7 tendances en matière de cybersécurité à surveiller à l'approche de 2024

Les défis et les opportunités, anciens et nouveaux, façonneront une autre année dans le domaine de la cybersécurité.

Carrie Pallardy ⋮

Maksym Yemelyanov via Alamy Stock

En un coup d'œil

- L'IA générative va alimenter des cyberattaques plus sophistiquées ainsi que des capacités de défense et de détection plus avancées.
- Les auteurs de menace tirent parti de la complexité des chaînes d'approvisionnement et ciblent des fournisseurs tiers pour atteindre leurs objectifs.
- Alors que de plus en plus de personnes adoptent une approche axée sur le cloud, les acteurs de la menace cherchent des moyens de cibler les environnements hybrides et multicloud.

Les responsables de la cybersécurité sont confrontés à un vaste paysage de menaces, à des piles technologiques en expansion et à des budgets limités.
Le début d'une nouvelle année est l'occasion d'évaluer les plus grands risques de sécurité et de déterminer comment utiliser les ressources disponibles pour défendre au mieux leurs entreprises.
Quelles sont les principales tendances en matière de sécurité que les RSSI et autres responsables de la sécurité doivent prendre en compte à l'approche de 2024 ?

Quatre experts en sécurité partagent leurs prévisions et la manière dont les responsables de la sécurité peuvent se préparer pour l'année à venir.

Menaces et défense de l'IA

L'explosion et l'adoption rapide de l'IA générative ont été une tendance déterminante de 2023, et elle ne montre aucun signe de ralentissement.
Cette technologie va alimenter des cyberattaques plus sophistiquées ainsi que des capacités de défense et de détection plus avancées.

« Nous avons à peine effleuré la surface en termes d'amélioration potentielle des capacités que ce type d'outils pourrait apporter aux attaquants et aux défenseurs », a déclaré à InformationWeek Kelli Vanderlee, directrice principale du fournisseur de solutions de renseignement sur les menaces Mandiant Intelligence, qui fait partie de Google Cloud.

Dans ses prévisions de cybersécurité 2024, Google Cloud décrit les façons dont l'IA sera utilisée pour alimenter des attaques de phishing professionnalisées et à grande échelle et des opérations d'information évolutives.
L'IA va permettre aux acteurs de la menace de créer plus facilement des campagnes d'ingénierie sociale propres et convaincantes à grande échelle.
La technologie sera également utilisée pour générer de fausses nouvelles et des photos et vidéos deepfake.

À lire aussi :Ce que les RSSI doivent savoir sur les acteurs étatiques

Au fur et à mesure que les attaquants renforcent leurs capacités d'IA, les défenseurs doivent faire de même.
« L'intégration des outils d'IA doit rester à l'avant-garde de la cyberdéfense, en s'intégrant aux renseignements sur les cybermenaces, à la gestion de la surface d'attaque, à la détection et à la réponse pour faire face au nombre et à la sophistication écrasants des attaques », a déclaré Yuval Wollman, directeur de la cybersécurité et directeur général d'Israël chez UST, une société de solutions de technologie numérique, à InformationWeek dans une interview par e-mail.

Les équipes de cybersécurité pourront utiliser l'IA pour étendre les capacités d'analyse des menaces.
Wollman s'attend également à ce que l'IA générative soit capable de créer du contenu prédictif à l'aide de comportements et de modèles d'attaque, ce qui donnera aux équipes de cybersécurité la possibilité d'adopter une approche proactive de la défense.

Bien que l'IA évolue rapidement, elle n'est pas encore capable de remplacer les talents humains en cybersécurité. Andrius Useckas, CTO et RSSI chez ThreatX, une société de protection des API et des applications Web, souligne que l'IA est toujours basée sur des règles.
« Si vous voulez que votre environnement soit sécurisé, vous avez toujours besoin de ce test d'intrusion annuel

», explique-t-il.
« Vous avez toujours besoin d'un véritable pirate éthique, d'un véritable humain, de l'autre côté, pour essayer de s'introduire dans votre système et de le répliquer exactement de la même manière qu'un véritable attaquant essaierait de s'introduire dans votre système. »

À lire aussi :Passer le relais de la sécurité : planification de la relève des RSSI

Tensions géopolitiques et acteurs de l'État-nation

Les cyberattaques menées par des acteurs de la menace d'États-nations, ainsi que par des groupes d'hacktivistes à motivation politique, se poursuivront en relation avec les conflits actifs en Ukraine et à Gaza.
Vanderlee souligne que les attaques dans ces régions peuvent avoir une probabilité plus élevée d'impact cinétique.
Par exemple, Sandworm, un acteur malveillant lié à la Russie, a perturbé l'alimentation électrique en Ukraine et provoqué une panne de courant à la fin de 2022.

« Ce sont certainement des choses à surveiller, surtout si vous faites des affaires dans ces régions ou dans des pays situés autour de ces régions », explique M. Vanderlee.

Les cybermenaces des États-nations vont au-delà de ces deux conflits.
Les prévisions de cybersécurité 2024 de Google Cloud mettent en évidence les « quatre grands » acteurs étatiques-nations : la Chine, la Russie, la Corée du Nord et l'Iran.

La Chine a mis au point une opération sophistiquée de lutte contre les cybermenaces afin d'atteindre diverses priorités à long terme.
On s'attend à ce que les acteurs de l'espionnage basés en Chine continuent de trouver des moyens de ne pas être détectés et d'éviter d'être attribués.
« Nous nous attendons à ce que les acteurs de la menace chinois continuent de trouver des moyens très innovants et intéressants de cibler les appareils périphériques, afin de trouver des moyens de minimiser les possibilités de détection », a déclaré M. Vanderlee.

À lire également :Rapport 2023 sur les cyberrisques et la résilience : comment les DSI se battent en duel contre la catastrophe en 2023

L'Ukraine restera une cible privilégiée des cybermenaces russes, mais les sanctions continuent de nuire à la Russie.
En conséquence, il pourrait poursuivre davantage de vols de propriété intellectuelle pour compenser, selon le rapport de Google Cloud.

Les cybermenaces en provenance de la Corée du Nord sont souvent motivées par des raisons financières.
« Les auteurs de menace nord-coréens sont vraiment remarquables par leur persévérance et leur créativité », a déclaré M. Vanderlee.
« Ils ont été particulièrement doués pour exécuter des compromis sur la chaîne d'approvisionnement au cours de la dernière année... en menant des campagnes d'ingénierie sociale intéressantes et complexes.

Selon le rapport de Google Cloud, l'activité de menace associée à l'Iran sera probablement motivée par la collecte de renseignements, les opérations d'information et les attaques potentiellement perturbatrices et destructrices.

Attaques de la chaîne d'approvisionnement

Les auteurs de menace tirent parti de chaînes d'approvisionnement de plus en plus complexes et ciblent des fournisseurs tiers pour atteindre leurs objectifs.
Bien que la complexité de la chaîne d'approvisionnement soit la réalité de nombreuses organisations, M. Wollman indique que des efforts sont déployés pour réduire les risques.

« Il y a eu une tendance marquée à la visibilité de la chaîne d'approvisionnement et à la consolidation des fournisseurs afin de minimiser les risques liés aux cybermenaces de plus en plus sophistiquées », explique-t-il.

Étant donné que le risque lié aux tiers reste un facteur important, les responsables de la sécurité seront chargés de faire preuve de diligence raisonnable à l'égard des fournisseurs externes.
À quoi ressemble leur posture en matière de cybersécurité ?
Si un fournisseur est compromis, quel impact cela a-t-il sur votre organisation ?
Avoir une compréhension adéquate des risques liés aux tiers est une étape importante pour minimiser les dommages potentiels d'une attaque de la chaîne d'approvisionnement.

Donner la priorité à la sécurité du cloud

La migration vers le cloud continue d'être un thème important dans le domaine de l'informatique.
Alors que de plus en plus d'entreprises adoptent une approche axée sur le cloud, les acteurs de la menace cherchent des moyens de cibler les environnements hybrides et multicloud.

Mandiant a observé que les acteurs de la menace ciblaient les environnements cloud et cherchaient des moyens de gagner en persistance et de se déplacer latéralement en 2023, selon les prévisions de cybersécurité 2024 de Google Cloud.
Cette tendance devrait se poursuivre jusqu'en 2024 ; les acteurs de la menace vont chercher des moyens d'exploiter les erreurs de configuration du cloud et de se déplacer latéralement dans les environnements multicloud.

« La gestion de la posture de sécurité du cloud (CSPM) est en train de devenir une partie intégrante de l'architecture de sécurité du cloud, d'autant plus que la visibilité devient de plus en plus difficile à obtenir dans les environnements multicloud », explique M. Wollman.

Rançongiciels

Les rançongiciels restent une activité rentable pour les acteurs de la menace, et ils vont continuer à rechercher des vulnérabilités qui leur permettent d'exécuter ces attaques. Useckas explique que ces attaques ne s'arrêteront pas et qu'il existe en fait une tendance à la double attaque par ransomware.

« Lorsqu'une personne est attaquée par un rançongiciel, elle peut récupérer à partir de sauvegardes ou payer la rançon, puis subir une autre attaque juste après parce que... Les attaquants sont toujours intégrés dans le système », explique-t-il.

En septembre, la division Cyber du FBI a publié une notification du secteur privé mettant en garde contre la tendance croissante des attaques de ransomware doubles, qui impliquent le déploiement de deux variantes de ransomware différentes dans un court laps de temps.

L'hameçonnage est un moyen courant de lancer une attaque par rançongiciel, et l'utilisation malveillante de l'IA est susceptible de rendre les escroqueries par hameçonnage plus difficiles à détecter.
« Il faut absolument que... éduquez votre peuple autant que possible et ensuite, évidemment, ayez également une défense en couches », explique Useckas.

Zero-Day Exploits

Au total, 87 vulnérabilités zero-day ont été découvertes en 2023, contre 52 en 2022, selon le Zero-Day.cz Tracking Project.

« Au cours des dernières années, la Chine a réalisé plus d'exploits zero-day que n'importe quel autre pays.
Et nous nous attendons à ce que cela se poursuive, et cela devrait être une grande menace pour une variété d'organisations », a déclaré Vanderlee.

Alors que les groupes parrainés par des États-nations ont toujours été les principaux acteurs de la menace derrière les exploits zero-day, cela est en train de changer, selon le rapport Key Forecasts 2024 de la société de cybersécurité ZeroFox.
Le rapport souligne que les groupes de rançongiciels comme CL0P exploitent également les vulnérabilités zero-day.

AJ Nash, vice-président et membre émérite du renseignement chez ZeroFox, exhorte les responsables de la sécurité à adopter une vision plus large des zero-days et à reconnaître les menaces potentielles qu'ils représentent dans le monde interconnecté d'aujourd'hui.

« Arrêtez de penser à toutes ces choses dans des petits silos et des petits seaux.
Si vous êtes un fabricant aux États-Unis et qu'il y a un exploit zero-day contre [une] société de services financiers en Asie, arrêtez de supposer que cela ne vous dérange pas, que cela ne devrait pas être votre problème », prévient-il.

Examen réglementaire

En 2023, un certain nombre de responsables de la cybersécurité se sont retrouvés sous le microscope réglementaire.
L'ancien directeur de la sécurité d'Uber, Joseph Sullivan, a été condamné à trois ans de probation et à payer une amende de 50 000 $ pour son rôle dans la réponse à une violation de données en 2016 dans l'entreprise.
Tim Brown, RSSI de SolarWinds, fait également l'objet d'une action en justice.

La Securities and Exchange Commission (SEC) a intenté une action en justice contre lui et SolarWinds, alléguant qu'il n'avait pas maintenu de contrôles de cybersécurité adéquats avant une cyberattaque en 2019.

Ces cas très médiatisés pourraient indiquer la possibilité d'une plus grande responsabilisation au niveau des particuliers et des entreprises.
« Je pense que nous plaçons les RSSI dans une position très difficile où ils doivent faire des choix entre leur propre patrimoine personnel et leur plan de rémunération, qui est souvent très fortement utilisé pour maintenir le cours de l'action à la hausse et réduire vos dépenses, plutôt que de faire ce qui est le mieux pour la sécurité », explique M. Nash.

La surveillance réglementaire continue pourrait changer la façon dont les entreprises abordent la cybersécurité.
« Je pense qu'au fur et à mesure que nous commencerons à voir une plus grande responsabilisation, cela pourrait changer la façon dont les organisations choisissent de prioriser leurs dépenses et la façon dont elles choisissent de communiquer à leurs propres dirigeants et au public quant à leur degré de sécurité », déclare Nash.

Se préparer pour l'année à venir

Les ransomwares, les exploits zero-day, les acteurs étatiques, les attaques de la chaîne d'approvisionnement, la sécurité et les réglementations du cloud ne sont pas des concepts nouveaux pour les responsables de la sécurité.
Et l'avènement de l'IA générative a été au centre des discussions informatiques pendant une grande partie de l'année 2023.
Le début d'une nouvelle année donne aux responsables de la sécurité l'occasion d'examiner toutes ces tendances et de réfléchir à ce qu'elles signifient pour leur entreprise.
Votre pile technologique est-elle préparée aux menaces les plus pressantes ?
Des éléments de votre environnement doivent-ils être mis à jour ?
Votre programme d'application de correctifs et votre processus de gestion de l'infrastructure sont-ils à jour ?
Disposez-vous d'un plan d'intervention en cas d'incident de ransomware ?
Avez-vous l'équipe qu'il vous faut ?
Comment votre organisation utilise-t-elle l'IA et quels sont les risques ?

« Comment puis-je classer les choses que je veux accomplir et comment voulons-nous dépenser nos ressources pour mieux défendre notre organisation au cours de la prochaine année ? », demande M. Vanderlee.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231219
"C'est ensemble qu'on avance"