96% des attaques informatiques peuvent être évitées

Si les solutions de sécurité se développent, les armes des cybercriminels aussi. Que ce soit par des moyens techniques (attaques massives, automatisées ou manuelles, ciblées ou non, nouvelles générations de malwares, vols et exploitations de données, etc.) ou par manipulation humaine (phishing, ingénierie sociale, etc.), **les tentatives d'intrusion des systèmes d'information des entreprises ne cessent d'augmenter**.

En témoigne le rapport *Verizon Data Breach Investigations Report 2011* (DBIR), élaboré en collaboration avec les Services secrets américains et la Dutch national high tech crime unit (NHTCU), qui dresse l'état des lieux de la cybercriminalité dans le monde sur ces sept dernières années (soit quelques **1700 infractions étudiées représentant plus de 900 millions de fichiers compromis**). Ses auteurs constatent une recrudescence des cas de compromissions de données, toutes techniques confondues. Et celles-ci sont nombreuses.

« Le fait est qu'il n'est pas nécessaire de mobiliser des méthodes ultra sophistiquées pour accéder aux données stratégiques des entreprises, précise cependant **Cyril Simonnet**, responsable des ventes de solutions de sécurité chez Verizon Business. *Souvent, d'ailleurs, les victimes ignorent qu'elles ont été attaquées jusqu'à ce qu'un tiers les en informe, et il faut reconnaître que quasiment toutes les intrusions auraient pu être évitées. »*

Comment? En commençant par **appliquer simplement les règles de sécurité de base**. Car selon le rapport, la majorité des attaques sont le fait de piratage (50 %) et de corruption du système par des programmes malveillants (49 %). Lesquels sont souvent injectés par l'obtention d'autorisations ou de mots de passe faciles à deviner ou volés. *« Les cybercriminels pratiquent également de plus en plus de petites attaques opportunistes, qui parviennent à atteindre les systèmes des entreprises avec des méthodes peu sophistiquées. »*

Pour échapper à ces attaques «peu sophistiquées», Verizon propose une série de recommandations simples et néanmoins fondamentales pour la sécurité des entreprises, quelle que soit leur taille, grands comptes comme PME :

• **Se concentrer sur les contrôles essentiels** : beaucoup d'entreprises font l'erreur de viser un très haut niveau de sécurité sur certains points tout en négligeant complètement les autres. On est bien mieux protégé lorsque les normes élémentaires sont appliquées dans l'ensemble de l'organisation, sans aucune exception.

• **Ne conserver que les données utiles** : si vous n'avez pas besoin de ces données, ne les conservez pas. En revanche, les données utiles doivent impérativement être identifiées, surveillées et stockées en lieu sûr.

• **Sécuriser les services d'accès à distance** : restreindre les autorisations à des réseaux et adresses IP prédéfinis, pour limiter les accès publics. Les entreprises ont aussi intérêt à restreindre l'accès aux informations sensibles au sein du réseau.

• **Surveiller les comptes des employés ayant les droits les plus larges** : la meilleure approche consiste à faire confiance à l'utilisateur après avoir vérifié sa probité lors de l'embauche, et en lui accordant des droits d'accès limités en fonction de son rôle ou de ses responsabilités. Les managers doivent fournir des consignes de sécurité claires et vérifier que les collaborateurs respectent effectivement les règles et procédures en place.

• **Vérifier régulièrement les comptes utilisateurs** : s'assurer que les comptes actifs sont valides, utiles, correctement configurés et que les droits d'accès correspondants sont adéquats (les moins permissifs possibles).

• **Gérer et analyser les logs (fichiers-journaux)** : il ne s'agit pas de les étudier par le menu, mais de s'intéresser aux principaux problèmes. L'important est d'abaisser le délai de détection des infractions à quelques jours seulement, contre des semaines, voire des mois. Pour protéger au mieux les données, privilégier les processus de surveillance et d'alerte les plus intelligents, efficaces et réactifs.

• **Sensibiliser les employés** aux méthodes d'ingénierie sociale et aux différents vecteurs d'attaques qu'elles représentent : leur apprendre à s'interroger avant de cliquer sur un lien et à se méfier des pièces jointes aux e-mails dont ils ne connaissent pas l'expéditeur.

Des mesures de bon sens relativement simples à mettre en oeuvre. Elles devraient permettre de **parer 96 % des infractions** analysées par Verizon, selon Cyril Simonnet. Pourquoi guérir plutôt que prévenir, en somme?