Universités : faire face aux enjeux de cybersécurité

La sécurisation des établissements d'enseignement supérieur représente un défi bien plus grand que celle des autres types d'organisation, qu'il s'agisse d'organismes publics, d'organisations à but non lucratif ou d'entreprises privées. Les établissements d'enseignement supérieur privilégient généralement les environnements informatiques en libre accès, recherchant le juste équilibre entre leur intérêt à faciliter les échanges d'idées et la nécessité de se doter d'une cyberdéfense en mesure de protéger la propriété intellectuelle contre le vol.

En effet, la forte augmentation de cyber-attaques enregistrée au cours des trois dernières années ne concerne pas exclusivement le secteur privé. Les universités constituent autant de cibles alléchantes pour n'importe quel cybercriminel, car leurs réseaux contiennent une multitude d'informations sensibles, telles que les données financières des étudiants, les numéros de sécurité sociale et les informations relatives à la recherche de haut niveau.

La nature de ces informations fait des universités des cibles de choix pour des hackers chevronnés qui sont souvent soutenus par des gouvernements étrangers pour lesquels ces informations sont extrêmement précieuses.

Une protection cauchemardesque

Alors qu'ils contiennent des IP lucratives et une quantité considérable d'informations à caractère personnel, les réseaux universitaires comptent parmi les plus difficiles à sécuriser. D'abord, le nombre élevé d'étudiants et de membres du personnel qui se connectent au réseau chaque jour contraignent les universités à déployer des centaines, voire des milliers de points d'accès qui, à la différence des entreprises privées, sont pratiquement impossibles à sécuriser parfaitement.
Ces circonstances facilitent considérablement l'ancrage initial dans le réseau, une des étapes les plus difficiles et les plus longues du cycle de vie d'une cyber-attaque.

Ensuite, étant donné que les établissements d'enseignement supérieur sont souvent propices au développement de réseaux à trafic intense, ils sont contraints de déployer un système décentralisé doté de différentes fonctions chargées chacune de la sécurité de leur propre part du réseau. Si cette pratique est courante dans le secteur privé, le déploiement d'une série homogène de politiques de sécurité s'avère particulièrement difficile dans un environnement universitaire.

Pour compliquer les choses, un nombre croissant d'étudiants se connectent désormais au réseau avec leurs appareils personnels (BYOD) ce qui accroit la surface d'attaque contre un établissement d'enseignement supérieur présentent par rapport à une entreprise privée. Parallèlement, le flot continu d'étudiants sur le campus rend d'autant plus difficile de distinguer les véritables menaces des activités bégnines – et néanmoins indésirables – telles que le téléchargement de torrents.

Cette culture du libre accès a également une incidence négative sur le comportement des utilisateurs face aux risques, car les étudiants tendent à se sentir moins responsables de leur

activité sur le réseau que le personnel d'une entreprise. En d'autres termes, les utilisateurs des réseaux de l'enseignement supérieur ont tendance à cliquer plus facilement sur des pièces jointes et des liens suspects, tandis que le volume considérable de messages électroniques que s'échangent les étudiants et le personnel de l'université en utilisant des adresses officielles fait des universités la cible idéale pour les campagnes d'hameçonnage.
Les attaques d'ingénierie sociale – telles que l'envoi de logiciels malveillants à travers des comptes Facebook et Twitter – sont particulièrement efficaces dans les universités en raison de l'utilisation quasiment universelle de ces services de la part des étudiants.

Enfin, l'intégration généralisée de dispositifs IoT faiblement sécurisés au sein des universités facilite davantage encore les violations du réseau. En 2017, des hackers ont par exemple utilisé des outils de forçage faciles à obtenir pour utiliser les mots de passe par défaut de plus de 5 000 dispositifs IoT d'une université américaine (dont le nom n'a pas été révélé).

Ces dispositifs leur ont ensuite permis d'implémenter un réseau zombie destiné à attaquer le réseau de l'université. Non seulement, de tels incidents perturbent gravement les activités quotidiennes mais ils compromettent également durablement la réputation de l'établissement.

Renverser la tendance grâce à l'IA

Au lieu de s'attacher à construire des murs de protection autour des réseaux du campus, les équipes de sécurité devraient plutôt se concentrer sur le contrôle et le traçage des dispositifs du réseau, et s'assurer qu'une alerte leur soit transmise dès qu'un incident se produit.

En effet, face à une surface d'attaque aussi grande à protéger, et autant de dispositifs IoT et BYOD mal sécurisés et connectés en permanence, les hackers finissent inévitablement par franchir le périmètre du réseau. La solution idéale consiste donc à être en mesure de voir l'intérieur du réseau et, à terme, de neutraliser les attaques qui se sont déjà infiltrées.

Malheureusement, cette visibilité de l'intérieur du réseau est précisément la fonctionnalité la plus limitée des outils de sécurité utilisés traditionnellement par la plupart des universités. En se limitant à rechercher des menaces connues sur le périmètre du réseau à l'aide de règles et de signatures fixes, les outils classiques ont toutes les chances de ne pas détecter la prochaine attaque inédite qui sera portée contre les universités du monde entier. Il est dont impératif pour ces institutions d'apprendre la leçon avant qu'il ne soit trop tard.

Les systèmes de sécurité utilisant l'intelligence artificielle savent différencier les comportements normaux et anormaux de chaque utilisateur, dispositif et réseau, et peuvent ainsi détecter et réagir à la moindre anomalie symptomatique d'une cyber-attaque en cours.

Le premier objectif d'un réseau universitaire est d'offrir des environnements d'apprentissage hautement accessibles sur la plateforme la plus sécurisée possible. Les universités devraient adopter la cyber-IA si elles souhaitent protéger la recherche et les IP sans nuire à l'interconnectivité qu'un campus est supposé offrir.