FOCUS OP DE
HOGE RISICO'S!

Dat informatiebeveiliging een onderwerp is waar ook een MBO-instelling aandacht aan moet geven, is onderhand wel bekend. De laatste jaren zijn allerlei organisaties geconfronteerd met beveiligingsincidenten en hoewel het MBO gelukkig geen voorpaginanieuws is geworden in deze, wordt het inzicht breed gedeeld dat er wat moet gebeuren. JAAP DE MARE

Informatiebeveiliging heeft de hoogste prioriteit

Maar wat? Er zijn talloze initiatieven, o.a. van saMBO-ICT en Kennisnet, om instellingen veiliger te maken. Zo is er een MBO 'normenkader' opgesteld (op basis van het normenkader van het hoger onderwijs) met 85 'statements' die op verschillende volwassenheidsniveaus ingevuld kunnen worden, en wordt er jaarlijks een benchmark uitgevoerd waarin instellingen kunnen zien waar ze staan ten opzichte van de collega-instellingen t.a.v. het normenkader. Verder worden er regelmatig masterclasses georganiseerd, is er een actief netwerk van verantwoordelijken van alle instellingen, worden 'best practices' uitgewisseld, et cetera.

Maar de materie is taai. Implementatie van het normenkader heeft het risico om te ontaarden in een papieren tijger, in allerlei procedures en protocollen die veel inspanning van alle betrokkenen vereisen, maar die nauwelijks, of slechts indirect, leiden tot concrete verbeteringen. Of die niet evenwichtig zijn: de voordeur krijgt vier sloten, maar de achterdeur blijft open staan.

Hoe kan een instelling hier greep op krijgen? Hoe kan voorkomen worden dat een school op de voorpagina van de kranten komt door een beveiligingsincident? Kort gezegd: door de risico's te inventariseren en eerst de grootste risico's aan te pakken, en van daaruit de aanpak te verbreden.

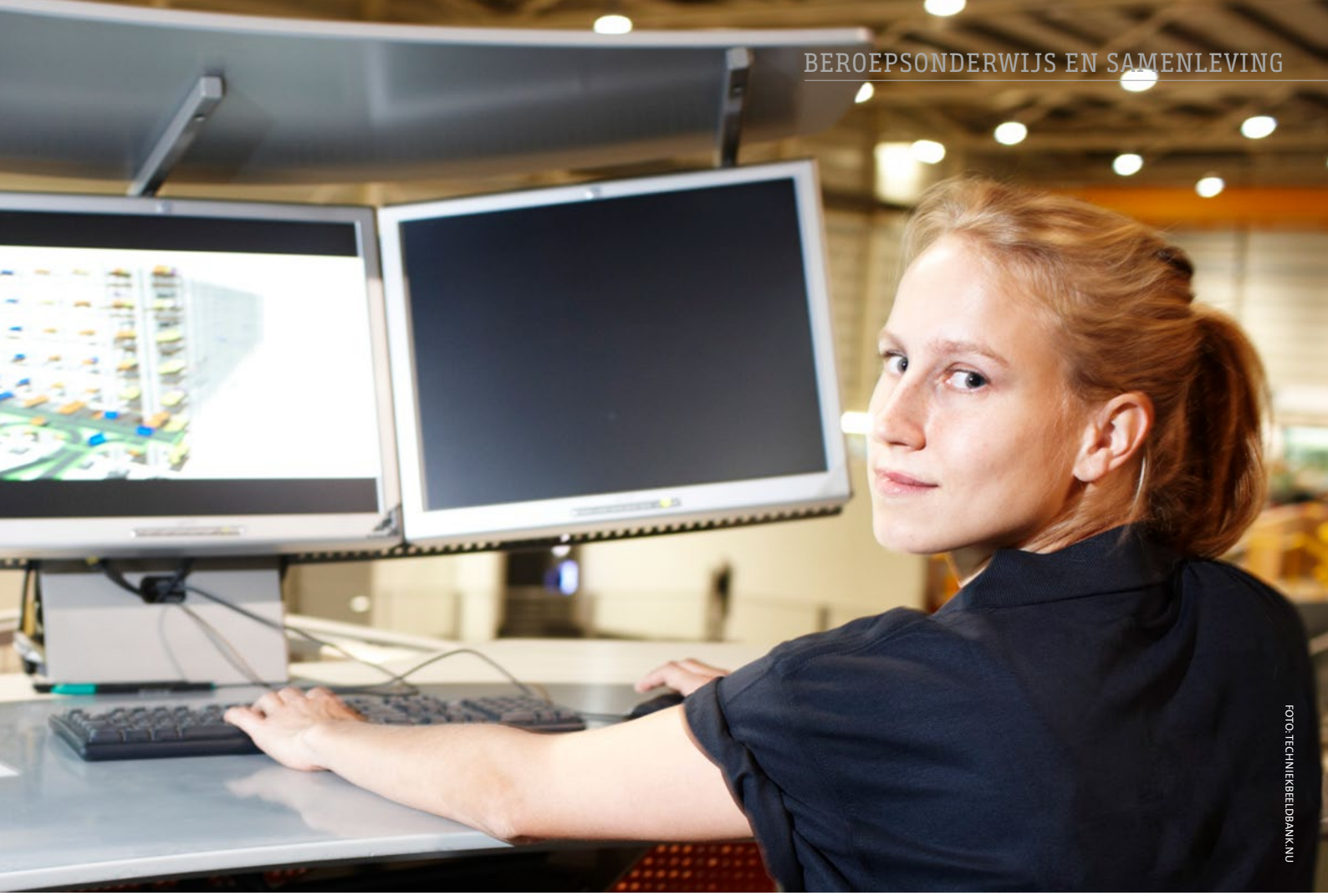
RISICOANALYSE

De eerste stap is dus een risicoanalyse: wat kan ons overkomen? Nu liggen de risico's van de diverse onderwijsinstellingen in elkaars verlengde, dus als vertrekpunt kan heel goed het 'Cyberdreigingsbeeld' worden gebruikt dat Surf ieder jaar publiceert. Daar worden hoge, midden en lage risico's geïdentificeerd, en iedere instelling kan snel zien of de hoge en midden risico's zoals die door Surf worden genoemd, binnen de instelling afdoende worden afgedekt.

Zo is de beveiliging van digitale toetsen één van de hoge risico's die Surf identificeert. De centrale examens taal en rekenen (COE) die door het College voor Toetsen en Examens worden georganiseerd met behulp van Facet zijn goed beveiligd, maar hoe is dat voor de instellingsexamens? Bij veel instellingen ligt de lat daar aanzienlijk lager dan bij de centrale examens, en is b.v. de toegang tot internet voor studenten onvoldoende geblokkeerd tijdens het examen. Instellingen zouden dan gebruik kunnen maken van de 'Safe Exam Browser', een open source hulpmiddel dat de computer effectief afsluit van alles behalve het examen. Verder wordt onderzocht of Facet niet breder kan worden ingezet. Maar naast de technische ingrepen zijn er ook organisatorisch maatregelen nodig om de veiligheid te borgen; het Surf 'Werkboek Veilig Toetsen' biedt hier allerlei aanknopingspunten.

WACHTWOORD

Een ander hoog risico ontstaat als studenten het wachtwoord van een docent achterhalen en als docent inloggen.



Werknemer Jorine (27 jaar) werkt aan een 3D-computersimulatiemodel van een geautomatiseerd material handling systeem

Vooral als docenten zelf cijfers ingeven in het Student Informatie Systeem of toegang hebben tot examenopgaven is dit dodelijk – maar ook het kunnen sturen van rare mailtjes kan grote gevolgen hebben. In een onderwijsomgeving is het voor studenten veelal niet moeilijk om het wachtwoord van een docent te achterhalen: door over de schouder mee te kijken als de docent inlogt op het digibord, of als de docent inlogt met zijn iPad terwijl die op de beamer is aangesloten, of met technische hulpmiddelen als een 'keybord logger' (een apparaatje dat tussen een toetsenbord en een pc wordt geplaatst waarmee alle toetsaanslagen, dus ook het wachtwoord, worden vastgelegd). En met het 'Single Sign On' dat de meeste instellingen hebben geïmplementeerd, kan een kwaadwillende daarmee inloggen in alle systemen waar de docent toegang toe heeft.

De combinatie gebruikersnaam/wachtwoord biedt onvoldoende veiligheid in een onderwijsomgeving. Iedere instelling doet er daarom goed aan om zo snel mogelijk 'tweede factor authenticatie' te implementeren, waarbij een extra controle wordt uitgevoerd op basis van een apparaat dat men moet hebben. Dat kan b.v. een 'token' zijn (een usb-stick die in de computer moet worden gestoken bij het inloggen), maar dat kan tegenwoordig ook met een app op de mobiele telefoon, of door de laptop van de docent eenmalig te registreren. Deze tweede factor authenticatie wordt door allerlei partijen aangeboden (o.a. Microsoft en Surf) op verschillende beveiligingsniveaus, en is niet duur meer.

QUICK WINS

Deze voorbeelden geven aan dat er diverse 'quick wins' te halen zijn die ook bij medewerkers en studenten het vertrouwen geven dat informatiebeveiliging aandacht heeft. Maar daarnaast zijn meer structurele maatregelen nodig. Het instrumentarium dat saMBO-ICT en Kennisnet bieden geeft daarvoor de nodige handvatten, en ook de accountant geeft dit onderwerp de nodige aandacht en doet aanbevelingen. En het is ook goed om af en toe 'ethical hackers' in te huren die op zoek gaan naar mogelijk gaten in de beveiliging; EDP auditors bieden deze dienstverlening aan en het is soms onthutsend om te zien hoe snel de jongelui die deze onderzoeken doen, fouten in de beveiliging ontdekken.

> EEN SCHOOL MOET ZUINIG ZIJN OP ZIJN KROONJUWELEN EN DIE ADEQUAAT BEVEILIGEN

DE AUTEUR IS ADVISEUR VAN HET ONDERWIJS, EN ALS INTERIM INFORMATIEMANAGER VERANTWOORDELIJK GEWEEST VOOR INFORMATIEBEVEILIGING BIJ ENKELE ROC'S.