KEEPER®

L'avenir de la défense

Les responsables informatiques se préparent à faire face à des cybermenaces sans précédent

March 2024

Les cyberattaques sont plus sophistiquées que jamais et les responsables informatiques se sentent mal équipés pour faire face aux nouvelles menaces

Une enquête mondiale menée en 2024 par Keeper Security en partenariat avec TrendCandy Research auprès de plus de 800 responsables informatiques et de la sécurité révèle que les cyberattaques gagnent en sophistication grâce à de nouvelles menaces liées à l'intelligence artificielle (IA) et à des techniques d'attaque avancées et émergentes. Tout en faisant face à ces nouvelles menaces, les responsables informatiques doivent également gérer un volume croissant d'attaques. En effet, 92 % des personnes interrogées indiquent que les cyberattaques sont plus fréquentes aujourd'hui qu'elles ne l'étaient il y a un an. En 2024, la sécurité s'avère de plus en plus complexe avec les enjeux plus importants que jamais.

Keeper Security, le principal fournisseur de logiciels de cybersécurité Zero-Trust et Zero-Knowledge protégeant les mots de passe, les clés d'accès, les accès à privilèges, les secrets et les connexions à distance, a voulu cartographier le paysage de la cybersécurité en 2024. Keeper a demandé à une agence de recherche indépendante de recueillir les points de vue des responsables de la sécurité dans le monde entier sur les tendances en matière de cybersécurité et sur l'avenir de la défense.

Les cyberattaques sont plus fréquentes et de plus en plus sophistiquées

Avec l'évolution rapide des menaces, les nouvelles réglementations, les progrès tels que les clés d'accès et la prolifération d'appareils (des ordinateurs de bureau aux casques d'informatique spatiale), la cybersécurité est plus critique que jamais. Une écrasante majorité (92 %) des responsables informatiques et de la sécurité déclarent que la cybersécurité est leur priorité numéro un.

Ces dirigeants ne peuvent pas se permettre de se déconcentrer, car 92 % des personnes interrogées révèlent également qu'elles ont constaté une augmentation des cyberattaques d'une année sur l'autre. Les cybercriminels font preuve de créativité et d'acharnement dans leur mission visant à briser les solutions sécurisées historiques et à infliger un maximum de dommages aux organisations vulnérables.

L'impact des cyberattaques augmente avec leur volume : 73 % des personnes interrogées ont subi une cyberattaque qui a entraîné une perte financière. L'impact financier direct est l'une des nombreuses conséquences d'une cyberattaque réussie, au même titre que l'interruption de l'activité, la perte durable de revenus, l'attrition de la clientèle et des partenaires, et la réputation ternie.

Les responsables informatiques identifient les parties de leur organisation qui ont fait l'objet d'attaques

KEEPER

Alors que les incidents de cybersécurité sont de plus en plus fréquents et coûteux, 95 % des responsables informatiques déclarent que les cyberattaques sont également plus sophistiquées que jamais, et qu'ils ne sont pas préparés à cette nouvelle vague de vecteurs de menaces.

95%

des responsables informatiques déclarent que les cyberattaques sont également plus sophistiquées que jamais

Selon les personnes interrogées, les nouveaux types d'attaques les plus graves sont les suivants

1. Attaques basées sur l'IA
2. Technologie Deepfake
3. Attaques de la chaîne d'approvisionnement
4. Cloud Jacking
5. Attaques de l'Internet des objets (IoT)
6. Exploitation des réseaux 5G
7. Attaques sans fichier

KEEPER

Vecteurs d'attaque : les responsables informatiques se sentent mal équipés pour les contrer

35% Attaques basées sur l'IA

30% Technologie Deepfake

29% Exploitations des réseaux 5G

25% Cloud Jacking

23% Attaques sans fichier

Les attaques basées sur l'IA sont considérées comme le vecteur de menace émergente le plus grave et le plus difficile à gérer. Les acteurs malveillants utilisent l'IA pour accélérer et développer des techniques d'attaque courantes telles que le phishing et le craquage de mot de passe. Cette situation met en évidence la nécessité d'une approche proactive de la cybersécurité, qui combine des mécanismes de défense avancés et les bonnes pratiques de base pour atténuer et combattre les menaces en constante évolution.

Au niveau mondial, les responsables informatiques prévoient d'augmenter leur sécurité globale en matière d'IA par le biais des mesures suivantes

Chiffrement des données

51%

Formation et sensibilisation des employés

45%

Systèmes de détection des menaces avancés

41%

Alors que les cybermenaces continuent de s'aggraver et d'évoluer, les responsables informatiques doivent adapter leurs tactiques et leurs stratégies, en utilisant une approche multicouche de la sécurité, afin de garder une longueur d'avance.

Les vecteurs d'attaque actuels ne montrent aucun signe de ralentissement

Alors que les nouvelles menaces se profilent à l'horizon, les responsables informatiques doivent lutter contre les vecteurs d'attaque les plus courants, notamment

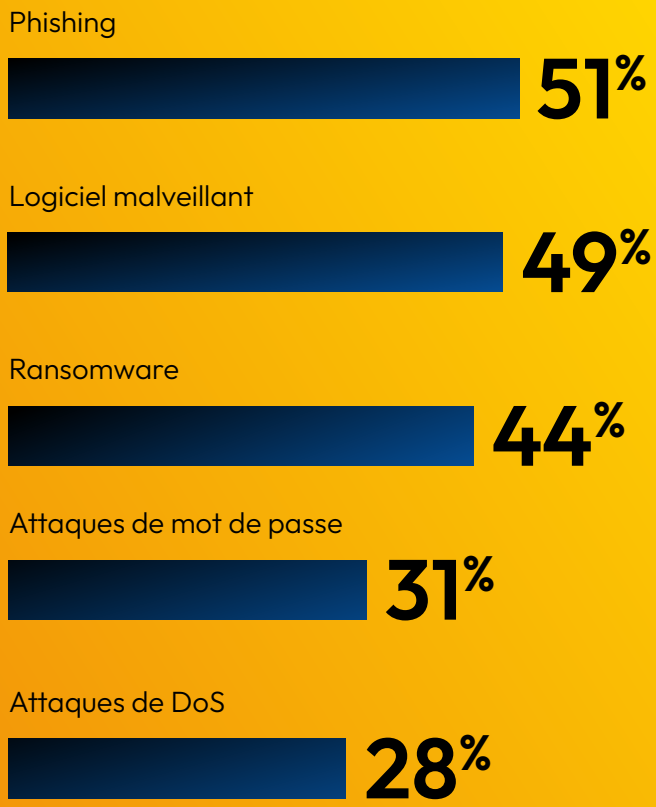
61%	59%	49%	38%	37%
Phishing	Logiciel malveillant	Ransomware	Attaques de mot de passe	Attaques de DoS

Les mots de passe et les identifiants volés ou faibles restent une des principales causes des violations. Cinquante-deux pour cent des personnes interrogées ont déclaré que l'équipe informatique de leur entreprise était confrontée au problème des mots de passe fréquemment volés, ce qui souligne l'importance de créer et de stocker en toute sécurité des mots de passe forts et uniques pour chaque compte.

Pour éviter que des identifiants ne tombent entre les mains d'acteurs malveillants, 72 % des entreprises surveillent le Dark Web à la recherche d'identifiants d'employés volés. Un service de surveillance du Dark Web permet aux organisations de se tenir au courant des informations relatives aux comptes et de prendre des mesures immédiates en cas de compromission des identifiants. L'adoption d'un gestionnaire de mots de passe dédié peut aider à résoudre ces deux problèmes de front, en offrant le plus haut niveau de chiffrement et de fonctionnalités telles que des analyses et des alertes sur le Dark Web.

KEEPER

Les cyberattaques se multiplient, selon les responsables informatiques



Aujourd'hui, une écrasante majorité (67 %) des entreprises luttent contre les attaques de phishing. L'explosion des outils d'IA a intensifié ce problème en augmentant la crédibilité des escroqueries par phishing et en permettant aux cybercriminels de les déployer à grande échelle. Quatre-vingt-quatre pour cent des personnes interrogées ont déclaré que le phishing et le smishing sont devenus plus difficiles à détecter avec la popularité croissante des outils alimentés par l'IA, et ont révélé que le phishing alimenté par l'IA est leur principale préoccupation (42 %) en matière de sécurité de l'IA.

Qui est à l'origine des attaques et qui est le plus exposé ?

Aujourd'hui, les trois sources les plus courantes de cyberattaques sont les suivantes :

Pirates indépendants

Groupes d'hacktivistes

Agents d'espionnage d'entreprise

Si de nombreuses attaques sont le fait de pirates indépendants ou de groupes d'hacktivistes à des milliers de kilomètres, elles peuvent également se produire dans l'arrière-cour d'une organisation : **40 % des personnes interrogées ont déclaré avoir subi une cyberattaque provenant d'un employé.** Cela souligne l'importance de déployer une technologie qui prévient les menaces internes intentionnelles et non intentionnelles.

Une solution de gestion des accès à privilèges (PAM) aide les administrateurs informatiques et le personnel de sécurité à gérer et à sécuriser les identifiants à privilèges et à appliquer le principe du moindre privilège. Si un cybercriminel parvient à accéder aux réseaux d'une organisation, les plateformes PAM minimisent le rayon d'action en empêchant les mouvements latéraux.

Qui est le plus exposé aux menaces externes ? Les cybercriminels sont attirés par les transactions monétaires et les informations personnelles sensibles qui peuvent être exploitées dans certains secteurs

Les trois secteurs les plus fréquemment piratés sont les suivants

Hôtellerie/Voyages

Des attaques se produisent chaque semaine, le ransomware et le logiciel malveillant étant les types de cyberattaque les plus courants

Fabrication

Des attaques ont lieu chaque semaine, le phishing et le logiciel malveillant étant les types de cyberattaque les plus courants

Services financiers

Des attaques ont lieu tous les mois, le phishing et le logiciel malveillant étant les types de cyberattaque les plus courants

Conclusion

Les attaques changent, mais les bonnes pratiques fondamentales en matière de cybersécurité ne changent pas

Les recherches de Keeper mettent en lumière les nouvelles façons dont les attaquants font des ravages dans les entreprises, les organisations de taille moyenne et les petites entreprises d'aujourd'hui. Avec les attaques alimentées par l'IA, les outils dans l'arsenal des cybercriminels deviennent de plus en plus sophistiqués. La technologie ne cessant de progresser, la lutte contre les menaces en constante évolution nécessite une adaptation permanente.

Malgré ce paysage de menaces en constante évolution, les règles fondamentales de la protection d'une organisation dans le paysage numérique restent pertinentes. Les organisations doivent donner la priorité à l'adoption de solutions qui préviennent les cyberattaques les plus répandues, notamment les solutions de mots de passe et de PAM. Un gestionnaire de mots de passe peut atténuer les risques en appliquant des pratiques strictes en matière de mot de passe, tandis que la PAM protège les ressources vitales d'une organisation en contrôlant et en surveillant l'accès de haut niveau, ce qui renforce collectivement les défenses et minimise les dommages potentiels en cas de cyberattaque réussie. L'intégration de ces solutions crée une approche de sécurité à plusieurs niveaux qui résiste à l'épreuve du temps, en limitant les accès non autorisés et améliorer la résilience globale de la cybersécurité – **aujourd'hui et à l'avenir.**