

Hoe voorzichtig zijn we met onze wachtwoorden? Bewaren we vertrouwelijke informatie altijd achter slot en grendel? Laten we waardevolle spullen niet onbeheerd achter? Twee mysteryguests gingen op zoek naar beveiligingshiaten op twee locaties van ROC Eindhoven. Ze kwamen terug met schokkende resultaten. Een reconstructie in vijf delen.

Beveiligingscampagne van start

# ‘Natuurlijk krijg je mijn wachtwoord... niet’

## DEEL 1

### Kasten en ruimtes

Mysteryguest 1 loopt door de gang en voelt aan de deuren. Een aantal is keurig afgesloten, maar één kantoor is open. Er is niemand aanwezig, papieren liggen op tafel, de pc is niet vergrendeld en kasten staan open. Dossiers met vertrouwelijke informatie over medewerkers zijn rustig te bekijken.

Mysteryguests 1 en 2 lopen een ruimte binnen waar een brief op de deur hangt met daarop de mededeling dat deze ruimte alleen toegankelijk is voor bepaalde medewerkers. Eén van deze medewerkers is in de ruimte bezig maar reageert niet op de onbekenden. Hij vraagt zelfs of de heren nog in de ruimte moeten zijn als hij weggaat.

Noud Heuvelmans, coördinator informatiebeveiliging van de dienst I&A: “In het kantoor met de geopende kasten kwamen op een bepaald moment wel medewerkers binnen. Zij reageerden toen wel meteen op de vreemde gasten. Uiteindelijk moesten ze hun vrijwaringverklaring laten zien om aan te tonen dat ze met toestemming in het gebouw waren. Helaas was het kwaad toen al geschied en stonden de geopende kasten met dossiers op foto. We moeten als medewerker meer durven vragen aan vreemden. Als er onbekenden op de gang lopen, vraag of je ze kunt helpen. En vraag door als het verhaal niet goed klinkt. Sluit kasten af en vergrendel je pc, ook als je maar even weg bent.

## DEEL 2

### Informatiebeveiliging

Mysteryguest 1 loopt op de gang. Een medewerker vraagt waar de onbekende naar op zoek is. De mysteryguest vraagt waar de tentamens en examens worden opgeslagen. De medewerker is niet achterdochtig en geeft de gevraagde info en vertelt ook waar en bij wie de sleutels van de kluis te krijgen zijn.

Noud: “In het onderzoek ging het ons met name om de menselijke kant van informatiebeveiliging. Hoe reageren onze medewerkers? Zijn ze loslippig, hebben ze iets door en komen ze in actie; handelt men doortastend en ontmaskeren ze de mysteryguests? De ‘mysteryguests’ hadden wel een verhaal klaar, maar daar was voor een oplettende ondervrager vrij eenvoudig doorheen te prikken. Men is niet gewapend tegen het zogenoemde ‘social engineering’ waardoor informatie ontfutseld kon worden of verzoeken worden uitgevoerd.”

## DEEL 3

### Het vrijgeven van wachtwoorden

Mysteryguest 2 loopt een kantoor binnen. Daar zitten enkele medewerkers aan hun bureau. De mysteryguest vertelt dat hij een onderzoek doet naar de sterkte van wachtwoorden. Voor dit onderzoek heeft hij wachtwoorden nodig. Of de medewerkers die even willen geven.

Noud: “Dit vage verhaal was voor menigeen voldoende om het wachtwoord af te geven. ‘Tuurlijk, ik schrijf het even voor je op’, was het meest welwillende antwoord. Een enkeling verzette zich hiertegen of reageerde helemaal niet op het verzoek. Er was vrijwel niemand die precies wilde weten waarom er wachtwoorden nodig waren voor het onderzoek. De ongenode gasten hebben met de passwords, in combinatie met de nog makkelijker verkrijgbare inlognamen, ingelogd en als bewijs een mail vanuit die computers gestuurd.”

## DEEL 4

### Persoonlijke spullen

Mysteryguest 1 weet dat diefstallen in het bedrijfsleven vaak door collega's worden gepleegd. Hij loopt de kantoren binnen om te kijken of er nog iets kostbaars is blijven liggen. Lang hoeft hij niet te zoeken: in een verlaten, open kantoor liggen een blackberry, portemonnee en een set autosleutels voor het grijpen. Bingo!

“Informatiebeveiliging gaat ook over je eigen spullen”, zegt Noud. “Berg je spullen op. Je wil niet dat andere mensen met jouw gegevens aan de haal gaan. En in telefoons en portemonnees zit een schat aan informatie. Zet je tas met je persoonlijke spullen achter slot en grendel. En vergeet daarbij ook de usb-sticks niet”.

## DEEL 5

### De ontmaskering

Mysteryguest 1 en 2 lopen een kantoor binnen en vragen aan een medewerkster of ze even een meting op haar pc mogen doen in verband met de snelheid van het netwerk. De medewerkster vertrouwt het niet en zegt dat ze daaraan niet mee wil werken en vraagt voor welke afdeling de heren werken. Daarop gaan de gasten haar kamer uit.

“Deze medewerkster reageerde heel alert”, vertelt Noud, “want nadat de gasten haar kamer hadden verlaten liet ze het er niet bij zitten en belde de servicedesk met het verhaal. Die stuurde meteen een medewerker van I&A erop af en die kwam de gasten in de gang tegen. Ook de I&A medewerker trapte niet in het verhaal dat de gasten ophingen en belde meteen de telefoonnummers die zij opgaven. Het verhaal rammelde, zoals afgesproken, aan alle kanten. Uiteindelijk waren de gasten gedwongen zich bekend te maken. Probeer assertief te zijn en een verhaal te verifiëren als je het niet vertrouwt.” <<



Vergrendel kasten als er niemand in het kantoor is.



De gelegenheid maakt de dief.



## Beveiligingscampagne

De rapportage van de mysteryguests was voor de dienst I&A reden om met een informatiebeveiligingscampagne te starten. Door middel van posters in de gebouwen worden medewerkers en studenten gewezen op de noodzaak van informatiebeveiliging. Op Fronter en Intranet staan artikelen en krijgen mensen tips hoe je je informatie kunt beveiligen. Na ongeveer een maand wordt gemeten of men bewuster met informatie omgaat.