En dan ligt het ICT-systeem **ineens plat...**

TEKST: **MARTIN VAN DEN BOGAERDT**

Cybercriminelen vormen een steeds groter gevaar, ook voor scholen. Dat kan ernstige gevolgen hebben voor de continuïteit van het onderwijs en grote financiële implicaties met zich meebrengen. Meestal moeten honderdduizenden euro's losgeld worden betaald om gegijzelde systemen vrij te kopen. Het is dus zaak om hackers buiten de digitale deur te houden. Scholen kunnen een cyberverzekering afsluiten.

Niet alleen bedrijven, ook onderwijsorganisaties hebben meer en meer te kampen met cybercriminaliteit. In de voorjaarsvakantie werd dat helaas weer duidelijk, toen bleek dat het openbare Staring College in Lochem en Borculo was getroffen door een aanval met *ransomware*. Dat is software die criminelen via een lek naar binnen brengen om computersystemen te gijzelen. Vervolgens eisen zij losgeld.
In de media verschenen veel berichten over de aanval op het Staring College, vooral nadat de school had besloten losgeld te betalen. Uit onderzoek van een securitybedrijf was gebleken dat er zoveel gegevens waren versleuteld, dat de continuïteit van het onderwijs en de examens in gevaar kwamen, vertelde bestuursvoorzitter Carlien Krist-Spit aan De Gelderlander. Ze sprak van een nachtmerrie. 'Het besluit dat we hebben genomen gaat in tegen al onze principes, het voelt heel slecht.' Omdat de daders toegang hadden tot privacygevoelige gegevens, heeft de school bij de Autoriteit Persoonsgegevens melding gemaakt van een datalek. Het is niet bekend hoeveel losgeld er is betaald en wat het heeft gekost om externe ICT-adviseurs in te huren. Na ruim een week kon het Staring College de lessen hervatten.

Steeds meer cyberincidenten

In februari maakten de Universiteit en Hogeschool van Amsterdam bekend dat 'onbekende derden' zich toegang hadden verschaft tot de ICT-omgevingen. Een woordvoerder liet aan nieuwssite NU.nl weten dat de aanvallers toegang hadden tot wachtwoorden van studenten en medewerkers. Vermoedelijk wilden de criminelen een aanval met *ransomware* uitvoeren.
Begin maart was er een ander incident. De media berichtten toen uitgebreid over digitale inbrekers die de persoonsgegevens van tienduizenden studenten en medewerkers van Hogeschool Inholland in handen hadden gekregen en deze data verkochten op een hackersforum.
De Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) is een andere organisatie die onlangs te maken kreeg met cybercriminelen. Zij drongen de systemen binnen en kregen toegang tot interne documenten. De daders eisten miljoenen euro's aan losgeld. Toen NWO aangaf niet te betalen, begonnen de hackers documenten te lekken. Pas na ruim een maand kon NWO het proces hervatten voor het verstrekken van subsidies voor wetenschappelijk onderzoek.

Universiteit Maastricht

Een geruchtmakende kwestie rond *ransomware* van wat langer geleden speelde eind 2019 in Limburg. Daar werden de computersystemen van de Universiteit Maastricht gegijzeld. De daders

De zwakste schakel is vaak menselijk handelen

kregen losgeld ter waarde van 197.000 euro aan bitcoins. De Inspectie van het Onderwijs oordeelde na onderzoek dat de universiteit niet goed was voorbereid op de digitale aanval, omdat op servers de laatste beveiligingsupdates niet waren uitgevoerd. Bovendien was niets gedaan met waarschuwingen van virusscanners, waardoor *malware* onopgemerkt bleef. Het ministerie van Binnenlandse Zaken concludeerde in 2020 dat digitale aanvallen weliswaar niet kunnen worden voorkomen, maar dat we wel weerbaarder moeten worden tegen cybercriminaliteit.

Waarom scholen?

De reden waarom cybercriminelen hun pijlen onder meer op onderwijsinstellingen richten, is dat scholen veel privacygevoelige gegevens verwerken. Bijvoorbeeld adres- en contactgegevens van leerlingen en personeelsleden, burgerservicenummers, betaalgegevens van onder anderen ouders en informatie over schoolprestaties, salarissen en gebeurtenissen in de privésfeer. Het mag duidelijk zijn dat deze data absoluut niet in verkeerde handen mogen vallen.

Daarbij komt dat scholen steeds afhankelijker worden van digitale technologie. Als cruciale gegevens en systemen niet beschikbaar zijn door een cyberaanval, heeft dat verlammende gevolgen. Zeker nu we er als gevolg van de coronacrisis aan gewend zijn geraakt dat een deel van de lessen online wordt gegeven. Bovendien kunnen scholen forse reputatieschade oplopen als hun digitale systemen worden lamgelegd. Dat is niet direct in geld uit te drukken, maar benadrukt wel dat iedereen in de school zich bewust moet zijn van de gevaren. Dat is extra belangrijk nu met digitaal onderwijs leraren en leerlingen vanuit steeds meer hoeken de ICT-systemen binnenkomen.

Cyberverzekering

Schoolbesturen die bij VOS/ABB zijn aangesloten, kunnen gebruikmaken van een aantrekkelijk ledenaanbod op het gebied van verzekeringen. Dit aanbod loopt via onze verzekeringspartner Aon.

De laatste tijd krijgen wij signalen binnen van leden die verontrust zijn over stijgende premies binnen het VOS/ABB-aanbod. Dat is een trend die te maken heeft met nieuwe risico's, waaronder de claimcultuur van ouders, maar zeker ook cybercriminaliteit.
Henri Damen van Aon vertelt dat het verstandig is verzekeringen van tijd tot tijd kritisch tegen het licht te houden. 'Ik adviseer altijd om je te verzekeren voor risico's die je financieel niet kunt dragen. In die zin kun je je afvragen of een inventarisverzekering een absolute noodzaak is. Het zal nooit zo zijn dat bij alle scholen van een bestuur tegelijk wordt ingebroken. Bovendien blijft de schade van een inbraak meestal beperkt. Stel je voor dat er 20 laptops worden gestolen. Kun je de financiële schade daarvan dragen? Als het antwoord daarop 'ja' is, kun je je afvragen of een inventarisverzekering noodzakelijk is.'
Bij cyberrisico's is dat volgens Damen een heel ander verhaal. 'Wij zien bij een *ransomware*-aanval bijna altijd dat de hele organisatie wordt geraakt. Het onderwijs komt stil te liggen, de bedrijfsvoering loopt in het honderd en het bestuur moet externe adviseurs inhuren om de digitale systemen weer op gang te brengen. Bovendien kun je genoodzaakt zijn om losgeld te betalen, ook al doe je dat natuurlijk het liefst niet. De schade loopt al heel gauw in de honderdduizenden euro's. Als het om zulke grote bedragen gaat, adviseer ik altijd om je daartegen te verzekeren. Het klopt dat je dan enkele duizenden euro's per jaar kwijt bent, afhankelijk van je omzet, maar dat is natuurlijk altijd veel minder dan de schade als je geen cyberverzekering hebt.'

Meer informatie: ga naar www.vosabbverzekeringen of neem contact op met Henri Damen van Aon: 06-13817417, henri.damen@aon.nl.

Systemen up-to-date

Ransomware-aanvallen, ook die op het onderwijs, zijn meestal het werk van georganiseerde cybercriminelen. Die kunnen vanuit Nederland opereren, maar ook vanuit het buitenland. Het gaat hierbij om goed voorbereide, stapsgewijze en

geavanceerde aanvallen waarmee grote bedragen kunnen worden buitgemaakt. Deze groepen hebben veel technische kennis en geld om hun winstgevende business voort te zetten.

Met organisatorische en technische maatregelen kan het risico op een aanval wel worden verkleind, maar helaas niet geheel worden weggenomen. Het is van belang om de ICT-systemen up-to-date te houden en eventuele lekken direct te dichten. Goede antivirussoftware is onmisbaar om *malware* onschadelijk te maken, net als goede e-mailbeveiliging om *phishing* te voorkomen. Dat is het hengelen naar persoonlijke gegevens, waaronder inloggegevens, via e-mails waarin kwaadaardige links zitten. Ook authenticatie in twee stappen is verstandig. Daarbij loggen gebruikers niet in met alleen een wachtwoord, maar ook met een code op hun mobiel.
Verder is het van groot belang om meerdere back-ups te maken van essentiële data, bijvoorbeeld op een externe harde schijf of in een aparte *cloud*-omgeving. Een ander punt is dat iedereen de gevaren moet kennen en daarnaar moet handelen. Ook hier geldt dat een ketting zo sterk is als de zwakste schakel. En die zwakste schakel blijkt in de praktijk vaak menselijk handelen.

Losgeld betalen voelt heel slecht

DDoS-aanvallen

Scholen worden niet alleen slachtoffer van *ransomware*, maar ook van DDoS-aanvallen. Die zijn veel eenvoudiger uit te voeren, maar kunnen ook veel schade aanrichten. DDoS staat voor *Distributed Denial of Service*. Cybercriminelen die zo'n aanval uitvoeren, zorgen ervoor dat ze met grote hoeveelheden dataverkeer een server, website of systeem overbelasten. Daardoor worden de ICT-voorzieningen traag of tijdelijk helemaal onbruikbaar.
De scholen die onder de Stichting Voortgezet Onderwijs Zeeuws-Vlaanderen vallen, hadden er onlangs maandenlang last van, meldt de Zeeuwse krant PZC. Dat was extra vervelend vanwege de corona-lockdown, omdat veel onderwijs online verliep en dat ineens erg lastig werd.

In 2020 was de Veluwse Onderwijsgroep enige tijd dagelijks doelwit van zware DDoS-aanvallen. Hierdoor konden docenten en scholieren niet goed gebruikmaken van digitaal lesmateriaal, websites en computerprogramma's. Een ander voorbeeld van een DDoS-aanval op het onderwijs, was die op het schoolsysteem Magister in 2019. Daardoor kon niemand meer bij cijfers, roosters en huiswerkopdrachten.

Tips van Kennisnet

Kennisnet heeft op zijn website een reeks maatregelen staan om de ICT-infrastructuur van scholen te beveiligen.

1. Breng devices in kaart: denk niet alleen aan desktops, laptops en tablets, maar ook aan printers, beveiligingscamera's, telefoons en andere apparaten die verbonden zijn met het netwerk.
2. Houd overzicht over netwerkinfrastructuur: hierbij gaat het om de firewall, switches en netwerkaansluitingen die nodig zijn om updates uit te voeren.
3. Houd zicht op accounts: welke 'gewone' gebruikersaccounts zijn er, welke accounts hebben bijzondere privileges en wie hebben een administrator-account?
4. Controleer toegang tot interne netwerk: welke externen kunnen in het netwerk van de organisatie? En moeten zij er wel in kunnen?
5. Sluit vrij toegankelijke fysieke netwerkaansluitingen af: maak zoveel mogelijk gebruik van (beveiligde) draadloze verbindingen.
6. Voorkom DDoS-aanvallen: de dienst Veilig internet van de onderwijscoöperatie SIVON biedt deze functionaliteit standaard.
7. Neem maatregelen tegen ransomware: maak iedereen in de organisatie bewust van het gevaar, maak back-ups en installeer laatste updates van besturingsprogramma's.
8. Versleutel data: gebruik wachtwoorden om gegevens te beschermen.

De brochure *8 maatregelen om uw ict-infracstructuur te beveiligen* staat op www.kennisnet.nl.

Reputatieschade niet uit te drukken in geld

Wees alert!

Voor het uitvoeren van een DDoS-aanval hoef je geen whizzkid te zijn. Het is eenvoudig en vaak voor slechts een paar tientjes online te bestellen via speciale websites. Daarom gaat bij een DDoS-aanval op een school vaak de verdenking uit naar leerlingen, maar dat is niet altijd makkelijk te bewijzen. In maart 2019 echter werd een jongen uit Den Haag veroordeeld tot jeugddetentie voor onder meer het uitvoeren van DDoS-aanvallen op zijn school. Hij maakte daarvoor gebruik van een *botnet*. Zo'n netwerk bestaat uit duizenden computers en andere digitale apparaten, waarvan de eigenaren vaak niet eens weten dat ze daarin zitten. Via zo'n netwerk kunnen hackers ICT-systemen massaal aanvallen en platleggen.

Eind maart kwam in het nieuws dat leerlingen van de christelijke scholengemeenschap CSG Comenius Mariënburg in Leeuwarden DDoS-aanvallen uitvoerden op hun eigen school. Daardoor haperde ruim een week het internet. Locatiedirecteur Freek Polter sprak in de Telegraaf van 'een ernstig feit waarmee 1500 leerlingen en 150 personeelsleden' werden benadeeld. De leerlingen deden het uit verveling, vermoedde hij, 'maar deze grap gaat over de grens van een kwajongensstreek'. Uiteindelijk deed de school geen aangifte. De Leeuwarder Courant meldt dat de school ervan heeft geleerd en de computersystemen beter gaat beschermen.

Spelenderwijs leren over cyberveiligheid

HackShield is een online game-platform om leerlingen van 8 tot en met 12 jaar bewust te maken van de gevaren van cybercriminaliteit.

Bij Radio Rijnmond vertelt oprichter Tim Murck van HackShield dat hij samenwerkt met de politie en gemeenten, 'want ook zij hebben er baat bij dat slimme kinderen opstaan die niet alleen zichzelf, maar ook hun omgeving slimmer maken op het gebied van cyberveiligheid'.

Het plan ontstond toen gamedesigners en videomakers met elkaar om tafel zaten. Zij verbaasden zich erover dat digitale geletterdheid nog geen onderdeel is van het curriculum van het onderwijs. Hackshield begon vorig jaar in zeven gemeenten, maar inmiddels zijn dat er tientallen en hebben tienduizenden leerlingen er een account. 'De meesten vinden het heel leuk. Ze gaan op pad met fictieve karakters en moeten bijvoorbeeld *dark hackers* verslaan. Tuurlijk, we zijn geen Fortnite, maar wél een stuk leuker dan de gemiddelde lesboeken', aldus Murck.

Ga voor meer informatie naar www.joinhackshield.nl.

De reportage van Radio Rijnmond staat op www.rijnmond.nl ('Game leert kinderen meer over cybercrime: 'Zij maken zo hun ouders en grootouders ook slimmer'').