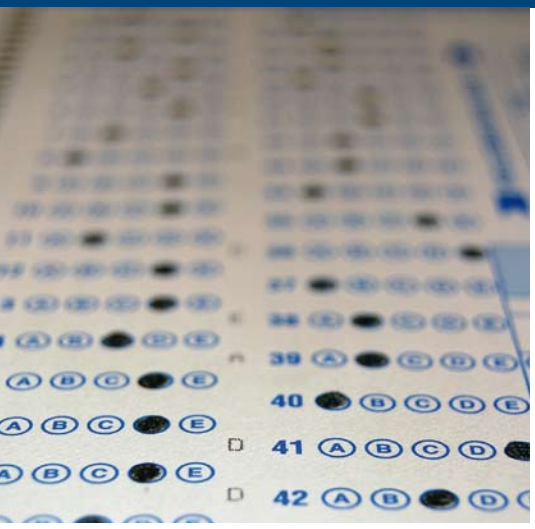


IT-beveiligingstesten als onderdeel in IT-audits

Ir. P. Kornelisse RE CISA
is director bij KPMG IT Advisory en verantwoordelijk voor de groep die zich richt op IT-beveiliging, zowel in de vorm van advies- als van auditdiensten. Dit betreft onder andere ethical hacking, QA- en beoordelingsdiensten inzake netwerk- en platformbeveiliging (security baselines), zoals voor internetomgevingen, Windows en Unix.

kornelisse.peter@kpmg.nl

M.R.A.M. Smeets MSc
is adviseur bij KPMG IT Advisory en werkzaam in de unit ICT Security & Control. Hij is specialist op het gebied van beveiliging van besturingssystemen, netwerkinfrastructuren en IT-beveiligingstesten. Zijn werk bestaat uit het uitvoeren van zowel IT-audits als IT-beveiligingstesten.

smeets.marc@kpmg.nl

Ing. M. van Veen MSc
is adviseur bij KPMG IT Advisory en werkzaam in de unit ICT Security & Control. Hij is specialist op het gebied van IT-advies, IT-auditing, IT-security assessments en IT-beveiligingstesting. Zijn kennisgebied reikt van IT-governance tot security settings: board to bit.

vanveen.michiel@kpmg.nl

Ir. Peter Kornelisse RE CISA, Marc Smeets MSc en ing. Michiel van Veen MSc

Voor beveiligingsonderzoeken worden naast audits steeds vaker beveiligingstesten ingezet. Bij het uitvoeren van beveiligingstesten wordt de effectiviteit van beheersings- en beveiligingsmaatregelen getest. Vreemd genoeg worden audits en beveiligingstesten niet vaak gecombineerd, terwijl zij elkaar een meerwaarde kunnen bieden. Sterker nog, mogelijk dienen beveiligingsonderzoeken gezamenlijk te worden uitgevoerd om de vraag van de klant goed te kunnen beantwoorden.

Inleiding

IT-auditors voeren onderzoeken uit naar IT-omgevingen. Vaak wordt bij een dergelijk onderzoek gekozen voor het uitvoeren van een formele audit. Met een audit is op voorhand een duidelijke structuur van werkzaamheden voorhanden. Bijvoorbeeld is het helder hoe het feitenonderzoek plaatsvindt en op welke wijze conclusies worden getrokken.

In toenemende mate zien wij dat cliënten vragen hebben over de IT-beheersing in combinatie met de aanverwante informatiebeveiliging. Vaak wordt dan gekozen voor een IT-audit van IT-beveiligingsprocessen. Dan kunnen onderwerpen worden geadresseerd zoals het verkrijgen van toegang van gebruikers tot de data en het monitoren van beveiliging.

Naast audits vinden beveiligingstesten plaats. Dit zijn zogenaamde overeengekomen specifieke werkzaamheden waarbij een feitenonderzoek naar beveiligingsmaatregelen plaatsvindt. Feitenonderzoek richt zich niet op getroffen maatregelen, maar op de effectiviteit van een stelsel van maatregelen. Een beveiligingstest maakt dan ook gebruik van een andere aanpak, met andere resultaten.

De reguliere IT-audit heeft een meer procesgerichte aanpak, terwijl de IT-beveiligingstest een meer gegevensgericht onderzoek is. Maar beide onderzoeken worden uitgevoerd om eenzelfde onderzoeksgebied te analyseren. Zouden we de twee onderzoeken dan juist goed kunnen combineren? Hebben beide onderzoeken een grote overlap, of vullen zij elkaar juist aan? Om antwoord te geven op deze vragen is het interessant de beide soor-

ten onderzoeken nader te beschouwen. Vervolgens behandelen we de aanwezige onderlinge versterking om te komen tot inzicht in de synergie.

IT-auditing

IT-auditing is een feitenonderzoek met een vaste structuur en een duidelijke onderzoeksaanpak. Voor het vergaren van de feiten worden de volgende technieken toegepast:

- interview van het management en personeel;
- inspecteren en beoordelen van documentatie omtrent proces en organisatie;
- observatie van getroffen maatregelen;
- her-uitvoeren van maatregelen.

Tijdens de interviews met management en personeel wordt beoogd helder te krijgen welke processen plaatshebben binnen de organisatie. Binnen de processen wordt beoordeeld of de procedures worden gevolgd zoals in opzet vastgelegd. Dit heeft tot doel om te beoordelen of afdoende maatregelen zijn geïmplementeerd binnen de procedures (in opzet) en of deze ook daadwerkelijk zijn geïmplementeerd en worden uitgevoerd (bestaan). Als laatste kan ook worden gecontroleerd of de maatregelen gedurende een bepaalde periode actief waren (werking). De maatregelen zijn binnen het toetsingskader gevangen in zogeheten controls. De controls tezamen dienen een integraal en afdoend complex van maatregelen te vormen teneinde in control te zijn van de processen en de organisatie. Een IT-audit heeft hierbij een sterke nadruk op de IT.

Door het inspecteren van de documentatie wordt een beeld verkregen van de opzet van processen, controls, evenals van configuratie-instellingen in de IT-omgeving. Door de opzet te toetsen aan het bestaan en vice versa wordt de werkelijke effectiviteit van de geïmplementeerde controls duidelijk.

Toetsing moet de werkelijke effectiviteit van de geïmplementeerde controls duidelijk maken

Ter aanvulling op interviews en het inspecteren van documentatie wordt gebruikgemaakt van observatie en het her-uitvoeren van controls. In beide gevallen test een IT-auditor als het ware zelf de aanwezigheid, en dus de effectiviteit, van de control. Een passend voorbeeld is te zien binnen het onderwerp van de fysieke beveiligingsmaatregelen. Fysieke beveiligingsmaatregelen worden geïmplementeerd om de toegang tot ruimten binnen bijvoorbeeld een datacenter te controleren. Zo dienen bezoekers met een bezoekerspas niet in staat te zijn bepaalde delen van een datacenter te betreden. Wanneer de IT-auditor een bezoekerspas aanvraagt en deze bij een paslezer houdt, kan hij observeren of hem de toegang wordt geweigerd daar waar in opzet bedoeld. Op basis van de uitkomst van deze test stelt de IT-auditor vast of deze control daadwerkelijk effectief is (de toegang wordt geweigerd).

Naast het bevragen van management en personeel om vast te stellen of geïmplementeerde maatregelen overeenkomen met in opzet vastgelegde procedures, is het noodzakelijk om de IT-systemen ook te toetsen. Deze systemen vormen de basis van de geautomatiseerde processen en procedures. De IT-systemen ondersteunen de processen in een bedrijf en dienen dus ook controlemaatregelen geïmplementeerd te hebben. Een deel van de controls is dus geautomatiseerd. Het betrekken van de IT-systemen binnen het onderzoek naar de beheersing van IT is noodzakelijk.

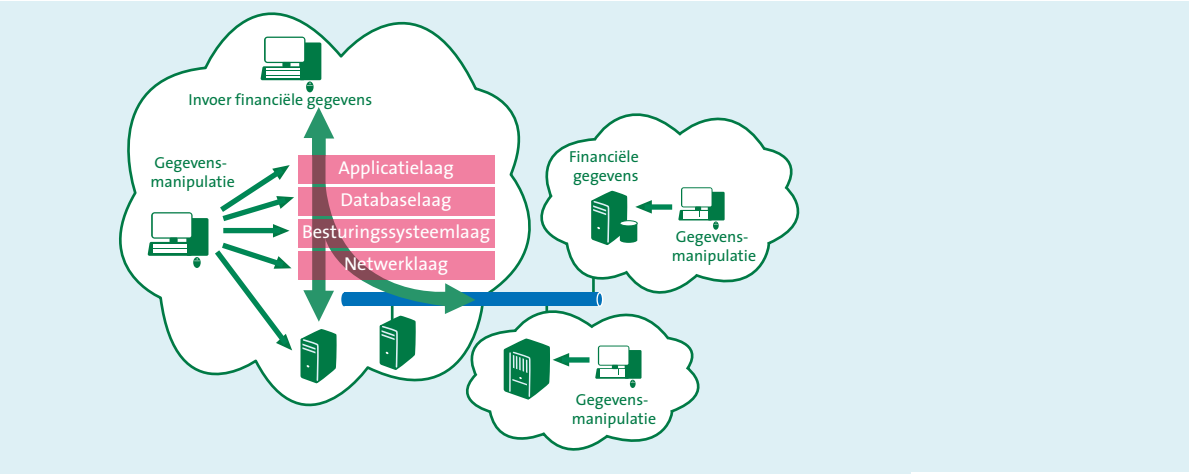
Het onderzoeken van de IT-systemen en de onderlinge samenhang van geïmplementeerde controls als onderdeel van het feitenonderzoek kost veel tijd (en vraagt dus een groot budget). Het onderzoeken van tientallen applicaties, databases, honderden servers en netwerkapparatuur is een noodzaak, echter niet praktisch haalbaar. Om toch een integrale en correcte uitspraak te doen over het bestaan van controlemaatregelen binnen de IT-infrastructuur, wordt een aantal technieken toegepast: scoping en sampling.

Scoping wordt gebruikt om slechts de relevante IT-infrastructuur in het onderzoek te betrekken. Bij een onderzoek naar bijvoorbeeld de informatiebeveiliging van de financiële gegevens worden alleen de financiële systemen meegenomen; andere systemen dus niet.

Sampling wordt gebruikt om binnen de geselecteerde systemen, specifieke systemen en configuraties te bekijken. Sampling wordt zodanig intelligent uitgevoerd dat een uitspraak over de sample iets zegt over de verzameling waaruit deze voortkomt. Zo wordt een sample genomen uit een groep van gelijksoortig ingerichte systemen, bijvoorbeeld fileservers. Door het onderzoeken van de inrichting van één van de file servers is de inrichting van de overige gelijksoortig ingerichte fileservers onderzocht.

Deze aanpak lijkt solide om te komen tot een onderbouwde uitspraak. Echter, deze aanpak introduceert een drietal problemen:

1. Niet alle systemen worden onderworpen aan een onderzoek.



Figuur 1. **Samenhang en complexiteit van IT-omgevingen vormen een uitdaging binnen een IT-audit voor een juiste uitspraak.**

2. De systemen worden vervolgens niet in detail onderzocht. Naast een beperkt feitenonderzoek op systeemniveau speelt nog een ander probleem: de *integrale* beoordeling van de geautomatiseerde controls. Hoe beoordeelt men de invloed van een netwerkconfiguratie op een geautomatiseerde controlemaatregel in een server of een database?
3. Een juiste integrale beoordeling van de IT-omgeving is praktisch niet haalbaar door de complexiteit van de IT-omgeving en de onderlinge dynamiek van de geïmplementeerde controlemaatregelen.

De huidige IT-auditaanpak voor het beoordelen van het bestaan van controlemaatregelen binnen de IT-infrastructuur is niet efficiënt en slechts beperkt effectief. Doordat de systemen technisch gezien slechts beperkt worden bekeken, neemt het risico van een foute uitspraak door de IT-auditor toe. Zo kan een IT-auditor ten onrechte claimen dat het IT-beheer op orde is en de informatiebeveiliging op niveau, terwijl het ondersteunende feitenonderzoek beperkt is geweest.

Beveiligingstesten

Auditors voeren al lange tijd beveiligingstesten uit. Een beveiligingstest is een technisch onderzoek naar de effectiviteit van de beveiligingsmaatregelen inzake IT-objecten. Deze effectiviteit wordt vastgesteld door te zoeken naar zwakheden en door die zwakheden eventueel uit te buiten. Een dergelijk onderzoek dient te worden uitgevoerd door iemand die kundig is op het gebied van technische IT-beveiliging. Tevens dient deze persoon de gevonden kwetsbaarheden te kunnen vertalen naar bedrijfsrisico's. Deze vertaling naar bedrijfsrisico's is cruciaal om een uitspraak te kunnen doen over de effectiviteit van de IT-beveiliging.

De reden van uitvoeren

De klanten die deze dienst afnemen hebben vaak duidelijke vragen, zoals: is mijn IT-omgeving bestand tegen cyberaanvallen? En als men slaagt in een succesvolle aanval, welke bedrijfsgegevens worden gecompromitteerd? Hoe kan de IT-beveiliging van de omgeving verder worden verbeterd? Allemaal valide vragen, temeer omdat IT-objecten continu staan blootgesteld aan hackers en kwaadwillend personeel. De klant heeft behoefte te weten welke risico's er zijn, wat de kans van optreden van die risico's is, wat de impact is, en hoe deze risico's verlaagd kunnen worden.

Maar waarom beantwoorden we deze vragen door middel van een IT-beveiligingstest en niet door middel van een reguliere IT-audit? Het antwoord daarop is goed uit te leggen door een zijstap te maken naar de wereld van brandoefeningen.

Een brandoefening wordt binnen gebouwen met regelmaat uitgevoerd. Een brandoefening wordt voornamelijk uitgevoerd om een ontruiming wegens brand in het gebouw zo echt mogelijk te simuleren. De brandoefening staat niet op zichzelf. Diverse plannen, overleggen en trainingen voor personeel zijn hieraan voorafgegaan. Daarnaast zijn brandvoorzieningen in de gebouwen aanwezig. Echter, de brandoefening is de ultieme test of al het voorbereidende werk ook *effectief* is. Door alle maatregelen te testen weet men of deze maatregelen in de praktijk echt werken, of dat er toch een en ander misgaat. Meer dan eens komt door de brandoefening naar voren dat er toch nog zaken over het hoofd zijn gezien. Denk hierbij aan elektrische deuren die (toch) niet opengaan, knelpunten van mensenstromen of brandmelders die dienst weigeren.

Een IT-beveiligingstest kan hiermee worden vergeleken. Het is de test of de beveiliging afdoende effectief is door het uitvoeren van een simulatie, of dat toch nog wat zaken over het hoofd zijn gezien.

Soorten van beveiligingstesten

Beveiligingstesten bestaan in vele smaken. Dergelijke testen kunnen als volgt worden gerubriceerd:

- *Black box.* De aanvaller heeft geen enkele informatie over de objecten in scope.
- *Grey box.* De aanvaller heeft beknopte informatie over het object. Denk hierbij aan een netwerkarchitectuur met verkeersstromen of afgeleide informatie zoals de opzet van een gebruikersnaam.
- *White box.* De aanvaller heeft veel informatie over het object en zelfs een bepaalde vorm van toegang. Denk hierbij aan een webapplicatie waar de aanvaller inloggegevens voor heeft. Het doel is om meer rechten te krijgen binnen de applicatie.

Een term die vaker wordt gebruikt is 'double'. Een double black box-test betekent dat de aanvaller geen enkele informatie heeft over de objecten in scope. Daarnaast is de IT-organisatie niet op de hoogte van de beveiligingstest. Daardoor wordt de effectiviteit van de beheerorganisatie inzake het herkennen, lokaliseren en mitigeren van een aanval ook getest. Deze test simuleert het best een werkelijke aanvalssituatie.

Mogelijke objecten van onderzoek

Beveiligingstesten kunnen zich richten op een veelheid van objecten. Denk bijvoorbeeld aan:

- externe website;
- aanwezigheid op het internet (alle systemen aan het internet maar ook de publieke informatie zoals Google en RIPE);
- het interne netwerk voor kantoorautomatisering;
- applicaties zoals een intranet of een CRM-systeem;
- databases;
- mobiele apparatuur (bijvoorbeeld een telefoon of PDA);
- personeel.

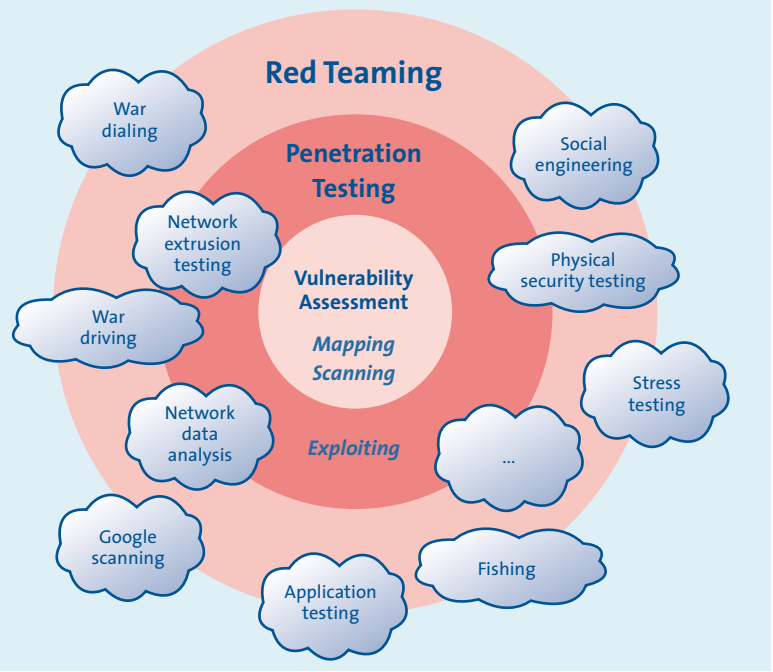
Hoewel het personeel strikt genomen geen IT-object is, kan het personeel wel object van onderzoek zijn. Om maatregelen op het niveau van het personeel te testen, wordt een zogeheten social engineering test uitgevoerd. Met een dergelijke test wordt onderzocht of het personeel zich houdt aan het beveiligingsbeleid van het bedrijf. Denk hierbij aan het doorlaten van personen zonder pasje bij een elektronisch beveiligde deur, het niet afsluiten van ongebruikte computers, het opschrijven van wachtwoorden bij de computer of het communiceren van wachtwoorden via de telefoon.

Wijze van onderzoek

Beveiligingstesten zijn, op social engineering tests na, technische onderzoeken. Hierbij wordt direct met de techniek gecommuniceerd. Het gebruik van programmatuur ter ondersteuning van het onderzoek is dan ook een logisch gevolg. Dit kan veel tijdwinst opleveren. Bijvoorbeeld: het proberen van een aantal wachtwoorden vindt geautomatiseerd sneller plaats dan met de hand. Tevens kan de tester ondertussen zijn aandacht dan ergens op richten. Maar let op, de programmatuur ten behoeve van IT-beveiligingstesten dient louter ter ondersteuning, want zij kan slechts simpele taken automatiseren. De resultaten van de programmatuur dienen altijd gevalideerd te worden door de tester. Vanwege de complexiteit kan nooit op de pure uitkomst van de programmatuur worden vertrouwd, omdat de programmatuur vaak zogenaamde false-positives (niet bestaande zwakheden) rapporteert. Het bekende credo '*a fool with a tool is still a fool*' gaat hier dan ook zeker op.

Het uitvoeringsproces van een IT-beveiligingstest is terug te brengen tot de volgende stappen: mapping, scanning en exploiting. De keuze van deze stappen, samen met de objecten, bepaalt de mate van intrusie. We herkennen hierbij de volgende onderverdeling: vulnerability assessment, penetration testing en red teaming. Het verschil hiertussen is het beste uit te leggen aan de hand van figuur 2.

In de mappingfase wordt gekeken welke systemen überhaupt aanwezig zijn in het netwerk en welke services actief zijn op die



Figuur 2. **Overzicht van soorten IT-beveiligingstesten.**

systemen. Tevens worden metadata uit zoekmachines of andere publieke bronnen geraadpleegd. In de scanningfase worden versies van software herkend en worden de objecten onderworpen aan scans op zoek naar zwakheden. Deze twee fasen samen zijn onderdeel van een 'vulnerability scan'. In deze twee stappen wordt veel gebruikgemaakt van geautomatiseerde tools.

Een volledige penetration test omvat ook de derde stap: exploiting. In deze stap worden gevonden zwakheden uitgebuit om zo in de systemen te kunnen inbreken. Dat kan door middel van een exploit, stukken programmacode die een kwetsbaarheid uitbuiten. De aanvaller laat het object in kwestie acties uitvoeren die de aanvaller toegang verschaffen. Na een succesvolle exploitingfase heeft de aanvaller toegang verkregen tot het object met bijbehorende gegevens.

De term red teaming is een uitbreiding op penetration testing en is afkomstig uit de militaire wereld waar het in gevechtsimulaties wordt gebruikt. Bij red teaming is het doel het belangrijkste. De trukendoos mag volledig open; alle acties die men kent mogen worden gebruikt. Bij IT-beveiligingstesting kan men hierbij denken aan een bedrijf dat louter is geïnteresseerd of inbreken mogelijk is, in de brede zin van het woord. Een combinatie van social engineering (manipuleren van mensen), phishing (ontlokken van gevoelige informatie, zoals gebruikersnaam en wachtwoord) en war driving (zoeken naar en toegang verkrijgen tot het draadloos netwerk van het bedrijf) met interne en externe penetratietesten kan dan bijvoorbeeld worden gebruikt om het doel te bereiken.

Wijze van rapporteren

Een beveiligingstest is, net als een IT-audit, een feitenonderzoek. Echter, bij een beveiligingstest worden alleen negatieve feiten gerapporteerd, bijvoorbeeld: '*De gebruikte wachtwoorden voor het systeemaccount zijn gelijk aan de standaardwachtwoorden van de fabrikant, en daardoor gemakkelijk te raden*'.

Door een zwakheid te vinden of door in te breken op een systeem kan worden aangetoond dat de beveiliging niet afdoende is. Andersom kan niet worden geredeneerd. Als het niet lukt zwakheden te vinden of in te breken, dan betekent dat niet dat deze zwakheden er niet zijn. Een hacker met ongelimiteerde tijd of budget zal vrijwel altijd kunnen inbreken. Immers, een hacker hoeft zich niet te houden aan gemaakte afspraken over de toegestane aanvallen!

Het eindresultaat van een IT-beveiligingstest is een rapport of presentatie met negatieve bevindingen en aanbevelingen ter verbetering.

Bij red teaming mag de trukendoos volledig open; alle acties die men kent mogen worden gebruikt

Overeenkomsten en verschillen van IT-audit en IT-beveiligingstest

Om een beeld te krijgen van de overeenkomsten en verschillen tussen werkzaamheden inzake IT-audits en -beveiligingstesten hebben wij deze uitgezet op basis van een aantal aspecten.

1. Soorten onderzoeken

De soorten IT-audits zijn in te delen op basis van de hoeveelheid assurance: redelijke mate van zekerheid, beperkte mate van zekerheid en feitelijke bevindingen. Daarbij zijn de eerste twee soorten vaak van toepassing als de uitkomst van het onderzoek niet alleen voor de opdrachtgever maar ook voor derden toegankelijk is. Denk bijvoorbeeld aan een SAS70, TPM of jaarrekeningcontrole. De laatste soort (feitelijke bevindingen) wordt vaak gebruikt door bedrijven om een nulmeting uit te voeren of om zichzelf te verbeteren. Deze informatie is niet bedoeld voor derden, omdat er geen conclusie is verbonden aan de feitelijke bevindingen.

De soorten IT-beveiligingstesten zijn terug te brengen tot: vulnerability assessment, penetratietest en red teaming. De eerste test gaat in op het in kaart brengen van geverifieerde zwakheden. De tweede en derde test gaan een stap verder door de gevonden zwakheden daadwerkelijk uit te buiten. Bij red teaming is het arsenaal aan toegestane middelen onbeperkt, terwijl dit bij een penetratietest zich beperkt tot een bepaalde scope. De IT-beveiligingstest lijkt qua soort sterk op het onderzoek van feitelijke bevindingen bij de IT-audit.

2. Publiek

Het publiek van een IT-audit en een IT-beveiligingstest is verschillend. Zoals gezegd kan een rapport van een IT-audit ook voor derden zijn. Bij IT-beveiligingstesting is dit niet het geval. Immers, alle gevonden kwetsbaarheden zijn dan beschikbaar voor de buitenwereld. Dit is niet wenselijk. Een ander verschil is dat het publiek van een IT-beveiligingstest vaak sterke affiniteit heeft met IT (bijvoorbeeld een IT-manager) en niet zozeer met bedrijfsprocessen. Bij een IT-audit bestaat het publiek naast de opdrachtgever soms uit derden en heeft het publiek vaak meer affiniteit met bedrijfsprocessen en risico's dan met de techniek. Een voorbeeld hiervan zijn CEO's, CFO's en CIO's als opdrachtgever. Derden zijn bijvoorbeeld toezichthouders of (in het geval van outsourcing) de demandorganisatie.

3. Toetsingsnormen van een IT-audit en een IT-beveiligingstest

IT-audits worden uitgevoerd op basis van verschillende toetsingsnormen. Dit is afhankelijk van het precieze doel van het onderzoek en de omgeving waarin het onderzoek plaatsvindt. Op het gebied van IT-beheer en informatiebeveiliging zijn de toetsingsnormen bijvoorbeeld Cobit, ITIL en ISO 27001.

Voor IT-beveiligingstesting echter zijn geen algemeen en internationaal geaccepteerde toetsingsnormen voorhanden. Wel zijn er initiatieven om te komen tot dergelijke toetsingsnormen. Een voorbeeld hiervan is OWASP: Open Web Application Security Project. OWASP is een verzameling toetsingsnormen voor webapplicaties.

4. Uitvoering van een IT-audit en een IT-beveiligingstest

Het onderzoek van een IT-audit vindt plaats op basis van documentatiestudie, interviews en observaties. Er wordt uitgegaan van de bekende maatregelen binnen het bedrijf, waarvan opzet, bestaan en werking van deze maatregelen worden getoetst. De nadruk ligt op de opzet, het bestaan en de werking van het beleid en de procedures. De techniek krijgt slechts beperkte aandacht.

Een IT-beveiligingstest heeft juist de focus op de techniek. Deze vindt plaats op basis van een black box-benadering. Dit betekent dat er wordt uitgegaan van het onbekende in plaats van het bekende: de tester weet niet welke maatregelen er zijn getroffen. De focus ligt op de daadwerkelijke effectiviteit van de maatregelen die in de techniek zijn geïmplementeerd. Deze maatregelen worden getest door te bekijken of deze omzeild kunnen worden.

5. Kwaliteitsaspecten van een IT-audit en een IT-beveiligingstest

Een IT-audit kan zich richten op een groot aantal kwaliteitsaspecten. Denk hierbij aan performance, toekomstvastheid, (beheer)kosten, projectplanning, etc. Daarbinnen wordt een IT-audit ook vaak gebruikt voor beveiligingsonderzoeken. De kwaliteitsaspecten komen precies overeen met die van een IT-beveiligingstest:

Beschikbaarheid

Kernvraag: zijn de systemen altijd beschikbaar? Onderwerpen die aan bod komen zijn bijvoorbeeld het gecontroleerd laten verlopen van wijzigingen in de IT-omgeving, redundantie van IT-systemen en reservekopieën van gegevens.
Bij een IT-audit worden voor dit aspect vaak het beleid en de procedures rondom change management, redundantie en back-up & recovery bekeken.
Bij een IT-beveiligingstest wordt getracht om IT-objecten onbeschikbaar te maken in de omgeving, door deze bijvoorbeeld te overstelpen met bevragingen of juist gegevens toe te sturen.

Vertrouwelijkheid

Kernvraag: kan iemand bij gegevens die hij/zij niet mag zien? Hierbij wordt vaak gekeken naar de autorisaties die gebruikers hebben op de gegevens. Zo zouden de medewerkers van een verkoopafdeling geen inzicht moeten hebben in de gegevens van de HR-afdeling.
Bij een IT-audit ligt de nadruk op de procedures rond het aanmaken, wijzigen en verwijderen van gebruikersaccounts en de autorisaties die bij de gebruikersaccounts horen. Ook wordt aandacht besteed aan de periodieke controle van die accounts en autorisaties. Tevens is er aandacht voor de opzet en het bestaan van beveiligingsinstellingen in de IT-omgeving.
Bij een IT-beveiligingstest wordt getracht die geïmplementeerde maatregelen te testen en waar mogelijk te omzeilen.

Integriteit

Kernvraag: kan iemand gegevens zonder toestemming aanpassen? Ook hierbij wordt vaak gekeken naar de autorisaties die gebruikers hebben op de gegevens.
Voor zowel een IT-audit als een IT-beveiligingstest gelden dezelfde aandachtsgebieden als bij vertrouwelijkheid. Echter, hier wordt ook gekeken naar de daadwerkelijke mogelijkheid voor gebruikers om gegevens te manipuleren.

6. Onderzoeksobjecten van een IT-audit en een IT-beveiligingstest

De onderzoeksobjecten bij een IT-audit bestaan in hoofdzaak uit mensen, processen en (zij het beperkt) IT-systemen. Hierbij ligt de focus op de samenhang van deze drie objecten.

Bij een IT-beveiligingstest is het accent juist omgekeerd. De onderzoeksobjecten bij een IT-beveiligingstest zijn de IT-systemen. Soms zijn dit ook mensen (bijvoorbeeld bij een social engineering test), waarmee er dus een overlap is met een IT-audit, zij het met een andere invalshoek.

7. Reikwijdte van een IT-audit en een IT-beveiligingstest

De reikwijdtes van een IT-audit en een IT-beveiligingstest verschillen onderling. Onder reikwijdte wordt hier verstaan: de objecten die bekeken worden en de mate van detail waarin dit gebeurt.

Een IT-audit dekt voornamelijk het gebied af van beleid en procedures. Er wordt gekeken naar de volledige opzet van het beleid en de procedures. Ook wordt er gekeken naar enkele samples van het bestaan. Tot slot wordt die bestaanscontrole toegepast op gegevens die over een periode zijn verzameld. Hieruit blijkt de werking. De onderliggende techniek krijgt beperkte aandacht en wordt niet in (individueel) detail bekeken.

Aspecten	IT-audit	IT-beveiligingstest
Soort onderzoek	Redelijke mate van zekerheid Beperkte mate van zekerheid Feitelijke bevindingen	Feitelijke bevindingen: Vulnerability assessment Penetratietest Red teaming
Publiek	Affiniteit met bedrijfsprocessen Soms voor derden	Affiniteit met techniek/IT Niet voor derden
Toetsingsnormen	Cobit, ITIL, ISO 27001	Geen internationaal geaccepteerde toetsingsnormen
Uitvoering	Documentatiestudie, interviews en observatie van opzet, bestaan en werking. Weinig aandacht voor techniek.	Testen van de effectieve maatregelen. De werking van de maatregelen wordt als geheel getest. Veel aandacht voor techniek in detail.
Kwaliteitsaspecten	Een ruime verzameling van kwaliteits-aspecten waaronder securityaspecten.	Alleen securityaspecten: beschikbaarheid, vertrouwelijkheid en integriteit. Veel aandacht voor techniek in detail.
Onderzoeksobjecten	De IT-organisatie en haar (proces-gerelateerde) maatregelen: mensen en processen. IT in beperkte zin.	De technische infrastructuur en integrale effectiviteit van technisch geïmplementeerde maatregelen.
Reikwijdte	Beleid en procedures in de breedte en diepte. Techniek alleen globaal en zonder diepgang.	Techniek in de breedte en diepte tot in detail. Beleid en procedures alleen heel globaal voor root cause analyse en bedrijfsrisico's.

Tabel 1. **Aspecten van IT-audit en IT-beveiligingstest vergeleken.**

Een IT-beveiligingstest dekt zoals gezegd andere zaken af. De focus ligt juist niet op het voorgenomen beleid en de procedures, maar op de implementatie van de maatregelen in de techniek. De techniek krijgt veel aandacht. Verder wordt zoveel mogelijk getracht om de techniek tot in individueel detail te bekijken. De geïdentificeerde problemen worden vertaald naar bedrijfsrisico's en mogelijke root causes. Een harde relatie tussen de geïdentificeerde problemen en het beleid en procedures is niet te geven, zonder het beleid en de procedures onderzocht te hebben.

Voordelen van een beveiligingstest als onderdeel van een IT-audit

Uit tabel 1 kunnen we concluderen dat IT-beveiligingstesting voordelen heeft ten opzichte IT-auditing. Een aantal daarvan is goed toepasbaar tijdens IT-audits en levert direct voordelen op voor IT-audits.

Snelheid

Het uitvoeren van een vulnerability scan of een penetratietest gaat relatief snel. Binnen enkele uren ontstaat een eerste beeld. Bijvoorbeeld: is het updaten van software consequent uitgevoerd? Het grote aantal objecten dat tegelijk kan worden bekeken (geautomatiseerd) biedt ook snelheidsvoordeel. Dit heeft als bijkomend voordeel dat men zou kunnen kiezen om periodiek een, deels geautomatiseerde, test uit te voeren. Hierdoor ontstaat een beeld over een langere periode en kan mogelijk meer gezegd worden over de werking van de maatregelen in de loop van de tijd.

Controle van bestaan van objecten

Bij een IT-securityscan wordt begonnen met te onderzoeken welke objecten daadwerkelijk aanwezig zijn op een netwerk, in tegenstelling tot het vertrouwen op de lijst van systemen aangereikt door de klant. Hierdoor kan het voorkomen dat objecten worden (her)ontdekt. Denk bijvoorbeeld aan een systeem dat men vorig jaar al dacht te hebben uitgefaseerd of aan een niet-geautoriseerde netwerkkoppeling naar internet of een ander bedrijf.

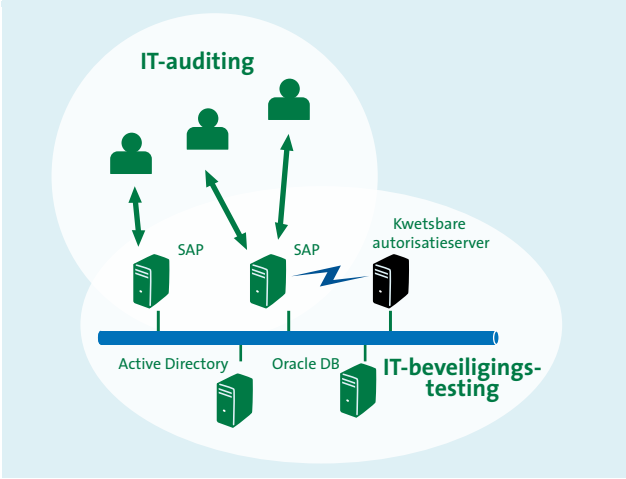
Scopingondersteuning

Een IT-beveiligingstest kan een IT-audit helpen bij het maken van de juiste keuzen omtrent scoping, sampling en de onderwerpen die extra aandacht behoeven binnen de IT-audit. Als uit de IT-beveiligingstest blijkt dat veel Windows systemen niet geüpdatet zijn, is dit voor een IT-audit een goed startpunt om het updatebeleid onder de loep te nemen en daarnaast de Windows beheerorganisatie extra aandacht te geven.

Het resultaat van een IT-beveiligingstest maakt de impact van een kwetsbaarheid heel duidelijk

Verminderde capaciteit

IT-omgevingen groeien en zullen vooral nog meer blijven groeien. Tevens worden systemen steeds afhankelijker van de invoer vanuit andere systemen. Deze samenhang en complexiteit van de verschillende maatregelen binnen de IT-omgevingen kunnen verstrekkende gevolgen hebben die op het eerste gezicht niet altijd even duidelijk zijn. Een IT-beveiligingstest kan deze

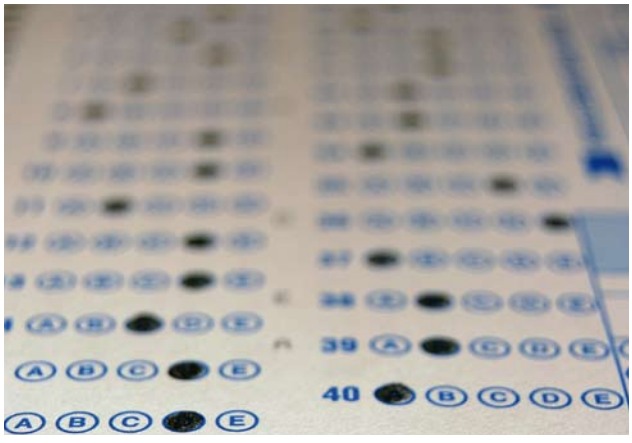


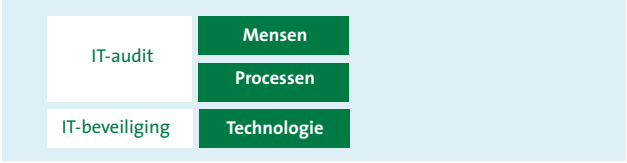
Figuur 3. **IT-beveiligingsonderzoek ondersteunt IT-audit door het versterken van de breedte en diepte van het onderzoek.**

samenhang van technische componenten duidelijk aantonen door te zoeken naar de zwakste schakel in het beveiligingsmodel. Op basis van een dergelijk onderzoek kan blijken dat de functiescheiding in een applicatie niet gewaarborgd is door kwetsbaarheden in onderliggende databases, besturingssystemen of netwerk.

Duidelijke impact

Het resultaat van een IT-beveiligingstest maakt de impact van een kwetsbaarheid heel duidelijk. 'Wij waren in staat ongeautoriseerde betalingen te verrichten' is immers duidelijker dan 'De autorisaties van het betaalsysteem en het controlesysteem zijn onvoldoende gewaarborgd. Dit kan leiden tot ongeautoriseerde betalingen'. Het risico is in beide gevallen gelijk, maar de impact is duidelijker doordat de eerste formulering veel concreter is.





Figuur 4. **Synergie tussen IT-audit en IT-beveiligingstesting.**

Voordelen IT-audit bij een IT-beveiligingstest

IT-auditing heeft ook een aantal voordelen ten opzichte van beveiligingstesten. Deze zijn samen te vatten tot onderstaande punten:

Root cause analyse

Techniek wordt ingericht en bestuurd door mensen. Mensen kunnen fouten maken. Deze fouten komen tot uiting in de implementatie van de techniek. Maar het hoeft niet zo te zijn dat de fout alleen daar ligt. Doordat een IT-audit ook kijkt naar het beleid en naar procedures kan het een grondigere root cause analyse maken.

Toekomstvastheid

Daar waar een IT-beveiligingstest een momentopname is kan een IT-audit een periode van tijd onderzoeken. Dit heeft tot gevolg dat een IT-audit ook een betere uitspraak kan doen over een toekomstige tijd. Als procedures worden gevolgd en periodieke controles plaatsvinden geeft dat meer waarborgen voor de toekomst dan dat een object op een bepaald moment veilig is ingericht.

Conclusie

Nu we de twee verschillende onderzoeken besproken hebben, is duidelijk dat ze elkaar aanvullen juist op de plekken waar zij zwaktes vertonen. Wanneer we de combinatie van IT-audit en IT-beveiligingstesting gebruiken ontstaan er twee voordelen:

1. *Efficiëntie (budget).* Door de juiste onderzoeksaanpak te kiezen voor de verschillende onderzoeksobjecten kan het onderzoek veel efficiënter worden uitgevoerd.
2. *Verlaging audit risk.* Door de juiste onderzoeksaanpak te kiezen voor de verschillende onderzoeksobjecten kan het onderzoek veel meer in de diepte en breedte worden uitgevoerd en wordt de IT integraler getoetst.

Bovenstaande voordelen tonen aan dat een technische IT-audit dan ook veel baat heeft bij een IT-beveiligingstest.