Cybersécurité : les changements de comportements pendant la pandémie ont-ils fait ressurgir les menaces internes ?

Selon les différentes organisations à l'origine de ces statistiques, les implications financières ne sont pas moins importantes, allant de 257 200 euros pour un incident par négligence à 730 145 euros pour le vol d'identifiants, sur un seul incident. Avec une partie grandissante de la main-d'œuvre mondiale travaillant désormais en dehors du bureau, ces chiffres ne feront qu'augmenter. L'évolution vers le travail à distance et le développement des systèmes d'information dans le cloud, associés à la pression financière, l'insécurité de l'emploi et l'anxiété générale d'une pandémie mondiale, ont créé une cyber-tempête parfaite – plus d'un tiers des entreprises signale une augmentation des menaces internes depuis mars 2020 (34 %).

S'adapter à un nouvel environnement

La clé d'une cybersécurité solide est l'adaptabilité, et nous en sommes témoins : rien n'exige une plus grande adaptabilité qu'une pandémie mondiale. Mais si le renforcement des défenses pour éviter la recrudescence des attaques relève d'une défense classique, s'adapter au changement massif des habitudes et des mentalités est tout autre chose.

Vos employés travaillent désormais en dehors des habitudes et processus de bureau, et beaucoup n'y sont pas encore habitués. Ils peuvent être déstabilisés, plus facilement distraits par les tâches familiales, et plus enclins à commettre des erreurs de base.

L'environnement familial plus détendu peut également créer des ruptures avec les bonnes pratiques de sécurité habituellement utilisées au bureau. Par exemple, utiliser son ordinateur personnel pour travailler, ou inversement se servir de sa machine professionnelle pour des activités personnelles, mais également écrire ses mot de passe ou ne pas se déconnecter correctement des systèmes de l'entreprise.

Ensuite, il y a le danger permanent du phishing. Les environnements personnel et professionnel se chevauchant, les utilisateurs peuvent être plus enclins à cliquer sur un lien suspect chez eux que dans le cadre plus formel du bureau et les cybercriminels en sont bien conscients. Depuis le début de la pandémie, nous avons vu des centaines d'attaques de phishing liées au COVID-19, poussant les victimes à cliquer sur les liens, à télécharger des pièces jointes et à ressaisir ou partager leurs identifiants. Il suffit d'un seul employé distrait pour mettre en péril la sécurité de toute l' entreprise.

Outre les comportements potentiellement à haut risque, les équipes de sécurité doivent redoubler de vigilance et surveiller les mauvaises pratiques qui peuvent réapparaitre, comme les employés qui se connectent à des heures inhabituelles. Du jour au lendemain, la télémétrie disponible a complètement changée. Pour s'adapter à ce changement, il faut un œil attentif et une stratégie solide capable de défendre de l'intérieur.

Les effets psychologiques néfastes de la pandémie

Malheureusement, le risque accru d'erreurs n'est pas la seule faille permettant l'accès aux cybercriminels opportunistes. La pression psychologique de la vie en confinement peut céder la place à une menace plus sourde – l'acteur interne malveillant. Si les collaborateurs malveillants sont évidemment moins courants, ils peuvent être bien plus dangereux… Beaucoup utilisent la connaissance du système interne pour échapper aux défenses, et prennent des mesures spécifiques pour couvrir leurs traces, ce qui les rend beaucoup plus difficiles à détecter et à contenir. En moyenne, un incident interne malveillant coûte 631 900 euros, soit plus du double de celui d'une menace par négligence.

Le risque de menaces malveillantes n'est pas nouveau. Mais face au nombre d'employés mis à pied, confrontés à des licenciements et potentiellement sous pression financière, les organisations doivent être en alerte. Même les utilisateurs les moins avertis en matière de technologie sont probablement conscients de la valeur de l'information en cas de fuite de données et partage d'informations sensibles.

De même pour les employés qui ont un grief contre leur entreprise. Les fuites de données font régulièrement la Une des médias, leurs conséquences dévastatrices sont bien connues : sanctions venant des autorités, atteinte à la réputation et pertes financières importantes.

Soudain, un employé mécontent pourrait entrevoir ici une vengeance apparemment simple et efficace…

Construire une défense de l'intérieur pour l'extérieur

Il n'est jamais facile de détecter les menaces internes. Il est encore plus difficile de les détecter en dehors des bureaux, où les contrôles sont moins importants et où les normes de sécurité sont moins strictes. L'efficacité d'une défense solide réside dans la mise en place d'une stratégie flexible, robuste et sur plusieurs niveaux qui combine les personnes, les processus et la technologie.

Les menaces d'acteurs internes sont particulières car elles disposent déjà d'un accès légitime aux systèmes et aux données de l'entreprise – ce vecteur d'attaque unique nécessite une défense unique. Il n'est évidemment pas productif de bloquer, compliquer excessivement l'accès à ceux qui doivent travailler au sein de vos réseaux, mais vous devez garantir que l'accès est vraiment strictement contrôlé et n'est accordé que sur la base du besoin d'en connaître.

Commencez par mettre en œuvre une solution complète de gestion des accès privilégiés (PAM) pour surveiller l'activité du réseau, limiter l'accès aux données sensibles et interdire le transfert des données en dehors des systèmes de l'entreprise. Il ne devrait y avoir, par défaut, aucune confiance entre votre technologie et vos employés. Une demande de connexion en dehors des heures habituelles peut être légitime, mais elle ne doit pas être normalisée. Les contrôles doivent être étanches, en signalant et en analysant chaque événement pour déceler toute négligence ou acte illicite.

Complétez ces contrôles techniques par des procédures humaines claires et complètes régissant

l’accès au réseau, les privilèges des utilisateurs, les applications non autorisées, le stockage externe, la protection des données, etc.

Comme le plus grand facteur de risque d’attaque interne est votre personnel, celui-ci doit être au cœur de votre stratégie de défense. Vous devez créer une culture de la sécurité via une formation continue de sensibilisation aux menaces internes. Chaque membre de votre entreprise doit savoir comment repérer et contenir une menace potentielle et, qu’elle soit intentionnelle ou non, comment ce comportement inadapté peut mettre votre entreprise en danger.

Cette formation doit être approfondie et adaptée au climat de l’instant. Si l’environnement de travail est plus détendu, les meilleures pratiques en matière de sécurité restent toujours d’actualité, peut-être plus que jamais.