Cyberveiligheid middelbare scholen, de dreigingen op een rijtje

Het onderwijs digitaliseert in een rap tempo. Toetsen worden digitaal afgenomen, huiswerk wordt op computers gemaakt en cijfers worden digitaal bijgehouden. Door de groei van de hoeveelheid data en door de toegenomen connectiviteit is ook de kans op cyberincidenten aanzienlijk gestegen.

Door **Malini Witlox**

In opdracht van SURF, de ict-samenwerkingsorganisatie van het hoger onderwijs, deed Deloitte onderzoek naar de veiligheid van informatie. Een deel van de conclusies uit het rapport Cyberdreigingsbeeld is ook relevant voor het middelbaar onderwijs. Van de leerling die vooraf een digitale toets probeert te bemachtigen tot een leerling die een 3 graag omzet in een 8. De dreigingen op een rijtje.

Vroeger was het voor de schooldirecteur of docenten simpel. Een vaste computer was nog niet met het internet verbonden, maar werd bestuurd door diskettes en stand alone software, van interne en externe netwerken was nog geen sprake en van tablets en smartphones had nog geen mens ooit gehoord. Met de toegenomen connectiviteit stijgt ook de kans op cyberdreigingen, aldus Niek IJzinga, Senior Manager bij Deloitte Risk Services. Aan de ene kant weet een middelbare scholier misschien minder van computers dan een student die een ict-studie doet, aan de andere kant hebben middelbare scholieren ook minder besef van de consequenties van hun handelen. Volgens de onderzoekers zijn er drie soorten kwetsbaarheden, met de mens, met processen en met technologie. IJzinga pleit voor een verhoging van het beveiligingsbewustzijn. Er zijn schattingen dat in 2012 tweederde van alle datalekken veroorzaakt werd door menselijke fouten. Op het gebied van bewustzijn en cultuur valt nog veel te verbeteren. ‘Leerlingen hebben niet altijd hightech kennis nodig, soms is het lowtech. Een docent gaat even naar het toilet en vergrendelt de computer niet, leerlingen kunnen dan snel even op zoek naar toetsen of cijferlijsten.’

Niek IJzinga

KWETSBAARDER

Een van de dreigingen komt van cloud computing. Het aantal mobiele apparaten en aan internet gekoppelde devices groeit snel. Documenten, foto’s en andere bestanden worden steeds vaker opgeslagen in de cloud, bij providers buiten de instellingen om. Door de hyperconnectiviteit zijn scholen kwetsbaarder voor aanvallen van buitenaf. Ook worden websites en social-mediakanalen van middelbare scholen veel bezocht. Daardoor is het een interessant doelwit voor activisten of boze leerlingen die de site van een school hacken of het social media account willen overnemen.
Volgens IJzinga ligt de dreiging niet alleen op het vlak van onderwijs, maar ook bij ondersteunende zaken, zoals de studentenadministratie. ‘Persoonlijke gegevens van studenten en medewerkers worden digitaal opgeslagen. Deze gevoelige informatie kan op straat komen te liggen als er niet zorgvuldig mee wordt omgesprongen.’ Hoe meer gegevens er over personen uitlekken (zoals namen, geboortedata, adressen), hoe gemakkelijker het wordt om er identiteitsfraude mee te plegen. Bovendien kan je als school de privacywet overtreden als je niet oppast. Ook operationele systemen worden steeds meer via internet aangestuurd, zoals rolluiken, camera’s en thermostaten. Scholen moeten zich daar bewust van zijn en zorgen dat deze apparaten voldoende beveiligd zijn.

CYBERCRIMINALITEIT

Er zijn tal van incidenten in de media geweest, waarbij scholen in het hoger onderwijs de dupe werden van cybercriminaliteit. Zo had in 2014 de Haagse Hogeschool te kampen met een studente die inzage had in de tentamenopgaven en datzelfde jaar pleegden studenten van de Universiteit Amsterdam massaal fraude bij het tentamen statistiek door twee browsers te openen bij het maken van de toets. Op de eerste

browser vulden ze het antwoord in en zagen ze direct het goede antwoord, dat namen ze over in de tweede browser waarna ze die toets verstuurden. Alle gemaakte tentamens werden ongeldig verklaard. Hetzelfde kan een middelbare school overkomen, ook daar worden steeds vaker digitale toetsen afgenomen.

BEVEILIGINGSMAATREGELEN

Middelbare scholen kennen niet altijd speciaal daarvoor aangestelde ict-beheerders of security officers. Lastig, volgens IJzinga want die expertise is eigenlijk wel noodzakelijk. Nu het aantal mobiele apparaten groeit, groeit ook het aantal netwerken waarop de data wordt gedeeld, bijvoorbeeld via het thuisnetwerken of openbaar wifi. Gegevens gaan van apparaat naar apparaat en van omgeving naar omgeving. Denk aan een leerling die op zijn mobieltje even zijn cijfers wil raadplegen. Om het dataverkeer bij deze toenemende variëteit aan apparaten verantwoord te beveiligen zijn meer beveiligingsmaatregelen nodig. Andere gevaren die de onderzoekers detecteren, zijn identiteitsfraude waarbij leerlingen zich voordoen als anderen om betere studieresultaten te krijgen of een DDOS-aanval, waardoor het netwerk uren onbereikbaar kan zijn voor studenten en medewerkers. Lastig want als onderwijsmiddelen door zo'n aanval, door een virus of door malware onbereikbaar worden, kunnen de lessen stil komen te liggen. Zeker nu scholen massaal gebruikmaken van Studieweb of Blackboard kunnen de problemen zich opstapelen en kunnen testresultaten zelfs verloren gaan. 'Er zijn subtiele manieren om cijfers te manipuleren. Een oudere broer kan het lastige proefwerk maken, werkstukken kunnen van Google overgeschreven worden. Er zijn wel manieren om dit te checken, maar dat is niet waterdicht', aldus IJzinga.

ALLES IS TE HACKEN

Het is voor scholen niet mogelijk om zich volledig tegen alle dreigingen te beschermen. Preventieve maatregelen kunnen echter de risico's verkleinen. Zo kun je eisen dat leerlingen en medewerkers sterke wachtwoorden gebruiken die regelmatig worden veranderd. Ook moeten scholen eigenlijk steeds beter zorgen voor monitoring van wat er allemaal op hun digitale netwerken gebeurt. Voor het detecteren van dreigingen en incidenten is tegenwoordig geavanceerde technologie beschikbaar. Door snel in te grijpen, worden de gevolgen van een beveiligingsincident geminimaliseerd. IJzinga: 'Belangrijk is dat schoolbesturen zich bewust zijn van de risico's. Dat was ook deels het doel van ons onderzoek voor het hoger onderwijs. Ict-beheerders lezen er nog wel eens wat over, maar schooldirecteuren zijn vaak met heel andere dingen bezig. We hopen de boodschap met ons rapport beter over voetlicht van de bestuurder te krijgen. Maar we moeten ons er ook bewust van zijn dat er geen 100 procent beveiliging bestaat. Studenten zijn opgegroeid in een digitale wereld, die weten vaak veel meer dan hun ouders of docenten. Heel veel tools om iets te hacken download of koop je online. En dan heb ik het nog niet over de gevaren van digitaal pesten of problemen door onhandigheden. Project X in Haren was eigenlijk gewoon een onhandige uiting in de cyberwereld met onbedoelde effecten. En dan heb je nog scholieren die zich via chatboxen laten verleiden tot seksuele handelingen.' <<