L’employé comme pion dans la lutte pour la cyber-sécurité | Denis JACOPINI

Les études ne le démentiront pas, les employés apparaissent comme l'une des causes principales, volontairement ou non, des fuites de données et des atteintes aux dispositifs de sécurité IT au sein des entreprises. Par conséquent, outre les protections adéquates contre les attaques par des hackers externes, les entreprises ont tout intérêt à passer les dispositifs de sécurité internes de leur organisation au peigne fin. La résistance de la chaîne est en effet celle de son maillon le plus faible…

L'employé en tant que hacker
Il ressort du rapport de la RAND intitulé « Markets for Cybercrime Tools and Stolen Data » que l'élément humain reste un point faible. Parfois, des actes de malveillance entrent en jeu, comme par exemple l'employé mécontent ou envieux qui disperse ou subtilise les informations confidentielles d'une entreprise. En janvier, Morgan Stanley licenciait un travailleur, qui avait prétendument subtilisé des données personnelles (en ce compris des numéros de compte) concernant près de 900 de ses clients et les avait brièvement publiées sur Internet. Néanmoins, le plus souvent, les cyber-incidents connus par une entreprise peuvent être imputés à des actes de négligence, ce dont les criminels tirent volontiers profit. Selon le rapport de la RAND, lesdites campagnes de « phishing » et « spear-phishing » augmenteront substantiellement et sont en même temps de plus en plus sophistiquées. Un exemple connu de spear-phishing concerne la fuite de données – entretemps devenue tristement célèbre – de la chaîne de magasins américaine Target. Les enquêteurs avaient découvert que les hackers avaient obtenu l'accès aux systèmes informatiques de Target au moyen d'un e-mail de spear-phishing adressé à un employé de l'un des fournisseurs externes de Target.
Les conséquences de tels actes de malveillance ou de négligence sont souvent tout sauf anecdotiques. Dans l'exemple de Target, le préjudice se chiffre actuellement à plus de 162 millions de dollars. L'attaque faite sur la marque et la perte de parts de marché constituent à cet égard des dommages importants. Les employeurs se sentent souvent impuissants dans ce genre de situation et observent les bras ballants la manière dont une cyber-attaque cause un préjudice grave à leur entreprise. Cependant, cela ne devrait pas être le cas. Ci-dessous, nous esquissons certains outils ou méthodes pouvant aider à mobiliser vos propres employés, en tant que frères d'armes privilégiés dans la lutte pour la cyber-sécurité.

L'employé en tant que pion contre les hackers
La prévention est et reste le meilleur remède. Les mesures suivantes – spécifiquement en lien avec les activités des employés – fonctionnent en tout cas comme mesures préventives :

– Des dispositifs de sécurité adéquats
Outre la sécurisation effective des données et de l'infrastructure de l'entreprise, il est recommandé de couler les règles d'entreprises concernant la protection des données, la sécurité des systèmes, l'utilisation d'appareils propres (ordinateurs portables, smartphones, tablettes) au sein du réseau de l'entreprise, le travail à distance et d'autres encore, dans ce que l'on appelle des « policies ».

– Des formations périodiques et adaptées pour les employés
Afin de pouvoir mettre en oeuvre les protocoles de sécurité mentionnés ci-dessus de manière effective, les employés au sein de l'entreprise devraient au moins être au courant de leur existence, ainsi que de leur contenu (ainsi que de toute modification), ce que l'on obtient en donnant des formations périodiques et adaptées. Un employé qui de manière durable est bien informé sur ses responsabilités en termes de cyber-sécurité au sein de l'entreprise, et qui sait comment traiter des informations sensibles et confidentielles concernant l'entreprise ou les personnes, constituera une cible moins évidente pour les hackers externes et sera plus attentif. Une telle approche met également l'accent sur l'intérêt que l'entreprise porte à la sécurité de ses propres systèmes et données.

– Un screening adéquat des nouveaux employés
Lors du recrutement et de la sélection de nouveaux employés, l'employeur scrute de plus en plus souvent le profil d'un candidat sur les réseaux sociaux (Facebook, Twitter etc.). Attention cependant : l'employeur peut consulter ces données, mais ne peut les traiter sans respecter les règles légales sur la protection des données personnelles. En outre, il existe également une interdiction de discrimination : le fait de vérifier des informations qui sont publiées par un candidat sur un réseau social ne peut mener à une sélection inéquitable.

– Prévoyez un dispositif d'alerte adéquat
Afin de révéler certains sujets, que l'employé ne peut faire remonter via la voie hiérarchique habituelle et pour lesquels il n'existe pas de procédure ou organe organisé par la loi, l'on peut prévoir un dispositif d'alerte (« whistleblowing ») au sein de l'entreprise. Ce dispositif doit être établi conformément à la législation sur la vie privée et aux recommandations de la Commission de la protection de la vie privée sur le sujet.

– Surveillance de l'utilisation d'Internet et des e-mails par les employés
Une autre mesure de prévention importante réside dans l'installation d'un système au moyen duquel le contrôle de l'utilisation d'Internet et des e-mails par les employés peut être effectué par l'employeur. En effet, une entreprise qui est victime d'une cyberattaque et suppose que l'un de ses membres du personnel en est responsable, ne peut pas rechercher l'employé coupable à la légère. L'employeur doit, à cet égard, respecter la législation sur la vie privée, en ce compris la CCT n° 81, qui met en balance le droit à la vie privée de l'employé et le droit de surveillance de l'employeur.

Un tel système de contrôle ne peut (i) être institué sans que l'employeur en ait informé le conseil d'entreprise et les employés individuellement sur tous les aspects du contrôle ; (ii) seulement être implémenté qu'en raison d'une finalité légitime, telle que par exemple la sécurité et le bon fonctionnement technique du système de réseau IT de l'entreprise. En outre, l'employeur ne peut effectuer qu'un contrôle graduel et progressif. En premier lieu, seuls les contrôles généralisés et anonymes (au moyen d'échantillons) sont autorisés sans que les données puissent être individualisées et donc sans pouvoir cibler un employé en particulier. Ce n'est que lorsque l'employeur suspecte qu'un abus par un employé a eu lieu qu'il peut procéder à l'individualisation des données personnelles afin de pouvoir rechercher le « coupable ».

Conclusion
En résumé, l'on peut dire qu'au vu des atteintes à la réputation et autres conséquences financières des cyber-incidents sur les entreprises, il vaut mieux prévenir que guérir. La mise en application des mesures décrites ci-dessus constitue en tout cas un pas dans la bonne direction.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://datanews.levif.be/ict/actualite/l-employe-comme-pion-dans-la-lutte-pour-la-cyber-securite/article-opinion-373053.html