On récolte ce que l'on sème : la cybersécurité commence avec les employés

Il est souvent dit que « la folie consiste à faire la même chose encore et encore et à attendre des résultats différents » (Rita Mae Brown), une affirmation qui s'illustre bien souvent en cybersécurité. En effet, les comptes à privilèges sont les plus utilisés pour mener à bien une cyberattaque ; et, selon un récent rapport de Verizon, les mots de passe volés sont responsables des violations de données dans 29% des cas, prenant la première place des causes de compromissions. Pourtant, et malgré les multiples campagnes de sensibilisation et mises en garde, les entreprises continuent d'axer leur sécurité sur des solutions périmétriques ; on sait pourtant que cette stratégie est insuffisante, notamment une fois que le cybercriminel parvient à s'introduire dans le réseau ou contre une menace interne posée par des employés mécontents.

Selon David Higgins, EMEA Technical Director, chez CyberArk, bon nombre d'entreprises ne placent pas leurs employés au centre de leur stratégie de cybersécurité, mettant en danger sur le long terme leurs informations sensibles et leurs activités opérationnelles.

Face aux techniques des hackers qui évoluent constamment, les entreprises doivent absolument mettre en place des programmes de formation et de sensibilisation réguliers afin de se prémunir autant que possible contre les vulnérabilités générées par des employés malveillants, négligents ou mal informés. En effet, l'un des défis majeurs de toute entreprise est l'erreur humaine : les clics sur des liens de phishing racoleurs à priori légitimes, les visites de sites internet infectés par un ransomware, ou encore les individus ne suivant pas à la lettre les procédures ou règles de sécurité. Or, les entreprises considèrent souvent que leurs employés sont les seuls responsables en cas de compromission, ce qui trahit un manque de concentration sur ce qui est vraiment important pour l'organisation et nécessite donc d'être protégé : les données, les applications et les accès critiques. Si les comportements des employés en matière de cybersécurité peuvent toujours s'améliorer, les employeurs sont les premiers responsables en cas de faille. Ils doivent veiller à la mise en place d'une politique de sécurité du moindre privilège, afin de limiter les accès aux actifs et fichiers selon les réels besoins des collaborateurs.

En effet, nos récentes recherches ont aussi révélé qu'un nombre considérable d'employés ont accès à des informations sensibles et inutiles dans le cadre de leurs tâches quotidiennes. 46 % des personnes interrogées auraient eu accès aux bases de données RH des employés, ce qui rend possible des compromissions d'informations confidentielles en cas de vol d'identifiants ; tandis que trois sur dix (29 %) accèderaient aux comptes bancaires de leur entreprise facilitant le vol d'argent via des identifiants légitimes. D'ailleurs, la plupart des études conduites actuellement sur le sujet par les acteurs du marché, démontrent que les entreprises ne peuvent pas compter uniquement sur leurs employés, ni sur la mise en place de défenses périmétriques, pour sécuriser leurs données.

Les organisations s'exposent en outre à des risques supplémentaires en permettant aux employés d'accéder à des informations hautement confidentielles, essentielles à la croissance et à la pérennité des activités opérationnelles : du chiffre d'affaires, aux projets de développement commercial de leur organisation, en passant par les plans de RD, ou autres informations relatives à de nouveaux produits ou services. Il s'agit là d'une voie royale pour les individus malveillants, externes comme internes, à même de mettre en péril la situation financière de l'entreprise, de voler ou dupliquer la propriété intellectuelle et par conséquent de mettre en danger sa position sur le marché.

Finalement, fournir aux employés un accès illimité à des informations confidentielles accroît considérablement leur vulnérabilité. Les entreprises doivent donc adopter des contrôles proactifs leur permettant de gérer plus efficacement les informations d'identification, d'empêcher l'escalade de privilèges et de protéger leurs salariés contre les menaces internes et externes ; sans pour autant perturber leur activité. De plus, l'adoption d'outils avancés surveillant tous les accès à privilèges, et analysant et détectant les comportements à hauts risques, permet aux organisations de gérer efficacement les privilèges, sans perturber les activités opérationnelles. L'objectif est donc de positionner la sécurité comme un allié auprès des employés, plutôt qu'un couperet potentiel. »