

# Werkt de beveiliging wel?

Hoe goed de beveiliging (op papier) ook in elkaar zit, het kan geen kwaad om van tijd tot tijd een test uit te voeren waarbij een ethische binnendringer kijkt of de beveiliging echt wel zo goed werkt. Hoe gaat dat in zijn werk bij het testen van de toegangsbeveiliging? REIN DE VRIES \*

**S**teeds meer organisaties die willen weten hoe hun toegangsbeveiliging in de praktijk uitpakt en hoe weerbaar de organisatie is tegen buitenstaanders die kwaad in de zin hebben, gaan over tot het daadwerkelijk testen van de weerbaarheid. Hoe bestand is de organisatie tegen bedrijfs-spionage, tegen al te nieuwsgierige personen, tegen sabotage, enzovoort? Organisaties willen weten of de genomen maatregelen - organisatorisch, technisch en gericht op de medewerker - doeltreffend (effectief) en doelmatig (efficiënt) zijn.

## Deming

De behoefte om te willen weten of en hoe goed het werkt, komt met name voort uit de Deming-kwaliteitscirkel (Plan-Do-Check-Act) die steeds meer organisaties voor hun managementsystemen, zoals ISO 9001, gebruiken. Organisaties die ook hun beveiliging goed op de rit willen hebben als 'managed system', realiseren zich dat er naar doeltreffendheid moet worden gekeken om de cirkel rond te krijgen.

In de Plan-fase hebben risicoanalyse en andere methodes de beheersdoelen, beveiligingseisen en concrete beveiligingsplannen opgeleverd. Geselecteerde beveiligingsmaatregelen zijn vervolgens ten uitvoer gebracht (de Do-fase). Veel organisaties laten het hier verder bij en trekken de conclusie dat de beveiliging werkt omdat er nooit incidenten plaatsvinden. Maar is deze conclusie wel gerechtvaardigd? Immers, een incident is slechts een incident als het

voorval op enige wijze wordt opgemerkt en van hetgeen je niet opmerkt, heb je geen weet. Je kunt dus niet weten of de beveiliging echt goed haar werk doet. Of misschien zo af en toe faalt en dus (te) zwak is.

Om te weten of bijstelling of -sturing nodig is, is meer nodig. Een test uitgevoerd door een derde partij kan hierbij behulpzaam zijn. Het levert de voor bijstelling benodigde inzichten op. Uitvoering door een derde partij zorgt voor het doorprikken van beveiligingsblindheid. Onvermoede kwetsbaarheden en zwakke plekken van uiteenlopende aard komen aan het licht. De blackbox-uitvoering, waarbij geen tot nauwelijks voorinformatie aan de binnendringer is gegeven, voorkomt reacties als 'ja, maar zo kan ik het ook'.

## Test

Een MysteryGuest-test is een onderzoek waarbij een of meer professionele en (uiteraard) ethische binnendringers de opdracht krijgen om zichzelf vanuit de positie van niet-bevoegd persoon toegang te verschaffen tot de organisatie om vervolgens een specifieke missie uit te voeren.

De wijze waarop dit moet plaatsvinden, het doen en laten van de binnendringende professional(s), moet van tevoren nauwgezet worden afgestemd tussen de uitvoerende partij en de organisatie.

Dergelijke binnendringacties leveren met name inzichten op wat betreft de menskant. Immers, veel is gelegen aan de factor 'mens': is men alert, heeft

men iets door? Komen medewerkers in actie of zien ze passief toe? Is men (te) loslippig? Handelt men doortastend? Ontmaskeren medewerkers de binnendringer nog voordat hij heeft kunnen toeslaan?

Maar ook in *technisch* en *organisatorisch* opzicht kan een test veel opleveren. Technische voorbeelden zijn er te over zoals deuren die niet goed of niet snel genoeg in het slot vallen, deuren die met niet veel moeite te openen blijken te zijn, camera's die niet goed gericht zijn en constructies die weliswaar mooi zijn vormgegeven door de architect, maar niet 100 procent het doel treffen.

## Voorbeeld

Een voorbeeld van een zwakte in de organisatie is het volgende. De binnendringer is opgemerkt, is staande gehouden en gevraagd naar de reden van zijn aanwezigheid. Vanwege het ontbreken van een legitieme reden is hij direct naar de uitgang begeleid en gemaand te vertrekken.

Op zich is dat geen onaardig resultaat, maar men heeft verzuimd de ware identiteit te achterhalen van de binnendringer: wie was het nou eigenlijk? Het enige wat de organisatie achteraf in handen heeft, zijn (misschien) videobeelden en herinneringen van medewerkers zoals 'een kleine blonde persoon'.

Daarnaast is niet gecontroleerd of de binnendringer ondertussen al een buit had bemachtigd. Misschien had de binnendringer reeds kans gezien om informatiedragers te ontvreemden (di-

gitale én papieren dragers), informatie op een meegebrachte usb-stick te zetten, foto's te maken met een smart-phone of spyware of af luisterapparatuur te plaatsen.

### Doel

Om de juiste gewenste resultaten op te leveren, moeten MysteryGuest-acties goed worden afgestemd tussen de contactpersoon bij de opdrachtgever en de coördinator van de actie bij de opdrachtnemer.

Een goede intake is een absolute must. Vooral het feitelijke doel achter de actie is van wezenlijk belang. Welk specifiek doel heeft de opdrachtgever ermee voor ogen?

Is de actie bedoeld als nulmeting, om inzicht te bieden in de huidige situatie, of dient de actie vooral om het bewustzijn te verhogen?

Als de insteek het verhogen van bewustzijn is, moet er bijvoorbeeld meer interactie met medewerkers worden gezocht, moet er onder andere meer kattenkwaad worden uitgehaald en zal meer moeten worden getracht om tegen de lamp te lopen.

Bij een statusmeting moet de binnendringer zich terughoudender opstellen, om gedurende een tijdslot zijn waarne-



mingen te kunnen doen. Interactie met medewerkers moet daarbij niet uit de weg worden gegaan, maar ook niet specifiek worden opgezocht.

De intake moet ook uitsluitel geven over andere zaken, bijvoorbeeld of de binnendringer gevaar loopt (zoals van-

over gedrags- en/of huisregels (in veel organisaties niet of slechts gebrekkig voorhanden) helpt om te anticiperen op te verwachten gedrag en om de bevindingen te scoren.

Verder moeten specifieke afspraken worden vastgelegd over het verkrijgen

### Aandachtspunten bij MysteryGuest-bezoeken

- » Zorg voor een **goede afstemming** vooraf tussen opdrachtgever en opdrachtnemer.
- » Maak helder wat het **doel** is achter de test (bijvoorbeeld nulmeting of verhogen bewustzijn).
- » Maak duidelijk of de binnendringer eventueel **gevaar** loopt.
- » Denk goed na over de **dag** waarop de binnendringer de organisatie bezoekt.
- » Zorg voor **enige informatie** vooraf (bijvoorbeeld een plattegrond en bekendheid met gedrags- en/of huisregels).
- » Maak specifieke afspraken over het verkrijgen van **bewijsmateriaal** (foto's, filmmateriaal en tastbare zaken).
- » Spreek af hoe de binnendringer zich **bekend kan maken** bij ontdekking.

## De uitvoering van een test door een derde partij zorgt voor het doorprikken van de beveiligingsblindheid

wege radioactieve straling) en of er gevaar is voor het aanmerkelijk verstoren van bedrijfsprocessen. Het ontvreemden van een document kan meer consequenties hebben dan je in eerste instantie vermoedt.

Ook de weekdag kan van belang zijn: bij veel organisaties zijn vrijdag en woensdagmiddag erg rustige dagen en daardoor minder of niet representatief voor de 'normale' situatie.

Het budget in tijd dat beschikbaar is voor de uitvoering, is vaak beperkt. Enige informatie vooraf, zoals een plattegrond, kan helpen om de beschikbare tijd effectiever te besteden. Dit pleit voor een niet 100 procent blackbox-uitvoering. Het beschikken

van bewijsmateriaal (bijvoorbeeld foto's, filmmateriaal en tastbare zaken), het inspecteren van zaken en het penetreren van diverse soorten ruimtes (denk aan de directievloer, technische ruimtes, medicijnkasten, enzovoort).

### Uitkomsten

Een goede voorbereiding is eveneens belangrijk voor het opleveren van de juiste uitkomsten. De organisatie beoogt een zekere mate van weerbaarheid tegen aanvallen te bereiken en dus moet je proberen daar met je binnendringactie niet te ver boven te gaan zitten en niet te 'spartaans' aan te vallen. Dat heeft geen zin. Als je het echt wilt, lukt het altijd wel om ergens binnen te geraken. »

## SAMENVATTING!

- » Steeds meer organisaties willen weten of hun toegangsbeveiliging in de praktijk werkt.
- » Om te weten of bijstelling of -sturing nodig is, kan een **MysteryGuest-test** behulpzaam zijn.
- » Zo'n test is een onderzoek, waarbij een professionele binnendringer zich als niet-bevoegd persoon **toegang verschaft** tot de organisatie om vervolgens een specifieke missie uit te voeren.
- » De wijze waarop dit moet gebeuren, moet van tevoren **nauwgezet** worden **afgestemd** tussen de uitvoerende partij en de organisatie.

Als medewerkers niet goed getraind zijn, kun je beter het echte identiteitsbewijs laten afwijken van eventueel gebruikte dekmantels en zorgen voor niet-werkende telefoonnummers ('nooit van gehoord, kennen we niet'). Zo bied je de ongetrainde medewerker een kans om succesvol te zijn. Het aanspreken van een onbekende is veelal al een hele prestatie van medewerkers en het (durven) vragen naar de reden van aanwezigheid en een geldig identiteitsbewijs nog veel meer. Het is zaak om tijdens de voorbereiding een aantal realistische testcases

te ontwerpen die aan de beantwoording van de onderzoeksvraag tegemoetkomen. Denk daarbij aan scenario's die zich in werkelijkheid zouden kunnen voordoen, dat wil zeggen invulling geven aan de vraag hoe een eventuele kwaadwillige te werk zou kunnen gaan om een bepaald doel te bereiken. Dekmantels kunnen hierbij worden gebruikt, maar de testcases moeten altijd realistisch blijven (dit is een criterium). Naast het testen en meten van de huidige status kunnen binnendringacties ook worden gebruikt voor het verkrij-

gen van beeldmateriaal voor awarenesscampagnes en opleidingsdoelinden. De herkenbaarheid van de eigen bedrijfssituatie heeft hierbij een aanmerkelijk versterkend effect. «



\* Rein de Vries is adviseur informatiebeveiliging en directeur bij LBVD Informatiebeveiligers. Hij heeft voor dit artikel geput uit ervaring met het coördineren van meer dan dertig MysteryGuest-acties.

(Advertentie)



Elegant, intelligent en 100% controle!

**Nieuw!**



DOM SICHERHEITSTECHNIK  
**DOM Guardian®**

DOM Guardian® is het nieuwste elektronische deur beslag. Hij is betrouwbaar, toegankelijk en snel te monteren. Met zijn flexibele programmeringsmogelijkheden is er voor iedere behoefte een oplossing. DOM Guardian® is verkrijgbaar als offline variant waar hij de autorisaties van de transponder leest en verkrijgbaar als online variant, waar de DOM Guardian® zijn gegevens draadloos ontvangt via het TCP/IP netwerk d.m.v een RF Netmanager. Met DOM Guardian® heeft u niet alleen een elegant en intelligent product, u krijgt hier mee 100% controle over uw gebouw!

**VEILIGHEID, KWALITEIT, DOM.**

www.dom-nederland.nl


