Cybersécurité : l'heure du bilan de santé informatique a sonné

Selon une étude récente de l'Institut de Recherche Technologique SystemX, 50 000 PME françaises ont été victimes d'une cyberattaque en 2017.

Auparavant, les cybercriminels visaient principalement les consommateurs et les grandes entreprises, plus lucratifs. S'il s'agit toujours de cibles de choix, les solutions de sécurité actuellement à leur disposition les aident à contenir les menaces. Les hackers visant les plus vulnérables, ils se tournent alors de plus en plus vers les PME. Beaucoup d'entre elles manquent en effet de ressources et de savoir-faire pour déployer elles-mêmes des règles et des outils de cybersécurité efficaces.

Lorsqu'une attaque fait la Une des journaux, les dirigeants peuvent être amenés à penser « heureusement que mon entreprise n'est pas touchée », ou bien « cela ne nous arrivera jamais ». En réalité, il s'agit plus de chance et de malchance qu'autre chose. Pour éviter d'être le prochain sur la liste des pirates, la première étape incontournable consiste à faire un bilan de santé IT complet. Les petites entreprises victimes d'une compromission le font souvent après l'attaque, lorsqu'il est déjà trop tard. Plus inquiétant encore, seulement 45 % d'entre elles font effectivement de tel bilan, selon une étude Avast. Alors que le volume d'attaques augmente, il est urgent que les PME fassent le point régulièrement sur la protection de leurs infrastructures, leurs systèmes et leurs procédures internes, et qu'elles prennent des mesures immédiatement si le bilan n'est pas optimal. Mener proactivement des tests et vérifier que les employés suivent les bonnes pratiques en termes de cybersécurité est devenu vital.

Pour s'assurer que leur sécurité est optimale, les entreprises doivent en priorité analyser quatre points clés :

- Le routeur : il s'agit de la porte d'entrée pour tous les objets connectés au sein de l'organisation, et peut donc les compromettre lorsque son mot de passe n'est pas protégé. Si un service en ligne, utilisé en interne, a été compromis, il y a de fortes chances que les identifiants soient vulnérables. Il est donc important de changer régulièrement les mots de passe de tous les appareils et utilisateurs.

- Les mises à jour : les organisations doivent les installer dès leur disponibilité, car elles incluent souvent la correction de vulnérabilités. Peu importe le nombre d'employés, il faut que tous les terminaux connectés au réseau, tels que les ordinateurs, les téléphones ou encore les imprimantes, bénéficient des mises à jour dans les meilleurs délais. Elles peuvent être effectuées la nuit sur la plupart des appareils. Par conséquent, il n'y a pas d'excuse valable pour ne pas les faire ou pour les reporter à un moment jugé plus opportun.

- Une solution de sécurité à jour : elle détectera et bloquera les logiciels malveillants, tels que les ransomwares, avant qu'ils ne causent des dégâts. Elle signalera de plus les malwares « enregistreur de frappes », capable de récupérer tous les mots de passe créés par les employés. De tels outils

seront à même de protéger effectivement les organisations si, et seulement si, ils sont à jour.

- Des mots de passe forts : cela consiste à retenir une phrase, ou une série de mots, et à la personnaliser en ajoutant des caractères spéciaux - nombres, symboles, ponctuations - afin de créer un identifiant unique et complexe pour chaque compte. Des combinaisons simples, tels que le nom d'un proche, d'un animal de compagnie, ou encore « motdepasse » et « 1234 », doivent être bannis. Enfin, ceux utilisés pour des comptes personnels sont à différencier des professionnels, pour contenir les risques en cas de compromission.

Ensuite, trois mesures importantes sont à appliquer :

- Changer les mots de passe régulièrement : une fois les étapes précédentes effectuées, il est vivement conseillé de mettre en place une procédure obligeant les employés à changer leurs codes d'accès tous les trimestres. Cette mesure simple réduit fortement les cybermenaces, dont la fraude en ligne, le vol de données et le piratage.

- Déployer une double authentification : elle offre une couche supplémentaire de sécurité pour les accès vers le réseau de l'entreprise ou les sites web, tels que Google Drive. Les employés peuvent ainsi utiliser leur téléphone portable, sur lequel ils recevront un code à usage unique, à renseigner sur l'ordinateur au moment de se connecter. Cette technique vérifie donc l'identité de l'utilisateur et rend plus difficile l'accès au réseau par des personnes malveillantes.

- Déterminer des règles de sécurité : pour une protection durable, les PME sont encouragées à accroitre les connaissances et compétences de leurs employés en matière de cybersécurité, et à rendre obligatoires les bonnes pratiques en ligne. Il est essentiel que des programmes de formation soient implémentés pour faire connaitre les menaces les plus courantes, telles que le ransomware et le phishing, afin que les équipes reconnaissent facilement et rapidement toute tentative d'attaque. Le risque de compromission sera dès lors réduit. Le dialogue sur les pratiques en place, et leur évolution, doit s'ouvrir et être encouragé de manière formelle au moins plusieurs fois dans l'année.

Parce que la question n'est plus « si » mais « quand » une entreprise, quelle que soit sa taille, sera victime d'une cyberattaque, les PME doivent sérieusement considérer le cyber-risque, adopter les bonnes pratiques et mettre en place des outils adaptés, sans oublier de les faire évoluer en fonction des besoins et des menaces. Un enjeu majeur dans un contexte de digitalisation croissante des organisations et de la sophistication grandissantes des attaques.