

Toegangsbeheer: een kat-en-muisspel

Wat is ervoor nodig om mensen die niet tot je organisatie behoren fysiek afdoende te weren zodat ze geen waardevolle bedrijfsmiddelen zoals informatie(dragers) kunnen bemachtigen? Wat is er nodig om ervoor te zorgen dat kwaadwilligen het terrein niet zomaar kunnen betreden of zich onbevoegd in bedrijfspanden kunnen begeven? Dit artikel gaat in op het profijt dat een organisatie kan hebben van goed voorbereide en uitgevoerde MysteryGuest-acties. [REIN DE VRIES *](#)

De meeste organisaties hebben er wel over nagedacht hoe ze een kwaadwillende buitenstaander kunnen weren en hebben een zekere mate van beveiliging – niet alleen fysiek – geïmplementeerd. Hekken, sloten, camera's, beveiligers enzovoort zorgen voor een harde schil aan de buitenkant die voor onbevoegden lastig tot niet te doorbreken is. Althans, velen – en niet alleen insiders – verkeren in die veronderstelling. De vraag is of die veronderstelling terecht is. En een logische vervolgvraag is: als iemand kans heeft gezien de harde buitenschil te doorbreken, wat is hij dan verder bij machte te doen? De medewerkers van de organisatie zijn scherp en alert gemaakt, echter hoe gemakkelijk (of moeilijk) is het om desondanks aan waardevolle informatie te komen? Ten slotte: kun je als ongenode gast met een 'buit' ongeïdentificeerd weer vertrekken? Nadrukkelijk spreken we niet over 'onopgemerkt'. De aanwezigheid zal altijd wel worden opgemerkt. De vraag is of het daarbij blijft.

Plan-Do-Check-Act

Steeds meer organisaties die willen weten hoe hun toegangsbeveiliging in de praktijk uitpakt en willen weten 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 bedrijfsspionage, tegen 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.

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 management-systemen, zoals ISO9001, gebruiken.

MysteryGuest-acties leveren met name inzichten op wat betreft de menskant

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 nimmer 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 MysteryGuest-test uitgevoerd door een derde partij is hierbij behulpzaam. 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 MysteryGuest(s) 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 MysteryGuest(s), moet van tevoren nauwgezet worden afgestemd tussen de uitvoerende partij en de organisatie.

MysteryGuest-acties leveren met name inzichten op wat betreft de menskant. Immers, 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 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: zorgen dat niemand naar binnen kan glippen.

Voorbeeld

Een voorbeeld van een organisatorische zwakte is de volgende. De MysteryGuest 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 klein blond persoon'. Daarnaast is niet gecontroleerd of de binnendringer ondertussen al een buit had bemachtigd. Misschien had de MysteryGuest reeds kans gezien om informatiedragers te ontvreemden

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

Penetratietest

Het uitvoeren van een MysteryGuest-test is te vergelijken met het uitvoeren van een penetratietest op een informatiesysteem (computer), waarbij van buitenaf via een netwerk wordt getest of het systeem te overmeesteren is door gebruik te maken van kwetsbaarheden en/of zwakke plekken (zie dit als het doorbreken van de harde buitenschil) en onbevoegd lees- en schrijftoegang kan worden verkregen tot informatie of anderszins onbevoegd handelingen op het systeem kunnen worden uitgevoerd. Beide tests geven inzicht in de doeltreffendheid van getroffen maatregelen. Bij een penetratietest op informatiesystemen zijn dit bijvoorbeeld de werking van patchmanagement, of het werken met inrichtingsblauwdrukken zijn doel treft, of de personen die het



stelsel hebben ingericht en geconfigureerd (kan ook een derde partij zijn) bekwaam genoeg zijn en of het doorvoeren van wijzigingen beheerst genoeg plaatsvindt.

Doel

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

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

De testcases moeten in alle gevallen realistisch blijven

drachtnemer. Een goede intake is een absolute must. Vooral het feitelijke doel achter de actie is van wezenlijk belang. Welk specifiek doel heeft de opdrachtgever er mee 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 bijvoorbeeld meer interactie met medewerkers worden gezocht, moet onder andere meer kattenkwaad worden uitgehaald en zal meer moeten worden getracht om tegen de lamp te lopen.

Bij een statusmeting moet de MysteryGuest zich terughoudender opstellen, om gedurende een tijdslot zijn waarnemingen 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 MysteryGuest gevaar loopt (zoals vanwege 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 is vrijdag een erg rustige dag en daardoor niet representatief voor de 'normale' situatie). Het budget in tijd dat beschikbaar is voor de uitvoering, is beperkt en enige informatie vooraf, zoals

een plattegrond, kan helpen om de beschikbare tijd effectiever te besteden. Dit pleit voor een niet geheel blackbox-uitvoering. Het beschikken 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 zullen nog specifieke afspraken moeten worden vastgelegd over het verkrijgen van bewijsmateriaal (bijvoorbeeld foto's, film-

Uitkomsten

materiaal en tastbare zaken), het inspecteren van zaken en het penetreren van diverse soorten ruimtes (denk aan de directievloer, technische ruimtes, enzovoort).

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 MysteryGuest-actie 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. Als medewerkers niet goed getraind zijn, kun je beter het echte identiteitsbewijs laten afwijken van eventueel gebruikte dekmantels en zorgen voor niet-werkende telefoon-

nummers ('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 die 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 immer realistisch blijven (dit is een criterium).

Naast het testen en meten van de huidige status kunnen MysteryGuest-acties ook worden gebruikt voor het verkrijgen van beeldmateriaal voor awarenesscampagnes en opleidingsdoeleinden. 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.*

Samenvatting

- » Steeds meer organisaties willen weten hoe hun toegangsbeveiliging in de praktijk uitpakt en hoe **weerbaar** de organisatie is tegen buitenstaanders die kwaad in de zin hebben.
- » Die behoefte komt voort uit de **Deming kwaliteitscirkel** (Plan-Do-Check-Act) die steeds meer organisaties voor hun managementsystemen gebruiken.
- » Om te weten of bijstelling of -sturing nodig is, kan een **MysteryGuest-test** behulpzaam zijn.
- » Een MysteryGuest-test is een onderzoek, waarbij een of meer professionele 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, moet van tevoren **nauwgezet** worden **afgestemd** tussen de uitvoerende partij en de organisatie.