

## SECURITY AWARENESS IN HET MBO

*Noud Heuvelmans is coördinator Informatiebeveiliging vanuit de afdeling Informatiemanagement, onderdeel van de dienst Informatisering en Automatisering van ROC Eindhoven. Hij is onder meer verantwoordelijk voor het aandragen en opstellen van informatiebeveiligingsbeleid, maatregelen en procedures, en het houden van toezicht op handhaving.*



*Rein de Vries is directeur en mede-eigenaar van LBVD Informatiebeveiligers en adviseert opdrachtgevers met betrekking tot het onderwerp informatiebeveiliging. Zijn focus ligt daarbij met name op statusonderzoek en het komen tot een praktische maar toch doeltreffende invulling van informatiebeveiliging.*



**Vanuit informatiebeveiligingsperspectief wordt vaak het menselijk gedrag als zwakke schakel beschouwd. In sectoren met een intrinsiek 'open karakter', zoals de gezondheidszorg en het onderwijs, kunnen we wellicht zelfs spreken over de zwakste schakel. Recentelijk is voor ROC Eindhoven een bewustwordingscampagne geïnitieerd. Omdat anderen wellicht hun voordeel kunnen doen met de leerpunten, onderstaand een verslag van het doorlopen traject.**

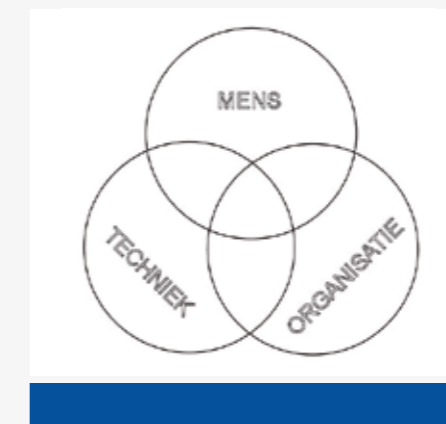
ROC Eindhoven bestaat uit 18 scholen voor middelbaar onderwijs, een school voor volwasseneneducatie en een school voor voortgezet onderwijs. Deze scholen verzorgen in totaal bijna 300 beroepsgerichte opleidingen voor circa 22.500 studenten. De scholen worden ondersteund door diensten op het gebied van onderwijsbeleid, huisvesting, financiën, personeelszaken, communicatie, ICT en projecten. Dit wordt gerealiseerd door circa 1500 personeelsleden en met een jaaromzet van circa 110 miljoen euro.

Informatie wordt gezien als een van de belangrijkste productiefactoren bij ROC Eindhoven. Het zorgvuldig omgaan met informatie(systemen) dient dan ook integraal onderdeel te zijn van de dagelijkse praktijk van alle medewerkers. Zowel in de primaire onderwijsprocessen als in de secundaire ondersteunende processen zijn er talloze voorbeelden te vinden die bijdragen aan de betrouwbaarheid van informatie.

De afgelopen jaren zijn er aanvullend op deze reguliere aandacht een aantal specifieke maatregelen geïnitieerd en/of uitgevoerd, zoals aanscherping van het wachtwoordbeleid, sterkere (2-factor) authenticatie ten behoeve van

externe (VPN-)toegang voor medewerkers, herziening van het privacyreglement verwerking studentgegevens en de gedragscode gebruik ICT-middelen. In 2010 is met het vaststellen van het informatiebeveiligingsbeleid het kader bepaald voor toekomstige maatregelen en investeringen in informatiebeveiliging en de verantwoordelijkheden in de organisatie.

Het bovenstaande stelsel aan maatregelen raakt echter alleen nog maar de techniek en de organisatie. Dit is echter ontoereikend om informatiebeveiliging daadwerkelijk op het gewenste niveau te brengen en te houden. De factor 'mens' verdient evenveel aandacht als techniek en organisatie.



Om inzicht te krijgen in het beveiligingsbewustzijn van de medewerkers is er met behulp van een enquête een nulmeting uitgevoerd.

### Enquête

Maar liefst 44% van de per e-mail benaderde medewerkers heeft de enquête volledig ingevuld (42% van de medewerkers is werkzaam bij een school en 54% van de medewerkers is werkzaam bij een dienst).

In het algemeen geldt dat men 'enigszins tot redelijk bewust' (score 2 en 3 op een schaal met als maximum 4) is van het belang en de inhoud van informatiebeveiliging.

Bij de uitvoering van maatregelen en bewustwordingscampagnes ten behoeve van informatiebeveiliging verdienen met name de volgende items nog de aandacht:

- geheimhouding, identificatieplicht en anti-virussoftware worden in het algemeen herkend als onderdeel van informatiebeveiliging. Minder bekend zijn de fysieke beveiligingsmaatregelen;



Postbus 7  
2600 AA Delft  
Rotterdamseweg 183c  
015 2682533  
www.lbvd.nl

- een meerderheid is zich (in meer of mindere mate) bewust van de vertrouwelijkheid van bedrijfsinformatie van ROC Eindhoven;
- nog niet iedereen vergrendelt zelf het systeem en/of sluit de deur bij het achterlaten van een lege kamer (afhankelijk van een risico-afweging);
- het is nog niet voor iedereen duidelijk waar informatiebeveiligingsincidenten gemeld dienen te worden;
- over informatiebeveiliging en de daarbij binnen ROC Eindhoven van toepassing zijnde afspraken is nog onvoldoende gecommuniceerd.

Naar aanleiding van deze bevindingen is besloten tot een bewustwordingscampagne informatiebeveiliging. Om deze maximaal effect te laten hebben helpt het als er wordt gerefereerd aan significante beveiligingsincidenten in de eigen praktijk. Omdat deze zich, voor zover bekend, gelukkig niet recentelijk hebben voorgedaan, zijn deze gecontroleerd geïnitieerd door middel van MysteryGuest-acties.

**MysteryGuest**

Een MysteryGuest-actie is een onderzoek waarbij een of meer specialisten (in dit geval afkomstig van LBVD) de opdracht krijgen om zichzelf als niet



bevoegd persoon toegang te verschaffen tot een doelobject van de opdrachtgever om vervolgens een specifieke missie uit te voeren. De wijze waarop dit moest plaatsvinden, het doen en laten van de MysteryGuest(s), was van tevoren nauwgezet afgestemd. MysteryGuest-acties testen in feite hoe weerbaar de organisatie is tegen eventuele onbevoegden die op welke manier dan ook trachten toegang te krijgen tot informatie. Niet alleen in digitale en papieren vorm, maar ook zoals deze vastligt in de medewerkers van de organisatie.

**Velen reageren niet of amper op vreemde gedragingen van Mystery Guests**

Veel is gelegen aan 'De Factor Mens'. Is men scherp, heeft men iets door? Komen medewerkers in actie of zien ze passief toe? Is men (te) loslippig? Handelt men doortastend? Ontmaskeren medewerkers de MysteryGuest nog voordat hij/zij heeft kunnen toeslaan? De uitvoering is uitgevoerd door twee samenwerkende MysteryGuests en heeft plaatsgevonden gedurende twee testdagen op twee locaties van ROC Eindhoven.

De werkzaamheden van de eerste dag waren oriënterend, inventariserend en terughoudend van aard. Hierdoor werden er geen incidenten veroorzaakt of de ware identiteit prijs gegeven. Op de tweede dag werden de grenzen opgezocht en werd bij gelegenheid bewust provocerend opgetreden tot het moment dat er tegen de lamp werd aangelopen.

**Bevindingen**

- Veel medewerkers reageren niet of amper op vreemde gedragingen van de MysteryGuests. Medewerkers die wél reageren vragen niet of niet ver genoeg door. Slechts een beperkt aantal medewerkers reageert zeer adequaat door naar autorisatie en/of legitimatie van de MysteryGuests te vragen of te escaleren naar bijvoorbeeld beveiliging.
  - Veel kantoren waren bij afwezigheid op slot, met name waar zich ook veel studenten ophielden.
  - Niet alle medewerkers vergrendelden bij het verlaten van de werkplek hun desktopsysteem of laptop.
- Deze bevindingen zijn geanonimiseerd teruggekoppeld aan de directeuren van de diensten en scholen van de be-

zochte locaties en de directe 'slachtoffers' van de MysteryGuests. Daarnaast zijn de resultaten achtereenvolgend gepresenteerd aan alle directeuren en de adjunctdirecteuren Bedrijfsvoering.

**Vertaling naar de praktijk geeft beveiliging betekenis**

**Campagne**

Direct aansluitend is over alle locaties van ROC Eindhoven een bewustwordingscampagne gestart, waarbij met behulp van prikkelende teksten op posters zowel medewerkers als studenten gewezen worden op hun eigen gedrag met betrekking tot zorgvuldig omgaan met informatie.

Op de posters wordt gewezen naar 'tips & tricks' op intranet en Fronter (elektronische leeromgeving). Daarnaast is in het personeelsblad een artikel gewijd aan de MysteryGuest-acties (zie kader). De aanpak is daarbij bewust zeer sterk op de dagelijkse gang van zaken gericht door middel van aansprekende praktijkvoorbeelden. Immers, pas als de vertaling naar de eigen praktijksituatie wordt gemaakt, krijgt informatiebeveiliging betekenis.

Na afloop van de bewustwordingscampagne zal er op basis van de eerder uitgevoerde enquête worden vastgesteld

hoeveel effect de bewustwordingscampagne heeft gesorteerd. De uitkomst maakt het mogelijk om de aanpak van toekomstige campagnes waar nodig bij te stellen.

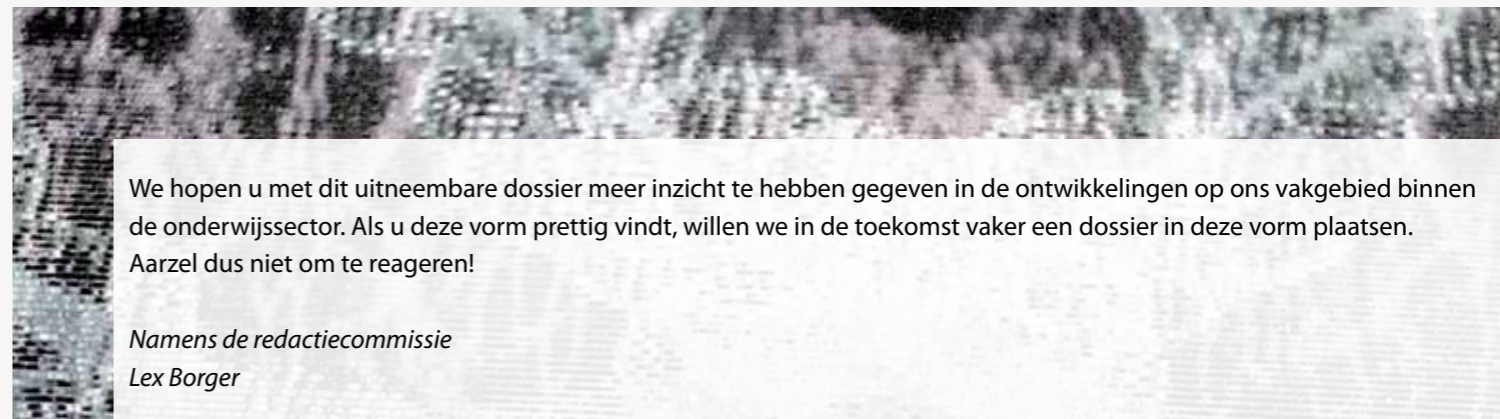
**Conclusie**

Een MysteryGuest-actie is een zeer krachtig begin van een bewustwordingscampagne informatiebeveiliging. Via zo'n vooropgezette actie krijgt de organisatie niet alleen inzicht in de

actuele kwetsbaarheid die de factoren met zich meebrengt, maar ook waardevol materiaal uit de praktijk om de bewustwordingscampagne te voeden. Het is niet ergens gebeurd. Nee, het is hier gebeurd. De anekdotes, belevenissen en het beeldmateriaal spreken aan en zorgen voor discussie omdat het de eigen omgeving betreft. De diverse voorvallen, mits breed uitgemeten, doen de ogen openen en beseffen dat je als medewerker (of student!) er zelf deel van uitmaakt en er wat aan kunt doen.

**Leerpunten en adviezen voor andere instellingen**

- Laat buitenstaanders de MysteryGuest-actie uitvoeren. Volslagen vreemden die succesvol zijn geweest geven een veel groter effect dan de beveiliging die een loopronde heeft gedaan en schendingen heeft geconstateerd.
- Werk met heldere doelstellingen en onderzoeksvragen. Deze geven richting aan de MysteryGuest-actie en zorgen voor een adequate en effectieve uitvoering.
- Leg de nadruk op zones met een verhoogd risico, zoals de computerruimte en andere ruimten waar je waardevolle bedrijfsmiddelen aantreft, maar zie overige ruimten niet over het hoofd.
- Ontziet de directie- of CvB-vloer niet. Ook de directie of het CvB kan een 'target' zijn.
- Laat de MysteryGuests veel interactie met medewerkers opzoeken ('social engineeren'). Hier komen sprekende belevenissen uit voort.
- Lok tegen het einde van de actie incidenten uit die een organisatie-brede uitwerking hebben, bijvoorbeeld met inschakeling van de leidinggevende, de directeur, ICT of de beveiliging. Laat de MysteryGuest een aantal keren bewust tegen de lamp lopen, althans, *als dat lukt!*



We hopen u met dit uitneembare dossier meer inzicht te hebben gegeven in de ontwikkelingen op ons vakgebied binnen de onderwijssector. Als u deze vorm prettig vindt, willen we in de toekomst vaker een dossier in deze vorm plaatsen. Aarzel dus niet om te reageren!

Namens de redactiecommissie  
Lex Borger