Comment lutter contre les menaces qui viennent de l'intérieur ?

Les experts en cybersécurité concentrent majoritairement leurs efforts contre les menaces qui viennent de l'extérieur. Et pour cause, depuis plusieurs années, les cybercriminels ne cessent de diversifier leurs approches : attaques par compromission d'emails professionnels (BEC), attaques par compromission de comptes internes (EAC), rançongiciels et toujours phishing…
Il existe toute une série de menaces, qui, une fois mises en œuvre, permettent à son auteur, désormais infiltré dans les systèmes d'une organisation, d'y causer de sérieux dommages.

Mais parfois, les menaces viennent directement de l'intérieur…

Souvent difficiles à détecter, ces menaces internes sont pourtant de plus en plus courantes et peuvent elles aussi avoir de graves conséquences. Selon une récente étude, leur fréquence a augmenté de 47% en seulement deux ans et elles coûteraient aux entreprises 31% de plus qu'en 2018.

Attention toutefois à ne pas se méprendre : les menaces internes ne sont pas forcément le fait d'individus malveillants. Beaucoup sont considérées comme involontaires, comme l'installation d'applications non autorisées ou l'utilisation de mots de passe faibles ou réutilisés.

Mais « erreur humaine » ou « acte de malveillance », se protéger contre les menaces internes n'est pas chose aisée, la menace étant dans tous les cas déjà derrière la principale ligne de défense, externe, de l'entreprise. Dans le cas d'un employé malveillant, rien de plus simple pour lui que d'utiliser ses accès privilégiés et des informations essentielles en sa connaissance pour éviter de se faire détecter.

Comprendre les menaces internes

Loin d'une approche basée sur une méfiance excessive envers les collaborateurs, qui aurait pour seul impact la rétention d'informations nécessaires à une bon fonctionnement d'entreprise, il existe plusieurs mesures moins drastiques qui peuvent être mises en œuvre pour détecter les menaces internes, à condition d'en comprendre les étapes.

Dans un premier temps, cela consiste à comprendre ce qui peut pousser un collaborateur à passer à l'acte. Les facteurs de motivation sont classiquement regroupés en trois catégories :

· Un acte Involontaire : la menace vient parfois d'employés négligents qui installent des applications non autorisées, perdent du matériel ou réutilisent plusieurs fois le même mot de passe.

· La motivation émotionnelle : certains employés peuvent être en quête de vengeance personnelle contre leur entreprise. Ils cherchent alors à nuire à sa réputation en divulguant des informations confidentielles ou en perturbant le bon fonctionnement des systèmes internes.

· La motivation financière : tirant profit de leurs accès privilégiés, les employés malveillants

n'hésitent pas à monnayer des données sensibles, un accès au réseau interne ou à entraver le bon fonctionnement de certains systèmes pour tenter d'influencer le prix des actions de l'entreprise.

La seconde étape est de réaliser que toute personne ayant accès au réseau de l'entreprise représente potentiellement une menace, et ce, quel que soit son niveau hiérarchique.

Si certains utilisateurs privilégiés sont étroitement encadrés, des employés « voisins » situés à un niveau hiérarchique légèrement inférieur, ou collaborant ponctuellement sur un projet, ont généralement une activité plus difficile à suivre. Ils auront pourtant un accès à ces données sensibles nécessaires pour faire leur travail et avec un contrôle beaucoup plus léger de leurs actions.

Enfin en troisième étape, il faut réaliser que loin, très loin, perdus dans l'organigramme, peut-être simplement moins sensibilisés aux bonnes pratiques de sécurité, des collaborateurs vont potentiellement constituer une menace involontaire mais bien réelle.

Comment repérer les signaux d'alerte

Les attaques externes « frontales » sont généralement détectées en quelques heures, voire rapidement en quelques minutes. En revanche, les menaces internes, résultant d'une première compromission, peuvent passer sous le radar pendant de longues périodes. Seulement 10 % des cas sont découverts dans les jours qui suivent une attaque, tandis que 40 % restent dissimulés pendant une période pouvant aller jusqu'à cinq ans.

Repérer le potentiel d'une menace interne avant qu'un vrai accident ne se produise est essentiel pour la sécurité d'une organisation. Certes, il ne s'agit pas d'une science exacte et aucune technologie ne n'éliminera jamais totalement le risque d'attaque, mais il existe des moyens de le réduire considérablement.

Dans le cadre de menaces involontaires, il est important de rester attentifs à détecter les pratiques de sécurité peu rigoureuses. Pour déjouer les intentions malveillantes, il faut envisager de surveiller les activités anormales des utilisateurs, bien avant que des actions frauduleuses ou malveillantes ne soient mises en place. Les entreprises doivent alors rester vigilantes à toute tentative inhabituelle ou répétée d'accès aux systèmes internes, en particulier sans raison valable ou si elle est hors du champ d'action de l'employé. Cette même vigilance doit s'appliquer aux employés qui commencent soudainement à travailler à des heures inhabituelles sans raison.

Une défense en profondeur

La détection et la protection contre les menaces internes nécessitent la mise en place d'une défense plus solide, combinant outils, règles de sécurité et formations.

Outre la surveillance des comportements inhabituels, il est essentiel de mettre en œuvre des politiques concernant l'utilisation de l'email, les dispositifs de stockage externes et le BYOD.
Ces règles simples de sécurité doivent être approuvées, en prérequis, par toute personne ayant accès aux systèmes de l'entreprise – employés, sous-traitants et tout autre tiers.

Enfin, les employés doivent être régulièrement formés afin de s'assurer qu'ils ne constituent pas une menace involontaire pour leur entreprise. La formation doit couvrir un large éventail de sujets, allant des motivations des cybercriminels, des mécanismes d'attaques aux mauvaises pratiques pouvant nuire à la sécurité de toute une organisation.

En fin de compte, si la lutte contre les menaces internes peut être difficile, elle n'est pas impossible, mais la transparence et la vigilance sont essentielles. En outre, l'objectif est de créer une culture d'entreprise où la cybersécurité est au premier plan des préoccupations de chacun.
La préparation des employés aux menaces ne peut qu'augmenter les chances de succès de déjouer les pièges des cybercriminels.

Sans compter l'importance cruciale pour chaque entreprise de savoir qui a accès à des données confidentielles, tout comme de comprendre pourquoi et comment ils y accèdent.

Plus la gouvernance et la connaissance de « l'habituel » sont fortes, plus il est alors facile de déceler irrégularités ou changements de comportement vers de « l'inhabituel » – et plus vite il est possible de contrer la vraie menace, potentiellement très lourde de conséquence.