Een serious game voor informatiebeveiliging

Elke organisatie heeft cruciale informatie waarvan de organisatie in hoge mate afhankelijk is. Er kan veel misgaan met deze informatie. Daarom is beveiliging ervan onmisbaar. In de praktijk blijkt goede informatiebeveiliging echter lastig te realiseren. Dit komt enerzijds doordat het complexe materie is, en anderzijds doordat de gangbare opleiding en training op het gebied van informatiebeveiliging wel wat te wensen overlaat. Het is vooral lastig om het menselijke aspect goed voor het voetlicht te brengen. Een realistische simulatie, een serious game, kan helpen het broodnodige inzicht in informatiebeveiliging te verbeteren.

Auteur: **Dr. Marcel Spruit**, lector informatiebeveiliging aan de Haagse Hogeschool en adviseur aan Het Expertise Centrum. Hij is te bereiken op m.e.m.spruit@hhs.nl.

Inleiding

Informatie speelt een cruciale rol in onze maatschappij. Ook in organisaties. Organisaties zijn in hoge mate afhankelijk van allerlei informatie. Het kan dan gaan om personeelsinformatie, marktinformatie, opdrachtinformatie, financiële informatie, etc. Elke organisatie vereist dat belangrijke informatie correct en op de juiste tijd beschikbaar is en dat vertrouwelijke informatie niet op straat belandt. Gezien het aantal beveiligingsincidenten dat optreedt, is dat niet zo eenvoudig. Waar ligt dat dan aan? Als we naar de oorzaken van beveiligingsincidenten kijken, zien we dat de meeste incidenten terug zijn te voeren op menselijk falen. Blijkbaar zijn mensen de zwakke schakel in de informatieverwerking. Anderzijds zijn het ook de mensen die informatiebeveiliging in moeten vullen en tot een succes moeten maken.

In het algemeen kunnen we zeggen dat informatiebeveiliging een sterke menselijke-organisatorische component heeft. De theorie ervan wordt door verscheidene instellingen in het middelbaar en hoger onderwijs aangeboden. Voor de ‘klas’ blijkt echter dat kennis over de menselijke-organisatorische component moeilijk omgezet kan worden naar inzicht. Met aanschouwelijke middelen is het mogelijk om de studenten meer inzicht in de menselijke-organisatorische component van informatiebeveiliging te laten krijgen. Dat was de reden om de hier besproken information security game te ontwikkelen.

Er bestaan al games op het gebied van informatiebeveiliging, maar deze richten zich vooral op het aspect vertrouwelijkheid. In de meeste gevallen gaat het om scenario’s waarin iemand vertrouwelijke gegevens verliest, of een spion op tijd moet

ontmaskeren. In de praktijk komen dergelijke scenario's weliswaar voor, maar ze zijn niet representatief voor de problematiek van informatiebeveiliging.

Waar gaat het dan wel om? In de praktijk blijkt het lastig om een ondersteunende discipline, zoals informatiebeveiliging, bij het management en de collega's op de agenda te krijgen. Bovendien is het lastig om de juiste balans te vinden tussen het eigen werk en informatiebeveiliging. Naast gebrek aan kennis en inzicht spelen ook eigenbelang en kortetermijndenken een rol.

Uitgangspunten

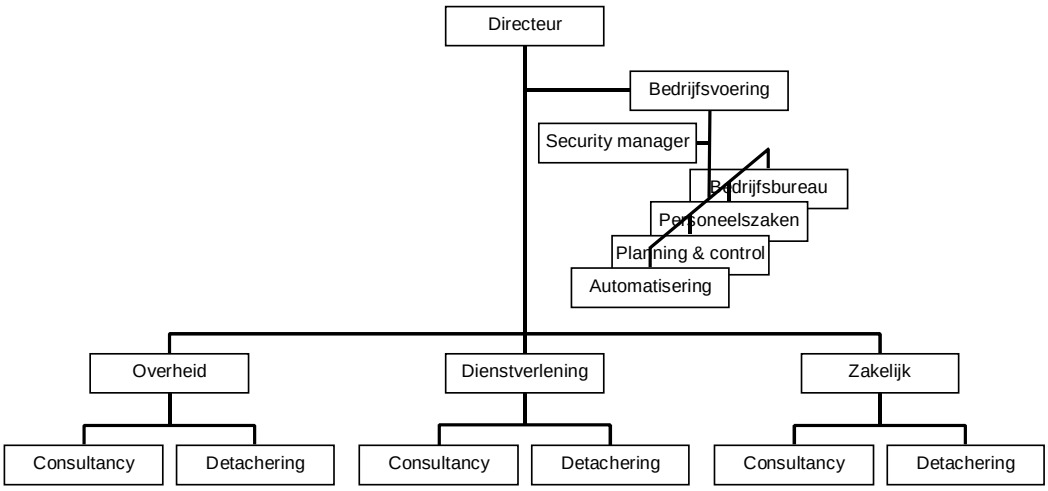
De information security game is een managementgame die specifiek ontwikkeld is om het inzicht in de menselijke-organisatorische component van informatiebeveiliging te vergroten. De game heeft tot doel de deelnemers inzicht te laten krijgen in de praktijk van informatiebeveiliging in een organisatie, aan de hand van realistische bedreigingen en dilemma's in een gesimuleerde bedrijfssituatie. Van de deelnemers wordt verwacht dat zij de basistheorie van informatiebeveiliging voldoende beheersen (Overbeek e.a., 2005). Verdere voorkennis is niet nodig.

De game speelt zich af in het hypothetische bedrijf Insecure, een middelgroot adviesbureau. De deelnemers aan de game krijgen verschillende functies in dit bedrijf toebedeeld.

De game kan in drie uur uitgevoerd worden, inclusief een inleidende presentatie en een nabespreking. De game doorloopt een aantal ronden, waarbij iedere ronde een vaste periode van een jaar representeert. De game verloopt zonder hulp van een computer, hoewel een laptop gebruikt kan worden om een inleidende presentatie te ondersteunen en om de berekening van scores in de game te vergemakkelijken.

Situatieschets

Het bedrijf Insecure is een middelgrote onderneming die zich richt op het leveren van managementadviezen en -ondersteuning aan merendeels grote bedrijven en instellingen. Insecure heeft ongeveer 150 medewerkers in dienst. Een aanzienlijk aantal van deze medewerkers werkt extern op een klantenlocatie. De organisatie van Insecure is op hoofdlijnen geschetst in onderstaand organogram.



Figuur 1: Organogram van Insecure.

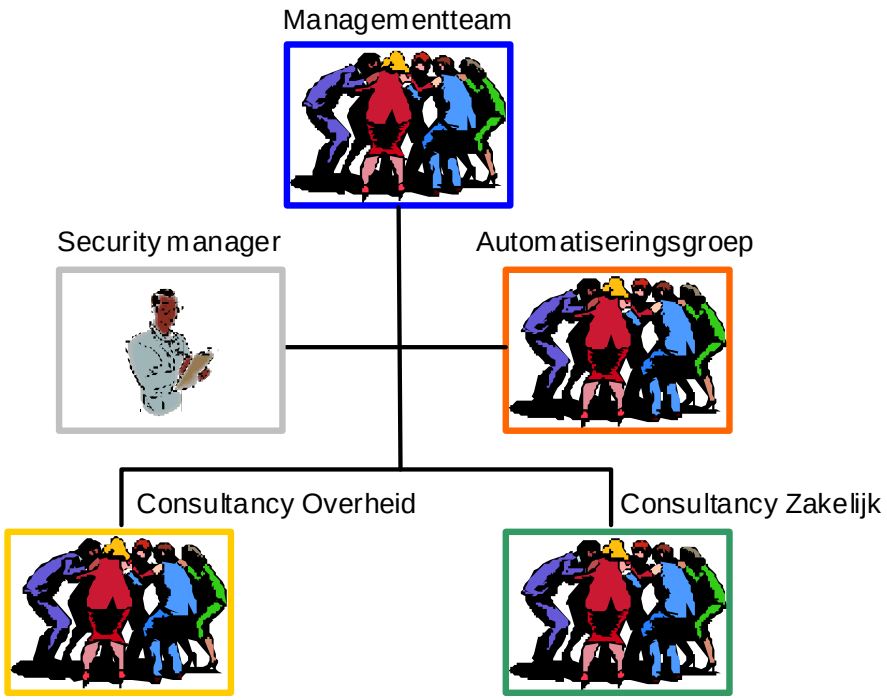
Het primaire proces van de organisatie is belegd bij een drietal branchegeoriënteerde afdelingen: Overheid, Dienstverlening en Zakelijk. Deze afdelingen hebben ieder een consultancygroep en een detacheringsgroep. Daarnaast is er een ondersteunende afdeling, de afdeling Bedrijfsvoering. De automatiseringsgroep en de security manager zijn in deze afdeling ondergebracht. De afdelingshoofden vormen samen met de directeur het managementteam.

De automatisering is niet uitbesteed, maar er is wel gekozen voor het consequent toepassen van standaard ‘off the shelf’ hardware en software.

Structuur van de game

De information security game speelt zich af met de volgende functionarissen van Insecure:

- Het managementteam (directeur en afdelingshoofden).
- De automatiseringsgroep (hoofd IT en IT-beheerders).
- De security manager.
- Een of twee consultancygroepen (per groep een groepshoofd en consultants).



Figuur 2: De groepen in de information security game.

Alle functionarissen hebben hun eigen werk en hebben daar hun handen vol aan. Daarnaast moeten zij ook nog aandacht besteden aan informatiebeveiliging. Alleen voor de security manager geldt dat primaire werk en informatiebeveiliging samenvallen. Voor de andere functionarissen is het de kunst om naast het eigen primaire werk ook nog tijd te vinden voor beveiliging; niet te weinig, maar ook niet te veel.

Gedurende de gesimuleerde jaren, gebeurt het een en ander. Ieder doet zijn primaire werk en doet daarnaast wat nodig is aan informatiebeveiliging. In de tussentijd manifesteren zich bedreigingen. Als de juiste maatregelen getroffen zijn, is dat geen probleem. Zo niet, dan leidt dat tot incidenten, en daarmee kosten.

Informatiebeveiliging kost dus altijd geld: voor maatregelen, of anders door incidenten. Net als in het echt. De kunst is de kosten voor zowel maatregelen als incidenten te minimaliseren. Maar er is, ook net echt, weinig tijd om dat eens goed uit te gaan zoeken. Alle tijd die aan informatiebeveiliging wordt besteed, gaat af van de tijd voor het primaire werk, en het primaire werk levert juist geld op.

De reeks bedreigingen die zich gedurende de game manifesteert, ligt vast en is gebaseerd op praktijkervaring en -onderzoek (SpLo, 1996; BSI, 2007; CSI, 2008). Hetzelfde geldt voor de schade die optreedt bij incidenten en de kosten die gemoeid zijn met het nemen van beveiligingsmaatregelen. Op deze manier zijn de optredende bedreigingen en de kosten voor maatregelen en incidenten tamelijk realistisch.

Welke bedreigingen zich manifesteren, wordt de deelnemers uiteraard niet van tevoren verteld. Ze weten dat de situatie realistisch is, maar ze hebben in het algemeen geen goed beeld van de bedreigingen die in de praktijk optreden en de schade die dat kan veroorzaken. Zij kunnen, en moeten, hierover wel een inschatting maken. Maar in feite weten ze even weinig als functionarissen ‘in het echt’. De kosten voor het treffen van maatregelen zijn daarentegen wel bekend. Uiteindelijk moeten de deelnemers zelf maatregelen treffen en daarvoor betalen.

Karakteristieke elementen

In de game spelen de deelnemers de rol van verschillende functionarissen. De game zou te gecompliceerd worden als het werk van alle verschillende functionarissen nagebootst zou moeten worden. Gelukkig is dat ook niet nodig. Het gaat per slot van rekening niet om de inhoud van het werk, maar om het vinden van de balans tussen het werk en informatiebeveiliging. Voor de game volstaat het als iedere deelnemer aantrekkelijk werk heeft en daarmee een nuttige bijdrage aan de eigen groep kan leveren.

In de game wordt het primaire werk van iedere functionaris gesymboliseerd door het oplossen van puzzels. Iedere deelnemer die een puzzel oplost, creëert een financiële bijdrage aan het groepsbudget. De meeste mensen vinden puzzels maken aantrekkelijk werk en de financiële beloning maakt het werk nuttig voor de groep. Daarmee voldoet het oplossen van puzzels als primair werk voor de deelnemers.

Een cruciaal aspect van de security game is dat de deelnemers de juiste balans tussen werk en informatiebeveiliging niet al te gemakkelijk bereiken. Elke deelnemer kan goede redenen vinden om te weinig of juist te veel aan informatiebeveiliging te doen. Te weinig aandacht voor informatiebeveiliging kan veroorzaakt worden doordat de deelnemer zich mee laat sleuren door het primaire werk, puzzels oplossen, dat rechtstreeks tot beloning leidt. Te veel aandacht voor informatiebeveiliging kan veroorzaakt worden door het besef dat de game over informatiebeveiliging gaat. De deelnemer gaat zich dan op het gebied van informatiebeveiliging voorbeeldig gedragen en treft alle mogelijke maatregelen, maar creëert te weinig inkomsten voor de eigen groep.

In de hitte van het spel is het voor de meeste deelnemers niet duidelijk of zij wellicht te weinig of te veel aandacht aan informatiebeveiliging besteden. Gedurende het spel wordt het de deelnemers steeds duidelijker, want zowel een tekort als een overmaat aan aandacht voor informatiebeveiliging wordt in de game zichtbaar.

De game wordt gespeeld met meerdere groepen functionarissen. In de realiteit beïnvloedt het functioneren van één groep direct het functioneren van de andere groepen. Als bijvoorbeeld het managementteam niet goed functioneert, dan kunnen de

andere groepen ook niet goed functioneren. In de game is dat een nadeel. Wanneer je als groep niet goed kan scoren doordat één van de andere groepen er niets van bakt, dan is dat nogal onbevredigend. Als elke groep daarentegen volledig onafhankelijk opereert, dan is dat weinig realistisch en daardoor ook onbevredigend.

Binnen de game is gekozen voor een opzet met een zeer beperkte onderlinge invloed tussen de groepen: de groepen zijn in principe onafhankelijk, maar waar het de game niet teveel stoort zijn onderlinge invloeden ingebracht. In die situaties is het mogelijk dat één groep de andere groepen stoort. Deze stoorsituaties zijn gebaseerd op illustratieve voorbeelden van ongelukkig uitpakkende maatregelen. De effecten hiervan zijn voor de andere groepen weliswaar duidelijk merkbaar, maar de doorwerking ervan is beperkt. Voor de andere groepen betekent dit dat ze er iets aan kunnen doen, maar dat ze ook zonder er iets aan te doen goed kunnen functioneren.

Ervaringen

De information security game is inmiddels enige tientallen keren gespeeld, onder meer aan de Haagse Hogeschool, de Noordelijke Hogeschool Leeuwarden, de Open Universiteit, de Universiteit van Amsterdam en de Erasmus Universiteit. De reacties en evaluaties waren steeds zeer positief. Bovendien wijzen de reacties erop dat de game inderdaad het inzicht in de menselijke-organisatorische component van informatiebeveiliging verbetert.

Het is opvallend dat de deelnemers in de game veelal fouten maken die ook in soortgelijke functies in de praktijk gemaakt worden. Zo bekommeren de managers zich bijvoorbeeld te weinig om de werknemers, houden de automatiseerders te weinig rekening met het management en schuiven de consultants de informatiebeveiliging ongevraagd af op de automatiseerders. Over de hele linie blijkt dat de deelnemers moeite hebben met belangrijke aspecten voor informatiebeveiliging, zoals het zorgen voor draagvlak en het communiceren over informatiebeveiliging.

In de nabespreking herkennen de meeste deelnemers meestal hun belangrijkste fouten. Vaak echter pas nadat ze erop gewezen worden. Vanwege het groepsgewijze werken, zijn de deelnemers niet individueel verantwoordelijk voor deze fouten. Toch is de herkenning ervan relatief groot.

De game is in de huidige vorm zeer goed speelbaar. De ervaringen die hiermee opgedaan zijn, hebben geleid tot verfijningen in het draaiboek van de game. Verdere verfijningen die toegevoegd kunnen worden, zijn bijvoorbeeld het toevoegen van meer interacties tussen de groepen. Daarnaast is het mogelijk om computerondersteuning te realiseren, zodat bedreigingen zich geautomatiseerd bij de groepen manifesteren en ook de gevolgen hiervan geautomatiseerd bijgehouden kunnen worden.

Conclusie

De information security game is ontwikkeld om de menselijke-organisatorische component van informatiebeveiliging inzichtelijker te maken. De ervaring leert dat de game daar inderdaad in slaagt. Verdere verfijningen kunnen de game nog realistischer en dynamischer maken. Daarom wordt verder gewerkt aan het doorontwikkelen van de game.

Literatuur

BSI, *The IT security situation in Germany in 2007*, Federal Office for Information Security, 2007.

CSI, *2008 Computer crime and security survey*. Computer Security Institute, 2008.

P. Overbeek, E. Roos Lindgreen & M. Spruit, *Informatiebeveiliging onder controle*. Pearson Education, Amsterdam, 2005.

M.E.M. Spruit & M. Looijen, *IT security in Dutch practice*. Computers & Security, nr. 2, 1996, pag. 157-170.