X-Force

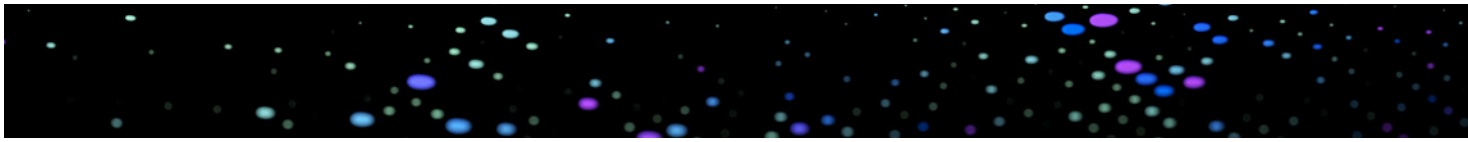
Rapport IBM Security X-Force 2021 sur les menaces internes

IBM Security X-Force Threat Intelligence

Rapport Special Intelligence T2 2021

IBM

Table des matières



Introduction

Le paysage des cybermenaces évolue sans cesse, car attaquants comme défenseurs font preuve d'innovation en exploitant de nouveaux procédés et technologies. Collectivement, les entreprises dépensent environ 60 milliards de dollars par an pour défendre leurs actifs et recruter des talents afin de prévenir les attaques et d'y répondre. Les dépenses de sécurité ont ainsi encore augmenté de 10 % en 2021.[1]

Alors qu'une grande partie de l'attention et des dépenses d'une organisation en matière de sécurité sont consacrées à la lutte contre les attaques provenant de l'extérieur, les menaces intérieures sont souvent négligées. Il s'agit des menaces provenant de l'intérieur de l'organisation. Les menaces intérieures, dont beaucoup s'avèrent dépourvues de malveillance ou accidentelles, peuvent causer des dommages dévastateurs en termes de vols de données, de pertes financières, de vols de propriété intellectuelle ou d'atteintes à la réputation. Dans une enquête de 2020, le Ponemon Institute a estimé que les organisations dépensent en moyenne 644 852 $ pour se remettre d'un incident lié à une menace interne, quelle que soit la source de l'incident.[2] Ce montant inclut le coût de la surveillance et de l'enquête sur les événements internes suspectés, ainsi que celui de la réponse aux incidents, de l'endiguement, de l'éradication et de la correction d'un incident interne.

Dans cet article, IBM Security X-Force donne la définition suivante d'un initié :

— L'initié fortuit : employé, fournisseur tiers ou sous-traitant négligent.[3]

— Initié malveillant : employé, fournisseur tiers ou sous-traitant délinquant ou malveillant.

1. https://www.infosecurity-magazine.com/news/global-cybersecurity-spending-to/
2. https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/
3. Un initié négligent est une personne qui provoque accidentellement un incident affectant la confidentialité, l'intégrité ou la disponibilité des données ou des systèmes dans une organisation. Cela n'inclut pas les incidents d'hameçonnage ou de piratage psychologique.

Grâce à des données propriétaires exclusives réunies lors d'enquêtes de réponses à des incidents réels, X-Force a analysé des incidents liés à des menaces internes suspectées, tant accidentelles que malveillantes, qui ont affecté des organisations entre 2018 et 2020. Cet article s'appuie sur des rapports en accès libre traitant des principales attaques par menace interne afin d'examiner les découvertes les plus importantes issues de ces données, notamment :

— Comment la plupart des attaques d'initiés sont détectées.

— Le rôle joué par le niveau d'accès dans les attaques internes.

— Les meilleures pratiques pour atténuer les menaces internes.

Principaux résultats de la recherche

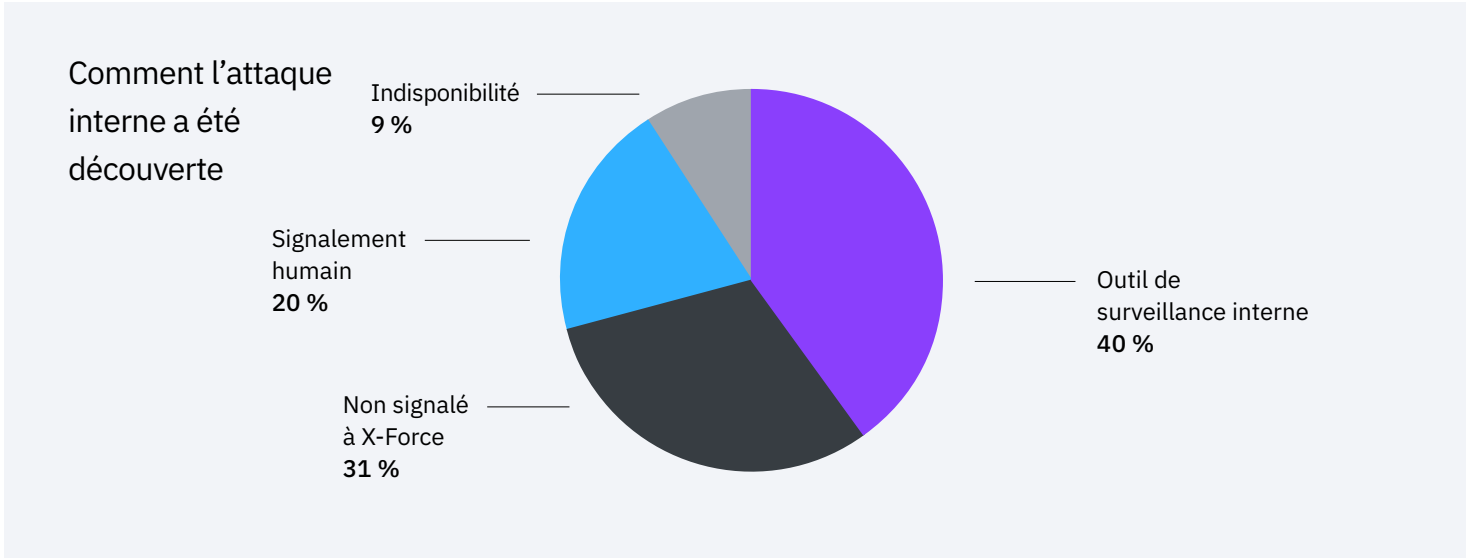
40 % des incidents ont été détectés au moyen d'alertes générées par un outil de surveillance interne.

40 % des incidents ont impliqué un employé disposant d'un accès privilégié aux actifs de l'entreprise.

Dans 100 % des incidents pour lesquels l'initié disposait effectivement ou probablement d'un accès d'administratif, cet accès privilégié a joué un rôle dans l'incident lui-même.

Détection des menaces internes

Par menaces internes, on entend généralement des attaques dans le cadre desquelles des utilisateurs légitimes disposant d'un certain niveau d'accès aux actifs de l'entreprise exploitent cet accès, que ce soit dans un but malveillant ou par inadvertance, et portent finalement atteinte à l'entreprise. Cette menace peut provenir d'un employé actuel ou ancien, ou encore d'un sous-traitant ou fournisseur tiers qui conserve un accès pour remplir une fonction commerciale prédéfinie.



Une analyse des menaces internes auxquelles X-Force a répondu depuis 2018 révèle que 40 % de ces incidents ont été détectés au moyen d'alertes générées par un outil de surveillance interne. Les signalements humains (par exemple, lorsque des employés signalent une activité anormale à leur entreprise) ont représenté 20 % des détections et une indisponibilité du système a alerté les équipes de sécurité dans 9 % des cas.

Dans le Rapport mondial sur le coût des menaces internes de 2020 du Ponemon Institute, à l'initiative d'ObserveIT et d'IBM, des outils tels que ceux d'analyse du comportement des utilisateurs (UBA), de gestion des accès privilégiés (PAM), de gestion des informations et événements de sécurité (SIEM), ainsi que des programmes portant sur le partage de renseignement sur les menaces et sur la formation et la sensibilisation des utilisateurs, ont permis aux entreprises d'économiser en moyenne trois millions de dollars grâce à la réduction et à l'élimination des risques internes.[4]

3 millions de dollars économisés

Des outils tels que l'UBA, la PAM, la SIEM et des programmes destinés au partage de renseignement sur les menaces ou à la formation et à la sensibilisation des utilisateurs ont permis aux entreprises d'économiser en moyenne trois millions de dollars grâce à la réduction et à l'élimination des risques internes.[4]

4. https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/

Manque de preuves et inconnues dans la recherche X-Force

En ce qui concerne les incidents internes pour lesquels la méthode de détection était de type « non signalé à X-Force » ou « absence de preuves », les équipes de réponse aux incidents de X-Force n'ont pas reçu suffisamment d'informations pour qualifier la découverte. Cette lacune s'explique souvent par le fait que de nombreuses entreprises manquent de visibilité sur leur environnement de référence et sur son fonctionnement. Pour détecter une activité anormale au sein d'un système, il est essentiel de comprendre l'aspect d'une activité normale de façon à repérer plus aisément, et avec certitude, les anomalies. En 2019, IBM a parrainé un rapport SANS[5] d'observation du paysage des menaces avancées qui pèsent sur les entreprises. Cette recherche a révélé que :

— 48 % des entreprises considéraient l'absence de visibilité sur leur infrastructure comme la principale lacune en matière de sécurité.

— 35 % estimaient qu'elles n'étaient pas en mesure de détecter les abus commis par les personnes internes à l'entreprise.

— 47 % des entreprises admettaient être incapables de se représenter l'aspect normal d'une activité de base au sein de leurs réseaux.

5. https://www.ibm.com/account/reg/us-en/signup?formid=urx-39989

Accès privilégié et accès administratif

X-Force a identifié deux types d'utilisateurs lors de l'analyse des incidents liés à des menaces internes.

Un **utilisateur privilégié** est défini comme étant une personne interne à l'entreprise qui a accès à des données sensibles. Ces données peuvent relever de la propriété intellectuelle, des données clients ou des informations des RH. Ces utilisateurs peuvent aussi être des personnes ayant accès à des informations commerciales sensibles, comme des données relatives aux fusions et acquisitions, ou à d'autres informations juridiques.

Les utilisateurs bénéficiant d'un **accès administratif**, aussi appelés administrateurs ou admin, sont définis comme des personnes disposant d'un accès de haut niveau aux systèmes informatiques dans le réseau. En théorie, ces types d'accès ne doivent pas se recouper. X-Force a cependant découvert que des utilisateurs finaux sont parfois surutilisés dans leurs environnements informatiques.

Les initiés disposant d'un accès administratif diffèrent de ceux bénéficiant d'un accès à des données sensibles dans l'environnement d'une entreprise. Il s'agit d'employés, sous-traitants et fournisseurs ayant accès à l'environnement informatique de l'entreprise et qui présentent un risque unique pour celle-ci en raison de leurs privilèges sur le réseau.

Exemples de rôles bénéficiant d'un accès privilégié

- Rôles RH
- Cadres supérieurs
- Rôles financiers
- Rôles juridiques
- Postes de recherche
- Autres rôles ayant accès aux éléments de propriété intellectuelle ou « joyaux » de l'entreprise, ou aux données des clients

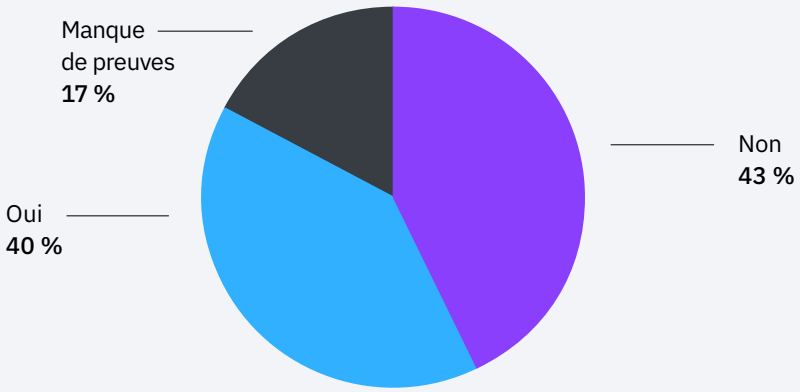
Exemples de rôles disposant d'un accès administratif

- Administrateurs de serveur
- Administrateurs informatiques
- Centre d'assistance
- Fournisseurs informatiques tiers
- Autres rôles susceptibles de modifier des configurations ou paramètres sur des systèmes informatiques

Qui observe les observateurs ?

Les initiés à l'origine d'incidents ont-ils généralement un accès privilégié ? Globalement parlant, oui.

L'initié avait-il un accès privilégié aux données ?



L'analyse des données X-Force montre que 40 % des incidents provoqués par des initiés ont impliqué un employé bénéficiant d'un accès privilégié à des actifs sensibles de l'entreprise. Pour cette recherche, X-Force a défini les accès privilégiés comme étant ceux dont disposent les personnes travaillant dans l'équipe informatique ou dans les services des ressources humaines, des finances ou de la sécurité, ou occupant des postes de cadres.

Dans les 17 % des données restantes, on ignore si l'initié avait ou non un accès privilégié à des données sensibles. Le nombre d'incidents provoqués par des utilisateurs avec accès privilégié pourrait donc être sensiblement supérieur.

Les personnes disposant d'un accès de niveau élevé à des actifs essentiels, tels que des parts de réseaux, des dispositifs de sécurité, des systèmes de messagerie, des données à caractère personnel (DCP) d'employés ou de clients, des éléments de propriété intellectuelle ou des données financières peuvent présenter un risque nettement plus élevé que celles dont les privilèges sont moindres.

Il est logique que les incidents provoqués par des initiés accidentels ayant un accès privilégié finissent par coûter plus cher aux organisations que ceux provoqués par des initiés accidentels dont le niveau d'accès est inférieur. Les incidents impliquant des initiés malveillants ayant un niveau supérieur d'accès privilégié ont un coût encore plus lourd et les attaques impliquant ces utilisateurs peuvent entraîner des violations de données à grande échelle. En 2018, par exemple, un agent immobilier australien travaillant pour une agence locale prestigieuse a été accusé d'avoir accédé à des bases de données confidentielles avant de quitter l'agence. L'agent a manipulé l'état des ventes potentielles dans le système en minimisant l'intérêt des clients potentiels. En outre, l'agent a reconnu avoir dérobé les fichiers de 200 clients pour solliciter un emploi auprès d'une nouvelle agence. On estime que cette attaque d'initié a coûté à l'agence concernée 30 millions de dollars en ventes potentielles de biens.[6]

L'une des meilleures méthodes de prévention des incidents liés au niveau d'accès des initiés consiste à adhérer aux principes du moindre privilège et à s'assurer que les utilisateurs ont le plus faible niveau d'accès nécessaire pour remplir leurs tâches au sein de l'entreprise. Cette prévention peut prendre la forme d'une solution de gestion des accès privilégiés (PAM) pouvant être élaborée autour d'un modèle Zero Trust.[7,8] L'objectif recherché par ce modèle est d'accorder à chaque personne ayant un compte d'utilisateur les privilèges les plus réduits possibles afin de limiter le risque qu'un utilisateur interne accède sans autorisation à des données ou à des actifs. L'importance de ce concept est encore plus critique dans le cloud qui accueille davantage de données et auquel des utilisateurs humains et non humains doivent avoir accès pour être opérationnels.

Le Rapport mondial sur le coût des menaces internes de 2020 a montré que seules 39 % des entreprises ont adopté une forme de gestion des accès privilégiés.[9] En outre, il révèle que l'adoption d'une solution de PAM se traduit par une économie de 3,1 millions de dollars, soulignant ainsi l'efficacité de ces mesures.

39 %

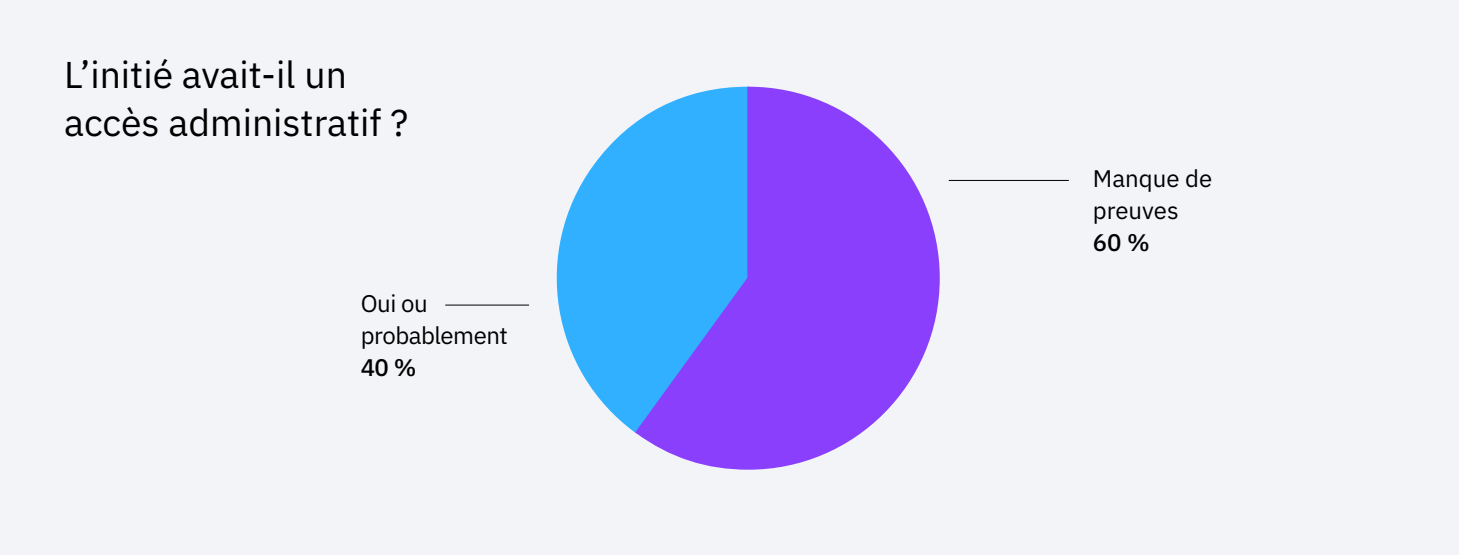
39 % des entreprises ont adopté une forme de PAM.[9] Cette adoption se traduit par une économie de 3,1 millions de dollars.

6. https://indaily.com.au/news/2018/10/23/harris-director-resigns-from-top-real-estate-post/
7. https://www.ibm.com/security/identity-access-management/privileged-access-management
8. https://www.ibm.com/security/zero-trust
9. https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/

L’accès administratif abusif est coûteux

Il existe de nombreux exemples de situations dans lesquelles des initiés ont abusé de leur pouvoir en tant qu’administrateurs dans des entreprises à des fins préjudiciables, par exemple par vengeance, par appât du gain ou avec d’autres intentions malveillantes. En février 2020, un ancien ingénieur de Microsoft, Volodymyr Kvashuk, a été reconnu coupable d’avoir utilisé son accès privilégié pour voler plus de 10 millions de dollars d’actifs numériques à l’entreprise.[10] L’accès administratif de Kvashuk a permis le vol sur la plateforme de vente au détail dont il était responsable.[11] Plus précisément, Kvashuk a utilisé les adresses e-mail de ses collègues et des comptes d’essai valides sur le système pour masquer son activité, notamment l’extraction de cartes cadeaux numériques. L’ingénieur a revendu sur Internet les cartes et autres actifs dérobés pour son profit personnel. Il a ensuite utilisé cet argent pour acheter une maison d’une valeur de 1,6 millions de dollars et une voiture Tesla coûtant 160 000 dollars.[12]

Accès administratif abusif en chiffres



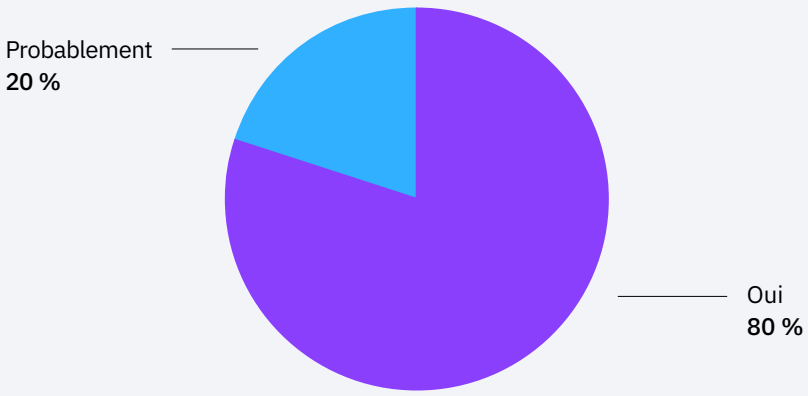
Dans 40 % des incidents auxquels X-Force a répondu entre 2018 et 2020, il a été confirmé que l’utilisateur interne disposait certainement ou probablement d’un accès administratif au réseau. Les analystes de X-Force ont déterminé le type d’accès d’initié en fonction des détails de l’incident lorsque le rôle spécifique de l’utilisateur n’était pas fourni par le client.

10. https://www.justice.gov/usao-wdwa/pr/former-microsoft-software-engineer-sentenced-nine-years-prison-stealing-more-10-million
11. https://apnews.com/article/seattle-retail-sales-james-robart-13f5a86053533b40034246ef37ecad8d
12. https://www.redmond-reporter.com/news/former-microsoft-employee-convicted-of-18-federal-felonies/

Ces incidents ont impliqué notamment l'exfiltration de données, la divulgation et la suppression de données sensibles, ainsi que l'installation de logiciels non autorisés. Plus précisément, certaines organisations ont perdu des pétaoctets de journaux supprimés des serveurs, ont subi des fuites intentionnelles de code source ou des pannes coûteuses en raison des agissements d'un initié ayant un accès administratif.

Plus intéressant encore, dans 100 % des incidents pour lesquels il a été confirmé que l'initié avait probablement ou certainement un accès administratif, cet accès privilégié a joué un rôle dans l'incident lui-même. (Voir le graphique ci-dessous.)

Le niveau d'accès privilégié au réseau a-t-il joué un rôle dans l'incident impliquant un initié ?



En d'autres termes, si l'initié n'avait pas disposé d'un accès administratif, l'impact de l'incident sur l'entreprise aurait été moindre ou, dans de nombreux cas, l'incident ne se serait tout simplement pas produit. X-Force a répondu à plusieurs incidents impliquant des initiés dans le cadre desquels des bases de données et des journaux essentiels ont été supprimés des serveurs. Si l'initié n'avait pas bénéficié d'un accès administratif à ces systèmes, l'incident n'aurait pas eu lieu.

Recommandations

X-Force considère que le nombre d'incidents liés à des initiés est sous-représenté dans les données de tiers. Il est probable qu'encore plus d'incidents de cette nature sont gérés en interne par les organisations sans être rendus publics par crainte d'engager la responsabilité de l'entreprise ou de porter atteinte à sa réputation.[13]

Les recherches et les données de X-Force soulignent la nécessité de considérer les menaces internes potentielles comme une composante importante d'un programme de sécurité de l'information en raison de l'impact que ces incidents peuvent avoir sur une organisation. Plus précisément, IBM Security émet les recommandations suivantes en ce qui concerne les menaces internes :

Les stratégies de défense en profondeur permettent de détecter les menaces internes.

Traditionnellement, on considère qu'une approche à plusieurs niveaux appliquée aux technologies et processus mis en œuvre par les organisations traite les menaces externes. Toutefois, la recherche X-Force indique que beaucoup de ces outils, y compris les solutions de gestion des informations et des événements de sécurité (SIEM), ont aussi joué un rôle essentiel dans la détection des menaces internes.

Comprenez ce qui est normal dans votre environnement.

La meilleure façon de détecter une activité suspecte, quel que soit le type d'attaquant, consiste à comprendre quel type d'activité est considéré comme normal au sein de votre réseau. S'assurer de posséder une bonne compréhension de l'activité de référence facilite la détection et le traitement rapides et efficaces des comportements anormaux. Une solide solution d'analyse du comportement des utilisateurs (UBA) peut fournir cette capacité et suivre les modifications de votre environnement dans le temps.

Examinez régulièrement les accès administratifs.

X-Force a découvert que plusieurs incidents impliquant des initiés administrateurs étaient probablement dus au fait que les utilisateurs disposaient de trop de privilèges. En matière d'accès administratif, un contrôle rigoureux des changements et des processus doit être mis en œuvre, en particulier sur les serveurs critiques. Envisagez des solutions technologiques qui accordent un accès administratif temporaire aux systèmes et fonctions sensibles et qui consignent ces autorisations.

13. https://www.darkreading.com/edge/theedge/fbi-encounters-reporting-an-insider-security-incident-to-the-feds-/b/d-id/1340016

Séparez vos équipes de sécurité des informations et d'administration informatique.

L'expérience de X-Force démontre qu'une approche équilibrée de la gestion de l'indépendance et de la gouvernance des équipes de sécurité et d'administration favorise une meilleure sécurité. Elle permet aussi aux équipes administratives d'avoir la flexibilité et la créativité nécessaires pour optimiser leur exploration et découverte des menaces tout en assurant à l'entreprise une supervision et une surveillance suffisantes pour minimiser les risques au sein de l'équipe.

Créez des profils de risque pour les rôles sensibles dans l'entreprise.

Puisqu'un accès privilégié a joué un rôle dans de nombreux incidents liés à des initiés auxquels X-Force a dû répondre, nous recommandons aux organisations d'envisager d'établir des profils de risque pour les postes ayant un accès administratif ou sensible aux systèmes ou données dans l'entreprise. La mise en œuvre d'une solution de gestion des accès privilégiés (PAM), qui s'articule autour d'un modèle Zero Trust, permet de limiter l'accès des utilisateurs et pourrait minimiser l'impact des incidents dus à des initiés.

Mettez à jour votre manuel de réponse aux incidents pour y inclure les menaces internes.

Une formation générale n'est pas suffisante pour ces incidents. Si la plupart des manuels de réponse aux incidents tiennent compte d'attaques externes, les organisations devraient envisager d'ajouter des scénarios de menaces internes accidentelles ou malveillantes. Envisagez de recourir à un partenaire susceptible de vous aider à développer des plans de réponse aux incidents et des manuels spécifiques afin de mieux vous préparer aux cyberattaques et d'y répondre.

Formez continuellement vos employés.

De nombreux programmes de formation annuels d'entreprise incluent les pratiques commerciales éthiques ainsi qu'une formation sur la manipulation sociale. Beaucoup des incidents auxquels X-Force a répondu ont été découverts par d'autres employés et non par la technologie. Les formations annuelles sur l'éthique commerciale ou la manipulation sociale des entreprises doivent expliquer aux employés comment signaler qu'ils soupçonnent un incident interne. La formation des employés basée sur les rôles ayant un accès privilégié peut également aider ces employés à reconnaître les signes révélateurs d'une anomalie de fonctionnement dans leur environnement.

Appuyez-vous sur des services d'information sur les menaces fiables.

Pour les clients, le défi consiste souvent à créer, gérer et rendre opérationnels les renseignements sur les menaces. Recherchez une solution permettant l'agrégation, l'automatisation et les intégrations requises pour rendre les renseignements sur les menaces opérationnels à grande échelle.

Les services de détection et de réponse gérés fournissent une protection ininterrompue.

Les services de sécurité par détection et réponse gérées (MDR) sont essentiels pour prévenir les menaces internes, les détecter et y répondre rapidement. Les solutions qui vont au-delà de la prévention traditionnelle au moyen d'un antivirus de nouvelle génération pour un blocage basé sur le comportement, des enquêtes et une gestion continue des politiques sont essentielles.

Découvrez comment IBM Security aide ses clients à sécuriser les environnements les plus complexes et critiques contre les menaces externes et internes.

En savoir plus sur IBM Security

IBM Security

Compagnie IBM France
17 avenue de l'Europe
92275 Bois-Colombes Cedex

Produit aux États-Unis d'Amérique
Mai 2021

IBM