Cybersécurité

Training Guide

Connaître les menaces qui pèsent sur votre entreprise

brother at your side | in[ctrl]

En partenariat avec KnowBe4 Human error. Conquered.

Le coût moyen mondial d'une violation de données en 2023 était de 4,45 millions de dollars / 3,51 millions de livres / 4,05 millions d'euros[1] - soit une augmentation de 15% sur 3 ans.

Lorsque le travail à distance est à l'origine d'une violation de données, le coût moyen par violation est plus élevé de 173 074 $ / 136 500 £ / 157 5062 €.

54% des entreprises déclarent que leur service informatique n'est pas assez sophistiqué pour faire face aux cyberattaques avancées.

Si des hackers tentaient aujourd'hui de percer votre système de cyberdéfense, y parviendraient-ils ? Si vous ne pouvez pas avoir immédiatement confiance dans la solidité de la cybersécurité de votre organisation, vous avez un gros problème. Et vous n'êtes pas le seul. Le maintien de systèmes informatiques sécurisés reste l'un des plus grands défis pour les décideurs informatiques (ITDM). Et comme les cybermenaces sont de plus en plus sophistiquées et que les organisations dépendent plus que jamais des systèmes numériques, le risque d'une attaque réussie n'a jamais été aussi important.

À la suite d'une étude menée par Brother, nous avons constaté que, malheureusement, de nombreux services informatiques se sentent terriblement mal préparés. Le manque de budget et de ressources/outils appropriés est l'une des raisons les plus citées pour lesquelles de nombreux directeurs informatiques s'inquiètent des attaques de cybersécurité et de leur capacité à s'en défendre avec succès.

54% des ITDM déclarent que le budget consacré au maintien de systèmes informatiques sécurisés est en augmentation.

Néanmoins, 44 % d'entre eux estiment que le maintien de systèmes informatiques sûrs reste leur plus grand défi, ce qui indique que les budgets ne sont probablement pas dépensés à bon escient.

Nous avons utilisé les données de Brother et établi un partenariat avec KnowBe4 pour mettre en évidence certains des risques auxquels les entreprises sont confrontées aujourd'hui, et comment la mise en œuvre d'une culture de la formation et de la connaissance de la sécurité peut permettre aux entreprises de rester en sécurité et de se préparer à d'éventuelles menaces.

Les humains sont la dernière ligne de défense lorsqu'il s'agit de la cybersécurité d'une organisation et bien que les services informatiques soient en fin de compte tenus responsables de tout problème de cybersécurité, la réalité est que chaque personne travaillant au sein d'une organisation a une part de responsabilité dans la prévention des atteintes à la sécurité. S'assurer que les employés comprennent cela et leur fournir les ressources et la formation nécessaires pour qu'ils soient conscients des menaces de cybersécurité et de ce qu'il faut faire pour les éviter devrait faire partie intégrante de la stratégie de toute organisation.

L'erreur humaine est l'une des principales causes de 95 % des cyberattaques.[4]

Basil Fuchs
Responsable des systèmes d'information
Brother International Europe

"Les risques pour la cybersécurité ne font qu'augmenter, ce qui est le résultat direct de la sophistication croissante de l'ingénierie sociale utilisée par les cybercriminels pour déclencher des attaques. Les cybercriminels jouent sur le fait que les employés doivent travailler rapidement et n'ont pas le temps d'analyser attentivement les messages pour y déceler les signes révélateurs d'une escroquerie".

[1]IBM [2]IBM [3]Sophos [4]IBM Cyber Security Intelligence Index Report

brother at your side | KnowBe4 Human error. Conquered.

Les plus grandes menaces qui pèsent sur les entreprises

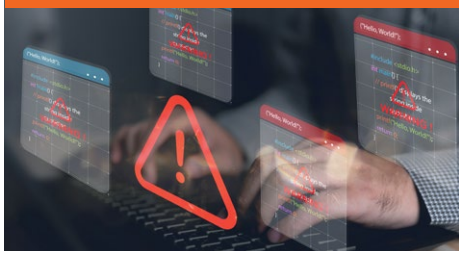
Brother a mené des recherches approfondies auprès de décideurs informatiques (ITDM) de toute l'Europe et les a interrogés sur les menaces de cybersécurité auxquelles ils sont confrontés et pour lesquelles ils se sentent sous-équipés. Sans surprise, il s'agit de domaines où l'erreur humaine peut jouer un rôle dans la réussite d'une attaque.

Dans ce guide, nous examinons les trois menaces de cybersécurité les plus fréquemment identifiées auxquelles les ITDM se sentent le moins bien équipés pour faire face, ainsi que les outils et techniques que votre organisation peut adopter pour renforcer ses défenses et minimiser le risque d'une atteinte à la sécurité.

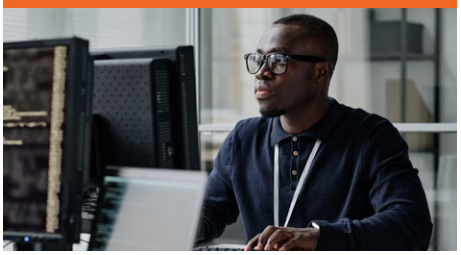
Ces menaces sont les suivantes

Attaques par hameçonnage

Malware



Sécurité des réseaux



Cependant, l'un des plus grands défis auxquels sont confrontés les ITDM est le besoin de formation pour renforcer ces domaines, beaucoup d'entre eux n'ayant ni le temps ni le budget nécessaires. L'humain étant le dernier rempart pour chacune d'entre elles, il est impératif que les équipes apprennent à identifier les risques et à y répondre rapidement et avec précision. Ne disposant pas des ressources internes nécessaires, de nombreuses entreprises comme Brother choisissent de faire appel à des partenaires pour combler cette lacune.

Russell Johnson
Responsable mondial de la cybersécurité
Brother International Europe

"Il est facile pour les entreprises de penser qu'elles peuvent s'occuper elles-mêmes de la formation à la cybersécurité, et laisser une partie externe s'occuper de vos pratiques de cybersécurité peut sembler aller à l'encontre de l'idée même d'une cyberdéfense efficace. C'est pourquoi de nombreuses organisations préfèrent conserver en interne la formation et le développement de cette partie intégrante de leurs opérations commerciales.
Toutefois, si vos équipes internes ne sont pas au fait des techniques de pointe utilisées par les pirates, vous ne pourrez pas former vos employés à la meilleure façon de maintenir vos cyberdéfenses, ce qui pourrait rendre vos systèmes d'information vulnérables aux attaques."

Les personnes jouent le rôle le plus important dans le maintien de la sécurité d'une organisation.

Nous avons également demandé aux ITDM si les défis informatiques devenaient plus ou moins importants dans notre étude, et 50 % d'entre eux ont déclaré que le maintien de systèmes informatiques sécurisés devenait de plus en plus difficile. Les pirates informatiques développent constamment de nouveaux outils et techniques pour enfreindre les défenses de cybersécurité, ce qui rend extrêmement difficile pour les organisations d'identifier les dernières approches et de s'en protéger efficacement. Pendant ce temps, la croissance de l'Internet des objets (IoT) continue de créer de nombreuses nouvelles cibles à exploiter pour les pirates.

Avec autant de points d'accès dans une entreprise, et un grand nombre de personnes travaillant en ligne à travers de multiples appareils et lieux, ce sont les personnes au sein d'une organisation qui sont souvent le maillon faible de toute stratégie de cybersécurité. Qu'il s'agisse d'un manque de formation, d'un oubli ou d'un simple manquement aux meilleures pratiques en matière de cybersécurité, ou encore d'un piège tendu par les cybercriminels, les employés sont certes votre meilleur atout, mais ils peuvent aussi être votre plus grande responsabilité.

Seuls 29% des ITDM placeraient la formation à la sécurité des utilisateurs en tête de leurs priorités.

Seule une entreprise britannique sur neuf a organisé une formation à la cybersécurité pour ses collaborateurs en 2022.

Javvad Malik
Responsable de la sensibilisation à la sécurité
KnowBe4

"La technologie et la formation s'entremêlent dans la sensibilisation à la sécurité en tirant parti des outils numériques pour dispenser une formation complète. La technologie facilite les modules interactifs, les exercices de simulation d'hameçonnage et l'accès aux ressources en ligne, ce qui permet aux employés d'assimiler efficacement les principes de la cybersécurité. La formation complète ce dispositif en inculquant une réflexion critique et les meilleures pratiques, ce qui permet au personnel de reconnaître les menaces et d'y répondre. Ensemble, ils créent un environnement d'apprentissage dynamique dans lequel les employés non seulement comprennent les risques de cybersécurité, mais acquièrent également les compétences nécessaires pour les atténuer. Des mises à jour régulières et des mécanismes de retour d'information permettent de s'aligner sur l'évolution des menaces, ce qui favorise une culture de la vigilance et de la résilience au sein de l'organisation."

Les pirates informatiques n'ont aucun scrupule à s'attaquer aux organisations de toute taille. Toutefois, ce sont généralement les petites et moyennes entreprises qui ne sont pas en mesure de réaliser des investissements importants en matière de cybersécurité qui courent le plus de risques.
Et comme le travail à distance est plus courant que jamais, il est particulièrement difficile pour les entreprises de s'assurer que leurs employés respectent les meilleures pratiques en matière de cybersécurité.

Créer une culture de la cybersécurité au sein de votre organisation

Une formation régulière à la cybersécurité devrait faire partie intégrante du développement professionnel continu (DPC) de tout employé. Cependant, cette pratique n'est pas aussi courante qu'elle devrait l'être.

Une formation efficace à la cybersécurité ne se limite pas à faire suivre aux employés des programmes de sensibilisation par intermittence. Les organisations qui sont réellement préparées aux attaques, et qui disposent des meilleures défenses contre celles-ci, ont la cybersécurité ancrée dans leur culture, et des employés qui renforcent inconsciemment leurs défenses jour après jour.

Russell Johnson
Responsable mondial de la cybersécurité
Brother International Europe

"Brother s'engage à créer une culture de cybersécurité à travers l'ensemble de son organisation. Et ce, parce que nous comprenons que la cybersécurité n'est pas un exercice de conformité. C'est une responsabilité collective et constante. Notre cybersécurité est aussi forte que nos collaborateurs, et donc en tant qu'organisation, la meilleure façon de nous protéger est d'investir en eux et de leur donner les connaissances et compétences nécessaires pour identifier et répondre aux menaces cybernétiques, où qu'elles se produisent."

60 % des décideurs informatiques des PME affirment que le département informatique est responsable de s formations à la cybersécurité dans l'entreprise.

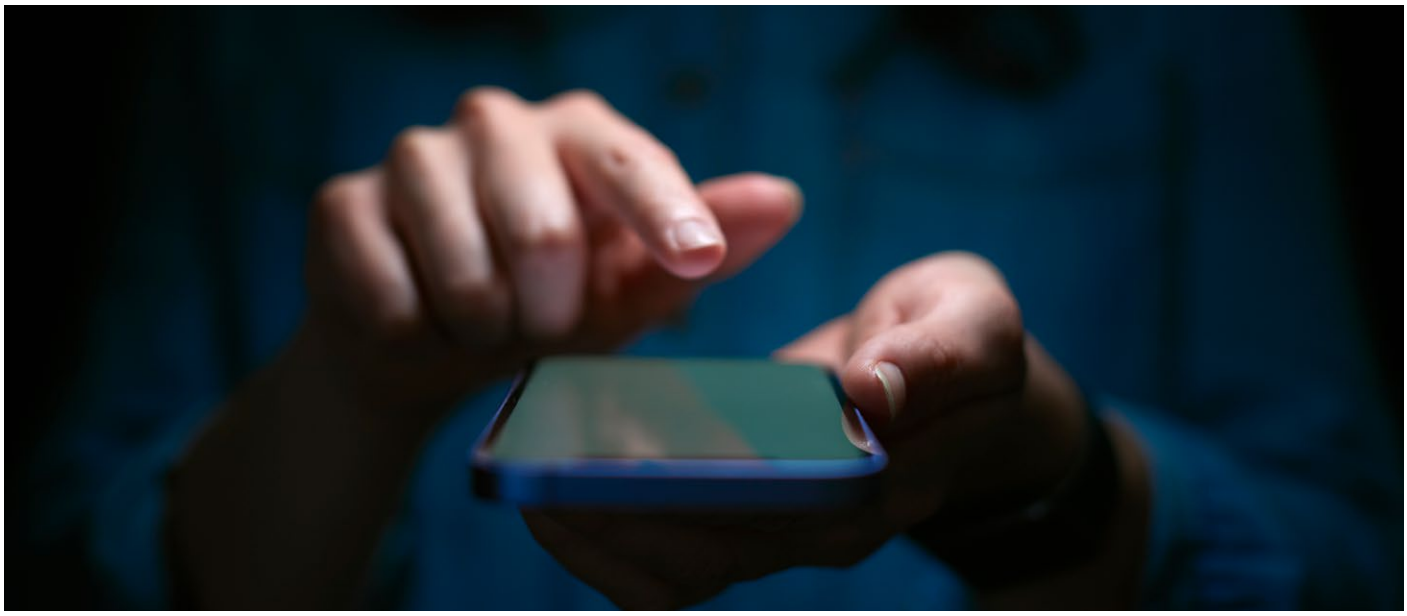
Russell Johnson
Responsable mondial de la cybersécurité
Bother International Europe

"Au cours des dernières années, nous avons considérablement renforcé notre sensibilisation à la cybersécurité chez Brother grâce à des tests de compétence en sécurité et à des formations en ligne, très ciblées et basées sur les faiblesses identifiées des utilisateurs. Nous complétons cela par des articles bimensuels ou moins fréquents, basés sur l'actualité et les tendances en matière de cybersécurité, ainsi que des intervenants invités pour vraiment engager nos équipes avec les derniers développements à connaître."

Les meilleurs conseils pour impliquer vos employés dans la cybersécurité

Les recherches suggèrent que les départements informatiques soient responsables de la création d'une culture de cybersécurité au sein de toute organisation, ce qui peut être difficile pour ceux qui ont des connaissances et des ressources limitées. Cela dit, des mesures devraient être prises dans chaque organisation pour les protéger. Cela signifie :

- Créer du contenu et des supports de formation qui résonnent avec les collaborateurs de l'ensemble de l'entreprise, à différents niveaux de compétence.
- S'assurer que le contenu utilisé pour la formation soit clair, pertinent et appuyé par des exemples concrets démontrant son application.
- Utiliser différentes techniques, telles que des newsletters, des vidéos, des affiches et même des événements, pour intégrer la formation à la cybersécurité à la culture de l'entreprise.
- Pour les organisations mondiales, s'assurer que le contenu soit non seulement correctement traduit, mais aussi adapté aux spécificités régionales pour avoir le plus grand impact.
- Favoriser de bonnes relations entre le département informatique et les employés de toute l'entreprise, en fournissant des retours positifs et des félicitations à ceux qui signalent des comportements ou des emails suspects, afin qu'ils sachent que leurs contributions sont appréciées.
- Encourager les leaders à partager leurs expériences et à montrer l'exemple.



Attaques par phishing (hameçonnage)

Le phishing (hameçonnage) est une technique utilisée par un cybercriminel qui se fait passer pour une personne ou une entreprise légitime, généralement par email, sur les réseaux sociaux ou par téléphone, afin d'obtenir des informations sensibles telles que des mots de passe ou des numéros de carte de crédit. Il est également utilisé comme outil de diffusion de logiciels malveillants. Le phishing reste l'une des formes les plus populaires de cyberattaque par ingénierie sociale.

74 % de toutes les violations de données impliquent l'élément humain.

Étant donné que les organisations dépendent fortement des canaux de communication numériques, cela constitue une voie d'exploitation parfaite pour les cybercriminels. Cependant, éviter une attaque par phishing repose presque entièrement sur la capacité de vos employés à la reconnaître et à l'éviter. Malheureusement, l'hameçonnage implique souvent l'usurpation de l'identité de marques bien connues telles que Microsoft, Amazon, DocuSign et Google pour tromper les utilisateurs. Plus de 30 millions de messages utilisant la marque Microsoft ou mentionnant des produits Microsoft ont été utilisés dans des attaques par phishing en 2022.

28 % des décideurs informatiques des PME disent que les attaques par phishing sont les violations de cybersécurité pour lesquelles ils se sentent le moins équipés pour faire face.

96 % des entreprises britanniques sont la cible principale des attaques de phishing en Europe, suivies par 94 % des entreprises en Espagne, 85 % en France et 79 % en Italie.

[5]Verizon's 2023 Data Breach Investigation Report [6]Forbes, 2023 [7]IT Governance

Comment les décideurs informatiques peuvent-ils se protéger contre les attaques par phishing ?

Étant donné que les attaques par phishing exploitent les faiblesses humaines, la seule véritable façon de protéger votre organisation contre elles est de s'assurer que tous les employés sont correctement formés pour les repérer et savent quoi faire s'ils en soupçonnent une. Et comme les méthodes d'attaque par phishing évoluent constamment, la formation et l'éducation sur les dernières techniques de phishing ne devraient pas être considérées comme un événement ponctuel, mais comme une mise à jour régulière donnée à tous les employés, quel que soit leur rôle au sein de votre organisation.

Comme couche de protection supplémentaire, les décideurs informatiques peuvent également mettre en œuvre des solutions logicielles de protection contre le phishing. Celles-ci fonctionnent en analysant divers éléments des messages et en signalant ou bloquant les contenus suspects, les empêchant ainsi d'atteindre votre boîte de réception ou votre navigateur web.

Signaux d'alerte de phishing

Une attaque par phishing réussie repose sur la nécessité de tromper les employés pour qu'ils cliquent sur quelque chose qu'ils ne devraient pas ou qu'ils le partagent. La seule façon de les empêcher de le faire est de leur offrir une formation régulière et des rappels sur les "signaux d'alerte" qui pourraient indiquer qu'un message est une tentative de phishing.

Les signaux d'alerte auxquels ils doivent prêter attention incluent :

- Un message provenant d'un domaine qui n'est pas le même que celui de l'entreprise qu'il est censé représenter.
- Des URLs qui ne correspondent pas dans une adresse de site web.
- Des erreurs d'orthographe et de grammaire.
- Des polices de caractères inhabituelles, surtout si la police semble changer au milieu d'un mot.
- La tentative de créer un sentiment d'urgence : "ce lien expire dans 48 heures" ou "dépêchez-vous de valider votre identité".
- Des salutations inhabituelles, telles que "Bonjour cher".

Vos équipes sont-elles capables de repérer un e-mail ou un message de phishing ? Auparavant, il était assez facile de les repérer grâce à des fautes d'orthographe et de grammaire évidentes, mais grâce à l'IA générative qui aide les escrocs à surmonter ces problèmes, la détection des messages de phishing devient plus difficile que jamais. Une façon de savoir à quel point vos équipes sont préparées est d'établir votre pourcentage Phish-prone™. Des tests de phishing réguliers devraient donc faire partie intégrante du plan de cybersécurité de toute organisation.

Russell Johnson
Responsable mondial de la cybersécurité
Brother International Europe

"Nous avons mis en place une série de mesures pour minimiser le risque de subir une attaque par hameçonnage. Voici quelques-unes des simulations d'hameçonnage que nous avons mises en place dans le cadre de notre cyber-stratégie :

- Les courriels axés sur les ressources humaines, portant sur des sujets tels que la maladie, les congés annuels et la signature de nouvelles politiques
- Les courriels des managers, qui demandent par exemple aux employés d'ouvrir, de lire et de signer rapidement des documents
- Les e-mails, comme les liens pour signer un document Google, ou l'accès à un SharePoint"

Pourcentage Phish-prone™ : Qu'est-ce que c'est et pourquoi est-ce important ?

Votre pourcentage d'exposition au phishing correspond au pourcentage d'employés susceptibles de cliquer sur un lien d'hameçonnage ou d'interagir avec un message d'hameçonnage de manière dangereuse. Il peut s'agir de saisir des données sur une fausse page de renvoi, d'ouvrir une pièce jointe ou de répondre au message.

Le pourcentage de personnes sujettes au phishing est calculé en divisant le nombre d'employés qui sont tombés dans le piège d'un test de phishing par le nombre d'employés qui ont été testés. Le résultat est ensuite multiplié par 100 pour obtenir le pourcentage. Par exemple, si une organisation compte 100 employés et que 20 d'entre eux ont cliqué sur un courriel d'hameçonnage lors d'un test, le pourcentage d'hameçonnage sera de 20 %.

"Ne paniquez pas si votre score de vulnérabilité au phishing est plus élevé que vous ne le pensez - c'est assez courant si vous n'avez jamais été soumis à un test de phishing auparavant. Chez Brother, nous avons pu réduire considérablement le nôtre en peu de temps grâce à une série d'outils de formation et de tests de phishing. En fait, nous atteignons maintenant notre référence industrielle de 6 %, ce qui prouve l'impact que peuvent avoir des tests constants et des formations régulières."

Tests d'hameçonnage et formation

Les tests d'hameçonnage constituent l'un des moyens les plus efficaces de déterminer le degré de préparation de vos équipes à une attaque au cas où votre organisation serait prise pour cible, et de réduire le score de votre organisation en matière d'hameçonnage.8 Le principe est simple. Les entreprises qui souhaitent tester leur personnel mettent en place des simulations de phishing (en interne ou par l'intermédiaire d'un partenaire spécialisé) qui tentent d'amener vos collaborateurs à divulguer des informations sensibles, mais sans risque réel. À la fin des tests, votre pourcentage d'exposition au phishing est calculé et comparé à celui d'autres entreprises de votre secteur (chiffre de référence).

Javvad Malik
Responsable de la sensibilisation à la sécurité
KnowBe4

"Le rapport 2023 Phishing by Industry Benchmarking Report de KnowBe4 révèle que 33,2 % des utilisateurs non formés échoueront à un test d'hameçonnage. Cependant, en mettant en place des formations à la sécurité et en s'engageant à développer une culture de la cybersécurité, les entreprises ont montré qu'il était possible de réduire ce chiffre à moins de 5,9 %, le taux de référence du secteur."

Russell Johnson
Responsable mondial de la cybersécurité
Brother International Europe

"Chez Brother, nous avons constamment réduit notre pourcentage de phishing au cours des dernières années. Nous avons commencé par un test d'hameçonnage de référence en mars 2022, qui a montré que notre pourcentage d'hameçonnage (Phishing Prone Pourcentage) était de 11,5 %. Nous avons ensuite mis en place une formation solide et des tests de sensibilisation en matière de sécurité afin d'identifier les principaux points faibles. Nous avons alors été en mesure d'organiser une formation corrective basée sur ces tests pour combler les lacunes. Nous avons envoyé plus de 30 000 e-mails de phishing, dont 17 000 au cours des 12 derniers mois. À l'heure actuelle, notre PPP n'est que de 5,2 %, l'objectif étant d'atteindre moins de 2 %.

La référence en matière d'hameçonnage est construite en trois phases :

Première phase : Un e-mail simulant un hameçonnage est envoyé à tous les utilisateurs qui n'ont reçu aucune formation préalable. Le pourcentage de personnes qui tombent dans le piège du courriel d'hameçonnage donne le pourcentage de référence. En moyenne, 33,2 % des employés seront victimes du courriel d'hameçonnage.

Deuxième phase : Les utilisateurs ont suivi une formation et ont été soumis à des tests d'hameçonnage, 90 jours après le premier hameçonnage.

Troisième phase : Le test est répété après 12 mois.

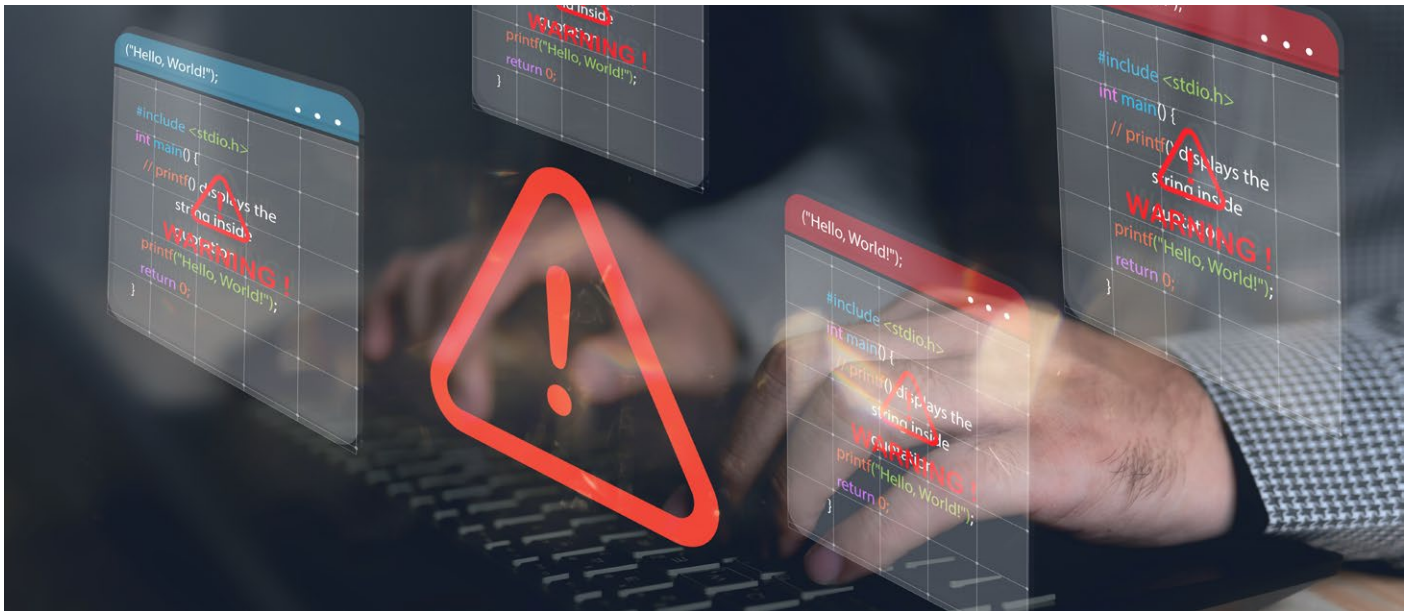
Sur la base de 32,1 millions d'e-mails de phishing envoyés à 12,5 millions d'utilisateurs, les données montrent que les résultats des tests de sécurité après 90 jours de formation chutent globalement de 33,2 % à 18,5 %. Ce pourcentage tombe ensuite à 5,4 % après 12 mois. Ces pourcentages varient en fonction du secteur d'activité, de la localisation et de la taille de l'organisation.

91 % des violations de données réussies commencent par une attaque de spear-phishing.[9]

Qu'est-ce que le spear-phishing ?

Le spear-phishing est un type d'attaque par hameçonnage qui vise des personnes ou des organisations spécifiques, généralement par le biais de mails malveillants. L'objectif du spear-phishing est de voler des informations sensibles telles que les identifiants de connexion ou d'infecter l'appareil de la cible avec des logiciels malveillants.

[8]KnowBe4 [9]KnowBe4



Logiciels malveillants

L'un des plus grands défis auxquels les ITDM sont confrontés est la menace d'un type de logiciel très spécifique, appelé malware, qui pénètre dans leur infrastructure informatique.

34% des ITDM déclarent que les logiciels malveillants/ransomwares sont la brèche de cybersécurité face à laquelle ils se sentent désarmés.[10]

Qu'est-ce qu'un logiciel malveillant ?

Les logiciels malveillants sont des logiciels conçus spécifiquement dans le but de perturber, d'endommager ou d'obtenir un accès non autorisé à un système informatique. Comme nous le savons, les attaques par hameçonnage sont souvent utilisées pour introduire des logiciels malveillants dans vos systèmes - en vous incitant à cliquer sur un lien dans un message d'hameçonnage ou à télécharger des pièces jointes.

D'autres façons dont les logiciels malveillants peuvent infecter votre appareil incluent :

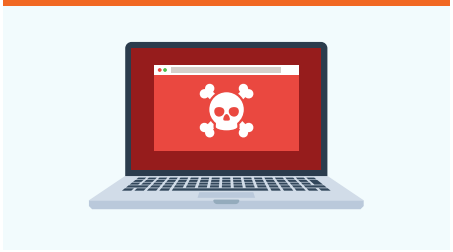
- Téléchargements automatiques depuis des sites web compromis
- Installation de logiciels infectés sur votre appareil
- Supports amovibles : clés USB et disques durs externes
- Logiciels obsolètes présentant des vulnérabilités de sécurité.

Plus de 100,884,532 dossiers connus font l'objet d'une attaque en Europe en Décembre 2023.[11]

[10]2023 Brother X Savanta ITDM priority survey [11]IT Governance

Les types de logiciels malveillants les plus dangereux : un aperçu

Le cheval de Troie



Un cheval de Troie est un virus qui peut endommager vos fichiers, modifier vos données, surveiller votre activité, voler des informations sensibles de votre appareil, rediriger le trafic Internet ou même créer des points d'accès clandestins à vos systèmes - tout cela à votre insu.

Le Ransomware

Les ransomwares sont un type de logiciel malveillant conçu pour bloquer l'accès à votre appareil et aux données qui y sont stockées jusqu'à ce que vous payiez une rançon aux pirates informatiques. Ils procèdent généralement en chiffrant vos fichiers de sorte que vous ne puissiez plus les voir ou les utiliser.

Les vers

Les vers sont un type de virus de type cheval de Troie, mais leur fonction principale est de se répliquer eux-mêmes et d'infecter d'autres appareils, tout en restant actifs sur les systèmes qu'ils ont déjà infectés.

Comment les ITDM peuvent-ils se protéger contre les attaques de ransomware ?

En janvier 2023, Royal Mail a été attaqué par l'un des ransomwares les plus dangereux au monde – LockBit – où la demande de rançon était de 80 millions de dollars.[2]

Comme nous le savons, de nombreuses attaques par ransomware sont réalisées via des attaques de phishing réussies, où les utilisateurs cliquent sur des liens illégitimes qui téléchargent des logiciels non sécurisés sur leur appareil. Cela signifie que l'une des façons les plus efficaces de protéger votre organisation contre ce type de menace est de s'assurer que vos équipes savent repérer et éviter les attaques de phishing. S'associer à un partenaire de confiance peut vous indiquer précisément si vos équipes sont efficaces pour les identifier.

D'autres mesures peuvent être prises pour éviter les attaques par ransomware :

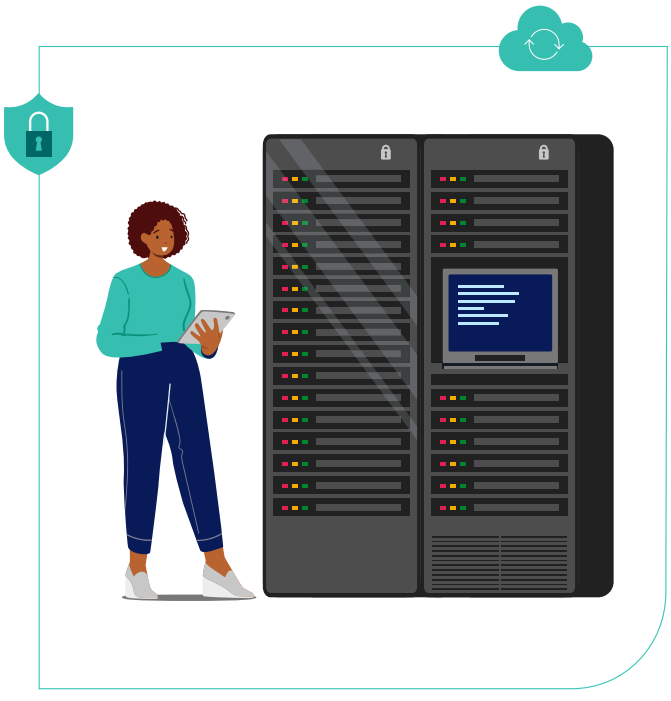
- Maintenir les logiciels à jour
- Déployer l'authentification à deux facteurs, en particulier pour les travailleurs à distance
- Demander aux utilisateurs de changer régulièrement leurs mots de passe
- Utiliser du matériel et des logiciels de sécurité, notamment des pare-feu, des applications de balayage de courrier électronique et des logiciels antivirus
- Effectuer des sauvegardes régulières et stocker le tout dans un environnement réseau séparé.

Javvad Malik
Responsable de la sensibilisation à la sécurité
KnowBe4

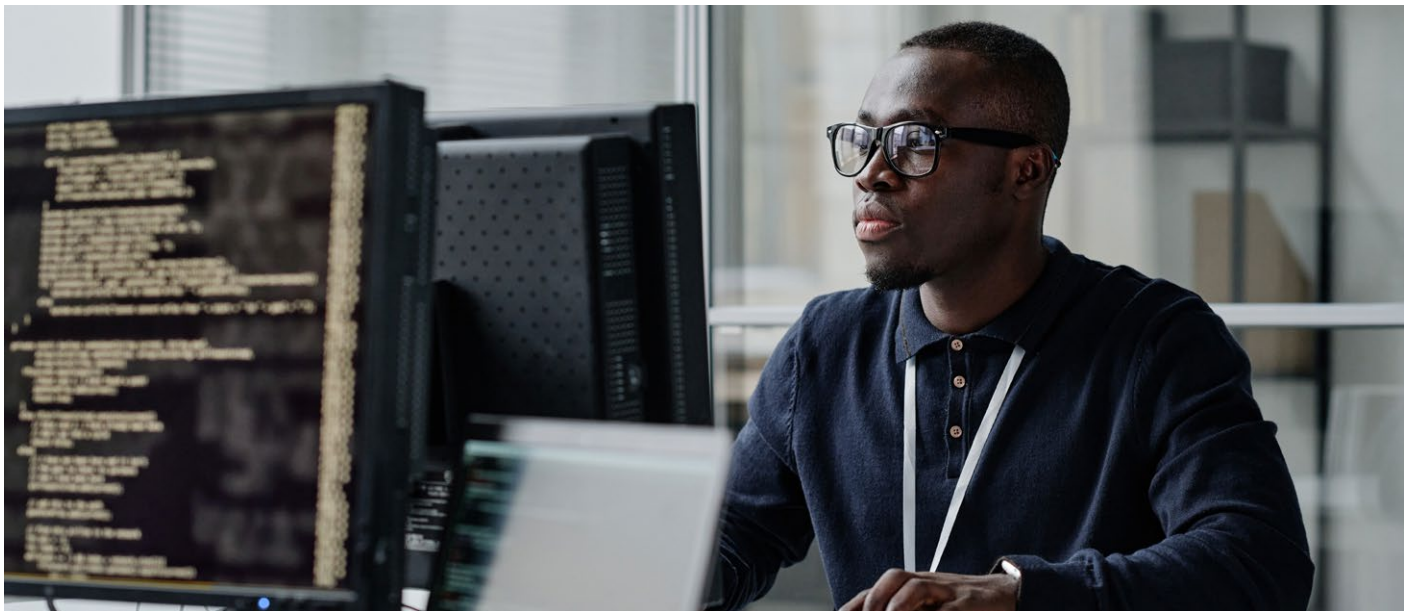
"Pour vaincre les ransomwares, les organisations peuvent utiliser des outils tels que RanSim, qui leur donne une vision à 360° de leur préparation à une attaque. RanSim simule 24 scénarios d'infection par ransomware et un scénario d'infection par cryptomining pour déterminer si un poste de travail est vulnérable".

Une autre option consiste à mettre en œuvre la methode SOAR - Security Orchestration Automation and Response (automatisation de l'orchestration de la sécurité et de la réponse). SOAR, qui est conçu spécifiquement pour les réponses et la gestion des menaces d'hameçonnage, peut réduire votre temps moyen de réponse (MTTR) et atténuer les menaces d'hameçonnage avant qu'elles n'atteignent les boîtes de réception de vos équipes. Cette attitude proactive à l'égard de l'hameçonnage est encore renforcée par :

- Des réponses automatisées aux courriels qui permettent aux services de communiquer rapidement avec les employés, réduisant ainsi les temps d'arrêt opérationnels
- L'identification de modèles qui permet à vos équipes de repérer les attaques rapidement
- La prise en compte d'attaques réelles pour les transformer en simulations lors de formation afin d'améliorer les compétences et l'expérience de vos employés.

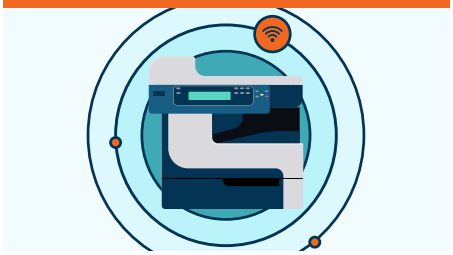


[12]bbc.co.uk [13]KnowBe4



La sécurité des réseaux

La sécurité des réseaux est un aspect souvent négligé par les entreprises. Nous savons qu'il s'agit d'un problème qui peut avoir des conséquences considérables. Cependant, nos recherches montrent clairement qu'il s'agit d'une priorité souvent négligée. La sécurité des réseaux fait référence aux processus et aux logiciels que vous utilisez pour protéger vos ordinateurs, vos imprimantes, votre réseau et vos données. Elle est généralement divisée en trois domaines :

Physique	Technique	Administratif
		
Contrôles de sécurité utilisés pour empêcher l'accès non autorisé aux réseaux physiques tels que les imprimantes, les routeurs et les disques durs ("terminaux").	Sécurité qui protège les données entrantes, sortantes et stockées sur le réseau.	Contrôles de sécurité pour le comportement des utilisateurs, tels que l'accès et les étapes d'authentification utilisées.

La partie la moins sûre d'un réseau est le point d'accès. C'est là encore que les utilisateurs entrent en jeu. Le travail hybride a créé de nouveaux défis pour les organisations et la sécurité des réseaux. Les travailleurs à distance sont susceptibles d'accéder aux serveurs de l'entreprise via des réseaux publics, qui offrent une protection bien moindre. La surface d'attaque est plus grande et les points d'entrée pour les cybercriminels sont plus nombreux. Il est également plus difficile pour les équipes informatiques d'identifier les attaques et d'y répondre.

Basil Fuchs
Directeur des systèmes d'information
Brother International Europe

"Dans le monde du travail digital et flexible d'aujourd'hui, la sécurisation des réseaux est cruciale pour protéger les données sensibles. Le modèle à confiance zéro, qui ne suppose aucune confiance inhérente, garantit que tous les utilisateurs et appareils sont vérifiés avant d'accorder l'accès. En limitant l'accès au strict nécessaire, cette approche réduit le risque de mouvements non autorisés."

L'accès au réseau sans confiance est un modèle de sécurité très efficace qui garantit que les utilisateurs n'ont que l'accès et les autorisations nécessaires pour remplir leur rôle. Il s'agit d'une approche très différente des VPN standard qui permettent à tous les utilisateurs d'accéder à l'ensemble du réseau. L'avantage d'une approche à confiance zéro est que si un utilisateur est compromis, les pirates ne pourront accéder qu'aux données qu'il peut consulter, et non au réseau dans son ensemble.

Nous avons également identifié des solutions rapides pour améliorer la sécurité de votre réseau :

1. Utiliser des certificats SSL
2. Demander aux travailleurs à distance de crypter leur réseau sans fil domestique avec le cryptage WPA2
3. Modifiez le nom et le mot de passe de votre routeur pour masquer votre identité
4. Désactiver le WPS sur les routeurs
5. Rappeler à tous les utilisateurs de sauvegarder régulièrement leurs appareils (imprimantes, scanners, etc.) et d'installer les mises à jour dès qu'elles sont disponibles.

Comment aborder la sécurité des réseaux

La sécurité des réseaux englobe de nombreux éléments différents, tous aussi cruciaux les uns que les autres. C'est particulièrement vrai à l'ère du travail hybride et à distance, où il n'est tout simplement pas possible pour les ITDM de visiter et de vérifier les installations à domicile ou même de voir leurs collaborateurs en personne avec une certaine régularité. Voici donc nos meilleurs conseils pour vous assurer que toutes les conditions sont réunies.

Utilisez des certificats SSL

Un certificat SSL (Secure Sockets Layer) et le protocole HTTP sont essentiels pour les ventes en ligne. Le certificat SSL protège les données échangées entre vos serveurs et vos clients contre le vol, confirme l'identité du serveur et crée un canal de communication crypté pour les transactions.

Maintenez le firmware de votre routeur à jour

Ceci est particulièrement important pour les travailleurs à distance, car le micrologiciel du routeur est préinstallé sur leurs appareils. Le micrologiciel du routeur devrait être mis à jour au moins une fois par an pour offrir la meilleure défense contre les cybermenaces.

Utilisez le WPA2

Wi-Fi Protected Access2, ou WPA2, est l'un des algorithmes de sécurité les plus puissants et les plus complexes disponibles pour protéger votre réseau Wi-Fi.

Mettre en place un VPN

Les réseaux privés virtuels (VPN) sont essentiels pour les travailleurs à distance, car ils réduisent le risque d'interception des informations lorsqu'elles circulent entre les réseaux. Les réseaux privés virtuels aident à protéger les travailleurs à domicile contre l'utilisation accidentelle de réseaux publics vulnérables.

Construisez vos pare-feux

Cela peut sembler évident, mais des pare-feu solides restent l'une des armes de cybersécurité les plus efficaces de votre arsenal. Veillez à disposer d'un pare-feu interne et d'un pare-feu externe, envisagez de superposer des pare-feu matériels et logiciels et veillez à ce qu'ils soient régulièrement mis à jour pour bénéficier d'une protection optimale.

Désactivez le partage de fichiers

Bien que la collaboration soit fondamentale pour les travailleurs à distance, le partage de fichiers représente une réelle opportunité pour les pirates d'accéder à des informations sensibles ou de causer des dommages à vos systèmes. La mise en œuvre de systèmes basés sur le cloud ou protégés par un mot de passe permet de collaborer sans rendre votre réseau vulnérable.

Sécurisez vos terminaux

En particulier les imprimantes. Les imprimantes et autres équipements enfichables tels que les scanners et les disques durs portables sont souvent négligés lorsqu'il s'agit de la sécurité du réseau. Assurez-vous que leur logiciel est à jour et envisagez l'impression sécurisée - une fonction qui permet aux utilisateurs de retarder l'impression jusqu'à ce qu'ils soient physiquement devant l'imprimante.

Sécurité de l'imprimante

La sécurité des imprimantes est un domaine qui est souvent négligé par les entreprises. Les imprimantes semblent souvent être des dispositifs assez sûrs, mais elles peuvent être utilisées par des pirates comme une porte dérobée pour pénétrer dans votre réseau. Et cela arrive plus souvent qu'on ne le pense.

Selon une étude de Brother, 95 % des organisations se préoccupent de la sécurité du réseau de leurs travailleurs hybrides.

Plus d'un incident de sécurité sur dix affectant une entreprise concerne une imprimante.[14]

En effet, la plupart des imprimantes modernes sont connectées à l'internet, et cette connexion réseau fonctionne dans les deux sens : de votre appareil à votre imprimante, mais aussi de votre imprimante à votre appareil. Alors que les utilisateurs n'hésitent pas à imprimer des informations sensibles, cette connexion bidirectionnelle peut être exploitée par des pirates intelligents si votre imprimante ne dispose pas de défenses aussi solides que votre ordinateur.

Security by Brother est notre approche de la sécurité des points finaux basée sur des solutions qui sécurisent l'impression professionnelle. Nous introduisons une triple couche de sécurité au niveau du réseau, des appareils et des documents pour garantir que vos informations ne sont vues que par ceux à qui elles sont destinées.

[14]Quocirca.

Pour finir

Nous avons constaté qu'une approche de la réduction des risques fondée sur le principe du "must have" et du "nice to have" est la meilleure façon de s'assurer que les budgets de l'ITDM soient dépensés de manière efficace. Nous pouvons les décomposer comme suit :

Éléments non négociables : antivirus, réseau privé virtuel, formation de base à la cybersécurité et gestionnaires de mots de passe.

Valeur ajoutée : éléments qui seraient bénéfiques, mais qui ne sont pas essentiels pour assurer un niveau de cybersécurité de base, tels que l'authentification multifactorielle et des sessions de formation régulières.

Après avoir identifié les risques les plus importants de votre organisation, cette méthode vous permet de déterminer les mesures de sécurité qui sont essentielles pour assurer la sécurité de votre organisation, et celles qui pourraient être extrêmement bénéfiques si vous avez le budget. Cette méthode est également un excellent moyen pour les ITDM d'obtenir un budget supplémentaire pour leurs défenses.

En fin de compte, la cybersécurité n'est pas une simple liste à cocher dans le cadre d'un exercice de formation de routine pour les membres de votre organisation. Pour assurer la sécurité de vos systèmes et de vos données, la cybersécurité doit devenir un mode de vie au sein de vos équipes - la détection des cyberrisques étant aussi naturelle que celle des risques routiers au volant.

Protegez votre entreprise

Contactez votre expert en sécurité Brother dès aujourd'hui

brother at your side | in[ctrl]

En partenariat avec KnowBe4 Human error. Conquered.