Cybercrime : 7,2 millions de dollars par an et par entreprise selon Ponemon

HP a sponsorisé une étude du cabinet Ponemon afin d'évaluer le coût du cybercrime pour les entreprises.

À travers ces investigations, le géant informatique vise d'une part à sensibiliser les dirigeants sur la nécessité d'investir pour protéger leur système d'information; d'autre part, à déterminer le niveau des investissements et les points de vigilance.

Une perte record de 58 millions en un an

Les représentants de Ponemon reconnaissent volontiers que l'exercice a ses limites. Cependant, il donne une idée de l'importance du phénomène, après les enquêtes de terrain. Le panel de 234 entreprises (États-Unis, Royaume-Uni, Japon, Allemagne, France et Australie) représente les divers secteurs économiques pour des entreprises plutôt au-delà de 2 000 salariés (seulement 13 % au-dessous).

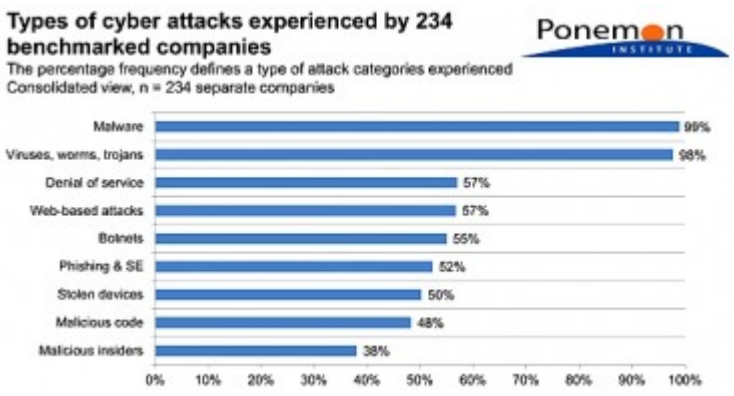
Le cybercrime représente un préjudice de **7,2 millions de dollars par an en moyenne**, pour une enveloppe individuelle allant de 375 387 à 58 millions de dollars, avec une **dépense médiane de 5,479 millions**. Sans polémiquer sur les dollars et la précision des chiffres (que Ponemon présente comme la mesure de ces quelques entreprises révélant une tendance, et non un résultat absolu), on constate qu'il s'agit néanmoins de sommes conséquentes.

Les sociétés de l'échantillon ont enregistré un total de **343 attaques réussies par semaine, soit 1,4 par organisation** ! Et lorsqu'on sait qu'un grand nombre d'attaques ne sont pas détectées, l'inquiétude devient légitime.

Lors de la même enquête en 2012, le total s'élevait à « seulement » à 262 attaques réussies par semaine. Le cybercrime se porte donc plutôt bien !

On voit bien ce qu'on analyse plus

Le tiercé des attaques les plus citées (et donc repérées) par les entreprises n'est guère surprenant : **logiciels malveillants** (99 %), **virus-vers-chevaux de Troie** (98 %), **dénis de service et attaques web** (toutes deux à 57 %).



En fait, les services informatiques ont généralement déployé des anti-virus et anti-malwares plutôt efficaces pour repérer la plupart d'entre elles. D'autant plus que les DSI automatisent ou sensibilisent les utilisateurs pour effectuer les mises à jour de ces outils. Plus encore, certains logiciels serveurs veillent aussi au grain dans le système d'information.

Les "**malware insiders**" (employé ou personne autorisée utilisant son accès aux données de façon nuisible ou illégale) arrivent en tête des **attaques qui coûtent le plus** aux entreprises. Sur l'évaluation annuelle moyenne des coûts liés aux attaques, ces attaques reviennent à 154 453 dollars par an pour chaque entreprise de l'échantillon. Un état de fait qui perdure depuis les débuts de l'informatique. Cette plaie béante a vraiment du mal à se refermer…

En seconde position, le déni de service se traduit, lui, par une facture moyenne de 140 000 dollars en 2013. Une place assez logique, puisque cette attaque peut bloquer l'accès au système et les échanges, engendrant rapidement des pertes immédiates (par exemple sur les sites d'e-commerce). Malgré les multiples mécanismes de protection existants, l'habileté des pirates continue de mettre à mal les équipements et logiciels réseau exposés.

Juste derrière, le phishing (usurpation d'identité) et les équipements volés dépassent la somme de 80 000 dollars par an. Quant aux virus-vers-chevaux de Troie et aux malwares, il arrive en queue de classement respectivement à 630 et 491 dollars !

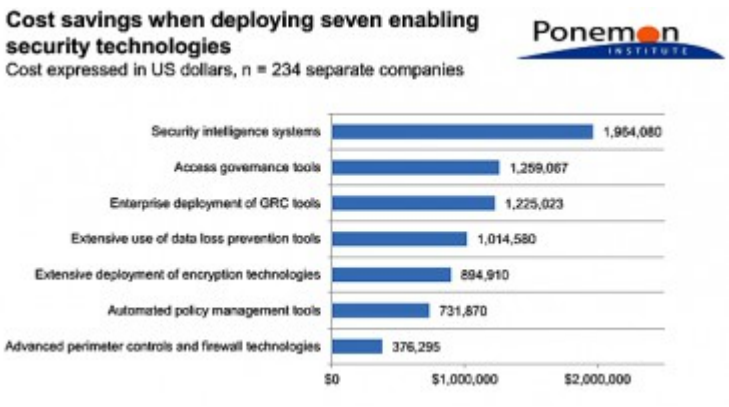
Parmi les "coûts externes" liés aux attaques, les sondés citent : **l'interruption d'une activité de l'entreprise** (38 %), **la perte d'informations** (35 %), **la perte de revenus** (22 %) ou les équipements endommagés (5%).

Quant aux coûts internes de lutte contre les attaques, la détection (29 %) et la reprise après incident (25 %) représentent les dépenses les plus importantes. L'endiguement (arrêter l'expansion d'une attaque, 15 %) ou l'investigation (14 %) devancent la gestion des incidents (10 %). On se demande alors si un schéma de prévention volontariste donnerait les mêmes résultats…

Un arsenal diversifié, à perfectionner…

Suite aux réponses, le cabinet Ponemon a dressé une liste des 7 technologies de sécurité déployées. On y retrouve le déploiement global d'outils de GRC (gestion de la gouvernance, du risque et de la conformité ; à 52 %), les firewall et contrôles périmétriques évolués (à 51 %) ou la prévention de pertes de données (à 49 %).

On comprend que le niveau de maturité, certes inégal, mérite encore d'être amélioré. En effet, seuls **49 % de ces entreprises utilisent un système de Security Intelligence** (analyse d'événements, détection anticipée, réponse rapide ou automatisée, etc.), et à peine 45 % ont adopté une solution de gouvernance des accès ! Plus révélateur encore, l'utilisation du chiffrement n'est citée que par 35 % des entreprises. Et logiquement, les outils d'automatisation de politiques automatisées nécessitant une bonne connaissance et un bon niveau de maturité restent moins répandus (27 %).



Pour Ponemon, la situation pourrait être rapidement améliorée au regard de l'efficacité de ces solutions pour épargner des pertes financières liées aux attaques. Ainsi, les systèmes de Security Intelligence auraient déjà préservé près de 2 milliards de dollars aux entreprises du panel. Les outils de gouvernance des accès auraient fait économiser plus de 1,25 milliard. Aux troisième et quatrième places, les outils de GRC affichent 1,225 milliard de pertes financières épargnées contre plus d'un milliard pour la prévention de perte de données.

Crédit photo : © drx Fotolia.com

Voir aussi

Silicon.fr étend son site dédié à l'emploi IT
Silicon.fr en direct sur les smartphones et tablettes