Cyberattaques : une entreprise sur deux touchée à cause de.... ses clients

Dans son étude « cyber insécurité : gérer les menaces de l'intérieur », Proofpoint, leader de la cybersécurité en entreprise, pointe la vulnérabilité humaine à l'origine des vols de données et des cyberattaques. Comment faire pour réduire ce facteur humain et sécuriser les entreprises ? Quelques pistes à suivre.

Temps de lecture : minute

29 octobre 2019

En 2017, Yahoo subissait une cyberattaque. Résultat : 3 milliards de comptes exposés. Un an plus tard, c'est Facebook qui avouait s'être fait subtiliser les données de 500 millions d'utilisateurs. Et ces deux géants ne sont pas les seuls. Sur les 300 cadres interrogés dans l'étude de Proofpoint, 86% indiquent avoir subi une cyberattaque au cours des 3 dernières années et 60% au moins 4. Et à ce jeu, aucune entreprise n'est épargnée, le facteur humain restant présent dans les petites comme les grandes structures.

Un risque humain connu et reconnu

Pour 48% des cadres interrogés, les failles humaines (malwares, emails frauduleux, phishing) figurent parmi les trois principaux facteurs d'attaques. Et contrairement aux idées reçues, les salariés ne sont pas les premiers touchés. Les hackers frappent souvent les entreprises à travers leurs clients (48%) puis leurs employés (43%) et enfin les travailleurs temporaires (38%). La famille et les proches des salariés sont cités en 6ème position, preuve que le problème ne se cantonne pas à

l’entreprise mais à son cercle élargi. Or, les dirigeants n’ont peu ou pas de mainmise sur ces individus.
Le risque zéro n’existe donc pas et la vulnérabilité liée aux facteurs humains ne peut que se limiter. Les cadres interrogés sont d’ailleurs conscients de la croissance de ce phénomène (47%) tout en restant assez confiants sur la capacité de leurs dirigeants à résoudre ces difficultés (76%). Ils reconnaissent pratiquement tous que des mesures sont déjà mises en place pour contrôler ces risques (96%).

Des dirigeants et des cadres engagés

Parmi les solutions citées, le cloud apparaît comme un premier élément de protection des données. Un cadre sur deux annoncent d’ailleurs y avoir transféré la moitié de ses données. Parmi le autres solutions envisagées pour lutter contre les violations de données, on trouve :

- Mettre en place une double authentification (93%)
- Réaliser des tests réguliers sur les données (96%)
- Intégrer des programmes sécurisés et faire migrer les données dans le cloud (96%)

Du côté des failles humaines, d’autres process sont proposés :

- Définir et limiter l’accès à certaines données (95%)
- Bloquer l’accès aux boîtes mails personnelles (91%)
- Renforcer l’information sur les enjeux liés à la sécurité (93%).

Impliquer et former pour mieux responsabiliser

Au niveau humain, les cadres ayant expérimenté plusieurs solutions soulignent l’efficacité des formations (35%) et l’élaboration commune des politiques de sécurité (34%). L’implication des salariés, quelque soit le

métier qu’ils exercent dans l’entreprise, est un facteur fondamental de réussite. Leur retour sur d’éventuelles failles permettra ainsi de prédire le type d’attaques employées, de même que l’analyse de leurs comportements et de leurs habitudes servira à établir des plans d’actions mieux ciblés.
Pour mieux sensibiliser les salariés, l’étude propose également de les mettre en situation de tentative de violation de données.

Paradoxalement, les entreprises peinent encore à mettre en place une unité de cybersécurité au sein de leur entreprise.

Créer une unité spécialisée, une idée trop peu suivie

Moins d’une entreprise sur deux a créé un pôle cybersécurité en charge de cette question. Au mieux, il s’agit du directeur de la technologie (26%), du service informatique (15%) ou d’un partage de responsabilité entre divers responsables (12%). Une situation qui ne convient pas aux cadres. Selon eux, le DSI doit en faire une partie intégrante de l'informatique (94%), et le rôle du RSSI devrait être renforcé pour qu'il fonctionne aux côtés du CIO plutôt que de lui rendre compte (91%).

Pour réduire le risque humain responsable de failles et de cyberattaques, misez sur la coopération et l’information de vos salariés pour leur inculquer les bonnes pratiques.

Article écrit par Anne Taffin