Gevaren uit digitale wereld

Het is hoog tijd dat het onderwijs cyberrisico's serieus neemt, vindt Henri Damen van VOS/ABB's verzekeringspartner Aon. 'De totale schade die hiermee samenhangt, is tegenwoordig in Nederland net zo groot als die van brand.'

TEKST **MARTIN VAN DEN BOGAERDT**

In gesprekken met onderwijsbestuurders en -managers merkt Henri Damen dat er in het onderwijs nog nauwelijks aandacht is voor cyberrisico's. Als voorbeelden noemt hij datalekken als gevolg van digitale inbraken of malafide mailtjes en het ongemerkt importeren van *ransomware*. Dat laatste is kwaadaardige software die computersystemen platlegt. De slachtoffers krijgen pas weer toegang tot hun bestanden als ze de internetcriminelen een bepaald bedrag betalen. 'De politie adviseert altijd dit niet te doen, maar ondertussen kun je helemaal niks meer. *Ransomware* maakt een enorme opmars. Er zijn tegenwoordig wel tienduizenden digitale sleutels bekend om systemen weer open te ▸▸

Digitale inbraak Edu-IX

Voor de zomervakantie werd bekend dat er was ingebroken in het centrale registratiesysteem Edu-IX.

Diverse leveranciers van digitale leermiddelen, zoals Iddink en Van Dijk, maken gebruik van Edu-IX. Het is mogelijk dat door de digitale inbraak naam, adres, woonplaats, geboortedatum, e-mailadres en het versleutelde wachtwoord van accounts zijn ontvreemd. De distributeurs maakten in reactie op de hack wachtwoorden onbruikbaar. Scholen en leerlingen zijn over het voorval geïnformeerd. Het incident is tevens gemeld bij de politie en de Autoriteit Persoonsgegevens (AP).

Meldplicht datalekken

Of een datalek moet worden gemeld bij de AP, is afhankelijk van de (potentiële) impact van het datalek op de bescherming van de persoonsgegevens en de persoonlijke levenssfeer van betrokkenen. De AP kan een boete geven als een datalek ten onrechte niet is gemeld. De maximale boete is 820.000 euro.

Meer informatie staat op de website autoriteitpersoonsgegevens.nl (home>melden>meldplicht datalekken).

maken, maar het is maar de vraag of de juiste sleutel voor jouw systeem erbij zit', aldus Damen.

Buitengewoon serieus probleem

Het vreemde is, vindt hij, dat iedereen zich wel bewust is van de risico's van bijvoorbeeld brand, maar nog nauwelijks van cyberrisico's, terwijl de schade die hierdoor ontstaat volgens hem tegenwoordig in Nederland net zo groot is als die van brand. 'Als het computersysteem van een school door *ransomware* platgaat, heb je een buitengewoon serieus probleem. Bij een datalek kunnen financiële en privacygevoelige gegevens op straat komen te liggen. Dat wil je als school natuurlijk niet. Denk niet alleen aan financiële gevolgen, maar ook aan reputatieschade. Misschien komen er na zo'n affaire wel minder leerlingen naar jouw school. Het kan zomaar zijn dat zulke kwesties bestuurders de kop kosten.'

A4'tje met gedragsregels

Uit de gesprekken die Damen op scholen voert, komt vaak naar voren dat als gevolg van het ontbreken van bewustzijn over cyberrisico's er geen beleid is op dit vlak.

> 'Ransomware en datalekken kunnen enorme schade opleveren'

'Het is de verantwoordelijkheid van de school om hier wel beleid op te hebben. Ik hoor nog wel eens dat er op advies van brancheorganisaties wordt gewacht, maar daar kom je als bestuurder niet mee weg als het misgaat. Het kan beginnen met een A4'tje met gedragsregels. Bijvoorbeeld over hoe personeel zorgvuldig omgaat met wachtwoorden, dat je je laptop niet onbeheerd laat aanstaan en dat je USB-sticks niet laat rondslingeren. Dat zijn stuk voor stuk tips waarvan je denkt dat ze niet meer dan logisch zijn, maar toch zie ik vaak dat scholen er helemaal niets over hebben afgesproken. Het begint dus echt met bewustwording en het opstellen van beleid!'

Nieuw model meldplicht datalekken

De Helpdesk van VOS/ABB heeft een nieuw model gemaakt voor de meldplicht van datalekken. Naar aanleiding van nieuwe wetgeving zijn ook modellen voor privacyreglementen geactualiseerd.

Organisaties die persoonsgegevens verwerken zijn op grond van de Wet bescherming persoonsgegevens verplicht om een ernstig datalek direct te melden aan de Autoriteit Persoonsgegevens. Deze plicht geldt sinds 1 januari 2016 ook voor scholen.
Deze nieuwe wetgeving heeft geleid tot aanpassingen in het Model privacyreglement verwerking leerlinggegevens en het Model privacyreglement verwerking personeelsgegevens. Aan de modellen is een modelprocedure voor de meldplicht datalekken toegevoegd. Verder zijn het Modelprotocol sociale media en de Modelregeling elektronische informatie- en communicatiemiddelen geüpdatet. De aangepaste modellen staan op www.vosabb.nl (home>downloads).

Let op: de modellen zijn alleen beschikbaar voor leden van VOS/ABB!
Informatie: Helpdesk, 0348-405250 van 08.30 tot 12.30 uur, helpdesk@vosabb.nl

Stappenplan

Een programma voor het verbeteren van de veiligheid van digitale netwerken en de bescherming van de privacy begint met de volgende stappen.

- Identificeer, classificeer en kwantificeer het gebruik van informatie en elektronische processen, inclusief de afhankelijkheid van externe providers.
- Implementeer *best practices* op het gebied van risicomanagement in samenhang met ICT-beveiliging, informatiebeveiligingsbeleid en bedrijfsprocedures. Denk hierbij ook aan toewijzing van aansprakelijkheid.
- Train en monitor werknemers, externe providers en andere partners met betrekking tot *best practices* op het gebied van informatiebeveiliging en risicomanagement.
- Bepaal de mogelijke financiële impact van netwerk- en privacyrisico's.
- Bepaal welke netwerkrisico's en privacyrisico's uw school kan dragen en hoeveel u eventueel wilt verzekeren.
- Controleer bestaande verzekeringspolissen op de mogelijke dekking voor netwerk- en privacyrisico's.
- Overweeg om een op maat gemaakte verzekering af te sluiten. Dit om financiële risico's af te dekken en om het risico van een inbreuk op de bestuurlijke verplichting van het management en het schoolbestuur te beperken.

Meer informatie op www.vosabb.nl (zoek op 'cyberrisico'). Informatie Aon: Henri Damen, 06-13817417, henri.damen@aon.nl, Ruud van Houten, 06-14875425, ruud.van.houten@aon.nl.