Alors que près de 80% des cyberattaques ciblent des écoles, comment sécuriser l'enseignement hybride ?

La digitalisation accÃ©lÃ©rÃ©e par la pandÃ©mie associÃ©e Ã la nÃ©cessitÃ© de sâ€™adapter rapidement Ã lâ€™enseignement Ã distance a fait des Ã©coles la cible idÃ©ale des cybercriminels. Compte tenu dâ€™un dÃ©savantage en termes de technologies et de compÃ©tences disponibles par rapport aux universitÃ©s, lâ€™enseignement primaire et secondaire Ã©tait par ailleurs encore moins prÃ©parÃ© Ã relever les nouveaux dÃ©fis en termes de sÃ©curitÃ© posÃ©s par une exposition accrue et des risques plus Ã©levÃ©s.

Les analystes en cybersÃ©curitÃ© affirment que lâ€™Ã©ducation est le secteur le plus vulnÃ©rable aux cyberattaques : il concentre selon Microsoft prÃ¨s de 80% des incidents liÃ©s Ã des malwares signalÃ©s au cours des 30 derniers jours. Sâ€™il est vrai que la sÃ©curitÃ© des donnÃ©es est une prioritÃ© pour tous les secteurs, dans lâ€™Ã©ducation, il est particuliÃ¨rement important de protÃ©ger les informations sensibles et la vie privÃ©e des utilisateurs, comme les informations personnelles des Ã©lÃ¨ves, de leurs familles et du personnel sur lâ€™ensemble des appareils utilisÃ©s.

Compte tenu du contexte dans lequel Ã©voluent actuellement les Ã©coles, qui fait se cÃ´toyer apprentissage virtuel, en prÃ©sentiel et Ã lâ€™aide dâ€™appareils personnels, les menaces potentielles sont nombreuses : citons parmi les plus frÃ©quentes, les ransomwares, les fuites de donnÃ©es, le phishing, les attaques DDoS (dÃ©ni de service distribuÃ©), lâ€™exploitation de vulnÃ©rabilitÃ©s IoT, lâ€™usurpation de domaines ou encore Ã©videmment le cyberharcÃ¨lement ou le doxing.

Le cyberharcÃ¨lement, une menace pour la sÃ©curitÃ© ?

Selon les chiffres de lâ€™UNICEF, au niveau mondial, 56,6 % des enfants Ã¢gÃ©s de 12 Ã 24 ans ont Ã©tÃ© victimes de cyberharcÃ¨lement. Bien que le cyberharcÃ¨lement ne relÃ¨ve pas officiellement de la cybercriminalitÃ©, cette limite peut parfois Ãªtre franchie. Dans les cas les plus malveillants, ce type de harcÃ¨lement peut donner lieu Ã une divulgation de donnÃ©es personnelles (on parle de Â« doxing Â») lorsque lâ€™harceleur parvient Ã prendre le contrÃ´le des comptes de messagerie ou de rÃ©seaux sociaux de ses victimes dans le but de publier leurs informations personnelles pour les mettre dans lâ€™embarras ou Ã sâ€™introduire dans leur appareil Ã lâ€™aide dâ€™un malware, accÃ©dant ainsi Ã leur localisation ou Ã des informations sensibles.

Selon les donnÃ©es de Statista, 6 % des utilisateurs de plateformes en ligne ont Ã©tÃ© victimes de piratage et 4 % ont perdu le contrÃ´le de lâ€™accÃ¨s Ã leurs appareils. Cela montre que le harcÃ¨lement en ligne peut Ã©galement devenir une menace pour la sÃ©curitÃ© numÃ©rique et quâ€™il doit donc Ãªtre pris en compte.

Parce que le fait dâ€™Ãªtre conscient du problÃ¨me ne le fait pas disparaÃ®tre, il est nÃ©cessaire dâ€™Ã©duquer les enfants et les adolescents afin quâ€™ils puissent assurer leur sÃ©curitÃ© en ligne et Ã©viter quâ€™une situation dÃ©jÃ dÃ©sagrÃ©able en soi nâ€™ait des consÃ©quences encore plus graves. Quelles mesures pendre pour minimiser la menace dâ€™une faille de cybersÃ©curitÃ© ?

Maintenir les logiciels Ã jour : les entreprises incluent souvent des correctifs de sÃ©curitÃ© et des amÃ©liorations dans les mises Ã jour des logiciels.
CrÃ©er des mots de passe forts : il est important de ne pas se contenter dâ€™utiliser un seul mot de passe simple et facile Ã retenir pour tous ses comptes.
Rester vigilant aux escroqueries : Ã©viter de cliquer sur un lien lorsque lâ€™on a un doute sur la source. En outre, il est important de ne jamais communiquer dâ€™informations personnelles par tÃ©lÃ©phone ou par SMS lorsquâ€™on a affaire Ã un numÃ©ro inconnu ou Ã un appel automatisÃ©.

Comment assurer la sÃ©curitÃ© dâ€™un enseignement hybride ?

Avec des centaines dâ€™Ã©lÃ¨ves et dâ€™enseignants qui doivent accÃ©der au rÃ©seau en toute sÃ©curitÃ© oÃ¹ quâ€™ils se trouvent, les Ã©coles constituent un environnement rÃ©seau complexe et exigeant qui doit impÃ©rativement Ãªtre protÃ©gÃ©. Heureusement, il existe une sÃ©rie dâ€™actions et dâ€™outils qui permettent dâ€™attÃ©nuer les risques en ligne pour les Ã©tablissements dâ€™enseignement :

Concentrer ses efforts sur la formation du personnel aux principes de base de la cybersÃ©curitÃ© et sâ€™assurer quâ€™ils comprennent la nÃ©cessitÃ© dâ€™appliquer certains protocoles en matiÃ¨re de protection des donnÃ©es.
DÃ©signer un responsable de la cybersÃ©curitÃ© pour veiller au respect des bonnes pratiques, avec des audits rÃ©guliers et un processus de signalement en place pour faire remonter tout problÃ¨me ou toute violation potentielle.
Chiffrer et sauvegarder les systÃ¨mes afin de garantir la rÃ©cupÃ©ration des donnÃ©es en cas de violation de la cybersÃ©curitÃ©.
Configurer des rÃ©seaux Wi-Fi sÃ©curisÃ©s qui utilisent un VPN pour toutes les connexions Internet.

En complÃ©ment, installer une solution de sÃ©curitÃ© unifiÃ©e qui protÃ¨ge les environnements, les utilisateurs et les appareils, constitue lâ€™option la plus efficace tout en Ã©tant facile Ã mettre en oeuvre, pour empÃªcher les attaques potentielles Ã tout moment.

La digitalisation de lâ€™enseignement prÃ©sente de nombreux avantages, mais ces avantages peuvent Ãªtre menacÃ©s par une cybersÃ©curitÃ© insuffisante. La formation dans ce domaine est importante, tout comme la mise en oeuvre par les responsables informatiques de nouvelles solutions qui protÃ¨gent les utilisateurs et leur permettent de tirer parti de toutes les possibilitÃ©s offertes par la technologie.