Insider threat:

tweekoppig monster

Er is tegenwoordig veel aandacht voor cybercriminelen en hackers die op inventieve manieren systemen weten binnen te dringen. Miljoenen privacygevoelige gegevens worden geroofd of systemen lamgelegd. De nieuwsconsument kijkt er al nauwelijks meer van op. Naast al die dreigingen van buitenaf zou bijna vergeten worden dat het gevaar ook van binnenuit kan komen.

tekst Paul Koedijk

Vooral bij fraudeonderzoekers is bekend dat het overgrote deel van de fraudegevallen zich binnen organisaties afspeelt. Hoewel er dus in dat opzicht sprake is van een oud fenomeen, is er desalniettemin sprake van een hernieuwde aandacht voor gevaren van binnenuit in organisaties. Die aandacht is dusdanig dat 'insider threat' als het nieuwe 'buzzword' wordt gekwalificeerd in de wereld van security. De Amerikaanse president heeft zelfs een special Insider Threat Task Force in het leven geroepen. Maar insider threat – we houden de Engelse term aan – is een breder fenomeen dan alleen de acties van mensen die in de ogen van een deel van de buitenwereld prijzenswaardige klokkenluiders zijn.

VIJF TYPEN

Het Britse Centre for the Protection of National Infrastructure (CPNI) heeft in 2013 een rapport gepubliceerd op basis van onderzoek naar interne bedreigingen. Daarbij zijn honderdtwintig gevallen van insider threat geanalyseerd. De onderzoekers kwamen daarbij tot een classificatie van vijf typen dreigingen van binnenuit:

1. Zonder toestemming openbaar maken van gevoelige informatie
2. Procescorruptie (zeg maar 'fraude')
3. Faciliteren van toegang door derde partij tot bedrijfsgegevens
4. Fysieke sabotage
5. Elektronische of IT-sabotage

In 76 procent van de onderzochte gevallen kwam het initiatief tot dergelijke acties van de betrokkenen zelf; slechts bij zes procent van de incidenten was er sprake van bewuste infiltratie. De implicatie hiervan is dat mensen pas op het idee kwamen nadat ze als werknemer waren aangenomen. Het onderzoek wees verder uit dat de motieven van de betrokken werknemers vaak complex zijn; naast financieel gewin (47%) speelden ideologie (20%), streven naar erkenning (14%) en loyaliteit (richting vrienden/familie/geboorteland) (14%) een rol.

TWEE NIVEAUS

Factoren die in de hand werken dat een insider threat zich manifesteert bewegen zich op twee niveaus, dat van het individu en dat van de organisatie. Op individueel niveau gaat het om persoonlijkheidskenmerken, iemands levensstijl en persoonlijke kwetsbaarheden als gevolg van (tijdelijke) omstandigheden, en ten slotte gedrag op de werkvloer.

Op het niveau van de organisatie spelen maar liefst negen factoren een rol. Slecht management is daarbij prominent. Daarbij gaat het vooral om gebrek aan supervisie en het niet onderkennen en oplossen van problemen op de werkvloer. De andere factoren betreffen het slecht gebruik maken van audit functies, gebrek aan veiligheidsmaatregelen, gebrekkige security cultuur, slechte personeelskeuze qua geschiktheid voor het vervullen van gevoelige functies, slechte pre-employment screening, slechte interne communicatie tussen business units over mogelijke problemen, en ten slotte het gebrek aan besef bij het hoger management van het personeelsrisico in combinatie met tekortschietende governance.

MAATREGELEN

Wat kan er gedaan worden tegen insider threats? De eerste horde dient een degelijke screening te zijn van nieuw personeel. Die kan worden uitgebreid met speciale persoonlijkheidstesten, waarmee een indicatie kan worden verkregen van iemands integriteit. Derge-

lijke testen kunnen ook met regelmaat worden afgenomen nadat iemand is aangenomen. De NSA bijvoorbeeld is na alle ervaringen met Edward Snowden overgegaan op een systeem van 'continuous vetting' op basis van een risk managementbenadering.

Daarnaast hanteert de NSA sinds kort de zogenaamde 'dual approval approach'. Dit houdt in dat bepaalde handelingen (zoals het verplaatsen van een geclassificeerd bestand van de ene server naar de andere) vereisen dat ze worden uitgevoerd door twee personen met een security clearance.

Veel bedrijven en instellingen leggen nog altijd een zwaar accent op monitoring van computergebruik, waarbij bepaalde gebruikspatronen automatisch rode vlaggen genereren. Die benadering kan echter op steeds meer kritiek rekenen. De vooronderstelling bij een dergelijke beveiliging is dat je te maken hebt met wat domme gebruikers, die niet beseffen dat hun computergebruik wordt gemonitord op triviale criteria (zoals overmatig downloaden van bestanden). Dit soort monitoring levert veel zogenaamde 'valse positieven' op die alleen maar het zicht op echte gevaren vertroebelen, omdat ze de controllers overspoelen met loze meldingen. Vandaar het pleidooi om veel meer vanuit een risk-managementbenadering te monitoren: bepaal wat de gevoelige posities zijn en wie die bekleden, welke risico's daarbij in het spel zijn en pas je pakket van maatregelen daar op aan. Op die manier worden schaarse middelen het best gebruikt.

KWAADWILLIG

Kwaadwilligheid speelt een belangrijke rol bij insider threat, maar in feite is er sprake van een tweekoppig monster. Sommige auteurs die over insider threat schrijven, wijzen er op dat er nog een ander belangrijk facet is dat aandacht verdient. Er is in toenemende mate sprake van onbedoelde openbaarmaking van gevoelige informatie, soms als gevolg van in aanleg triviale menselijke fouten. Het 2014 Verizon Data Breach Report wees bijvoorbeeld op het fenomeen 'verkeerd bezorgd', waarbij als gevolg van onzorgvuldige e-mailbezorging gevoelige informatie onbedoeld terechtkomt bij iemand waarvoor die niet bedoeld is. Een codeerfout kan hetzelfde gevolg hebben. Bijna altijd gaat het daarbij om →

‘Insider threat’ is het nieuwe ‘buzz-word’ in security

menselijke fouten, vaak bij routinematig handelen.

Het gevaar van menselijk falen is bovendien toegenomen doordat organisaties steeds meer raken ingebed in een netwerk van toeleveranciers, (tijdelijke) adviseurs en personeel en zakenpartners. Auteur Eric Chabrow van de website GovInfoSecurity had het onlangs in dit verband dan ook over ‘een collectief ecosysteem van organisaties die tezamen de insider vormen’. En dus ook de insider threat.

Een ander aspect van niet-kwaadwillig gedrag – althans niet opzettelijk kwaadwillig – ligt in de wijze waarop veel werknemers aankijken tegen intellectueel eigendom. Beter gezegd: niet aankijken tegen intellectueel eigendom. Een in opdracht van Symantec uitgevoerd onderzoek naar het verdwijnen van intellectual property (IP) bracht naar voren dat werknemers op allerlei manieren IP buiten de organisatie brengen. Velen van hen mailen regelmatig zakelijke documenten van hun werkaccount naar hun privé-account of downloaden ze naar hun eigen tablets of smartphones. Anderen delen informatie in de cloud via file-sharing apps. Dat gebeurt zelden met toestemming van de werkgever. De informatie wordt bovendien zelden achteraf opgeruimd. Wanneer werknemers van baan veranderen nemen ze vaak gevoelige informatie mee. Een geval van kwaadwilligheid daargelaten speelt vaak onachtzaamheid of onvoorzichtigheid een rol. Ze zijn er zich niet van bewust dat ze daarmee zowel zichzelf als hun organisatie in gevaar brengen. Veel werknemers leven in de overtuiging dat het eigendom van IP ligt bij degene die het gecreëerd heeft en niet bij diens werkgever. Tezamen maakt dit alles duidelijk dat veel organisaties er niet in slagen om een veiligheidscultuur tot stand te brengen, waarin werknemers beseffen dat dergelijk gedrag niet is toegestaan. Werknemers zien daardoor niet of onvoldoende in dat ze zelf een rol te vervullen hebben als het gaat om informatiebeveiliging.

VERTROUWEN

Aan alle maatregelen tegen bedreigingen van binnenuit kleeft één problematisch aspect dat nog niet is benoemd. Alle acties die het voor insiders moeilijker maken om gegevens te verkrijgen of te manipuleren, hebben een grote schaduwzijde: ze geven allemaal aan dat de werkgever zijn werknemers niet vertrouwt. Of ze wel of niet security clearances hebben maakt daarbij niet uit. Binnen sommige Amerikaanse (overheids-) organisaties is de zogenaamde ‘continuous security clearance vetting’ van werknemers ingevoerd. Die is gebaseerd op een risk-managementbenadering waarbij de gevoeligheid en de omvang van programma’s en informatie waarmee iemand werkt leidend zijn. Daarbij wordt – naast de gebruikelijke informatievoorziening vanuit de organisatie zelf - gebruik gemaakt van een grote hoeveelheid gegevens uit onder meer commerciële databases. Deze ‘big data’ worden geanalyseerd om het gedrag van individuele werknemers te monitoren. De systemen genereren rode vlaggen die uiteen kunnen lopen van een aanhouding wegens rijden onder invloed of oplopende schulden op iemands credit card. Die kunnen weer aanleiding vormen om iemands vertrouwenspositie te herzien.

CULTUUR

Het gebrek aan vertrouwen dat uit deze verregaande vorm van monitoring spreekt kan een tegengesteld effect hebben op het moreel van werknemers. Nu zullen Amerikaanse monitorpraktijken niet volledig kopieerbaar zijn in Nederland vanwege de andere opvattingen (en regelgeving) over privacy die hier leven. Desalniettemin bestaat ook hier hetzelfde spanningsveld tussen vertrouwen en controle. Het paradoxale is dat uit het eerder genoemde CPNI-onderzoek naar voren komt dat in veel van de onderzochte incidenten een algehele onvrede met de organisatie een belangrijke aanvullende factor vormde. Het gaat bij het vraagstuk van de insider threat dus niet alleen maar over security culture; de cultuur van een organisatie als geheel en het welbevinden van de werknemers vormen een belangrijke factor bij het tegengaan van insider threat. Onderdeel van dat welbevinden is dat een organisatie overtuigend heeft weten over te brengen hoe en waarom voor een bepaalde balans tussen vertrouwen en controle is gekozen.■

Paul Koedijk is onderzoeker bij Integis.