Cybermoi/s : la nÃ©cessitÃ© de renforcer ses pratiques de sÃ©curitÃ©
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 27/10/2023 15:00:00

83 collectivitÃ©s et organisations ont souscrit Ã une Â« cybercharte Â» visant Ã accroÃ®tre la prise de conscience quant aux enjeux de la sÃ©curitÃ© en ligne.

Parmi les signataires, se trouvent lâ□□agence nationale de la sÃ©curitÃ© des systÃ¨mes dâ□□information (ANSSI) et la CNIL (Commission nationale de lâ□□informatique et des libertÃ©s), lesquelles prÃ©conisent des mesures Ã mettre en place au sein des structures, privÃ©es et publiques, en vue de garantir une meilleure protection.

Lâ□□une des mesures recommandÃ©es consiste Ã dÃ©ployer une authentification multi-facteur (MFA) rÃ©sistante au phishing, qui peut prendre la forme de clÃ©s de sÃ©curitÃ© matÃ©rielles ou dâ□□identifiants biomÃ©triques. Ce dispositif ajoute une couche de sÃ©curitÃ© supplÃ©mentaire, rÃ©duisant ainsi considÃ©rablement le risque de piratage.

Dans ce contexte, Fabrice de VÃ©sian, Sales Manager France chez Yubico, explique que les entreprises peuvent davantage optimiser leurs protocoles de sÃ©curisation des donnÃ©es en adoptant une approche de lâ□□authentification sans mot de passe. Cette dÃ©marche offre aux organisations une opportunitÃ© concrÃ¨te dâ□□Ã©riger une barriÃ¨re plus robuste contre les menaces potentielles, tout en favorisant une meilleure protection des systÃ¨mes critiques :

Â« Nos recherches ont dÃ©montrÃ© quâ□□en France, seuls 17 % des employÃ©s utilisent des clÃ©s physiques pour lâ□□authentification des comptes professionnels, soulignant ainsi l'urgence d'accroÃ®tre la sensibilisation des utilisateurs aux risques associÃ©s aux pratiques de sÃ©curitÃ© dÃ©passÃ©es. Il est impÃ©ratif que les entreprises prennent des mesures pour amÃ©liorer leur posture en matiÃ¨re de cybersÃ©curitÃ©, afin de rÃ©duire la vulnÃ©rabilitÃ© aux attaques par ransomware et au phishing.

Pour attÃ©nuer efficacement ces menaces, et comme le suggÃ¨rent lâ□□ANSSI et la CNIL, les entreprises doivent mettre en place une authentification multi-facteur (MFA) rÃ©sistante au phishing, telle quâ□□une clÃ© de sÃ©curitÃ© matÃ©rielle FIDO2. Cette approche en matiÃ¨re dâ□□authentification renforce significativement la protection des comptes professionnels et contribue Ã prÃ©venir les risques liÃ©s Ã la cybercriminalitÃ©.

Par ailleurs, les prises de contrÃ´le de comptes, le phishing et les attaques de type "man-in-the-middle" figurent parmi les mÃ©thodes les plus courantes aujourd'hui, susceptibles de conduire Ã une compromission de donnÃ©es.

Ces attaques ont des rÃ©percussions qui dÃ©passent le cadre de l'entreprise, et impactent directement les clients et les employÃ©s. L'authentification rÃ©sistante au phishing doit donc devenir la nouvelle norme de sÃ©curitÃ©, câ□□est une urgence au regard de lâ□□omniprÃ©sence des cybermenaces.

De plus, il est nÃ©cessaire quâ□□elles amÃ©liorent leurs pratiques de cybersÃ©curitÃ© et que les utilisateurs apprennent Ã se protÃ©ger en ligne, au-delÃ des identifiants classiques. La mise en place de formations rÃ©guliÃ¨res sur les cyber-risques revÃªt une importance cruciale pour garantir que les employÃ©s soient sensibilisÃ©s aux menaces numÃ©riques et sachent comment y rÃ©agir de maniÃ¨re adÃ©quate.

Alors que le paysage des menaces devient plus complexe et hostile, il devient crucial pour les entreprises de prendre des mesures proactives pour sÃ©curiser les opÃ©rations en ligne, quelle que soit leur taille, quel que soit leur secteur dâ□□activitÃ©.

Dans ce sens, lâ□□adoption de la MFA moderne offre non seulement une protection accrue pour les donnÃ©es sensibles de l'entreprise, mais contribue Ã©galement Ã renforcer la confiance des clients et la tranquillitÃ© d'esprit des employÃ©s, qui savent que leurs informations sont sÃ©curisÃ©es de maniÃ¨re optimale. Â»