CybersÃ©curitÃ© : le dÃ©fi des postes de travail partagÃ©s
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 2/8/2023 13:00:00

Les environnements de postes de travail partagÃ©s sont courants dans de nombreux secteurs, des terminaux de point de vente dans le commerce aux ordinateurs partagÃ©s dans les ateliers de fabrication, ou encore dans les Ã©tablissements et services de santÃ©, un secteur qui a Ã©tÃ© particuliÃ¨rement ciblÃ© par des cyberattaques au cours de ces derniers mois en France.

Selon Fabrice de VÃ©sian, Sales manager France chez Yubico, bien qu'il y ait une question dâ□□Ã©conomies de coÃ»ts et dâ□□augmentation de la productivitÃ© lorsque plusieurs collaborateurs partagent un mÃªme terminal, cela peut constituer une menace de sÃ©curitÃ© importante pour les entreprises si des mesures de protection solides ne sont pas prises pour s'assurer que seuls les bons utilisateurs peuvent se connecter :

Â« Les successions dâ□□Ã©quipes qui fonctionnent en roulement, les employÃ©s saisonniers et la collaboration au sein dâ□□un mÃªme service entraÃ®nent souvent des pratiques d'espace de travail partagÃ© non sÃ©curisÃ©es, telles que des identifiants de connexion partagÃ©s ou des notes sur des post-its visibles avec des mots de passe Ã©crits dessus.

Le secteur de la santÃ©, notamment dans les hÃ´pitaux ou les cliniques par exemple, comporte de nombreux postes partagÃ©s et sâ□□est retrouvÃ© de maniÃ¨re croissante dans le viseur des cybercriminels en quÃªte de donnÃ©es personnelles fiables, et donc lucratives.

De maniÃ¨re gÃ©nÃ©rale, les informations d'identification restent une cible de choix lors dâ□□une cyberattaque, avec 81 % des compromissions de donnÃ©es causÃ©es par des mots de passe volÃ©s ou faibles. Cela signifie que les informations d'identification statiques ne sont pas sÃ©curisÃ©es.

L'authentification multifacteur (MFA) est une premiÃ¨re ligne de dÃ©fense facile contre les risques posÃ©s par les espaces de travail partagÃ©s, mais toutes ses formes ne sont pas Ã©gales.

Les mÃ©thodes de MFA traditionnelles, basÃ©es sur les mobiles, que ce soit via les SMS, les mots de passe Ã usage unique et les notifications push, sont trÃ¨s sensibles aux cyberattaques telles que le phishing, les attaques par force brute, les attaques Man-in-The-Middle (MiTM), les logiciels malveillants et l'Ã©change de carte SIM.

Il faut Ãªtre conscient que lâ□□authentification multifacteur via un mobile prÃ©sente plusieurs failles de sÃ©curitÃ© importantes : il n'y a aucune garantie rÃ©elle qu'une clÃ© privÃ©e se retrouve sur un Ã©lÃ©ment sÃ©curisÃ© de l'appareil mobile.

Par exemple, un mot de passe Ã usage unique et une clÃ© privÃ©e peuvent en effet Ãªtre interceptÃ© d'une maniÃ¨re ou d'une autre, et il est impossible d'assurer une preuve de possession. Au-delÃ de la sÃ©curitÃ©, cette mÃ©thode dâ□□authentification pose d'autres dÃ©fis : les appareils mobiles peuvent manquer de batterie et leur utilisation peut mÃªme Ãªtre interdite, en particulier dans les fonctions en contact direct avec les clients ou dans les zones Ã haute sÃ©curitÃ©.

D'autre part, dans ces environnements sensibles, les utilisateurs ont parfois des gants, empÃªchant l'utilisation de certaines mÃ©thodes de connexion alternative telles que Windows Hello For

Business, ou bien il arrive que l'usage d'un mobile y soit simplement interdit, rendant ces mÃ©thodes traditionnelles inutilisables.

Remplacer lâ□□authentification multifacteur traditionnelle par des solutions modernes rÃ©sistantes au phishing, telles que les clÃ©s de sÃ©curitÃ© matÃ©rielles, est une stratÃ©gie efficace qui offre une protection accrue contre les attaques de plus en plus sophistiquÃ©es pour les environnements de postes de travail partagÃ©s ; un enjeu crucial au regard de lâ□□omniprÃ©sence des cybermenaces qui planent sur les donnÃ©es au sein des organisations, tous secteurs confondus.Â»