Het belang van forensic readiness

Voorbereid op fraude?!

Veel organisaties beschikken over adequate IT-securityvoorzieningen, maar relevante gegevens worden vaak niet of slechts ten dele bewaard. Ook blijkt de kwaliteit van in systemen vastgelegde gegevens niet altijd toereikend om die gegevens te gebruiken in een onderzoek. In dit artikel wordt vanuit het perspectief van de fraudeonderzoeker gekeken naar de (on)mogelijkheden van IT bij het beantwoorden van vragen over de omvang van een integriteitsschending. Jethro Vrouwenvelder *

Voor wie zich bezighoudt met security en IT, lijkt het op het eerste gezicht een weinig relevante vraag. In hoeverre is uw organisatie voorbereid op fraude? De vraag is niet of u op het punt staat om fraude te plegen. De vraag is of uw organisatie over voldoende en juiste gegevens beschikt om een onderzoek naar een onverhoopte fraude of integriteitsschending uit te voeren. De praktijk leert namelijk dat veel organisaties weliswaar over adequate IT-security-voorzieningen beschikken, maar relevante gegevens niet of slechts ten dele bewaren. Ook blijkt de kwaliteit van in systemen vastgelegde gegevens niet altijd toereikend om die gegevens te gebruiken in een onderzoek.
In dit artikel wordt vanuit het perspectief van de fraudeonderzoeker gekeken naar de (on)mogelijkheden van IT bij het beantwoorden van vragen over de omvang van een integriteitsschending, wie erbij betrokken was of waren en gedurende welke periode de schending heeft plaatsgevonden.

IT-security vs fraudeonderzoek

Bij de combinatie security en IT spelen de zogenaamde general-IT-controls en de application-controls een voorname rol. De general-IT-controls kunnen worden geduid als algemene beheermaatregelen, het fundament van IT-security. Hoewel de bestanddelen van de general-IT-controls in de literatuur niet eenduidig zijn beschreven, maken IT-beheer, (toegangs)beveiliging en continuïteit van de IT-omgeving onderdeel uit van de general-IT-controls. De application-controls zijn de beheermaatregelen die zijn geïmplementeerd in de geautomatiseerde administratieve systemen van een organisatie. Bijvoorbeeld instellingen die afdwingen dat het banknummer van een nieuw ingevoerde crediteur te allen tijde ingevuld wordt. De application-controls zijn van belang voor de kwaliteit (integriteit) van gegevens.
In het algemeen wordt de kwaliteit van de IT-security frequent getoetst, zoals tijdens een IT-audit in het kader van een jaarrekeningcontrole. Uit de praktijk van het fraudeonderzoek blijkt dat het vaker niet dan wel mogelijk is om de voor het onderzoek benodigde gegevens (volledig) te achterhalen en te ontsluiten. Dat probleem doet zich zelfs voor wanneer er sprake is van een positief oordeel over de kwaliteit van de IT-controls.

Gegevensbronnen

Ten behoeve van fraudeonderzoek zijn uiteenlopende bronnen van gegevens binnen organisaties voorhanden. Denk aan e-mailverkeer, gegevens op gegevensdragers, papieren bescheiden, gegevens uit financiële en administratieve systemen en gegevens van communicatiemiddelen, zoals mobiele telefoons en pda's.
Afhankelijk van het type fraude en de onderzoeksdoelstellingen kunnen gegevens in een onderzoek worden ge-

Case 1

Naar aanleiding van een tweede betalingsherinnering van een crediteur, werd bij een organisatie een onderzoek ingesteld. Al snel werden frauduleuze handelingen van een specifieke medewerker duidelijk. De medewerker had gewerkt op de afdeling die verantwoordelijk was voor het aanmaken van betalingsvoorstellen. Kort voor het onderzoek was de medewerker uit dienst getreden. Uit het onderzoek bleek dat de medewerker op basis van de toegangsbeveiliging van zijn account de digitale betaalbestanden had kunnen benaderen en manipuleren. Dankbaar maakte de medewerker gebruik van deze gelegenheid én van een zwakheid in de maatregelen van AO/IC. De zwakheid betrof het ontbreken van een controleren van het controletotaal dat in ieder betaalbestand werd verwerkt. De medewerker veranderde in de betaalbestanden de rekeningnummers van reguliere crediteuren in een eigen rekeningnummer. Aangezien de medewerker ook alle communicatie met crediteuren, waaronder de betalingsherinneringen, afhandelde, kon deze fraude ruim drie jaar lang worden gepleegd.

bruikt. Ter illustratie: om aan te tonen of een persoon op een zeker tijdstip aanwezig is geweest, kunnen onder meer gegevens uit de toegangsadministratie, het e-mailverkeer, het telefoonverkeer, inloggegevens op het netwerk, inloggegevens van computers, loggings van systeemmutaties en elektronische agenda's relevant zijn. Deze verschillende gegevens moeten dan wel beschikbaar zijn.

Beschikbaarheid van gegevens

In de twee kaders met cases staan voorbeelden uit de praktijk, waaruit problemen blijken met de beschikbaarheid van gegevens.

Bij case 1 werd het onderzoek naar de medewerker op een aantal punten bemoeilijkt. Allereerst werden de digitale betaalbestanden niet bewaard. Zodra een nieuw betaalbestand werd aangemaakt, werd het oude bestand overschreven. Het was daardoor in eerste instantie niet mogelijk om in historische betaalbestanden te zoeken naar gemanipuleerde betalingen. Daarnaast bleek de werkcomputer van de medewerker te zijn opgeschoond. Ook waren de netwerkbestanden van de medewerker gewist. Het opschonen van de computer en het wissen van netwerkbestanden waren onderdelen van de standaardprocedure voor afhandeling van de uitdiensttreding van medewerkers.
Om de problemen te omzeilen zijn uiteindelijk voor dit onderzoek digitale afschriften bij de bank opgevraagd. Op basis hiervan bleek dat in een periode van drie jaar ruim 500.000 euro naar drie verschillende rekeningnummers van de oud-medewerker was overgemaakt. De desbetreffende organisatie heeft na afloop van het onderzoek maatregelen genomen. Zo is in de procedure voor afhandeling van de uitdiensttreding van medewerkers opgenomen dat bestanden van oud-medewerkers zes maanden worden bewaard.

In de cases komen onvolkomenheden in de IT-security naar voren. Zo worden punten geraakt als (zwakheden bij) het maken van back-ups, toegangsbeveiliging, het vastleggen van configuraties en het voorhanden hebben van controles in applicaties. Ten aanzien van deze punten waren in de betreffende organisaties maatregelen getroffen die in de praktijk ook nog werden getoetst. Ze voldeden op het oog op veel vlakken aan de daaraan door de organisaties ge- »

Case 2

Een organisatie gebruikte een systeem waarmee pasjes van medewerkers konden worden opgeladen met een geldtegoed. Door contant geld in te voeren werd het pasje opgeladen. Vervolgens kon het pasje worden gebruikt voor het betalen in het bedrijfsrestaurant. Uit controlelijsten bleek dat wekelijks 500 euro uit het systeem verdween. Het ziekenhuis stelde een onderzoek in. Al snel bleek het nodig om oude versies van het systeem terug te laten zetten vanaf back-up. Op deze manier zou de omvang van de schade kunnen worden bepaald. Hoewel het systeem netjes werd meegenomen in de back-upcyclus, bleek het onmogelijk om oude versies terug te zetten. De voor het terugzetten van het systeem benodigde logbestanden werden namelijk nooit meegenomen in de back-ups.

stelde normen. Bijvoorbeeld het gegeven dat elektronische betaalbestanden worden overschreven zal niet snel als risico naar voren komen bij een toets van de IT-security-maatregelen. Daarbij geldt het argument dat er immers ook papieren afschriften of uitdraaien van internetbankieren beschikbaar zijn. Een dergelijke argumentering houdt echter geen rekening met het gegeven dat digitale betaalbestanden van grote waarde zijn bij onderzoek van integriteitsschending.

Forensic readiness

Tot nu toe zien we dat een adequaat pakket van beheermaatregelen met betrekking tot de IT-security niet automatisch betekent dat er ook adequaat onderzoek naar integriteitsschendingen mogelijk is. Het is daarom tijd voor een andere manier van denken, althans een aanvullende manier van denken. Het loont om als organisatie goed voorbereid te zijn in het geval dat een onderzoek moet worden ingesteld. Het voorbereid zijn op een onderzoek naar een integriteitsincident, wordt aangeduid met 'forensic-readiness'.

Het voorbereid zijn op een onderzoek naar een integriteitsincident wordt aangeduid met 'forensic-readiness'

In het *International Journal of Digital Evidence* (Winter 2004, Volume 2, Issue 3) is een artikel gepubliceerd waarin in een aantal stappen beschreven is hoe een organisatie forensic-readiness kan bereiken. Bekeken vanuit het perspectief van onderzoek naar integriteitsincidenten, volgen hieronder de meest relevante:

1. Het vaststellen van de processen waarin gegevens worden gegenereerd die noodzakelijk zijn in het geval van onderzoek. Het gaat hierbij om de bedrijfsprocessen die fraudegevoelig zijn. In aansluiting op de eerder besproken cases zou bijvoorbeeld het proces waarbij de betaalbestanden worden verwerkt in aanmerking komen.
2. Het bepalen van de gegevensbronnen van potentieel bewijsmateriaal.
3. Het bepalen van de wijze waarop het potentiële bewijsmateriaal wordt vastgelegd en gearchiveerd. Hierbij spelen kosten-batenoverwegingen een rol (denk aan opslagcapaciteit, de tijdsduur dat data opgeslagen moeten zijn, enzovoorts).
4. Het implementeren van beleid om potentieel bewijsmateriaal veilig op te slaan en te gebruiken. Daarbij is het goed om een scenario uit te werken hoe te reageren in het geval dat digitaal bewijs nodig is. Het is bijvoorbeeld van belang dat betrokkenen zo min mogelijk sporen en bewijzen kunnen vernietigen. Binnen veel organisaties is een Incident Response Program geïmplementeerd. Het scenario voor het veiligstellen van bewijs kan hiermee worden geïntegreerd.
5. Het proactief detecteren van mogelijke integriteitsschendingen. Niet alleen het verzamelen van bewijsmateriaal is belangrijk, ook is het zaak een schending tijdig op te sporen. Hiertoe kunnen digitale gegevens worden geanalyseerd en gemonitord, zodat 'verdachte' activiteiten in kaart worden gebracht. Technieken voor data-mining (gegevensanalyse) kunnen voor de detectie worden gebruikt.
6. Het opstellen van een procedure waarin criteria zijn opgenomen om te bepalen wanneer een formeel onderzoek wordt ingesteld waarbij gebruik wordt gemaakt van digitaal bewijsmateriaal. Omstandigheden die hierbij een rol spelen, zijn: omvang van mogelijke schade en reputatieverlies, wet- en regelgeving (inclusief wanneer een melding aan de toezichthouder plaats moet vinden, mogelijke impact op derden, enzovoort).
7. Het creëren en verhogen van bewustzijn bij de medewerkers om te voorkomen dat onzorgvuldig wordt omgegaan met digitaal bewijsmateriaal.

Voor deze stappen geldt dat rekening moet worden gehouden met alle relevante wet- en regelgeving. Privacy-aspecten, zoals geregeld in de Wet bescherming persoonsgegevens, spelen hierbij een belangrijke rol. Maar bijvoorbeeld ook instemming van een ondernemingsraad.

Een praktijkvoorbeeld laat zien dat het punt van het bewustzijn (punt 7) zeer relevant is. Een overijverige systeembeheerder heeft ooit een computer van een medewerker opgestart om op zoek te gaan naar bewijs ter bevestiging van geruchten. Door in te loggen op de computer werd de bewijskracht van de gegevens op de computer sterk verkleind. De desbetreffende medewerker, die bedrijfsgevoelige informatie doorstuurde naar een concurrent, kon nu aanvoeren dat hij niets had misdaan en dat de computer was gemanipuleerd. Anders gezegd, door het ontbreken van een zeker bewustzijn bij de systeembeheerder was bewijsmateriaal besmet geraakt.

Conclusie

Een goed pakket van beheermaatregelen met betrekking tot de IT-security betekent niet automatisch dat adequaat onderzoek naar integriteitsschendingen of -incidenten mogelijk is. Voor dergelijk onderzoek zijn veel, vaak gedetailleerde gegevens over een langere periode nodig. De eisen van beschikbaarheid en kwaliteit van de (gedetailleerde) digitale gegevens ten behoeve van zo'n onderzoek komen vaak niet aan de orde bij de gebruikelijke toetsing van de IT-security. De stappen voor 'forensic-readiness' bieden houvast voor aanvullende normen ten aanzien van de IT-security. Niet alleen zal met inachtneming van deze stappen in het geval van een integriteitsschending het onderzoek efficiënt en effectief uitgevoerd kunnen worden. Ook krijgt een organisatie een krachtig instrument in handen om proactief op zoek te gaan naar integriteitsrisico's en om vroegtijdig in te kunnen grijpen als zwakheden zijn geconstateerd. Wees voorbereid op fraude! «

**ing. J.V. Vrouwenvelder RE is onderzoeker bij Integis*