Ari Davies
Ivo Noppen MSc

Een groot deel van de informatiebeveiliging van processen en de operatie draait om compliance. Compliance is nuttig maar uiteindelijk moet informatiebeveiliging worden gezien als een groter geheel.

Informatiebeveiliging - buiten de geijkte paden treden

Bij het beschermen van informatie is de relatie tussen de interne auditfunctie (IAF) en het securityteam van een organisatie interessant. Beide zijn belast met een gelijksoortige taak: het beschermen van de (informatie van de) organisatie. De onafhankelijke IAF is verantwoordelijk voor toetsing en het afdwingen van compliancevereisten. Het securityteam streeft naar dezelfde doelen maar is ook operationeel verantwoordelijk voor de informatiebeveiliging. Een spanningsveld, omdat het securityteam door de operationele verantwoordelijkheid per definitie op een minder onafhankelijke manier de toetsing van de informatiesystemen kan inrichten dan de IAF.
In de organisatie draait informatiebeveiliging vaak om de volgende vraag: zijn het streven naar compliance en de activiteiten die we ondernemen voor informatiebeveiliging genoeg of zouden we nog aanvullende activiteiten moeten ondernemen? Deze vraag manifesteert zich bijvoorbeeld als volgt:

- We zijn compliant aan raamwerk X, hebben onze controlemaatregelen getest op basis van risicoanalyses en daarnaast voeren we penetratietests uit op IT-infrastructuur en applicaties. Maar zijn we hiermee wel veilig?
- We hebben monitoring en incident response ingeregeld. Maar is het wel afdoende getest en hoe zou het verantwoordelijke team reageren in geval van een daadwerkelijke aanval?
- Begrijpen we echt wat een aanvaller in onze omgeving kan doen en hoe hij een aanval zou uitvoeren?

Informatiebeveiliging versus computerbeveiliging
Om deze vragen te beantwoorden moet eerst worden bekeken wat informatiebeveiliging betekent wanneer dit begrip wordt afgezet tegen computerbeveiliging. Organisaties en hun medewerkers dienen zich te realiseren dat informatiebeveiliging over meer gaat dan alleen computerbeveiliging. Computerbeveiliging kan organisaties op een vals spoor van veiligheid zetten: 'zo lang onze infrastructuur en systemen veilig zijn, is onze organisatie veilig'. *Figuur 1* op pag. 30 laat het verschil zien tussen informatiebeveiliging en computerbeveiliging.
De fundamentele elementen van informatiebeveiliging, de 'drie-eenheid van informatiebeveiliging' omvatten de volgende elementen:

- Cyber gaat over de online wereld, internet, intranet en alle andere computernetwerken.
- Fysiek gaat over ongeautoriseerde toegang tot fysieke locaties. Denk hierbij aan gebouwen of serverruimten. Daarnaast betreft het veiligheid van de personen in deze locatie.
- De mens gaat over de sleutelrol die zij speelt in het behandelen van informatie binnen organisaties. Ook de mens is kwetsbaar voor aanvallen, zoals de 'social-engineeringaanval', waarbij een aanvaller het vertrouwen van de persoon probeert te misbruiken om informatie te verkrijgen of zich ergens toegang toe te verschaffen. Vaak is dit de meest genegeerde en verkeerd begrepen link die de fysieke en cyberwereld aan elkaar bindt.

Computerbeveiliging omvat slechts een van de hiervoor genoemde basiselementen. Het gaat hier over maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid te waarborgen binnen IT-infrastructuren of -systemen. Maatregelen gericht op de techniek dus. Informatiebeveiligingsbeleid is vervolgens het beleid binnen een organisatie die de drie basiselementen omzet in controls.

Palet aan opties

De harde realiteit is dat aanvallers zichzelf niet beperken tot het misbruiken van technische kwetsbaarheden in de IT-infrastructuur en -systemen. Aanvallers combineren alle aspecten van de 'drie-eenheid van informatiebeveiliging' om hiermee het pad te bepalen van de minste weerstand om de organisatie binnen te komen.

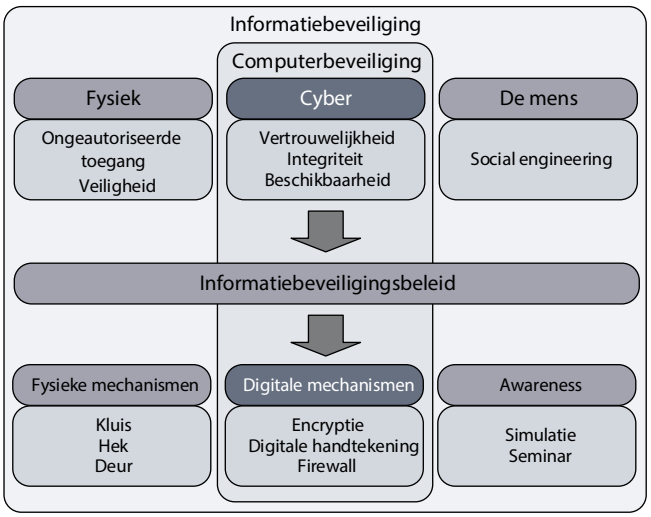
Dit betekent dat een aanvaller de keuze heeft uit een groot palet aan opties. Hij kan bijvoorbeeld gebruikmaken van het fysieke element aangevuld met het menselijke: zonder pasje achter iemand aanlopen door een geopende deur ('tailgating') en zich voordoen als een werknemer om zijn doelen te bereiken.

Uiteraard bestaan er verschillende manieren om toegang te krijgen tot een organisatie via het fysieke en menselijke element. Het meest voorkomende voorbeeld van misbruik van het menselijke element is social engineering en het zenden van phishing mails. Deze mails hebben tot doel het slachtoffer te manipuleren zodat deze zich schikt naar de wensen van de aanvaller. Om hierin te slagen gebruikt de aanvaller psychologische stimulansen, zoals complimenten, beloningen en zelfs angst. Een andere methode op het snijvlak van het fysieke en menselijke element is 'USB baiting'. Hierbij plaatst een aanvaller op strategische locaties binnen en buiten de organisatie USB-sticks of andere media waarop malware (kwaadaardige software) geïnstalleerd is. Doel is dat een slachtoffer de media in een computer laadt en de infectie verder verspreidt binnen het bedrijf.

Casus – Haven van Antwerpen

De laatste jaren hebben we verschillende voorbeelden gezien van succesvolle aanvallen door het combineren van de elementen cyber, fysiek en menselijk. Zo was er een aanval op de haven van Antwerpen door drugskartels. Met als doel drugs in te voeren op de Europese markt wierf het drugskartel hackers om in de systemen te komen waarmee ladingen, douanewerkzaamheden en de haveninfrastructuur worden beheerd. De aanvallers begonnen in dit scenario met het uitvoeren van simpele social-engineeringaanvallen om ervoor te zorgen dat medewerkers malware installeerden. Op het moment dat de malware werd ontdekt door de organisatie en extra beveiligingsmaatregelen werden geïnstalleerd, veranderden de aanvallers hun werkwijze. Door zich fysieke toegang te verschaffen tot het bedrijfsterrein konden de aanvallers keyloggingapparatuur (apparatuur die elke toetsaanslag registreert) direct aan de computers hangen. Tevens konden de

Begrijpen we echt wat een aanvaller in onze omgeving kan doen en hoe hij een aanval zou uitvoeren?



Figuur 1. Verschil tussen informatiebeveiliging en computerbeveiliging

aanvallers vanaf afstand via een draadloze verbinding een verbinding met het netwerk van de haven leggen. Een simpele en efficiënte oplossing vanuit het oogpunt van de aanvallers, die zo geen last meer hadden van de verscherpte aandacht op de extern bereikbare infrastructuur. De aanvallers zaten immers direct op het interne netwerk van de haven.

'Red teaming'

De voorbeelden uit de praktijk laten zien dat informatiebeveiliging fysiek, cyber en de mens omvat, omdat ook aanvallers van deze elementen misbruik maken. Dit betekent dat bestaande maatregelen zoals compliance assessments, raamwerken en zelfs penetratietesten, met een nieuwe vorm van beveiligingstests moeten worden aangevuld. Een nieuwe vorm van beveiligingstests wordt 'red teaming' genoemd, een term die oorspronkelijk uit de militaire wereld komt, net zoals vele andere termen binnen de informatiebeveiliging.

Beveiliging betekent altijd het een stap voor zijn van dreigingen en de daaraan gelieerde risico's. Daarnaast betekent veiligheid het begrijpen van de mogelijke bestaande dreigingsscenario's. Maar belangrijker nog is het begrijpen van het onbekende, het nog niet bedachte en dat waarvan niemand dacht dat het mogelijk was. Dit betekent dat we tests moeten uitvoeren die de 'known known' (compliance, frameworks) en 'known unknown' (penetratietesten) complementeren.

Binnen de informatiebeveiliging staat red teaming voor een aanpak waarin het management van een organisatie en het uitvoerende team van ethische hackers (red team) vooraf samen een lijst 'kroonjuwelen' van de organisatie vaststelt. Het is de taak van het red team om te komen tot een aanpak gebaseerd op scenario's die aanvallers zouden kunnen gebruiken om de kroonjuwelen te bemachtigen. Hierbij worden ook enkele doelen ('flags') vastgelegd die een mogelijke rol kunnen spelen in het verschaffen van toegang, bijvoorbeeld het verkrijgen van toegang tot een bepaald gebouw, of toegang tot systemen in het netwerk.

Het red team neemt vervolgens al deze informatie mee in een project waarin de scenario's worden uitgevoerd in de vorm van een gecontroleerd incident. Een red-teamingproject bestaat uit de volgende fasen:

Fase 1. ***Verzamelen van publieke informatie en verkenning***

Het red team, dat eigenlijk als aanvaller fungeert, probeert in deze fase een zo compleet mogelijk beeld op te bouwen van de organisatie met behulp van openbare bronnen waarmee een succesvolle aanval kan worden uitgevoerd op de gebieden cyber, fysiek en menselijk.

Fase 2. ***Fysieke toegang en social engineering***

Door gebruik te maken van fysieke aanvalstechnieken zoals 'lock picking' (het openen van sloten zonder gebruik te maken van de sleutel) en social-engineeringaanvallen zoals phishing, probeert het red team bij de organisatie in te breken en iets achter te laten waardoor ze zich in een volgende stap gemakkelijker toegang kunnen verschaffen. Bijvoorbeeld door het plaatsen van een stuk hardware zoals een WiFi access point of een key-logger, waarmee alle toetsaanslagen worden vastgelegd. Bij phishing hebben we het meestal over malware waarmee het red team vanaf internet toegang kan krijgen tot de computer.

Fase 3. ***Onderzoek en uitbreiden van de initiële toegang***

In de vorige fase heeft het red team zich succesvol toegang verschaft tot de organisatie via een geplaatst stuk hardware of software. Het doel is vervolgens de toegang binnen de organisatie te vergroten zodat, zelfs als de initiële toegang wordt verloren, het red team nog steeds een ingang heeft binnen de organisatie.

Omdat het red team zich in deze fase reeds toegang heeft verschaft tot het interne netwerk van de organisatie, zal het netwerk ook worden onderzocht en in kaart worden gebracht om de juiste weg te kunnen bepalen naar de vastgestelde doelen. Wie zijn de belangrijkste medewerkers? Waar bevinden zich de meest kritieke databases? Hoe werken betalingstransacties en waar bewaart de organisatie haar intellectueel eigendom?

Fase 4. ***Escalatie en eindspel***

Dit is de laatste en mogelijk meest kritieke fase van een red-teamingproject omdat de meeste doelen zullen worden bereikt. Alle voorgaande fasen waren een opstap naar deze kritieke fase en het red team is nu bezig met het vinden van kwetsbaarheden, hacken en het binnendringen van systemen binnen de IT-infrastructuur om de vooraf gestelde doelen te bereiken. Onder de radar blijven vliegen is in deze fase minder belangrijk dan in de voorgaande fasen omdat het red team het 'geluidsniveau' langzaamaan zal moeten opschroeven. Dit is niet alleen om de doelen te kunnen bereiken, maar belangrijker nog om de capaciteiten van het monitoring en incident responseteam van de organisatie te kunnen evalueren. Wanneer de gestelde doelen zijn behaald is de (optionele) laatste stap het gecontroleerd exfiltreren van de bemachtigde gegevens en het zoveel mogelijk opruimen van het bewijs van hun aanwezigheid.

Na deze vier fasen is het tijd voor een terugkoppeling met de organisatie, aangevuld met bijvoorbeeld het organiseren van een workshop waarin kennis wordt gedeeld over het oplossen van de kwetsbaarheden en het toepassen van verbeteringen binnen de organisatie.

Samengevat is red teaming:

1. Een poging de verschillende elementen, cyber, fysiek en menselijk, samen te brengen met het doel realistische feedback te krijgen over de volwassenheid van de informatiebeveiliging van een organisatie.
2. Het is niet alleen een middel om de bestaande beveiligingsmaatregelen binnen de organisatie te testen, maar ook om inzicht te krijgen in hoe verschillende interne teams, afdelingen of derde partijen omgaan met 'gecontroleerde incidenten'.
3. Red teaming verleent ondersteuning aan andere teams die onderzoeken doen gedreven door intelligence, zoals de incident response, monitoring en crisismanagementteams. Als je een dief wilt vangen moet je immers als een dief leren denken.

Conclusie

Voor de IAF bieden de geijkte paden van compliance en frameworks niet langer genoeg zekerheid dat de organisatie en haar gegevens veilig zijn. Daarom is het belangrijk te zoeken naar nieuwe, holistische en innovatieve manieren waarop organisaties hun kwetsbaarheden kunnen analyseren.

Tests gericht op alle elementen van informatiebeveiliging – bijvoorbeeld red teaming – kunnen een organisatie meer zekerheid bieden over de werking van hun maatregelen tegen cybercriminaliteit. Dit biedt een realistisch inzicht in de tekortkomingen van het informatiebeveiligingsbeleid en vooral ook de implementatie daarvan. Hiermee kunnen maatregelen getroffen worden om het vertrouwen in de beveiliging van de kroonjuwelen van de organisatie te verbeteren.

Tevens heeft de IAF een unieke positie als onafhankelijk bewaker van de organisatie en haar data. Vanuit deze positie heeft zij de mogelijkheid de organisatie te verbeteren en hiermee kunnen bestaande initiatieven zoals compliance en control testing worden aangevuld met bijvoorbeeld red teaming. Deze exercities kunnen – door de grote impact en zichtbaarheid van een dergelijk project – een grote impuls vormen om een organisatie weerbaarder te maken tegen cybercriminaliteit. **<<**

Ari Davies is senior manager en teamleider van Deloitte red teaming operations. Met zijn internationale ervaring binnen de security- en veiligheidssector heeft hij brede kennis opgedaan van de werkwijze van aanvallers en de beveiliging hiertegen.

Ivo Noppen is junior manager en houdt zich binnen Deloitte bezig met red teaming operations en penetratietesten. Naast het aansturen van teams voert hij voornamelijk red-teamingopdrachten uit waarbij hij onder andere het technische infrastructuurvlak bestrijkt.