Entreprises connectées : la dépendance au numérique accroît les risques

QBE

Introduction

Dans le monde entier, particuliers et entreprises s'appuient de plus en plus sur les technologies numériques. Usines, véhicules et autres appareils intelligents sont reliés à Internet, tandis que les entreprises utilisent le digital et l'intelligence artificielle (IA) pour automatiser des tâches aussi simples que complexes.

Le marché technologique mondial va croître de façon exponentielle au cours des cinq prochaines années. Le marché de l'IA en tant que service devrait presque décupler, passant d'environ 200 milliards de dollars à 1 850 milliards de dollars ; celui du logiciel en tant que service devrait tripler pour atteindre les 850 milliards de dollars et celui de l'infrastructure en tant que service devrait quintupler pour atteindre les 532 milliards de dollars. Les technologies numériques émergentes offrent donc de formidables opportunités.

Mais parallèlement, des cybercriminels volent des données sensibles pour extorquer ou escroquer des entreprises de toutes tailles dans tous les secteurs, tandis que d'autres acteurs malveillants utilisent la technologie pour déstabiliser leurs adversaires ou promouvoir leurs idéologies.

Perturbation technologique mondiale

La panne générale des systèmes exécutant le capteur Falcon de CrowdStrike le 19 juillet a mis en lumière l'interdépendance et la vulnérabilité des systèmes technologiques mondiaux. Sans compter Microsoft, la panne a coûté aux sociétés du Fortune 500 (les entreprises américaines ayant les 500 plus gros chiffres d'affaires) environ 5,4 milliards de dollars en dommages et 25 milliards de dollars en valeur boursière.

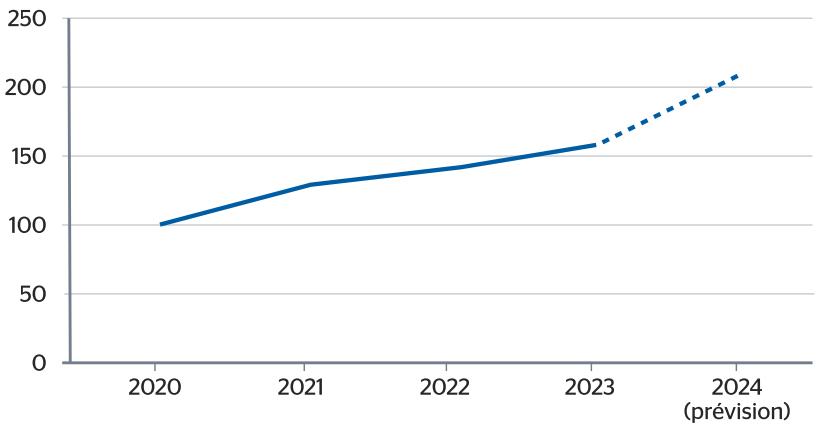
La mise à jour ratée de CrowdStrike a mis hors service environ 8,5 millions d'ordinateurs utilisant Windows. Cela représentait moins de 1 % du parc Windows, mais les perturbations ont touché le monde entier, surtout les secteurs de la santé et des transports, notamment aériens. Des cybercriminels ont profité de l'occasion pour lancer des campagnes de phishing, cherchant à compromettre des systèmes, à voler des données et à extorquer de l'argent. Dans le cas de CrowdStrike, une erreur était à l'origine des perturbations, mais l'intention de nuire motive de nombreuses attaques cybernétiques.

En juin 2017, des hackeurs ont ciblé des institutions ukrainiennes avec le logiciel malveillant NotPetya et cette cyberattaque massive s'est propagée à toute l'Europe, l'Amérique du Nord et l'Asie-Pacifique. NotPetya a touché des secteurs critiques tels que les transports et la logistique, causant des dommages estimés à 10 milliards de dollars. Bien qu'elle ait touché beaucoup moins d'appareils que l'incident CrowdStrike, l'attaque a causé beaucoup plus de perturbations du fait de sa nature intentionnelle.

A mesure que les interdépendances technologiques se renforcent, il devient davantage probable qu'une seule attaque perturbe beaucoup d'entreprises à la fois. Autrement dit, les entreprises risquent davantage de subir un incident cybernétique. Il se peut aussi que des acteurs malveillants décident de cibler des entreprises spécifiques pour causer des dommages plus importants, que ce soit pour réclamer des rançons ou pour déstabiliser des adversaires géopolitiques.

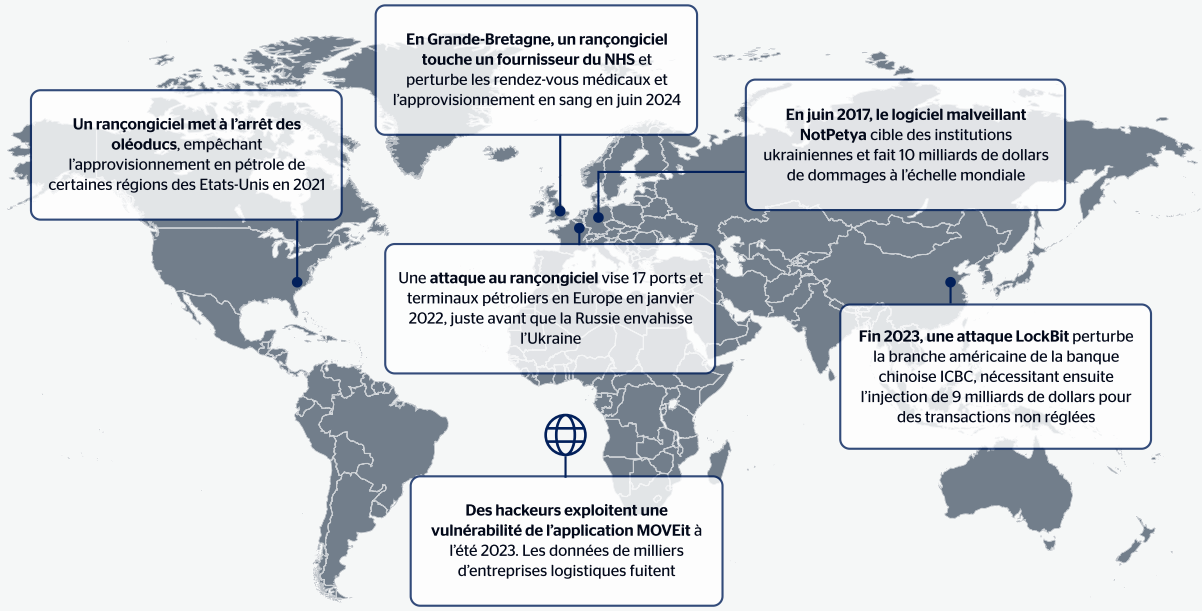
> Avec la panne CrowdStrike, les grandes sociétés américaines ont perdu 25 milliards de dollars en valeur boursière

Nombre de cyberattaques ayant causé des dommages et des perturbations



Source : ©Control Risks

Perturbations majeures liées à des cyberattaques



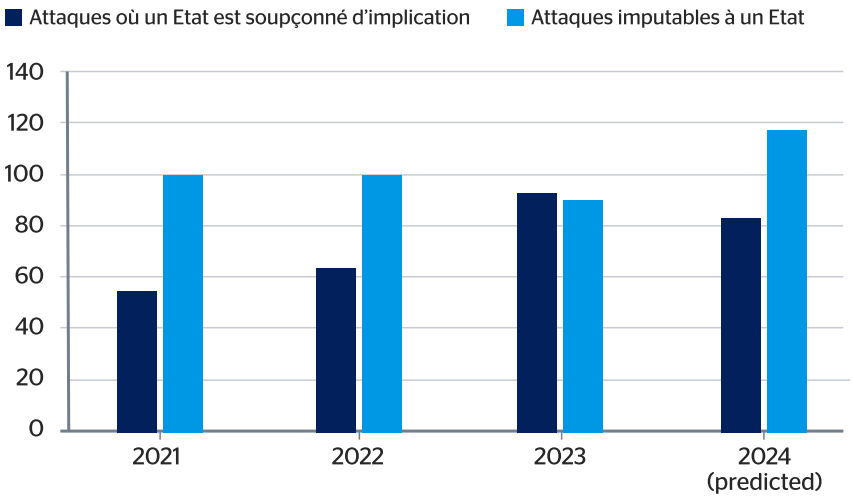
Attaques à effet boule de neige

Tandis que les tensions géopolitiques grandissent, le monde devient davantage multipolaire. Les cyberacteurs parrainés par des États sont de plus en plus déterminés à perturber les infrastructures critiques, par exemple par le biais de ransomwares. Ces attaques peuvent être motivées par des événements géopolitiques comme les conflits au Proche-Orient ou en Ukraine. Commanditées par des États et exécutées par des cybercriminels ou des activistes, elles peuvent cibler des secteurs stratégiques en dehors du théâtre des opérations. Les entreprises de l'énergie sont des cibles privilégiées pour les cyberattaques à effet boule de neige, qui peuvent déstabiliser les marchés financiers et les gouvernements.

Les entreprises de l'énergie sont des cibles privilégiées pour les attaques à effet boule de neige

Certains États ont mobilisé des ressources pour fabriquer des personnages fictifs de cyberactivistes à qui imputer des attaques perturbatrices et destructrices. Le but est de pouvoir nier être à l'origine des cyberattaques et ainsi se protéger contre des sanctions diplomatiques. Les infrastructures critiques sont des cibles privilégiées pour les attaques à effet boule de neige, car les acteurs malveillants pensent pouvoir les perturber sans nécessairement provoquer une réaction sur le champ de bataille. Par ailleurs, des unités d'espionnage se faisant passer pour des groupes de ransomware motivés par l'appât du gain prolifèrent, renforçant la menace qui plane sur la propriété intellectuelle et les données des entreprises.

Nombre de cyberattaques par procuration



Source : ©Control Risks

Soupçons d'implication russe dans la cyberattaque contre des terminaux pétroliers européens avant l'invasion de l'Ukraine

Une série de cyberattaques de grande ampleur a ciblé 17 terminaux portuaires en Belgique, en Allemagne et aux Pays-Bas en janvier 2022. Très probablement soutenues par la Russie, ces attaques par ransomware ont mis hors service des systèmes informatiques, affectant les opérations de chargement de produits pétroliers dans les ports. Elles ont été lancées trois semaines avant que la Russie envahisse l'Ukraine. C'est un exemple d'attaque à effet boule de neige ciblant un secteur et une région secondaires.

Facteurs contributant à la multiplication des incidents cybernétiques

Géopolitique

Les tensions entre les États-Unis et la Chine, l'accentuation de la multipolarité et les conflits en cours ont des répercussions dévastatrices sur les victimes visées et collatérales

Ransomware

Les groupes de cybercriminels sont plus actifs et dangereux que jamais avec un volume d'attaques en hausse et des recettes qui explosent avec des rançons réclamées plus elevées

Menaces liées aux tiers

Les fournisseurs d'infrastructures, les services logiciels, les hébergeurs de données et les technologies sont en première ligne et deviennent des cibles prioritaires

Technologie

Les progrés de l'IA introduisent rapidement de nouveaux risques, tandis que l'augmentation de l'interconnectivité et de l'interdépendance élargit la surface d'attaque de maniére exponentielle

Les attaques par ransomware ont augmenté de 74 % en 2023

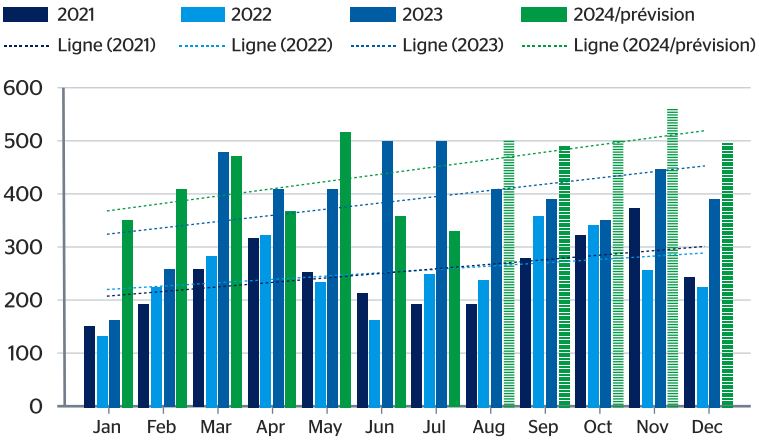
Ransomware

Le nombre d'attaques est en hausse et les recettes aussi

En 2023, les attaques par ransomware ou rançongiciel ont augmenté de 74 % par rapport à 2022, et le total des rançons versées par les victimes a dépassé 1 milliard de dollars au niveau mondial. Après que les forces de l'ordre ont démantelé le groupe Hive en 2022, l'écosystème des cybercriminels s'est fragmenté et le code du ransomware a fuité, permettant à des groupes plus petits de lancer leurs propres attaques.

Cette résurgence des ransomwares s'est poursuivie en 2024, le nombre de victimes rendues publiques atteignant les totaux mensuels les plus élevés des trois dernières années *(*notez que le graphique ci-dessous inclut MOVEit, un incident survenu en 2023 qui a fait de nombreuses victimes. En réalité, les chiffres de 2024 sont beaucoup plus élevés que ceux de 2023 si l'on exclut l'incident MOVEit comme une anomalie.)*

Nombre de victimes de ransomwares identifiées sur des sites de partage de données volées



Source : ©Control Risks

Nombre de victimes rendues publiques par des groupes de ransomware et de vol de données

2021	2022	2023	2024 (prévision)	2025 (prévision)
2 964	2 981	4 698	4 800	5 200

Source : ©Control Risks

Analyse sectorielle

Les attaques par ransomware ont été massives dans les secteurs de l'industrie, de la santé, de l'informatique, de l'enseignement et des services publics en 2023. La résilience étant variable d'un secteur à l'autre, les attaquants ciblent de plus en plus les secteurs verticaux mais se concentrent sur les secteurs de l'industrie et de la santé, où les perturbations opérationnelles sont extrêmement préjudiciables.

> 389 organisations de santé ont subi une attaque par rançongiciel en 2023 contre 214 en 2023 (+82 %)

Les ransomwares représentent un risque élevé pour les entreprises de fabrication et de production : 65 % du secteur a signalé une attaque par rançongiciel en 2023, avec un paiement de rançon de 2,4 millions de dollars en moyenne. Parmi les victimes du secteur, 62 % ont payé des rançons pour récupérer des données volées.

Il n'existe pas assez de renseignements pour calculer avec précision le montant moyen des rançons demandées, celles-ci variant considérablement d'une région, d'un secteur et d'une entreprise à l'autre. Cependant, les demandes se chiffrent probablement en dizaines de millions de dollars pour les grandes entreprises qui sont très vulnérables à des perturbations opérationnelles, et en centaines de milliers de dollars pour les organisations plus petites. Les montants les plus élevés sont vraisemblablement dans les secteurs de la santé, des services publics, de l'informatique et des communications et de l'industrie.

Les organisations de santé sont également des cibles très attractives, tout comme les autres secteurs qui détiennent de grands volumes de données personnelles et sensibles et ceux qui ont des exigences de performance. Le secteur de la santé est également perçu comme moins mature que d'autres secteurs en matière de cybersécurité. Ainsi, 389 organisations de santé ont subi une attaque par rançongiciel en 2023 contre 214 en 2022, soit une augmentation de 81,7 %.

La chasse au gros gibier

Les groupes de ransomware utilisent de plus en plus des techniques de « chasse au gros gibier », ciblant des entités connues qui génèrent des chiffres d'affaires élevés. La « chasse au gros gibier » leur permet de réclamer de plus fortes rançons en exploitant des perturbations opérationnelles un nombre de clients plus considérable.

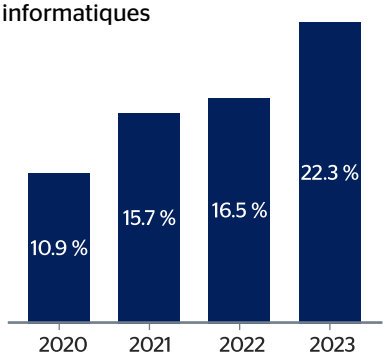
Ces dernières années, les forces de l'ordre ont obtenu de meilleurs résultats dans la lutte contre les groupes de ransomware, comme en témoignent le démantèlement du groupe Hive et les démantèlements partiels des groupes LockBit et BlackCat. Les groupes de ransomware ont donc cherché à maximiser les montants des rançons avant que les forces de l'ordre ne les rattrapent et ne saisissent leurs actifs et leurs infrastructures. Le montant moyen des rançons payées en 2023 a atteint 2 millions de dollars, contre 400 000 dollars l'année précédente. Le montant moyen a considérablement augmenté du fait de la chasse au gros gibier, certains acteurs malveillants ayant réclamé plus de 50 millions de dollars. Cependant, le montant médian des rançons demandées est resté stable, à environ 300 000 dollars.

En outre, les acteurs de la menace considèrent qu'il y a plus de chance que les grandes organisations paient une rançon. En moyenne, 61 % des entreprises enregistrant un chiffre d'affaires annuel de 5 milliards de dollars paient des rançons après une attaque, contre 25 % des entreprises dont le chiffre d'affaires annuel est inférieur à 10 millions de dollars. Certaines victimes au chiffre d'affaires élevé considèrent que les perturbations opérationnelles sont plus coûteuses que le paiement d'une rançon.

L'attaque LockBit visant ICBC illustre la menace opportuniste que représentent les ransomwares pour le secteur financier

Le groupe de ransomware LockBit a ciblé la branche américaine des services financiers de la Banque industrielle et commerciale de Chine (ICBC) en novembre 2023, perturbant les échanges sur le marché des bons du Trésor américain. Cette attaque a détourné des transactions financières et a empêché ICBC Financial Services de régler les transactions de bons du Trésor pour d'autres traders du marché, obligeant ICBC à injecter 9 milliards de dollars US dans sa branche américaine. Les attaquants ont probablement infiltré le réseau d'ICBC via un boîtier Citrix NetScaler qui avait une faille de sécurité non corrigée, ce qui leur a permis de contourner les mesures d'authentification.

Pourcentage des incidents cybernétiques mondiaux ayant touché des fournisseurs informatiques



Source : ©Control Risks

Attaques contre la chaîne d'approvisionnement

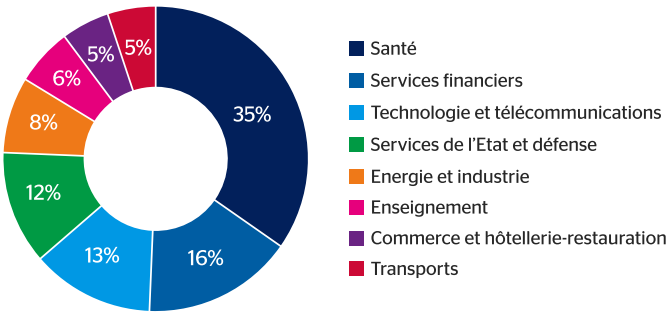
Incidents liés aux tiers

Au moins 22 % de toutes les violations de cybersécurité en 2023 découlaient probablement d'incidents qui à l'origine avaient une autre cible. Ce risque lié aux tiers est difficile à atténuer. Pour le maîtriser, les entreprises doivent adopter de bonnes pratiques en interne pour renforcer leur résilience face aux violations externes. Elles doivent tenir compte des mesures mises en place par leurs prestataires informatiques : quelles sont leurs politiques de cybersécurité, leurs stratégies d'atténuation et leurs contrats d'assurance ?

Secteur

Pour les cybercriminels, les fournisseurs informatiques, notamment de solutions SaaS (logiciel en tant que service), offrent une cible de choix. En 2023, 75 % des incidents liés à des tiers résultaient d'attaques ciblant en premier lieu des fournisseurs de services et de logiciels.

Part de chaque secteur dans les violations liées à des tiers en 2023



Graphique : Control Risks • Source : Security Scorecard

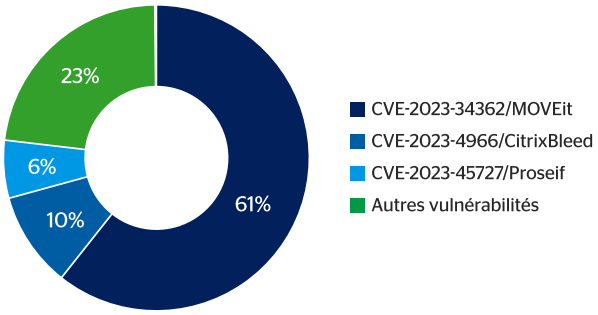
Trois vulnérabilités de la chaîne d'approvisionnement sont à l'origine de plus des trois quarts des attaques indirectes en 2023

Les attaques zero-day peuvent être les plus dévastatrices

Les fournisseurs informatiques sont des cibles privilégiées pour les groupes de ransomware qui peuvent ainsi toucher indirectement de nombreuses entreprises dans différents secteurs en une seule attaque. En outre, ces fournisseurs sont tenus par des contrats de niveau de service avec des clauses de disponibilité, et les pirates informatiques peuvent en jouer pour négocier la rançon.

En 2023, 64 % des violations via des tiers étaient liées au groupe de ransomware Clop exploitant un bug zero-day (une vulnérabilité inconnue et non corrigée). La vulnérabilité MOVEit était derrière 61 % des violations via des tiers, ce qui montre que ce type de risques peut avoir un impact bien concret sur la chaîne d'approvisionnement. Le graphique ci-dessous montre que plus de 75 % des incidents liés à des tiers en 2023 sont imputables à seulement trois vulnérabilités de la chaîne d'approvisionnement.

Part des différentes vulnérabilités à l'origine des incidents liés à des tiers en 2023

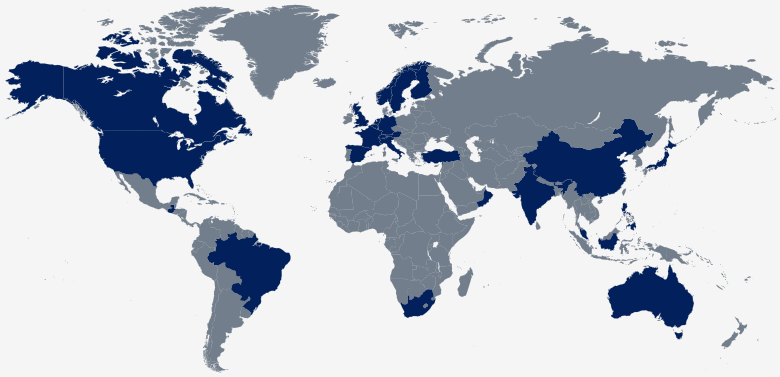


Graphique : Control Risks • Source : Security Scorecard

L'incident MOVEit montre que les attaques contre les fournisseurs informatiques peuvent avoir de vastes répercussions

Après avoir exploité une vulnérabilité zero-day dans le service de transfert de fichiers MOVEit en mai 2023, l'organisation cybercriminelle Clop a volé des fichiers à des entreprises qui ne savaient pas qu'elles étaient exposées à cette vulnérabilité. Cette fuite de données a touché au moins 2 180 organisations. Clop aurait perçu plus de 100 millions de dollars de rançons.

Répartition géographique des victimes de l'attaque contre MOVEit



Technologie

Menaces sur le cloud

Depuis que les entreprises ont adopté les services cloud, les acteurs malveillants ont développé des outils et des techniques pour accéder plus facilement et durablement aux applications qui utilisent ces serveurs à distance, afin d'explorer un réseau infecté et trouver d'autres vulnérabilités. Passer par des applications basées sur le cloud leur permet également de contourner les protocoles de détection classiques, comme l'analyse IP avancée. Les acteurs malveillants liés à un État et les cybercriminels de haut vol ont également migré vers le cloud, exfiltrant des données vers leur propre stockage.

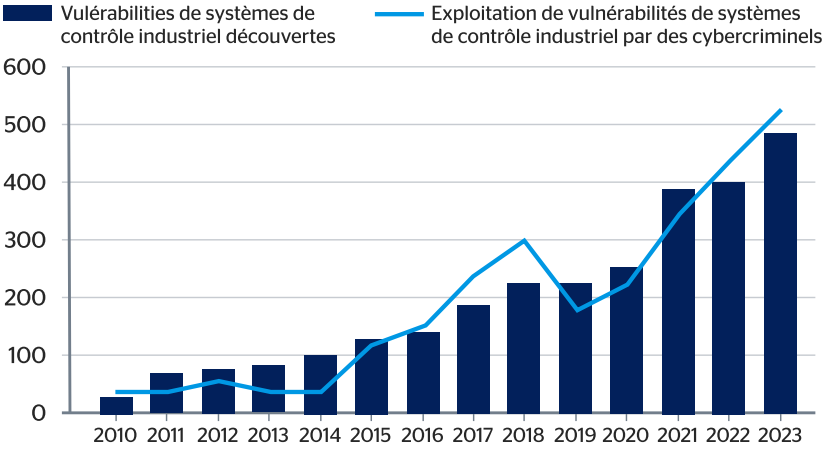
Technologie opérationnelle et Internet des Objets (IdO)

Les attaques par ransomware contre des entreprises du secteur industriel ont augmenté de 50 % en 2023 par rapport à 2022. Les attaques qui réussissent à perturber la technologie opérationnelle, c'est-à-dire les logiciels et le matériel qui contrôlent la production, aident les cybercriminels à extorquer de l'argent, car la perturbation a des conséquences financières plus lourdes qu'une rançon. Pour les acteurs étatiques, la perturbation de la technologie opérationnelle peut également remplir des objectifs stratégiques. Semer la pagaille dans la production manufacturière peut s'avérer lucratif ou stratégiquement utile, voire les deux.

L'ingénierie, l'industrie et les infrastructures de réseaux sont des cibles privilégiées pour les attaques ciblant la technologie opérationnelle. Les acteurs de la menace, aux capacités variables, ciblent de plus en plus la technologie opérationnelle qui utilise des appareils connectés à Internet. La prolifération des appareils IdO (Internet des objets), c'est-à-dire le matériel connecté à Internet sans fil, a probablement exacerbé ces menaces pour la technologie opérationnelle, en particulier dans les secteurs de l'industrie et des infrastructures de réseaux. Pour réduire ce risque, il convient de segmenter le réseau et de limiter ou de supprimer les ports exposés à Internet.

> Les attaques par ransomware ont augmenté de 50 % dans le secteur industriel en 2023

Nombre de vulnérabilités dans des sytèmes de contrôle industriel et d'incidents exploitant ces vulnérabilités



Source : ©Control Risks

L'intelligence artificielle peut aider à déceler des cyberattaques

Intelligence Artificielle (IA)

L'Intelligence Artificielle est en train d'évoluer. Elle a dépassé le stade des machines réactives (préprogrammées pour des tâches spécifiques) et est résolument entrée dans celui de l'IA à mémoire limitée, capable d'analyser de vastes ensembles de données pour prendre des décisions. Ce qui a des conséquences en matière de risques cyber. Par exemple, les outils d'IA générative open source peuvent écrire du code pour des logiciels nuisibles ou aider les acteurs malveillants à perfectionner leurs attaques traditionnelles ou ciblées (spearphishing).

À mesure que l'IA devient plus accessible et que les grands modèles de langage (LLM) prolifèrent, les acteurs de la menace aux capacités moindres, comme les cybercriminels et les cyberactivistes, peuvent lancer des attaques de plus grande ampleur plus rapidement. C'est cette augmentation en termes d'échelle et de vitesse qui aura l'impact le plus fort sur le paysage des cybermenaces.

Les criminels déploient des outils d'IA générative pour créer des deepfakes d'employés et de cadres afin d'escroquer des organisations de toutes tailles. Au début de l'année, une multinationale a perdu 20 millions de dollars à cause d'une attaque par deepfake. Cette technique n'est pas nouvelle (des cas auraient été signalés dès 2019), mais sa fréquence et ses chances de réussite augmentent considérablement avec l'IA, et les compétences nécessaires pour mener ce type d'attaque diminuent à mesure que la technologie s'améliore.

À l'inverse, l'IA contribue déjà à la détection des comportements malveillants dans les réseaux d'entreprise, et elle devrait continuer à améliorer les capacités de cybersécurité en général, avec une meilleure efficacité des activités de sécurité et de défense. Les entreprises vont de plus en plus utiliser l'IA générative et l'automatisation pour identifier les cyberattaques dans un paysage de menaces en constante évolution, où les acteurs malveillants innovent sans relâche.

Diversification des technologies

Le cloud et les technologies émergentes offrent aux entreprises des solutions d'infrastructure digitale à moindre coût. Cependant, la généralisation de l'infrastructure en tant que service et de l'IA en tant que service a augmenté la surface d'attaque des acteurs malveillants, leur offrant plus d'opportunités d'infecter de nombreuses victimes en une seule attaque.

La prolifération des appareils IdO permet de lancer des cyberattaques plus perturbatrices contre des services essentiels, comme l'alimentation en eau. Les progrès de l'IA générative permettent aux cybercriminels de créer des deepfakes de cadres d'entreprise pour faciliter des attaques d'ingénierie sociale. Les cyberactivistes, parfois parrainés par des Etats, utilisent les nouvelles technologies pour influencer des élections ou financer des campagnes en dehors des cadres légaux. De plus en plus d'acteurs malveillants développent leurs propres outils et exploitent l'IA pour automatiser la préparation d'attaques et déployer des logiciels malveillants. L'adoption de technologies émergentes à différentes échelles et à différents rythmes, selon le secteur et la région, élargit la surface d'attaque ; les organisations entrent dans la course pour se prémunir contre les risques cyber.

Des activistes ciblent la technologie opérationnelle et coupent l'alimentation en eau

En décembre 2023, le groupe d'activistes Cyber Av3ngers lié à l'Iran a ciblé des contrôleurs logiques programmables (PLC) fabriqués par la société israélienne Unitronics. Ces éléments étaient utilisés par une compagnie privée d'eau irlandaise. L'attaque a provoqué une coupure d'eau de deux jours pour les habitants d'Erris, en Irlande. Cyber Av3ngers a revendiqué les attaques des PLC dans le cadre de sa campagne contre des entreprises israéliennes sur fond de conflit entre Israël et le Hamas.

Conclusion

L'interdépendance technologique, renforcée par les progrès de l'interconnectivité, de l'IA et d'autres technologies émergentes, offre aux cybercriminels l'opportunité de frapper les entreprises. Les conflits mondiaux, les évolutions géopolitiques et l'essor de l'économie cybercriminelle devraient encore accroître les risques pour les organisations qui adoptent les nouvelles technologies dans leur fonctionnement.

L'interdépendance entre les secteurs et les entreprises rendra ces risques inévitables, les acteurs de la menace privilégiant le développement de programmes malveillants sophistiqués pour toucher la technologie opérationnelle ou les fournisseurs tiers de services et de logiciels. Cependant, l'IA et d'autres technologies continueront de se développer, contribuant à réduire et à prévenir différentes menaces qui exploitent l'interdépendance technologique.

Dans ce contexte, les entreprises doivent privilégier les stratégies de transformation numérique qui protègent des menaces futures. Elles doivent tenir compte des risques croissants d'incidents cybernétiques et mettre en place des protocoles pour réagir rapidement aux cyberattaques, en mettant toujours l'accent sur leur résilience.

Annexe – Références

Global ransomware threat expected to rise with AI, NCSC warns, ncsc.gov.uk
2023 Ransomware Attack Report, blackfog.com
Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline, chanalysis.comv
#StopRansomware: CLOP Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability, cisa.gov
Two-day water outage in remote Irish region caused by pro-Iran hackers, therecord.media
NCC Group Releases Annual Cyber Threat Monitor Report 2023, nccgroup.com
Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double, dni.gov
The State of Ransomware 2024, sophos.com
The State of Ransomware in Manufacturing and Production 2024, sophos.com
Helping our customers through the CrowdStrike outage, blog.microsoft.com
Dragos 2023 OT Cybersecurity Year in Review, dragos.com
Global Third-Party Cybersecurity Breach Report, securityscorecard.com

Nous avons publié une correction le 9 octobre 2024 pour rectifier un chiffre erroné dans l'analyse sectorielle en page 7. A l'échelle mondiale, 389 organisations de santé ont été confrontées à des attaques par rançongiciel en 2023 (Control Risks, 2024).

Cyber-assurance QBE

Les produits de cyber-assurance de QBE protègent contre tous les risques associés au numérique et fournissent un soutien essentiel en cas de cyberattaque. L'offre comprend QCyberProtect, une nouvelle cyber-assurance globale couvrant tous les sinistres causés par des cyber-risques actuels et émergents dans le monde entier, notamment la sécurité du réseau, la responsabilité en matière de protection de la vie privée, les interruptions d'activités informatiques et non informatiques et les atteintes à la réputation.

Une couverture sur mesure et un service individuel

Pour assurer votre protection, les souscripteurs de QBE collaborent étroitement avec vous pour créer une couverture adaptée à vos besoins spécifiques. Nous prenons le temps de comprendre votre activité pour vous fournir une couverture sur mesure qui vous protège contre les cyber-risques actuels et émergents.

Vous aider à gérer vos risques

Nous ne nous contentons pas de vous couvrir contre les risques, nous vous aidons à les maîtriser et à les réduire. Nous proposons des outils d'aide à la gestion des risques, notamment :

- QBE QCyberPrepare – une saferoom en ligne pour aider les clients à se préparer à un incident cybernétique.
- Accès gratuit au Portail de gestion des cyber-risques de QBE, qui fournit de nombreuses informations sur les cyber-risques et les moyens de vous protéger.
- Accès aux outils et services QBE, ainsi qu'à des remises sur une gamme de services de gestion des cyber-risques fournis par nos partenaires.

Assistance en cas de crise

Si vous subissez une cyberattaque, QBE vous fournit une assistance 24 h/24. Cela peut impliquer le déploiement d'une équipe d'experts pour déterminer comment la cyberattaque s'est produite et comment résoudre le problème, une aide juridique pour satisfaire aux exigences réglementaires, ou la préparation d'un communiqué de presse pour limiter l'impact sur votre réputation.

Pour en savoir plus, consultez Cyber Response - QBE France

Ce rapport a
été développé
pour QBE par
Control Risks

QBE European Operations

QBE Europe SA/NV
Tour CBX
1 passerelle des Reflets
92913 Paris La Défense Cedex
+33 (0) 1 80 04 33 00
QBEfrance.com

641209/2405