



# Mysterieuze gast over de vloer

## VOOROPGEZETTE INCIDENTEN WERKEN

*Bewustwording is een voorwaarde voor een goed geïmplementeerd informatiebeveiligingsbeleid. Bewustwording bij management met betrekking tot nut en noodzaak – maar ook bewustwording bij medewerkers aangaande regels, en de reason why. Hans Labruyère van LBVD informatiebeveiligers beschrijft hoe vooropgezette incidenten helpen bij het bevorderen van het ‘securitybewustzijn’.* HANS LABRUYÈRE

Incidenten hebben een positieve uitwerking. Ik noem dat ‘het Tonino Effect’. Dit incident is inmiddels ruim tweeënhalve jaar geleden, maar nog steeds weet iedereen waar dit over ging. Incidenten werken dus. Zo ook vooropgezette incidenten, variërend van de bekende hackpoging tot de inmiddels veel gekopieerde ‘Mystery Guest’.

Een Mystery Guest is een soort fysieke hacker: mister Nobody. Niet noodzakelijkerwijze een externe overigens: driekwart van de incidenten in ons vak komt niet van buiten. De vraag die een Mystery Guest voornamelijk moet beantwoorden is: wat kan iemand doen die binnen is (al dan niet met opzet)? De volgende vraag zou kunnen zijn: Hoe makkelijk is het om ongenood binnens te komen? Via een Mystery Guest wil je te weten komen wat de cultuur van het doelobject is; welk jargon wordt gebruikt en hoe de geldende regels eruit zien. De Mystery Guest moet een specialist zijn die zeer snel kan schakelen, een brede scope heeft en bovengemiddeld kan acteren.

Ook de opdrachtgever is bijzonder: er is veel lef voor nodig jezelf en je

organisatie zo kwetsbaar op te stellen. Er is durf nodig om je medewerkers op deze manier ‘aan te vallen’, en je open te stellen voor hun hoon, hun kritiek en teleurstelling.

### ISZF

Gemeenten dienen te voldoen aan eisen aangaande beveiliging van informatie. Dat is niet alleen wettelijk bepaald (regels omtrent GBA, SuwiNet, Privacywetgeving of de Archiefwet), maar dat is ook de stelling van ‘de burger’. Een gemeente is het knooppunt van informatie, en dient daar goed op te passen.

In Zuid-West Friesland hebben zes kleinere gemeenten en een gezamenlijke sociale dienst een shared service organisatie (SSO) opgezet, waarin de afdelingen ICT gezamenlijk worden ondergebracht: het ICT Samenwerkingsverband Zuidwest Fryslân (ISZF). “In 2004 zijn we als SSO gestart. Onmiddellijk liepen we er tegen aan dat een gezamenlijk informatie beveiligingsbeleid een must is”, vertelt Henk Post, sinds 2004 als Security Officer verbonden aan het ISZF. “Je moet afspraken maken wie waarover gaat en wat het niveau van

beveiliging is. Dat moeten gezamenlijke afspraken zijn, want we zitten allemaal op hetzelfde netwerk. Weliswaar opgedeeld in virtuele LAN’s, maar toch.”

### Beveiligingsbeleid

Een eerste stap was dus het opstellen van een gezamenlijk beveiligingsbeleid. Henk Post: “Een akkoord daarop kwam van het bestuur van onze organisatie ISZF. Vervolgens is het beveiligingsbeleid vastgelegd door alle deelnemende organisaties aan het ISZF en het ISZF zelf.”

In 2005 werd met behulp van het ISZF en collegae uit alle deelnemende organisaties het beleid uitgewerkt tot ‘handboeken beveiliging’. Hierin werd per organisatie het beleid uitgewerkt ▶





◀ naar concrete maatregelen. Alle betrokken gemeenten moesten door de wettelijk verplichte 'GBA audit' aantonen hoe de informatiebeveiliging van de afdelingen burgerzaken geregeld is. In een gezamenlijk project van het ISZF slaagden alle gemeenten hiervoor, en werden de accountants tevreden gesteld.

"Prachtig dus. Op papier was alles goed geregeld", aldus Post. "Maar als security officer van het ISZF zie ik ook gevaren in dit traject. Voor sommige aangesloten organisaties gold dat het

van de risico's." Al snel ontstond bij de Security Officer het idee om met een penetratietest en een Mystery Guest het onderwerp beveiliging eens op een out-of-the-box manier bij de mensen onder de aandacht te brengen. "Om eerlijk te zijn heb ik daar best wel even over gearzeld. Het kan niet missen of je haalt je hier als security officer veel ellende mee op de hals. Gaat men je na afloop feliciteren met het initiatief? Of word je aan de hoogste boom geknoot? Eigenlijk een beetje van beide... Soms moet je ook niet te bang zijn."

#### **Opdracht Mystery Guest**

Als onderdeel van een ruimere opdracht kreeg de Mystery Guest de uitdaging 'managers en medewerkers te laten zien dat het ook hén kan gebeuren', en dat het wellicht niet (voldoende) zou worden opgemerkt. Het primaire doel was bewustwording, bij zowel management als medewerkers.

stellen de aanvaller te pakken. Als die medewerker daaraan denkt.

Er is afgesproken gedurende meerdere dagen aanvallen te doen, om te voorkomen dat bevindingen als incidenteel worden afgedaan. Ook telefonische activiteiten konden worden ontplooid. Samen met de opdrachtgever is een mening gevormd omtrent privé zaken: PDA's, mobiele telefoons, maar ook tassen (soms met behoorlijke inhoud) en autosleutels. In de praktijk zijn voor dit soort opdrachten privéspullen waardevol: zij bieden de aanvaller de mogelijkheid 'iets van de eigenaar te leren', of iets voor de eigenaar te kunnen betekenen. Wat zou u doen als de Mystery Guest uw autosleutels heeft 'gevonden'? Zou u weigeren (later) even iets voor hem of haar op te zoeken, en te mailen? Zou u de link in de reply inderdaad niet openen? Voor de opdrachtgever vormen privéspullen de link tussen beveiligingsregels en noodzaak: thuis doe je ook de deur op slot, en berg je je spullen op – waarom dan hier niet?

## **"Het is ook niet leuk om te kijk gezet te worden, als jij degene bent die als 'het lek' in de organisatie wordt aangewezen"**

management vervolgens beveiliging van de agenda haalde. Dat lag immers bij het ISZF. Slechts af en toe kwam er een vraag om op de hoogste te blijven van de maatregelen die het ISZF allemaal trof op het gebied van beveiliging."

#### **Bewustwording**

Ondertussen bevindt het ISZF zich in een lastige positie. Enerzijds moet tegemoet worden gekomen aan de strengste eisen op het gebied van beveiliging, anderzijds leiden strenge maatregelen tot klachten bij 'lossere' organisaties. Die beseffen niet dat een open deur bij de één leidt tot een open deur bij alle ISZF organisaties.

Volgens Post vond er eind 2005 een omslag plaats. Na een aantal kleinere incidenten daagt het begrip dat er niet meer energie gestoken moet worden in nog meer 'regeltjes' van het ISZF. "Het echte probleem lag in bewustwording

Secundair doel was met die bewustwording het huidige beleid nog eens tegen het licht te houden, en daar waar nodig aanpassingen te doen. Maar dat moest dan wel door uit te gaan van de proceseigenaren - de gemeentesecretarissen - in plaats van de feitelijke (maar oneigenlijke) probleemeigenaar: de security officer van de ICT shared service organisatie.

Een Mystery Guest kan gebruik maken van een aantal 'smoezen' en dekmantels. Minimale kennis van de voorgestelde organisatie is vaak al voldoende om geloofwaardig over te komen. In beperkte gevallen wordt er gevraagd naar een ID, en voor die gevallen is er een (duidelijk uit knip-en-plakwerk, inclusief taalfouten vervaardigd) 'identiteitsbewijs' voorhanden. De naam op dat bewijs wijkt bewust af van de naam op het geldig ID van de Mystery Guest, om de medewerker van het doelobject in de gelegenheid te

#### **Aan de slag**

In de voorbereiding is door de opdrachtgever documentatie zoals telefoonlijsten overhandigd, waarna de Mystery Guest aan de slag kan. Zoals verwacht is de buitendeur, alsmede de 'publieke ring' binnen in het pand elektronisch afgesloten, maar als je er vriendelijk uitziet, en op het juiste moment een (fake) mobiel telefoongesprek voert, is menig passant vriendelijk bereid je binnen te laten. En doordat je toevallig net in gesprek bent, worden je lastige vragen veelal bespaard. Eenmaal binnen gebeurt er iets aardigs: de Mystery Guest valt in de categorie: 'Die zal hier wel horen, ▶





- ◀ want wij hebben een elektronisch afgesloten deur, en een balie.'

De ervaring leert dat Nederlanders vriendelijk antwoord geven als je ze iets vraagt. Ook de ISZF-medewerkers voldeden aan dat beeld: ze wilden hun pc best even opnieuw opstarten, zelfs als er foto's van worden gemaakt. Dat de camera wel erg lang in dezelfde houding

## Er is durf nodig om je medewerkers op deze manier 'aan te vallen', je open te stellen voor hun kritiek en teleurstelling

bleef, viel blijkbaar niet zodanig op, dat er een opmerking over werd gemaakt. Maar met de camera in filmstand kan later een 'afdruk' van gebruikersnaam en wachtwoord worden gemaakt. De aanvaller kan zich vervolgens voordoen als de eigenaar van dat systeem... met alle gevolgen van dien.

### Alibi

Het komt voor dat argwanende medewerkers de Mystery Guest wel aanspreken, maar 'ge-social engineerd' worden: ze stellen hun mening bij: 'als het loopt als een eend, en kwaakt als een eend, dan zal het wel een eend wezen.' Zo'n mening is voor de Mystery Guest een zegen, want veelal voelen deze mensen zich na de bijstelling een beetje lullig over hun eerdere argwaan, en zijn ze vervolgens bereid tot het beantwoorden van diepgaande vragen, en zelfs het begeleiden van de Mystery Guest, om aldus zijn alibi te vormen. Eén gemeentelijke manager stuurde zelfs een mail aan zijn interne collega's om hen te vertellen dat er een onderzoek gaande was, waarvoor hun medewerking vereist was, de vriende-

lijkheid ten top, natuurlijk.

Clean-desk, clear-screen: voor de Mystery Guest zijn er vaak geen geheimen. Vooral niet als de sleutel van de dossierkast op die kast ligt. Of in de bureaulade. Heeft uw collega ook gele plakertjes onder zijn muismat? Natuurlijk is het lastig als je scherm na tien minuten uit floept, maar het is veel lastiger als een vreemde (binnen die tien minuten) in staat is namens een medewerker een e-mail te sturen. Of een datadrager aan een open systeem te verbinden. Of nog erger.

### Het resultaat

De presentatie van de bevindingen geschiedt naast een rapportage idealiter (afhankelijk van de cultuur en populariteit van de opdrachtgever) 'en plein

publique': gelardeerd met plaatjes, filmpjes, voorbeelden, en onderling (leed-)vermaak. Daarbij is het overigens niet de bedoeling dat er afdelingen zwart worden gemaakt - het gaat om een positief leerproces.

"Wees van één ding verzekerd: dit vindt men niet leuk!", weet Post. Bij vrijwel alle aangesloten ISZF-organisaties bleek dat er genoeg mis was. "En natuurlijk brak er lichte paniek uit. Boze mensen, die zich afvroegen waar het ISZF zich mee bemoeide. Geschrokken mensen, die zich realiseerden dat ze net een uur tevoren iemand hadden laten meekijken hoe hun wachtwoord keurig voldeed aan allerlei eisen. Mensen die boos waren omdat ze zelf iemand in hun archieven hadden laten neuzen. Zo maar iemand die zich voor iemand anders uitgeeft! Dat moest toch niet mogen, dat doe je toch niet!"

"Het is ook niet leuk om te kijk gezet te worden, als blijkt dat jij degene bent die bezoekers in hun eentje door het pand laat lopen, als jouw pc eenvoudig gekraakt wordt, als jij degene bent die als 'het lek' in de organisatie

wordt aangewezen. Maar wat we niet direct verwacht hadden: op topniveau kon men de humor er ook wel van inzien. Grinnikend vertelden de topmanagers (gemeentesecretarissen) in hun regulier overleg de dag erna wat hun organisatie was overkomen. Het siert hen dat ze direct het nut van de exercitie inzagen, en de commotie susten. En natuurlijk stuurden zij de verontwaardigde managers (degenen die door de Mystery Guest in het ootje waren genomen) naar het ISZF om samen met hen de test te bespreken."

### Doel

Deze reactie beantwoordt vrij goed aan het eigenlijke doel van vooropgezette incidenten als Mystery Guest: 'het onderwerp bespreekbaar maken'. Want vaak valt niet te beoordelen of het erg is dat een document met salarisgegevens en sofinummer in de oud-papierbak werd teruggevonden (los van wettelijke eisen). Maar een Mystery Guest moet mensen er wel over laten nadenken. En meningen laten vormen, die op afwegingen gebaseerd zijn. En niet op: 'het gebeurt hier toch niet'.

Pas als er voldoende bewustzijn bij het management is om beveiliging van informatie op een voldoende serieuze manier te behandelen (of niet natuurlijk - maar dan geschiedt dat ook bewust), kan er bewustwording worden opgebouwd bij de medewerkers. Bewustwording bij medewerkers is noodzakelijk voor draagvlak, en dus uiteindelijk voor het welslagen van het informatiebeveiligingsbeleid - hoe uitgebreid of pover dat ook is.

**Hans Labruyère** is partner bij LBVD informatiebeveiligers. Hij is onder andere gastdocent bij het TIAS inzake social engineering.

