Orange
Cyberdefense

Cas Client

LUCA School of Arts opte pour des services ‘Detection & Response’ gérés, 24x7, suite à une attaque de type ransomware

En un coup d’oeil

3,500
Elle accueille chaque année quelque 3.500 étudiants.

700
Luca School of Arts a 700 membres du personnel.

5
L’institution compte 5 campus.

24x7
Linfrastructure IT est surveillée, 24x7, par le centre de télésurveillance (CyberSOC).

La LUCA School of Arts est l’une des Hautes Ecoles d’enseignement artistique les plus réputées de Flandre. L’institution propose 30 formations différentes de bachelier et master dans les domaines des techniques et arts audiovisuels, des arts plastiques, des arts de la scène et de la musique. La LUCA compte cinq campus: C-mine à Genk, l’institut Lemmens à Louvain, l’école Sint-Lukas à Bruxelles et à Gand, et Narafi à Bruxelles. La Haute Ecole dépend de l’Association KU Leuven. Elle accueille chaque année quelque 3.500 étudiants, répartis sur les différents sites et encadrés par environ 700 membres du personnel.

Des messages d’hameçonnage paralysent l’école

Aujourd’hui, la technologie est devenue une dimension indissociable du monde de l’enseignement, en particulier dans l’enseignement artistique. Toute une série de formations comportent un volet technologique — pensez par exemple à l’aménagement intérieur, au cinéma ou à la photographie — et les communications numériques y sont devenues une pratique intense. L’un des défis majeurs demeure toutefois le concept de BYOD. « L’ordinateur portable des étudiants est devenu, comme dans d’autres domaines, un instrument de travail qu’ils emmènent partout avec eux. Ils s’attendent à pouvoir l’utiliser dans un environnement sécurisé », déclare Wim Pauwels, responsable de l’infrastructure ICT de la LUCA School of Arts. « Contrôler une telle quantité d’équipements et, dans le même temps, garantir des services réseau de qualité, représente un réel défi en termes de sécurité. » En particulier au vu de l’augmentation exponentielle des cyber-attaques.

En soi, les établissements d’enseignement sont tout autant sujets à des cyber-attaques que les entreprises - ni plus, ni moins. « Par contre », souligne Wim Pauwels, « nous sommes davantage vulnérables parce que

« Grâce au service géré “detection & response”, l’équipe IT est rassurée et peut dormir sur ses deux oreilles. »

Wim Pauwels | Responsable Infrastructure ICT à la LUCA School of Arts

notre cohorte d’utilisateurs est beaucoup plus évolutive et fragmentée: des milliers d’étudiants et des centaines de membres du personnel. Sans compter que nous proposons également de très nombreuses applications. »

En mars 2020, la LUCA fut victime d’une cyber-attaque qui paralysa les systèmes informatiques. Il fallut tout d’abord intervenir rapidement afin de débarrasser les systèmes IT de tout ransomware. Dans le même temps, il fallut rechercher une solution afin d’éviter de telles attaques à l’avenir. « L’une des premières choses que nous avons constatée en première analyse fut que nos utilisateurs réagissaient assez facilement à des courriels d’hameçonnage et divulguaient ensuite leurs identifiants. Un point supplémentaire qui a retenu notre attention… », se remémore Wim Pauwels.

Managed Detection and Response

Pour éviter que de telles attaques se reproduisent à l’avenir, la LUCA School of Arts avait défini deux importants critères auxquels la solution devait satisfaire. Elle escomptait, à court terme, un redémarrage rapide et sécurisé des systèmes. La solution devait par ailleurs détecter des opérations suspectes effectuées sur les systèmes IT et être en mesure de les stopper. De préférence en mode 24x7. « Notre équipe IT interne est trop petite pour pouvoir assurer elle-même le suivi, à chaque instant, de tous les événements suspects. Nous avions donc absolument besoin d’un service géré de détection et réaction. Ce genre de détection et de suivi est en outre un exercice très complexe que nous préférons confier à de véritables spécialistes. »

Le choix s’est finalement porté sur Orange Cyberdefense. La société a proposé un service géré de détection de menaces axé sur les endpoints. Ce service géré de “detection & response” détecte les activités suspectes et les bloque automatiquement de telle sorte que le pirate informatique ne puisse se propager davantage subrepticement dans l’infrastructure IT de la Haute Ecole. La LUCA School of Arts peut également faire appel au centre de télésurveillance néerlandophone d’Orange Cyberdefense qui peut intervenir manuellement dans des cas exceptionnels.

Les avantages

Le principal avantage de la solution est la fiabilité de fonctionnement qu’elle procure. Wim Pauwels: « Nous avons désormais pu nous rendre compte qu’une cyber-attaque peut totalement paralyser une haute école ou n’importe quelle organisation. Ce service de Managed Threat Detection nous offre la possibilité de réagir immédiatement en cas d’activités suspectes sur l’appareil d’un utilisateur final. »

La démarche professionnelle d’Orange Cyberdefense représente un deuxième avantage. En combinant expérience et rapidité, la société a su activer rapidement le service. « Deux semaines après l’attaque par ransomware, nous avons démarré le déploiement du logiciel de détection et de réaction sur les endpoints. Et en à peine un mois, notre infrastructure IT était déjà surveillée, 24x7, par le centre de télésurveillance (CyberSOC) d’Orange Cyberdefense. L’ancrage local d’Orange Cyberdefense est une importante plus-value. Le fait que le CyberSOC soit néerlandophone a encore facilité les communications », souligne Wim Pauwels.

Le résultat

La haute école est aujourd’hui à nouveau pleinement opérationnelle. Plus de 600 agents logiciels de la solution de détection et de réaction pour endpoints sont déjà installés sur les équipements des utilisateurs finaux et sur les serveurs de la haute école. Tous ces appareils sont donc surveillés et

sécurisés 24x7. La haute école peut par ailleurs continuer d'offrir toutes ses applications dans un environnement convivial. « Le service a été activé voici six mois », commente Wim Pauwels. « Sur les seuls quatre derniers mois, nous avons détecté une moyenne de trois incidents suspects par mois. Le service les repère et le centre de télésurveillance d'Orange Cyberdefense nous avertit immédiatement s'il s'agit d'activités dangereuses. »

Le service géré de détection et de réaction intervient de manière pertinente en cas de détections. Orange Cyberdefense détermine rapidement les risques et impacts potentiels. Les détections que signale le logiciel sont une bonne base mais Orange Cyberdefense s'appuie par ailleurs sur ses propres analyses et connaissances pour procéder à une analyse pertinente. On ne saurait en effet sous-estimer l'importance d'un analyste de sécurité pour prendre la bonne décision.

L'avenir

La prochaine étape pour la LUCA consistera à renforcer la prise de conscience sécuritaire et à sensibiliser les utilisateurs. La LUCA School of Arts constate en effet que certains utilisateurs continuent de cliquer sur des liens contenus dans des courriels d'hameçonnage et de divulguer leur identifiant et mot de passe. « Après la cyber-attaque du printemps, nous avons à nouveau essuyé une attaque par hameçonnage. Plusieurs utilisateurs ont cliqué sur le lien. Heureusement sans conséquences négatives pour notre environnement informatique. Et cela grâce à la solution et au professionnalisme d'Orange Cyberdefense. Mais cela démontre à nouveau que nous devons continuellement sensibiliser les utilisateurs pour qu'ils identifient et bloquent ce genre de courriels. A court terme, nous ferons potentiellement appel pour cela à d'autres services d'Orange Cyberdefense », conclut Wim Pauwels.

- Solution idéale pour identifier rapidement d'importants risques.
- Environnement sécurisé: le service géré "detection & response" détecte automatiquement des activités suspectes et réagit de manière appropriée.
- CyberSOC: surveillance 24x7, analyse et alertes procurent les garanties nécessaires à la petite équipe IT.

Orange Cyberdefense

Orange Cyberdefense est l'entité du groupe Orange spécialisée en cybersécurité. En tant que prestataire de sécurité de référence en Europe, nous mettons tout en oeuvre pour bâtir une société numérique plus sûre. Nous sommes un prestataire de services de sécurité pilotée par les données et d'analyse de la menace, procurant une vision inégalée des menaces existantes ou émergentes. Orange Cyberdefense jouit d'une expérience de plus de 25 ans dans le domaine de la sécurité de l'information, emploie plus de 250 chercheurs et analystes dans 16 SOC, 10 CyberSOC et 4 centres CERT répartis dans le monde entier ainsi que des équipes commerciales et de support dans 160 pays. Nous sommes fiers de pouvoir affirmer que nous proposons une protection globale avec une expertise locale et que nous assurons le support de nos clients tout au long du cycle de vie des menaces.