

- https://www.hornetsecurity.com/fr/blog/ransomware-impact-report-2025-communique-de-presse/
- https://www.hornetsecurity.com/fr/blog/rssi-perspective/
- https://www.hornetsecurity.com/fr/blog/sharepoint-vulnerabilite/
- https://www.esteval.fr/article.41854.tribune-les-utilisations-malveillante-de-l-ia-comment-les-fournisseurs-d-ia-et-les-gouvernements
- https://www.abondance.com/20251016-1549012-anthropic-bloque-des-tentatives-de-piratage-visant-a-detourner-claude-ai-pour-le-cybercrime.html
- https://openai.com/fr-FR/global-affairs/disrupting-malicious-uses-of-ai-october-2025/
- https://actualitte.com/article/126414/legislation/ia-et-droits-d-auteur-feu-vert-pour-un-accord-historique-de-1-5-milliard
- https://www.europarl.europa.eu/topics/fr/article/20230601STO93804/loi-sur-l-ia-de-l-ue-premiere-reglementation-de-l-intelligence-artificielle
- https://www.hornetsecurity.com/fr/blog/directive-nis2/
- https://silexo.fr/article/148/nis2-et-dora-quelles-differences-quels-enjeux-quelles-obligations
- https://ossf.github.io/malicious-packages/stats/
- https://cpp.developpez.com/actu/376035/Le-projet-Safe-Cplusplus-visant-a-doter-le-langage-d-un-modele-de-securite-inspire-de-Rust-est-mis-de-cote-pour-donner-la-priorite-aux-Profils-une-alternative-controversee-proposee-par-le-createur-du-langage/
- https://www.youtube.com/watch?v=uDtMuS7BExE
- https://help.apple.com/pdf/security/fr_CA/apple-platform-security-guide-c.pdf
- https://secutec.com/fr/news/echoleak-first-zero-click-ai-attack-microsoft-365-copilot
- https://www.abondance.com/20251016-1549012-anthropic-bloque-des-tentatives-de-piratage-visant-a-detourner-claude-ai-pour-le-cybercrime.html?
- https://www.hornetsecurity.com/fr/ransomware-report/
- https://github.com/kgretzky/evilginx2
- https://www.proofpoint.com/us/blog/threat-insight/dont-phish-let-me-down-fido-authentication-downgrade
- https://www.riskinsight-wavestone.com/2025/03/ordinateur-quantique-et-cryptographie-post-quantique-quelle-strategie-adopter/
- https://fr.wikipedia.org/wiki/Algorithme_de_Shor
- https://fr.wikipedia.org/wiki/Algorithme_de_Grover
- https://github.com/microsoft/SymCrypt-OpenSSL
- https://developer.apple.com/videos/play/wwdc2025/314/
- https://fr.wikipedia.org/wiki/Mod%C3%A8le_du_fromage_suisse
- https://www.hornetsecurity.com/fr/blog/eviter-les-violations-de-conformite/
- https://www.hornetsecurity.com/fr/blog/attaques-contre-la-chaine-dapprovisionnement/
- https://www.hornetsecurity.com/fr/services/advanced-threat-protection/
- https://www.hornetsecurity.com/fr/services/security-awareness-service/
- https://www.hornetsecurity.com/fr/services/365-total-backup/
- https://www.hornetsecurity.com/fr/services/vm-backup/
- https://www.hornetsecurity.com/fr/services/365-total-protection/
- https://www.hornetsecurity.com/fr/services/365-permission-manager/
- https://www.hornetsecurity.com/fr/services/ai-cyber-assistant/
- https://www.hornetsecurity.com/fr/



À PROPOS DES AUTEURS

RÉDIGÉPAR

ANDY SYREWICZE

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

Andy est titulaire du prix Microsoft MVP dans le domaine de la Sécurité.

PAUL SCHNACKENBURG

Paul Schnackenburg a débuté dans l'informatique à l'époque où le DOS et les processeurs 286 étaient à la pointe de la technologie. Il dirige Expert IT Solutions, un MSP situé sur la Sunshine Coast en Australie.

Paul est un auteur technologique très respecté et actif au sein de la communauté. Il rédige des articles techniques approfondis, axés sur la cybersécurité, Microsoft 365 et les services cloud associés.

Il est titulaire des certifications MCSE, MCSA et MCT.