44 % DES ENTREPRISES FRANÇAISES PRÉOCCUPÉES PAR LES ATTAQUES DE PHISHING EN 2024

Paris, 04 juillet 2024

La cybercriminalité ne cesse d'augmenter et de se diversifier depuis plusieurs années : rançongiciels, fraudes, deepfake… Les exemples d'attaques en ligne sont de plus en plus nombreux et difficiles à détecter.

Pour faire face à ces cyberattaques, les entreprises se doivent de se protéger en utilisant différentes solutions.

Quelles cybermenaces les entreprises françaises appréhendent-elles pour 2024 ? Quelles sont celles auxquelles elles ont été confrontées au cours de l'année écoulée ? Quelles mesures ont-elles mises en place ? Afin de répondre à ces questions, plus de 2000 employés travaillant à temps plein au sein de structures déployant des mesures de cybersécurité ont ainsi été interrogés.

Ces risques qui préoccupent les entreprises en 2024

Dans le top 3 des préoccupations, les attaques de phishing se retrouvent en première place (pour 44 % des répondants). Derrière des communications d'apparence plus vraies que nature se cache parfois une cybermenace difficile à détecter, et ces dernières peuvent facilement passer pour une communication officielle d'entreprise. L'objectif de cette attaque est simple : inciter les utilisateurs à télécharger des logiciels malveillants ou à partager des informations et données sensibles.

Mentionnées en seconde position (34 %), les attaques par intelligence artificielle visent à reproduire le style et l'identité visuelle d'une marque quasi parfaitement, de sorte à les rendre presque indétectables pour l'œil humain.

Enfin, et en troisième position (32 %), sont mentionnées les attaques dites de "compromission du courrier électronique professionnel", aussi connue sous le terme "d'arnaque au président". Ces menaces consistent à tromper les employés d'une entreprise pour contourner les mesures de sécurité en place. En usurpant l'adresse

email par exemple d'un responsable, le pirate peut amener un salarié à faire des transferts d'argent ou encore à divulguer des informations confidentielles.

Violations des données, plus d'un quart des entreprises sont touchées

En 2023, ce sont 29 % des entreprises françaises qui ont été victimes d'une violation des données.

Bien que la plupart (51 %) de ces violations soient externes à l'entreprise, on constate cependant que des négligences en interne ont aussi lieu, telles que des données en ligne non sécurisées (selon 41 % des répondants), ou des actes malveillants menés directement par des employés (19 %).

Emails de phishing, 60 % des employés ont admis avoir eu des pratiques à risque

Parmi les répondants, 72 % affirment que leur entreprise a déjà été exposée à une menace de phishing par email :

- 21 % ont directement reçu un e-mail frauduleux,
- 36 % ont reçu ou ont connaissance d'autres collaborateurs ayant reçu un e-mail frauduleux,
- 15 % ont été informés de collaborateurs ayant reçu un e-mail frauduleux.

Cependant, la prudence au sein des collaborateurs ne semble pas être de mise. En effet, 60 % des employés dont l'entreprise a été exposée à une menace de phishing déclarent eux-mêmes (ou plusieurs de leurs collaborateurs) avoir cliqué auparavant sur un lien malveillant contenu dans un e-mail.

Attaques de ransomware, des entreprises de plus en plus exposées

Parmi les menaces pouvant affecter les entreprises, les attaques de ransomware sont plus récentes et ont pour but de verrouiller et encrypter les données, fichiers, ou systèmes d'une entreprise, les rendant inaccessibles et inutilisables jusqu'à ce qu'un paiement soit effectué.

Lors de cette étude, 45 % ont déclaré que leur entreprise a été victime d'une ou de plusieurs attaques de ransomware. Certaines d'entre elles effectuent un paiement afin de récupérer leurs informations et données sensibles, cédant ainsi à la demande des pirates. Pourtant, rien ne garantit la récupération de leurs informations : 14 % déclarent

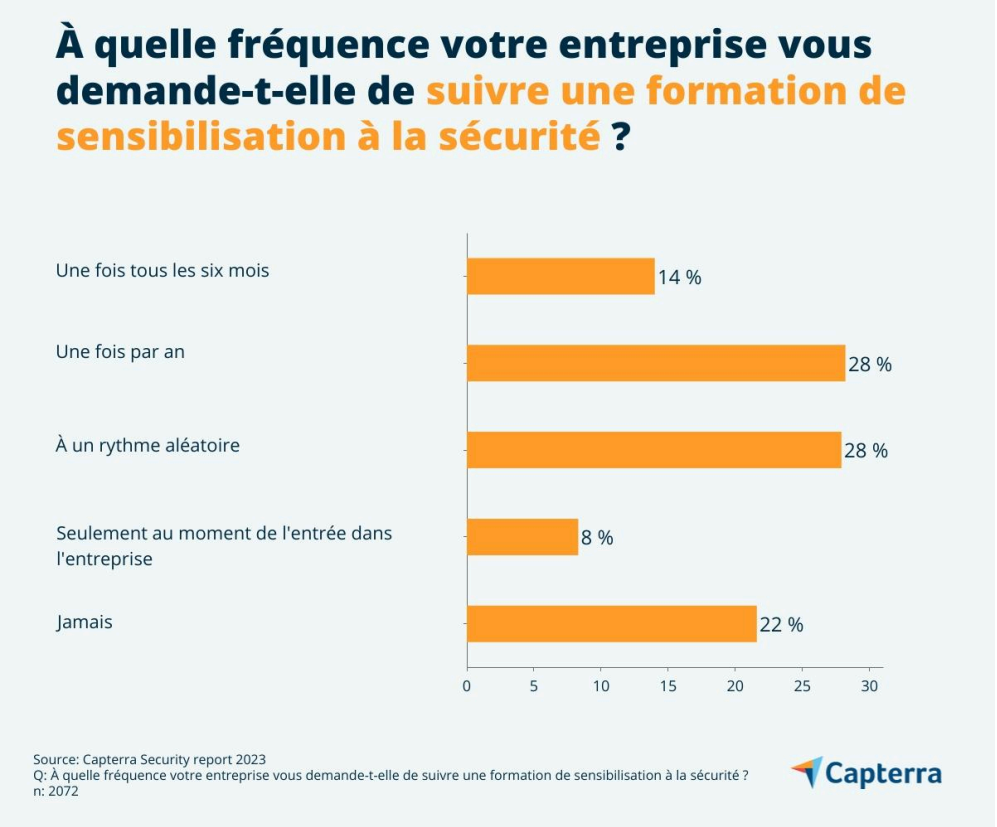
avoir constaté la perte définitive de leurs données, et ce, en dépit d'un paiement effectué.
C'est pourquoi il est important que les employés soient formés aux risques de cybercriminalité afin de pouvoir identifier clairement les attaques.

Vulnérabilité des systèmes et formation à la cybersécurité, deux axes à améliorer

L'une des premières opportunités pour des hackers est de profiter des potentielles vulnérabilités des systèmes et protocoles des entreprises. Lorsque nous avons demandé aux entreprises quelles sont les failles principales qu'elles ont pu identifier, les principaux risques suivants ont été évoqués :

Pour renforcer leurs défenses face aux attaques, il est donc fortement recommandé aux entreprises de s'efforcer de mettre à jour leur stratégie de cybersécurité, mais aussi, de déployer des mesures pour améliorer les points de vulnérabilité identifiés ci-dessus.

La majorité des employés n'ont pas une formation adéquate en cybersécurité
Les employés jouent un rôle majeur dans la protection des systèmes d'une entreprise et avec l'évolution constante des cyberattaques, leur formation devient cruciale. Selon notre enquête, plus d'un employé sur 5 n'a jamais reçu de formation à la cybersécurité et seuls 42 % des répondants affirment avoir une formation au moins une fois par an.



Parmi les contenus de formation principaux proposés, sont mis en avant ceux portant sur :

- la confidentialité des données (46 %),
- la sécurité sur site et l'accès aux bâtiments (35 %),
- la cybersécurité (34 %),
- les bonnes pratiques sur les réseaux sociaux (31 %).

En dépit des formations dispensées, un décalage est cependant observable dans la mise en pratique de certains principes de protection fondamentaux. Un mot de passe identique est par exemple utilisé pour plusieurs comptes par 50 % des employés, alors que l'usage de mots de passe différents reste fortement recommandé.

L’authentification à deux facteurs (2FA) trop peu utilisée
L’un des outils fortement recommandé pour protéger les accès est l’authentification à deux facteurs, qui requiert deux formes d'identification séparées et distinctes. Cependant, cet outil est utilisé par seulement 18 % des entreprises pour toutes les applications et 28 % de n’utilisent pas du tout.

Quelles actions pour la cybersécurité de demain ?

Bien que les avancées technologiques améliorent la sécurité des organisations, les cybercriminels utilisent également ces innovations afin de perfectionner leurs attaques.

Pour améliorer leur stratégie de protection, les points suivants sont à considérer pour les entreprises :

L’anticipation des menaces
Afin de se préparer face aux différentes cybermenaces, il est possible pour les entreprises d’utiliser certaines stratégies comme le compte-rendu d’un audit pour analyser les vulnérabilités matérielles et humaines. Cette stratégie est par ailleurs employée par 45 % des entreprises françaises.

La priorisation des menaces
Il n’est aujourd’hui pas possible pour une entreprise de contrer toutes les menaces existantes mais il est important de mettre en place une stratégie de priorisation. Celle-ci permettra de connaître les menaces capables d’impacter très négativement l'entreprise et de disposer d’un plan de réponse pour y faire face.

L’investissement et la veille en matière de systèmes de sécurité
Afin de disposer de la solution adaptée aux menaces en cours, effectuer une veille constante des solutions disponibles est essentiel : une entreprise peut ainsi s’assurer de disposer de mesures de défenses adéquates et adaptées aux véritables défis actuels de cybercriminalité

Méthodologie

Pour collecter les données de ce rapport, Capterra a mené une enquête en ligne du 10 au 26 novembre 2023 auprès de 2072 employés français. Au sein de ce panel, 1393 sont responsables, participent activement ou sont pleinement informés des politiques de sécurité informatique de leur entreprise. Un groupe de 679 répondants ne sont pas entièrement au fait des politiques de cybersécurité de leur entreprise et ont répondu à des questions spécifiques.

L'ensemble des répondants ont été sélectionnés selon les critères suivants :

- Réside en France
- Âgé(e) de 18 ans à 65 ans
- Employé(e) à temps plein
- Travaille au sein d'une entreprise de 1 à plus de 10 000 employé(es)
- Travaille au sein d'une entreprise disposant d'un système de sécurité

À propos de Capterra

Capterra est la destination n°1 afin de trouver le logiciel idéal. Notre plateforme comprend plus de 95 000 solutions parmi 900 catégories de logiciels et offre un accès à plus d'1,8 millions d'avis vérifiés, vous permettant de gagner du temps, d'accroître votre productivité et d'accélérer votre croissance.

Contact presse

Dorine Mandin - Marketing Specialist Capterra
dorine.mandin@gartner.com