Octobre 2025

Étude de Marché

Rapport 2025 sur les violations de la sécurité des emails

L'expérience et l'impact des violations de la sécurité des e-mails sur les organisations du monde entier

Barracuda®
Your business, secured.

Sommaire

Introduction

Ce rapport explore l'expérience et l'impact des violations de la sécurité des emails sur les organisations du monde entier au cours des 12 derniers mois. Il s'appuie sur les résultats d'une enquête internationale menée par Barracuda et Vanson Bourne auprès de 2 000 décideurs en informatique et en sécurité. Les résultats se révèlent globalement cohérents entre les pays et les secteurs étudiés. Le rapport met donc l'accent sur les conclusions d'ensemble et sur celles liées à la taille des organisations.

Ces conclusions montrent que les violations de la sécurité des emails affectent la plupart des entreprises. Elles montrent comment la complexité croissante du paysage des menaces email, conjuguée à des défis internes tels que le manque de compétences et l'absence d'automatisation de la réponse aux incidents, complique pour les organisations la détection, la gestion et la récupération après une violation.

Des temps de réponse retardés peuvent laisser les entreprises vulnérables à d'autres attaques, telles que les ransomwares, et à des dommages plus étendus.

Les conséquences d'une violation de la sécurité des emails sont considérables, allant des temps d'arrêt aux atteintes à la réputation et à la perte d'activité. Les coûts de récupération touchent tout particulièrement les petites entreprises.

L'objectif de ce rapport est d'aider les organisations à mieux comprendre les risques et les implications des menaces de sécurité des emails, et de mettre en évidence les domaines où elles peuvent être vulnérables.

Méthodologie

Barracuda a chargé l'agence d'études de marché indépendante Vanson Bourne de mener une enquête mondiale auprès de 2 000 preneurs de décision de haut niveau en matière de sécurité, occupant des postes informatiques et commerciaux dans des organisations comptant entre 50 et 2 000 employés et issues d'un large éventail de secteurs aux États-Unis, au Royaume-Uni, en France, dans la région DACH (Allemagne, Autriche, Suisse), au Benelux (Belgique, Pays-Bas, Luxembourg), dans les pays nordiques (Danemark, Finlande, Norvège, Suède), en Australie, en Inde et au Japon. Le travail de terrain a été mené en avril et mai 2025.

Résultats clés

78%

des organisations ont subi une violation de la sécurité des emails au cours des 12 derniers mois

71%

des organisations ayant subi une violation de la sécurité des emails ont également été touchées par un ransomware au cours de l'année

41%

ont subi une atteinte à leur réputation, et beaucoup ont perdu de nouvelles opportunités commerciales, nuisant à la croissance

50%

ont détecté la violation en moins d'une heure

47%

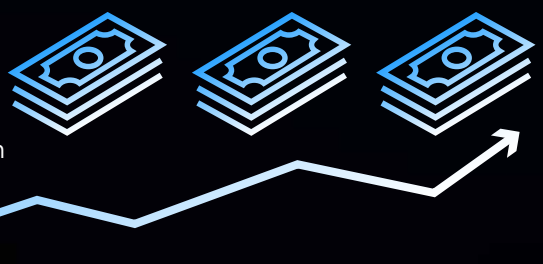
déclarent que les techniques d'évasion avancées sont le principal obstacle à une réponse aux incidents rapide

44%

affirment que le manque de réponse automatisée aux incidents retarde la détection, le confinement et l'élimination des menaces

217.068 USD

est le coût moyen de la réponse et de la récupération suite à une violation de la sécurité des emails



La plupart des entreprises subissent une violation de la sécurité des emails

L'enquête a révélé que 78 % des participants avaient subi une violation de la sécurité des emails au cours des 12 derniers mois.

Les victimes ont été touchées par un large éventail de types d'attaques, notamment le phishing et le spear phishing (par 27 % des victimes), la compromission de la messagerie professionnelle (24 %) et le piratage de compte (22 %).

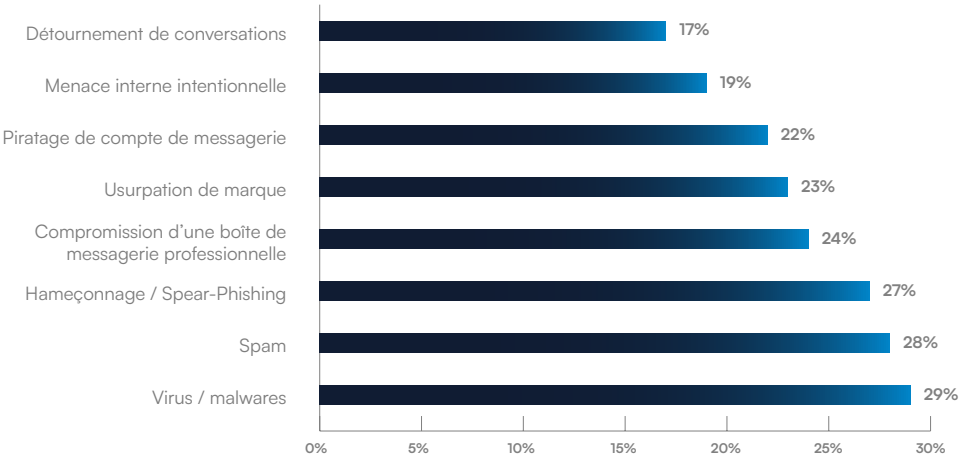


FIGURE 1

Parmi les types d'attaques par email suivants, quels sont ceux qui ont porté atteinte à votre organisation au cours des 12 derniers mois ?

Le paysage des menaces email est encore compliqué par le fait que de nombreux types d'attaques des emails sont interconnectés. Comprendre ces relations est essentiel pour bâtir des défenses efficaces.

Par exemple, le phishing agit souvent comme le point de violation initial, ouvrant la porte à des menaces plus avancées comme la compromission de la messagerie professionnelle (« Business Email Compromise » ou BEC), le piratage de compte et les ransomwares. Une fois les identifiants volés, les attaquants peuvent usurper l'identité d'utilisateurs internes pour rendre leurs emails plus fiables et augmenter la probabilité d'une compromission supplémentaire. Les techniques de spoofing renforcent l'efficacité du phishing et de la BEC en imitant des expéditeurs de confiance. En parallèle, le malware introduit par le phishing peut automatiser le processus d'attaque, récolter davantage d'identifiants et se propager sur le réseau.

La BEC est une menace ciblée et financièrement motivée. Les pirates usurpent l'identité de personnes ou d'entités de confiance pour inciter les employés à transférer de l'argent ou des informations sensibles. La livraison de malware et de ransomware est facilitée par des emails phishing contenant des pièces jointes ou des liens malicieux.

L'usurpation d'identité et le spoofing sont des techniques utilisées pour tromper les destinataires afin qu'ils fassent confiance à l'expéditeur. Ces tactiques sont couramment employées dans les campagnes de phishing, de BEC et de malware, Les pirates peuvent faire du spoofing de nom d'affichage, de domain ou utiliser des domaines sosies pour imiter des contacts légitimes, augmentant les chances que leurs messages soient ouverts et pris en compte.

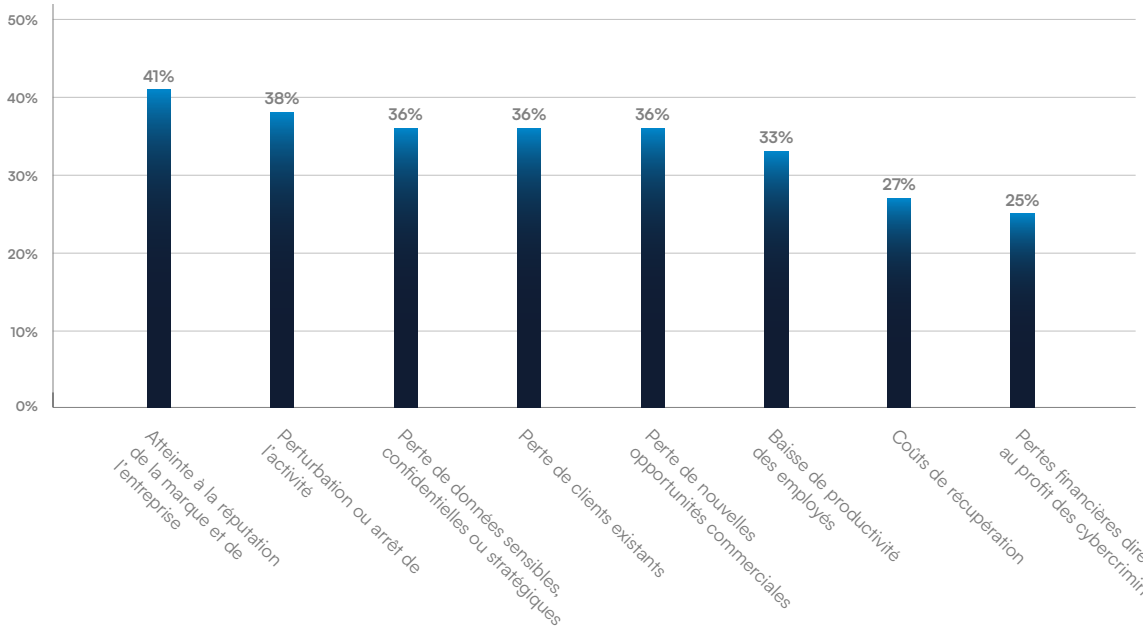
Tous les types de menaces email gagnent en complexité, en sophistication et en portée. De nombreuses campagnes de phishing les plus répandues sont développées et déployées à grande échelle par des plateformes disposant de ressources importantes. Les dommages que ces attaques peuvent causer sont considérables.

Une faille de sécurité des emails met en péril la croissance de l'entreprise

Selon les organisations interrogées, la conséquence la plus fréquente d'une faille de sécurité des emails est l'atteinte à la marque et à la réputation (citée par 41 % des personnes interrogées). Viennent ensuite les conséquences opérationnelles, notamment les temps d'arrêt et les interruptions d'activité (38 %), ainsi que la baisse de la productivité des employés (36 %). Plus d'un tiers (36 %) ont perdu des données sensibles et environ un quart ont perdu de nouvelles affaires (27 %) et des clients (25 %).

FIGURE 2

Quelles ont été les conséquences globales des violations de la sécurité des emails sur votre organisation ?



Les conséquences d'une atteinte à la réputation peuvent aller bien au-delà de la perception publique à court terme et avoir un impact profond et durable sur la santé financière, la situation juridique et l'orientation stratégique d'une entreprise.

L'impact sur les opérations commerciales et la productivité, ainsi que les pertes financières, la perte de données (en particulier si cela entraîne des violations de conformité et contractuelles), le vol de propriété intellectuelle et l'érosion de la confiance peuvent entraîner une perte de clients existants et de nouvelles opportunités commerciales. Cela a un impact tangible sur la croissance des revenus.

Il peut être difficile de chiffrer l'impact à long terme, mais il est possible de quantifier le coût de la réponse et de l'atténuation d'une violation de la sécurité des emails.

Le coût de la résolution d'une violation de la sécurité des emails touche plus durement les petites entreprises

Une violation de la sécurité des emails coûte en moyenne 217 068 $ à corriger, les petites entreprises étant touchées de manière disproportionnée.

L'enquête a porté sur des entreprises de 50 à 2 000 employés. Le coût moyen des mesures d'atténuation était de 145 921 $ pour les entreprises de 50 à 100 employés. Pour celles de 1 000 à 2 000 employés, le coût moyen était de 364 132 $.

Cela signifie que le coût moyen de récupération par employé pour les petites organisations (50 à 100 employés) est de 1 946 $, comparé à un coût moyen de récupération par employé de seulement 243 $ pour les grandes entreprises (1 000 à 2 000 employés).

	50 à 100 employés	101 à 250 employés	251 à 500 employés	501 à 1,000 employés	1,001 à 2,000 employés
Coût moyen par organisation pour atténuer la violation de la sécurité des emails la plus coûteuse au cours des 12 derniers mois	145 921 $	157 804 $	155 804 $	300 751 $	364 132 $
Le coût moyen par employé pour atténuer la violation de sécurité des e-mails la plus coûteuse au cours des 12 derniers mois	1 946 $	898 $	415 $	400 $	243 $

Les grandes organisations peuvent avoir de meilleures défenses et davantage de ressources en termes de compétences et de personnel pour détecter et répondre aux incidents de sécurité. Cela les rend mieux équipées pour faire face aux violations rapidement et efficacement, garantissant que chaque incident est moins coûteux par rapport à leur taille globale. Les petites organisations sont bien plus exposées.

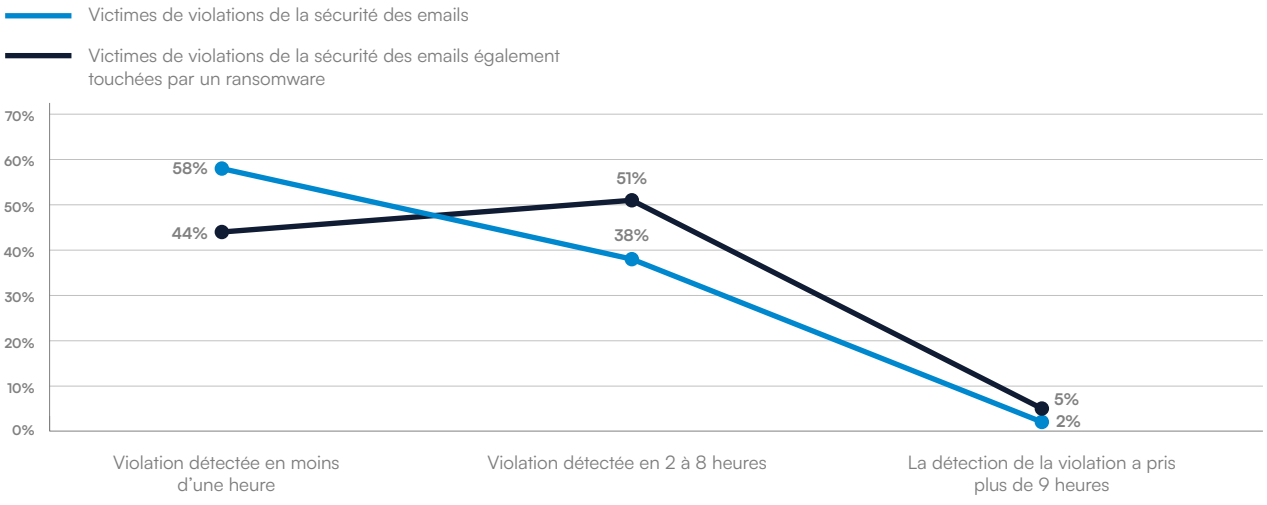
La capacité à détecter et à répondre rapidement aux menaces de sécurité est essentielle pour réduire l'exposition aux risques.

Les retards dans la détection et la réponse aux violations d'emails accroissent le risque d'attaques par ransomware

Il existe une corrélation entre le temps qu'il faut à une organisation pour détecter et atténuer une violation de la sécurité des emails et les chances d'être également touchée par un incident de Ransomware.

FIGURE 3

Temps moyen nécessaire pour détecter une violation de la sécurité des emails



Les recherches montrent que 71 % des organisations ayant subi une violation de la sécurité des e-mails signalent également avoir été touchées par un ransomware au cours des 12 derniers mois.

Cela pourrait être dû au fait que de nombreuses attaques par ransomware commencent par un email phishing apparemment anodin qui donne aux pirates un point d'entrée (par le biais d'identifiants volés ou d'un point d'accès compromis) et un canal pour livrer un ransomware et d'autres charges malicieuse par le biais de pièces jointes et de liens.

Si une violation de la sécurité des emails n'est pas détectée et contenue rapidement et efficacement, la chaîne d'attaque a le temps de se déployer. Les pirates peuvent ainsi voler des données, chiffrer des fichiers ou établir un accès persistant au réseau.

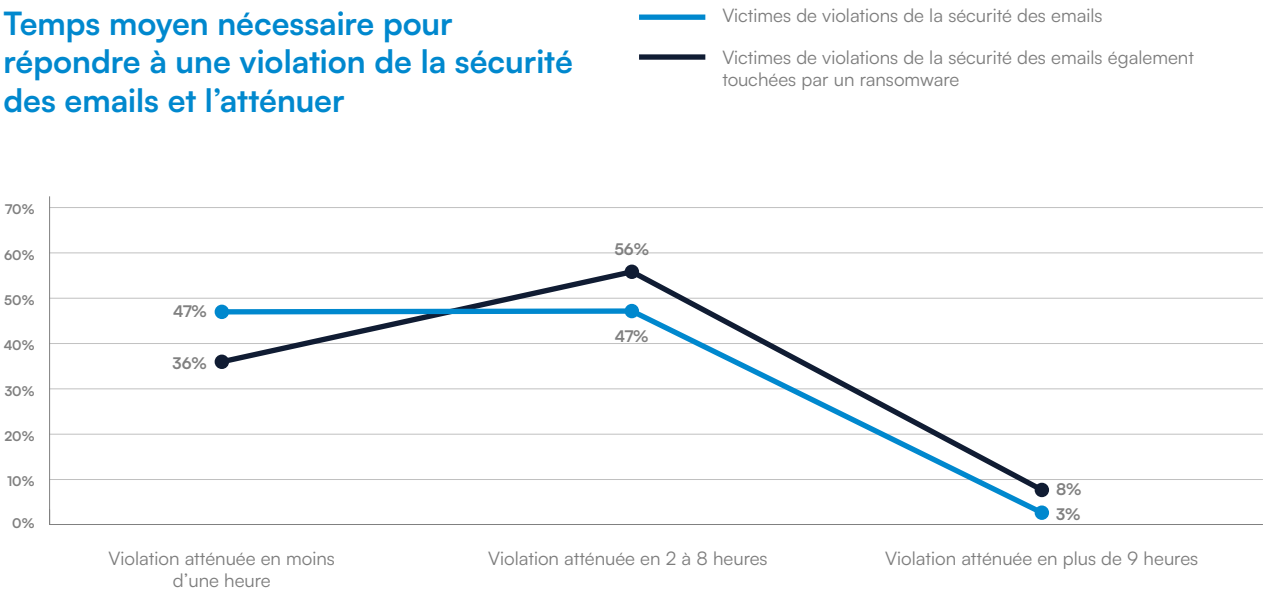
Les résultats montrent que les organisations qui ont mis plus de temps à détecter et à atténuer une violation d'email avaient une probabilité plus élevée d'être également touchées par un ransomware :

- 58 % des victimes de violations d'emails non touchées par un ransomware ont mis moins d'une heure à détecter la violation.
- Un peu moins de la moitié (47 %) ont atténué la menace dans l'heure suivant la détection.

- Toutefois, pour les victimes qui ont également subi un incident lié à un ransomware, la détection et l'atténuation ont souvent pris plus de temps : 51% ont mis entre deux heures et un jour ouvrable complet pour détecter la violation, et 56% ont mis entre deux et huit heures après la détection pour atténuer la menace.
- En bref : 64 % des victimes de ransomware mettent plus de deux heures à corriger une violation de la sécurité des emails.

FIGURE 4

Temps moyen nécessaire pour répondre à une violation de la sécurité des emails et l'atténuer



Ces conclusions soulignent l'importance de disposer de capacités efficaces de sécurité, de détection et de réponse aux menaces email dans le cadre d'une stratégie de cyberdéfense globale.

La réponse aux violations est entravée par la complexité des attaques, les facteurs humains et le manque d'automatisation

Il n'est pas toujours facile de réagir rapidement et efficacement à une violation de la sécurité des emails. L'enquête met en évidence les obstacles qui peuvent se dresser en chemin. Ces obstacles se répartissent en trois catégories : la complexité des attaques, les facteurs humains et les limites des outils de sécurité.

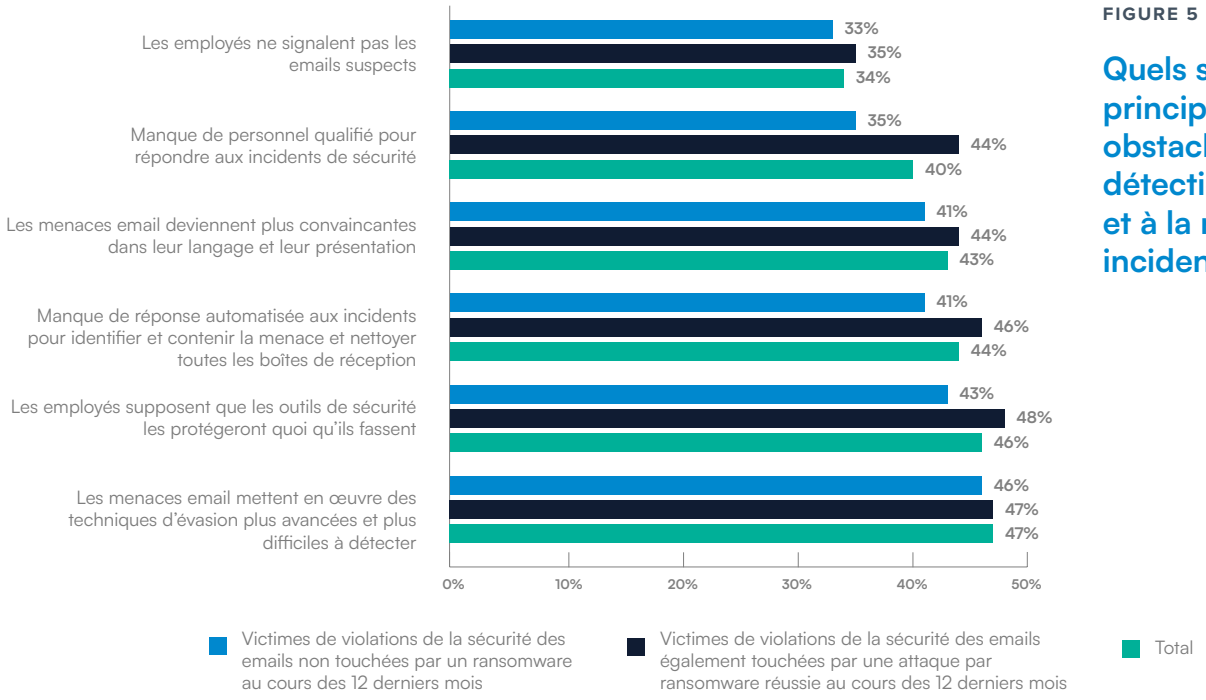


FIGURE 5

Quels sont les principaux obstacles à la détection rapide et à la réponse aux incidents

Les obstacles les plus cités dressent un tableau clair de la complexité croissante des menaces email et des défis internes auxquels les organisations sont confrontées pour y répondre efficacement une fois que les pirates ont réussi à franchir les défenses.

Sophistication des attaques

- Cité par 47 % des victimes de violations de la sécurité des emails, le plus grand obstacle à une réponse rapide aux incidents est la nature évolutive et de plus en plus évasive des menaces email, ce qui les rend plus difficiles à repérer et à supprimer des boîtes de réception une fois qu'elles réussissent à y accéder.
- Le problème est aggravé par la sophistication croissante des emails phishing eux-mêmes. Les pirates créent des messages au langage soigné, contextuellement pertinents et visuellement convaincants, imitant souvent des communications internes ou les marques de confiance. Selon 43 % des répondants, cela rend plus difficile pour les utilisateurs et les outils de sécurité de distinguer les emails malicieux des légitimes.

Le facteur humain

- Les conclusions suggèrent un niveau de complaisance parmi les employés, 46 % des participants déclarant que leurs collègues supposent que les outils de sécurité les protégeront quoi qu'il arrive.
- Environ un tiers (34 %) déclarent que les employés ne signalent pas les emails suspects. Cela peut également permettre aux menaces de persister dans les boîtes de réception, et peut être un signe que les employés ne savent pas à qui signaler ces emails suspects.
- Ces deux facteurs peuvent être abordés par la formation de sensibilisation à la sécurité, les incitations, les retours d'information, des mécanismes de signalement simplifiés et en favorisant une culture de sensibilisation proactive à la cybersécurité.

Outils de sécurité

- Le manque de capacités de réponse automatisée aux incidents est un obstacle important pour 44 % des participants à l'enquête. Sans outils automatisés capables d'identifier, d'isoler et de remédier rapidement aux menaces dans les boîtes de réception des utilisateurs, les équipes de sécurité sont contraintes à effectuer des processus manuels chronophages et sujets aux erreurs. Ce retard donne aux pirates plus de temps pour exploiter la violation, élever leurs privilèges ou se déplacer latéralement dans le réseau.

Pénurie de compétences

- Une pénurie de personnel de sécurité qualifié est un défi pour 40 % des répondants.
- C'est le domaine où l'écart entre les organisations qui ont également été touchées par une attaque par ransomware réussie et celles qui n'ont pas été affectées est le plus grand : 44 % des entreprises qui ont été victimes des deux types d'attaques ont signalé cela comme un obstacle, contre 35 % de celles non touchées par un ransomware. Si les organisations manquent d'expertise ou de capacité pour répondre efficacement à une violation détectée, cela peut conduire à un confinement retardé ou à une correction incomplète, permettant aux pirates de rester dans le réseau et de poursuivre leur attaque.

Conclusion

Le large éventail de menaces email ciblant les entreprises, les impacts tangibles, les coûts importants et la complexité croissante du paysage des cybermenaces soulignent l'importance de faire de la sécurité des emails une partie intégrante des stratégies de cyberdéfense basées sur des plateformes.

Une approche holistique de la sécurité des emails devrait allier les technologies de détection avancées alimentées par l'IA à l'éducation des utilisateurs, la réponse automatisée et une culture de sécurité forte.

Les conseils suivants peuvent être utiles :

Soutenir les employés

1. **Formez régulièrement vos employés** à reconnaître le phishing, le social engineering et les comportements suspects dans les emails.
2. **Facilitez le signalement des emails suspects par les employés** et assurez-vous que les signalements sont acheminés vers la bonne équipe pour une enquête et un triage rapides.
3. **Limiter l'accès aux systèmes et aux données sensibles**, en fonction des rôles professionnels. Cela minimise l'impact du vol d'identifiants et des mouvements latéraux suite à une compromission par email.

Outils de sécurité

4. **Mettez en œuvre l'authentification multifacteur (MFA)** pour les emails et vos autres systèmes critiques. Même si les identifiants sont volés par phishing, la MFA ajoute une défense robuste contre les accès non autorisés.
5. **Déployez des solutions de sécurisation des emails qui utilisent l'IA/ML** pour détecter le phishing, les malwares et les tentatives d'usurpation d'identité. Ces outils doivent être capables d'analyser le comportement de l'expéditeur, le contenu des messages et les pièces jointes en temps réel.
6. **Mettez en œuvre des protocoles d'authentification des emails conformes aux normes de l'industrie tels** que SPF, DKIM et DMARC pour vérifier l'identité de l'expéditeur et prévenir le spoofing. Ces protocoles aident à garantir que seuls les expéditeurs autorisés peuvent utiliser votre domaine.
7. **Automatisez la réponse aux incidents** à l'aide d'outils qui peuvent automatiquement identifier et mettre en quarantaine les email malicieux après livraison, les supprimer des boîtes de réception et lancer des flux de travail de confinement. Cela réduit le temps de présence des pirates et limite l'exposition.

Mesures à plus long terme

8. **Exploitez les flux de renseignements sur les menaces** pour rester au courant des menaces email émergentes, des domaines malicieux et des tactiques d'attaque. Intégrez ces données à vos systèmes de détection généraux et votre plateforme de sécurité.

9. **Effectuez des audits périodiques** des configurations de sécurité des emails et simulez des scénarios d'attaque (par exemple, phishing, BEC) pour tester vos capacités de détection et de réponse.
10. **Comprenez les exigences réglementaires et répondez-y** en veillant à avoir en place les mesures de sécurité des emails nécessaires pour une détection, une réponse et une protection des données robustes. Cela aidera également à respecter les exigences en matière de cyberassurance.

Dans le paysage actuel, où les menaces sont à la fois dynamiques et interconnectées, la sécurité des emails ne consiste plus simplement à bloquer le spam ou le phishing : elle vise à empêcher le premier domino de tomber, celui qui pourrait déclencher une cascade menant à la paralysie opérationnelle, à la perte de données, à une atteinte à la réputation et à des impacts commerciaux durables.

Barracuda en quelques mots

Barracuda est une entreprise mondiale de cybersécurité de premier plan qui offre une protection complète contre les menaces complexes aux entreprises de toutes tailles. Notre plateforme BarracudaONE alimentée par l'IA protège les e-mails, les données, les applications et les réseaux grâce à des solutions innovantes, à une plateforme XDR gérée et à un tableau de bord centralisé afin de maximiser la protection et de renforcer la cyber-résilience. Forte de la confiance de centaines de milliers de professionnels de l'informatique et de fournisseurs de services gérés dans le monde entier, Barracuda propose des défenses puissantes, faciles à acheter, à déployer et à utiliser.

À propos de Vanson Bourne

Vanson Bourne est un cabinet indépendant spécialiste des études de marché pour le secteur des technologies. Sa réputation de produire des analyses solides, fiables et basées sur des études est elle-même fondée sur des principes rigoureux ainsi que sur sa capacité à interroger des décisionnaires majeurs qui occupent des fonctions techniques et métier dans tous les secteurs et sur les marchés principaux. Pour plus d'informations, accédez à vansonbourne.com.