Orange
Cyberdefense

Customer stories

LUCA School of Arts gaat voor 24/7 Managed Detection & Response diensten na ransomware-aanval

Overzicht

3,500
Per Aceademiejaar zijn er zo'n 3.500 studenten per jaar.

700
Luca School of Arts heeft 700-tal personeelsleden.

5
De hogeschool zit verspreid over 5 Campussen.

24/7
Managed detection and response in de Nederlandstalige meldkamer.

LUCA School of Arts is één van de bekendste hogescholen voor kunstonderwijs in Vlaanderen. De onderwijsinstelling biedt 30 verschillende bachelor- en masteropleidingen aan in audiovisuele kunsten en technieken, beeldende kunsten, podiumkunsten en muziek. LUCA School of Arts zit verspreid over vijf campussen: C-mine Genk, Lemmensinstituut Leuven, Sint-Lukas Brussel, Sint-Lukas Gent en Narafi Brussel. De hogeschool behoort tot de Associatie KU Leuven. Per academiejaar zijn er zo'n 3.500 studenten op de verschillende locaties te vinden die begeleid worden door een 700-tal personeelsleden.

Phishing-mail legt school plat

Technologie is vandaag niet meer weg te denken in het onderwijs en zeker niet in het kunstonderwijs. Zo zijn er diverse opleidingen met een technologische insteek – denk maar aan interieurontwerp of film en fotografie -en wordt er daarnaast heel veel digitaal gecommuniceerd. Eén van de grootste uitdagingen is echter het BYOD-verhaal. "Ook voor studenten is hun eigen laptop een werkinstrument geworden dat ze overal meenemen. Ze verwachten dat ze dit in een veilige omgeving kunnen gebruiken", vertelt Wim Pauwels, verantwoordelijke voor de ICT-infrastructuur van LUCA School of Arts. "Die hoeveelheid toestellen controleren en tegelijkertijd goede netwerkvoorzieningen voorzien, is een uitdaging op vlak van security." Zeker met de exponentiële toename van cyberaanvallen.

Op zich zijn onderwijsinstellingen niet meer of minder vatbaar voor cyberaanvallen dan bedrijven. Wim Pauwels: "Wel is het zo dat we kwetsbaarder zijn omdat we een veel meer wisselende en gefragmenteerde gebruikersgroep hebben: duizenden studenten en honderden personeelsleden. Bovendien bieden we ook vrij veel toepassingen aan."

> Voor het IT-team betekent de managed detection & response dienst nachtrust en gemoedsrust. “
>
> **Wim Pauwels | Verantwoordelijke ICT-infrastructuur bij LUCA School of Arts**

In maart 2020 werd LUCA School of Arts getroffen door een cyberaanval. De IT-systemen waren hierdoor onbeschikbaar. In eerste instantie was er een snelle interventie nodig om de IT-systemen weer ransomwarevrij te maken. Tegelijkertijd moest er een oplossing gezocht worden om dergelijke aanvallen in de toekomst te vermijden. “Eén van de zaken die we tijdens een eerste analyse zagen, is dat onze gebruikers vrij gemakkelijk reageerden op phishing-mails en vervolgens zomaar hun logingegevens prijsgaven. Dat was ook een werkpunt”, aldus Wim Pauwels.

Managed Detection and Response

Om dergelijke aanvallen in de toekomst te vermijden, had LUCA School of Arts twee belangrijke criteria waaraan de oplossing moest voldoen. Op korte termijn werd een snelle en veilige heropstart van systemen verwacht. Daarnaast moest de oplossing verdachte operaties op de IT-systemen detecteren en deze ook kunnen stopzetten. Liefst 24/7. “Ons intern IT-team is te klein om op elk moment zelf alle verdachte operaties op te volgen. We hadden dus absoluut nood aan een Managed Detection & Response dienst. Bovendien is dat opsporen en opvolgen een heel complexe aangelegenheid. En dat laten we liever over aan echte specialisten.”

Uiteindelijk werd gekozen voor Orange Cyberdefense. Zij stelden een managed threat detectie dienst op basis van endpoint voor. Deze Managed Detection & Response dienst detecteert verdachte activiteiten en zet deze ook automatisch stop, zodat dat de aanvaller zich niet ongemerkt verder in de IT-infrastructuur van de hogeschool kan verspreiden. LUCA School of Arts kan ook beroep doen op de Nederlandstalige meldkamer van Orange Cyberdefense die manueel kan ingrijpen in uitzonderlijke gevallen.

De voordelen

Het grootste voordeel van de oplossing is de bedrijfszekerheid. Wim Pauwels: “We hebben nu kunnen merken dat een cyberaanval een hogeschool of om het even welke organisatie volledig kan platleggen. Deze Managed Threat Detection dienst biedt ons de mogelijkheid om direct op de bal te spelen bij verdachte operaties op een eindgebruikerstoestel.”

Een tweede voordeel is de professionele aanpak van Orange Cyberdefense. De combinatie van hun expertise en snelheid zorgde ervoor dat de dienst snel geactiveerd kon worden. “Twee weken na de ransomware-aanval konden we starten met de uitrol van de endpoint detection and response software. En na amper één maand werd onze IT-infrastructuur al 24/7 gemonitord door de meldkamer (CyberSOC) van Orange Cyberdefense. De lokale verankering van Orange Cyberdefense is een grote meerwaarde. Het feit dat het CyberSOC Nederlandstalig is, maakte de communicatie nog gemakkelijker”, verduidelijkt Wim Pauwels

Het resultaat

Momenteel is de hogeschool volledig heropgestart. Er zijn al meer dan 600 software agents van de endpoint detection and response oplossing geïnstalleerd op toestellen van eindgebruikers en op de servers van de hogeschool. Al deze toestellen worden dus 24/7 gemonitord en beveiligd. De hogeschool kan alle toepassingen ook blijven aanbieden in een gebruiksvriendelijke omgeving. Wim Pauwels: “De service-activatie gebeurde zo’n zes maanden geleden. Alleen al de voorbije vier maanden werden

gemiddeld zo'n drie verdachte incidenten per maand gedetecteerd. De service merkt ze op en de meldkamer van Orange Cyberdefense verwittigt ons direct als het inderdaad gevaarlijke operaties zijn."

De Managed Service Detection en response reageert op de gepaste manier op detections. Het risico en de mogelijke impact snel wordt hierbij snel bepaald door Orange Cyberdefense. De detections die de software geeft, is een goede basis, maar Orange Cyberdefense vertrouwt daarnaast op de eigen analyse en kennis om op een gepaste manier te analyseren. Het belang van een security-analyst is niet te onderschatten bij het maken van de juiste keuze.

De toekomst

De volgende stap in het verhaal van LUCA School of Arts is de security awareness verhogen en de gebruikers sensibiliseren. LUCA School of Arts ziet nog steeds gebruikers op links in phishing-mails klikken en hun login en wachtwoord prijsgeven. Wim Pauwels: "Na de aanval in het voorjaar, hadden we deze zomer opnieuw een phishing-aanval. Verschillende gebruikers hebben op de link geklikt. Gelukkig zonder negatieve gevolgen voor onze IT-omgeving. Dankzij de oplossing en professionaliteit van Orange Cyberdefense. Maar het toont nogmaals aan dat we de gebruikers continu moeten sensibiliseren om dergelijke e-mails te herkennen en te blokkeren. Wellicht zullen we in de nabije toekomst hiervoor een beroep doen op de andere diensten van Orange Cyberdefense", besluit Wim Pauwels.

- Ideale oplossing om groot risico af te dekken op korte periode.
- Veilige omgeving: de managed detection & response dienst detecteert automatisch verdachte operaties en reageert vervolgens op de gepaste manier.
- CyberSOC: 24/7 bewaking, analyse en alerting geeft het kleine IT-team de nodige zekerheid.

Over Orange Cyberdefense

Oran Orange Cyberdefense is de deskundige cybersecurity business unit van de Orange Group. Als Europa's go-to security provider streven zij naar een veiligere digitale samenleving. Zij zijn een threat research en intelligence-driven security provider die ongeëvenaarde toegang biedt tot huidige en nieuwe dreigingen.

Orange Cyberdefense heeft meer dan 25 jaar ervaring op het gebied van informatiebeveiliging, 250+ onderzoekers en analisten, 16 SOC's, 10 CyberSOC's en 4 CERT's verspreid over de hele wereld en verkoop- en dienstenondersteuning in 160 landen. Zij zijn er trots op dat ze met lokale expertise wereldwijde bescherming kunnen bieden en hun klanten gedurende de hele levenscyclus van een bedreiging kunnen ondersteunen.