

Authentification forte et formation : l'alliance optimale face aux cybermenaces

S curit 

Post  par : JPilo

Publi e le : 17/3/2023 14:00:00

Les violations de donn es continuent d' tre un r el fl au pour les entreprises et particuliers. En plus de causer de s v res dommages financiers, elles portent en effet atteinte   la r putation des marques et minent la confiance des consommateurs. Selon le rapport de l'Identity Theft Resource Center (ITRC), les vols d'informations sensibles auraient augment  de 41,5 % en 2022, par rapport   2021.

Ainsi, Fabrice de Vesian, Sales Manager chez Yubico, explique que les entreprises doivent investir sans attendre dans des syst mes de s curit  et des formations pour leur personnel, pour faire face aux cybermenaces de plus en plus complexes :

 « Selon nos recherches, plus de la moiti  (59 %) des employ s reconnaissent ainsi avoir recours   des noms d'utilisateur et des mots de passe comme principale m thode d'authentification, alors que moins d'un quart (23 %) des entreprises les consid rent comme les moyens les plus s rs pour se connecter.

De ce fait, pr s de 61 % des salari s fran ais interrog s s'accordent   dire qu'elles devraient passer   une approche MFA moderne efficace contre le phishing, telle qu'une cl  de s curit  mat rielle. En effet, 87 % des utilisateurs qui utilisent cet outil pour authentifier leurs comptes professionnels estiment qu'il s'agit d'une protection suffisante.

En effet, malgr  une digitalisation croissante, nombre d'organisations n'acc lent pas le renforcement des pratiques de cyber-hygi ne. En effet, certaines utilisent toujours des outils et des proc dures obsol tes, qui ne sont plus en phase avec les risques actuels. Pr s d'un tiers des employ s, expos s   une attaque en ligne au cours des 12 derniers mois, d clarent ainsi que leur entreprise se contente de r initialiser les mots de passe ou ont recours   des solutions provisoires.

Par cons quent, d'autres types d'approches pour v rifier l'identit  des utilisateurs sont   envisager ; telles que la connexion sans mot de passe   l' preuve du phishing et l'authentification forte   deux facteurs ou multifactorielle (2FA/MFA).

Ces solutions assurent un lien entre l'identification des utilisateurs internes et externes tout en restant faciles   utiliser et non chronophages. Plus particuli rement, les cl s de s curit  FIDO2 sont consid r es comme la r f rence pour une connexion r sistante au phishing, car elles s'appuient sur des protocoles d'authentification modernes efficaces contre ces cyberattaques.

Notre  tude d montre  galement que trop peu de salari s ne b n ficient de formations   la cybers curit  : 42 % des employ s ne sont pas tenus de suivre des formations r guli res sur la cybers curit  et environ un quart (24 %) disent que cela se produit rarement ou jamais.

Or, des employ s insuffisamment form s   la cybers curit  ne seront pas en mesure d'appliquer une cyber-hygi ne ad quate au quotidien, ni de r agir de mani re optimale en cas d'exposition   une menace ; ce qui peut entra ner des pertes financi res ou encore en termes d'image de marque. Les risques en ligne  voluent constamment, il est donc

imp ratif, pour toute entreprise, d en informer et de former leurs  quipes en cons quence.

Dans lâ€¢ensemble, ces r sultats indiquent que des entreprises ne d ploient pas encore des mesures de cybers curit  optimales et ne proposent pas les formations n cessaires   leurs  quipes. Cependant, sans cela, elles ne peuvent pas faire face au nombre croissant de menaces en ligne. Il est aussi indispensable de passer   des formes d authentification plus fiables, telles que la MFA r sistante au phishing.  »