Cyberveiligheid van steeds groter belang

Met welke cyberdreigingen heeft het onderwijs te maken? Wat kunnen de gevolgen zijn van een digitale aanval? En wat kun je doen om het cybercriminelen zo moeilijk mogelijk te maken? *Naar School* liet zich adviseren door twee cybersecurity-experts. 'Honderd procent veiligheid bestaat niet, kwetsbaarheden kunnen en zullen altijd worden gebruikt, maar je kunt het cybercriminelen wel zo lastig mogelijk maken.'

TEKST: **MARTIN VAN DEN BOGAERDT**
BEELD: **PR EN STOCK**

Richard Verbrugge is information security risk officer bij ABN AMRO en Michael Waterman is cybersecurity-architect bij ACA IT-Solutions. Zij benadrukken dat overal, dus ook in het onderwijs, het risico op een cyberaanval groeit door de toenemende afhankelijkheid en ontwikkelingen van digitale technologie. 'Meer digitalisering, outsourcing naar cloud-services en social media bieden hackers meer ingangen om aan te vallen', zeggen zij. ▸▸

Scholen moeten volgens Verbrugge en Waterman rekening houden met twee soorten aanvallers. ‘Aan de ene kant heb je de professionele cybercriminelen. Die zijn erop uit om vertrouwelijke informatie los te peuteren, reputatieschade aan te richten en processen te ontregelen met het uiteindelijke doel om scholen geld te laten betalen. Aan de andere kant heb je leerlingen die bijvoorbeeld examenstof willen binnenhalen of zomaar de school willen ontregelen. De gevolgen kunnen ook dan ingrijpend zijn. Denk aan een website die onbereikbaar wordt of aan systemen en data waar je niet meer bij kan, het verlies van gegevens of misbruik van IT-systemen, bijvoorbeeld via een e-mailaccount.’

Verbrugge en Waterman leggen uit dat cyberaanvallen meestal via mensen verlopen die zonder dat zij zich daarvan bewust zijn, bijvoorbeeld via mailtjes of geïnfecteerde websites, een kwaadaardig programma het systeem laten binnenkomen. ‘Elke dag worden duizenden nieuwe malwareprogramma’s gedetecteerd. Meer dan 85 procent van alle aanvallen begint via social engineering. Mensen klikken op links, openen bijlagen en voeren inloggegevens in.’ Ze wijzen ook op het risico van technische kwetsbaarheden, zoals verouderde software, zwakke toegangscontroles, onjuiste back-up-processen en het ontbreken van gegevensversleuteling.

Richard Verbrugge

Michael Waterman

TREF MAATREGELEN

Verbrugge en Waterman benadrukken dat cybercriminelen overal en op ieder moment van de dag kunnen toeslaan. ‘Een hacker heeft maar één kwetsbaarheid of ingang nodig om een aanval te doen slagen. Honderd procent veiligheid bestaat niet, kwetsbaarheden kunnen en zullen altijd worden gebruikt, maar je kunt het cybercriminelen wel zo lastig mogelijk maken. Bijvoorbeeld met multifactor-authenticatie en veilige back-ups en door alert te zijn op ongebruikelijk dataverkeer.’ Het is ook zaak om software up-to-date te houden, regelmatig systeemscans uit te voeren en te voorkomen dat leerlingen en personeelsleden zelf software kunnen installeren.

Bewustzijn creëren is ook essentieel: ‘Leer scholieren en medewerkers om veilig te werken met unieke en sterke wachtwoorden. Zorg ervoor dat iedereen verdachte e-mails en beveiligingsincidenten herkent en meldt. Daarnaast is het van belang om niet zomaar met iedere leverancier in zee te gaan, want ook een supply-chain-aanval behoort tot de risico’s. Je kunt specialisten laten checken of je alle zaken goed op orde hebt.’

DENK ALS HACKER

De cyberexperts adviseren ook altijd om je gezonde verstand te gebruiken. ‘Krijg je een factuur met een nieuw rekeningnummer? Verifieer dat dan, altijd! Bescherm jezelf ook tegen phishing. Dus klik niet op links en open geen bijlagen in een verdachte mail. Urgentie in een bericht kan een signaal zijn dat er iets mis is. Weet dat cybercriminelen inspelen op emoties. Dus berichten die je boos, bang of blij maken, zijn een signaal om extra alert te zijn. Vraag je altijd af als je een mailtje krijgt of het wel klopt. Accepteer ook nooit een uitnodiging via e-mail voor bijvoorbeeld LinkedIn, maar ga naar de app zelf. Cybercriminelen gebruiken vaak links die op een klein detail verschillen om je zo op het verkeerde been te zetten. Bijvoorbeeld een hoofdletter I in plaats van een kleine letter i, dus ook daar moet je alert op zijn. Het is verstandig om als school in de huid van de cybercrimineel te kruipen. Denk als een hacker. Hoe krijg je toegang? Hoe omzeil je authenticatie? Welke methoden of middelen kunnen hackers gebruiken? Draai het daarna om. Bedenk oplossingen. Hoe kunnen we de toegang beter beveiligen? Hoe kunnen we de verificatie verbeteren? Dit is een heel goede oefening, waarbij je overigens ook leerlingen kunt betrekken.’

CYBER-RESPONSE-PLAN

Een ander belangrijk punt dat Verbrugge en Waterman benadrukken, is dat alle organisaties een goed cyber-responseplan moeten hebben voor als het ondanks alle voorzorgsmaatregelen toch misgaat. ‘Wat als er een datalek is, als er een groot bedrag is weggesluisd of als alle systemen en data niet meer beschikbaar zijn? Het is goed om van tevoren te bedenken en vast te leggen welke stappen je dan neemt en met wie je contact moet opnemen.’ De experts wijzen erop dat er een meldplicht is. Scholen moeten cyberincidenten melden

Vrijblijvendheid geen optie meer

Bart Vogels

Cybercriminelen vormen voor scholen een steeds groter gevaar. Dat ziet ook het bij VOS/ABB aangesloten bureau Wijs Accountants, onderdeel van Crowe Foederer. Samen met ABN AMRO en ACA-IT Solutions organiseerde Wijs Accountants een webinar over digitale veiligheid in het onderwijs.

Als een digitale aanval slaagt, kan niet alleen het onderwijs plat komen te liggen. Ook kunnen cybercriminelen privacygevoelige informatie buitmaken en ermee dreigen die informatie te publiceren als er geen losgeld wordt betaald. ‘In de afgelopen jaren hebben wij het belang van cybersecurity al prominent onder de aandacht gebracht en ook dit jaar blijven wij de actuele ontwikkelingen aankaarten’, zegt Bart Vogels van Wijs Accountants. Zo wijst hij erop dat er een verplicht normenkader komt voor het primair en voortgezet onderwijs om te kunnen beoordelen waar de school staat ten aanzien van digitale veiligheid. Hierover zal in de jaarverslaggeving verantwoording moeten worden afgelegd. ‘Dus vrijblijvendheid is geen optie meer als het gaat om digitale weerbaarheid en privacy. Daarom zijn wij ook blij dat we als accountantskantoor dat gespecialiseerd is in onderwijs, gebruik kunnen maken van cybersecurity-specialisten, zoals van ons zusterbedrijf ACA-IT Solutions’, benadrukt Vogels.

Ga voor meer informatie over het versterken van IT-security naar de website van ACA-IT Solutions. Scan de QR-code:

Cyberverzekering must voor scholen

Henri Damen

In de top van onmisbare verzekeringen voor scholen staat de cyberverzekering op nummer 1. Dat benadrukt Henri Damen van VOS/ABB’s verzekeringspartner Aon.

Een bestuurdersaansprakelijkheids- of bedrijfsaansprakelijkheidsverzekering biedt geen dekking tegen cybercrime of datalekken, terwijl bestuurders en ook toezichthouders daar wel op kunnen worden aangesproken. ‘Daarom is een cyberverzekering écht een must. Die biedt uitgebreide dekkingen, ook tegen boetes en claims’, aldus Damen, die in dit kader ook wijst op de Algemene Verordening Gegevensbescherming (AVG).

Contact met Aon: Henri Damen, 06 13 81 74 17, henri.damen@aon.nl

Meer informatie over online veiligheid staat in het *CyberHulp magazine* van Aon. Scan de QR-code:

'Je kunt het cybercriminelen zo lastig mogelijk maken'

bij Computer Emergency Response Teams in Nederland (CERT.nl). Bovendien ben je verplicht om een ernstig datalek te melden bij de Autoriteit Persoonsgegevens (autoriteitpersoonsgegevens.nl). Dan heb je ook nog de aansprakelijkheidskwestie. Wie aansprakelijk is bij een cyberaanval hangt af van het incident. 'Bij nalatigheid kunnen daar wel degelijk consequenties uit voortvloeien. Bij een geavanceerde aanval, terwijl je veel maatregelen hebt getroffen, word je mogelijk niet verantwoordelijk gesteld.'

MENTALE IMPACT

Naast financiële schade en reputatieschade kan een cyberaanval ook op een ander vlak grote impact hebben: mentaal. Daarover vertelt Waterman uit eigen ervaring. Ruim een jaar geleden werd hij midden in de nacht gebeld met de mededeling dat ACA IT-Solutions was gehackt. 'Binnen tien minuten zat ik met collega's in een conference-call. Wat volgde, was een intensieve tijd waarin we – dankzij een goede back-up-voorziening en zonder noemenswaardige schade – weer zeer snel *up and running* waren. Binnen een week zelfs, en dat is ontzettend snel.' Maar de mentale impact wordt in zulke situaties nogal eens vergeten, zegt hij: 'Bij een cyberaanval is de focus gericht op de continuïteit van het bedrijf. Logisch natuurlijk, maar je moet ook zorgen voor de mensen. Het is namelijk een impactvolle ervaring als een organisatie wordt gehackt. Medewerkers kunnen zich zorgen maken: heb ik straks nog wel een baan?' Een ander belangrijk punt was volgens Waterman dan ook de communicatie. 'Zorg dat je de controle neemt naar buiten, maar ook intern, zodat er geen spookverhalen ontstaan. Wij communiceerden twee keer per dag. Ook als er geen voortgang te melden was.'

STRESS

ACA IT-Solutions deed na de hack die het bedrijf trof mee aan een onderzoek naar de mentale impact. Een belangrijke uitkomst was dat na verloop van tijd onder medewerkers stressgerelateerde klachten ontstonden. Bijvoorbeeld slaapproblemen, gevoelens van schuld of hulpeloosheid, hoofdpijn en spierpijn, maar ook slechte gewoontes, zoals ongezond eten, drinken en roken. 'Twee op de drie mensen krijgen negatieve gedachten naar aanleiding van cybercrime en een op de zeven heeft na een jaar symptomen die je als een trauma kunt bestempelen. Er kan ook vluchtgedrag ontstaan. Een op de vijf gaat op zoek naar een andere baan.' Waterman adviseert werkgevers om na een hack van de organisatie voor voldoende rust te zorgen en betrokkenheid te tonen. 'Interactie is belangrijk, medewerkers moeten weten dat zij hulpvragen kunnen stellen. Mensen zijn je belangrijkste assets, dus betrek hen bij het herstel van de organisatie.' ◂

Cyberthriller

Richard Verbrugge is naast information security risk officer bij ABN AMRO de auteur van *De lokroep van de schaduw*. Deze thriller gaat over een criminele bende die een graantje wil meepikken van het geld dat met cybercrime wordt verdiend.

De lokroep van de schaduw ◆ Uitgever: Elikser ◆ 232 pagina's ◆ € 22,50