INFORMATIEBEVEILIGING: LET VOORAL OOK OP HET GEVAAR IN EIGEN HUIS

David Upton en Sadie Creese

RISICOMANAGEMENT

De grootste bedreiging voor uw informatiesystemen kan een werknemer of een leverancier zijn.

In 2013 werden bij een cyberaanval op de Amerikaanse winkelketen Target de betaalkaartgegevens van zo'n veertig miljoen klanten en de persoonlijke gegevens van ongeveer zeventig miljoen klanten gestolen. De onderneming liep zware reputatieschade op, de winst kelderde en de CEO en CIO moesten opstappen. De dieven waren buitenstaanders, maar ze wisten in de systemen van Target te komen door zich voor te doen als een *insider* – een van de leveranciers van koelsystemen.

De gegevensroof bij Target is slechts één recent voorbeeld van een groeiend fenomeen. Externe aanvallen krijgen veel aandacht. Denk aan de veelvuldige *hacks* van intellectuele eigendom vanuit China, het Stuxnet-virus of de praktijken van Oost-Europese benden. Aanvallen waar aangesloten bedrijven of eigen medewerkers bij betrokken zijn, vormen echter een nog ernstiger bedreiging. *Insiders* kunnen een organisatie veel meer schade berokkenen dan externe hackers omdat ze veel gemakkelijker toegang kunnen krijgen tot systemen en veel meer gelegenheid hebben om in te breken. Ze kunnen de meest uiteenlopende schade veroorzaken: bedrijfsprocessen die stil vallen, verlies van intellectuele eigendom, reputatieschade, verlies aan vertrouwen onder beleggers en klanten, gevoelige informatie die gelekt wordt aan derden, waaronder ook de media. Volgens verschillende schattingen vinden er alleen al in de Verenigde Staten jaarlijks minstens tachtig miljoen aanvallen plaats op informatiesystemen waar *insiders* bij betrokken zijn. Het kunnen er echter nog veel meer zijn, want ze worden vaak niet gemeld. De schade loopt inmiddels in de tientallen miljarden dollars per jaar.

Veel organisaties erkennen dat ze nog steeds geen afdoende aanpak hebben om aanvallen met hulp van binnenuit tijdig te signaleren of te voorkomen. Dat komt onder meer doordat deze dreiging nog steeds wordt onderschat.

In de afgelopen twee jaar hebben wij (de auteurs) een internationaal onderzoeksproject geleid op dit terrein. Wij wilden organisaties helpen om bedreigingen van binnenuit sneller op het spoor te komen en tegen te gaan. Het onderzoek werd gesponsord door het Centrum voor de Bescherming van Nationale Infrastructuur (CPNI), een onderdeel van de Britse geheime dienst MI5. Ons team van zestien mensen bestond uit specialisten in computerbeveiliging, academici verbonden aan business schools die onderzoek doen naar corporate governance, docenten in management, experts in informatievisualisering en psychologen en criminologen van de universiteiten van Oxford, Leicester en Cardiff.

Onze multidisciplinaire aanpak leidde tot bevindingen die de gebruikelijke opvattingen en manieren van werken ter discussie stellen (zie kader 'Veel voorkomende methoden werken niet'). Een voorbeeld: veel ondernemingen proberen hun medewerkers ervan te weerhouden om met de computers van de organisatie websites te bezoeken die niet direct verband houden met hun

werk, zoals Facebook, datingsites en politieke sites. Wij denken dat medewerkers volledig vrij moeten worden gelaten in de sites die ze bezoeken, maar dat de werkgever daar toezicht op moet houden. Daar is kant-en-klare beveiligingssoftware voor te krijgen. Zulk toezicht levert belangrijke informatie op over het gedrag en de persoonlijkheid van medewerkers die kan worden gebruikt om gevaren op te sporen. In dit artikel bespreken we de effectieve methoden die in het onderzoek naar voren kwamen om de kans op aanvallen van binnenuit zoveel mogelijk te beperken.

HET RISICO WORDT ONDERSCHAT

Bedreigingen van binnenuit komen van mensen die hun rechtmatige toegang tot digitale informatie misbruiken. Ze willen doelbewust informatie stelen of de onderneming schade berokkenen, of ze laten onbewust gaten ontstaan in de systemen. Dit kunnen eigen mensen zijn (van de schoonmakers tot de directie), onderaannemers of externe leveranciers van gegevens en informaticadiensten. (Edward Snowden, die gevoelige informatie stal van de Amerikaanse National Security Agency, werkte voor een bedrijf dat diensten leverde aan de NSA.) Doordat ze er rechtmatig toegang tot hebben, kunnen ze computersystemen en gegevens stelen, verstoren of corrumperen zonder dat dit wordt opgemerkt door de systeembeveiliging. De beveiliging is namelijk gericht op de plekken waar het systeem kan worden binnengedrongen, niet op wie of wat al binnen is.

ALLES EN IEDEREEN IS KWETSBAAR

Volgens Vormetric, een vooraanstaand bedrijf op het gebied van computerbeveiliging, is 54 procent van de managers bij grote en middelgrote organisaties van mening dat het anno 2014 moeilijker is dan nog maar drie jaar geleden, in 2011, om aanvallen van binnenuit te signaleren en voorkomen. Bovendien neemt dat soort aanvallen toe, niet alleen in absolute maar ook in relatieve zin – volgens een studie van KPMG is het aantal aanvallen van binnenuit gestegen van vier procent van alle gemelde cyberaanvallen in 2007 naar twintig procent in 2010. Op grond van de bevindingen uit ons eigen onderzoek menen wij dat het percentage daarna verder is gestegen. Bovendien: zoals de aanval bij Target heeft laten zien, kunnen ook bij externe aanvallen insiders betrokken zijn – bewust of onbewust.

OORZAKEN VAN DE TOENAME

Diverse factoren in het veranderende IT-landschap verklaren de toenemende dreiging. Verrassend zijn die niet, en dat is nu juist het punt: organisaties zijn kwetsbaar voor aanvallen met behulp van of door mensen van binnenuit (*insiders*) doordat allerlei gewone 'deuren' niet 'in het slot vallen'.

Omvang en complexiteit van IT zijn drastisch toegenomen

Weet u welke mensen uw diensten in de Cloud beheren? Weet u met welke partijen u die servers (de Cloud) deelt? Weet u hoe veilig die servers zijn? En hoe betrouwbaar al die partijen zijn aan wie uw organisatie taken heeft uitbesteed, zoals call-centra, logistiek dienstverleners, schoonmaakbedrijven en externe dienstverleners voor personeelsadministratie en klantbeheer? In 2005 werd bij vier rekeninghouders van Citibank in New York in totaal bijna 350.000 dollar gestolen door medewerkers van een call-centrum in de Indiase stad Poona. De daders werkten bij een externe leverancier van software en IT-diensten van Citibank. Ze hadden persoonsgegevens, pincodes en rekeningnummers van klanten verzameld.

Het wemelt inmiddels van de sites in het *Dark Web* waar gewetenloze partijen grote hoeveelheden gevoelige informatie verhandelen. Op die illegale websites gaat van alles om – van wachtwoorden van klanten en creditcardgegevens tot intellectuele eigendom. *Insiders* zijn vaak bereid om anderen voor een spotprijs – vergeleken met de marktwaarde van de gegevens waar het om gaat – toegang te verschaffen tot dergelijke informatie. Zij zijn als het ware de loopjongens van de '*cybercrime-as-a-service*'-sector.

Werknemers gebruiken persoonlijke apparaten in hun werk

Steeds meer werknemers brengen hun werkgevers tegenwoordig in gevaar – vaak zonder het te beseffen – doordat ze taken voor hun werk doen op hun eigen elektronische

apparaten. Het aantal van die apparaten dat in omloop is groeit explosief en uit (onder meer) ons eigen onderzoek blijkt dat de beveiligingsteams bij ondernemingen niet zijn opgewassen tegen de gevaren die daardoor ontstaan. Volgens een recent rapport van Alcatel-Lucent zijn op ieder willekeurig moment wereldwijd zo'n 11,6 miljoen mobiele apparaten besmet en steeg het aantal mobiele *malware*-infecties in 2013 met twintig procent.

Dit betreft niet alleen smartphones en tablets. Het gaat ook om zoiets simpels als een USB-stick of de geheugenkaart in een telefoon. 'De beste manier om bij een onvoorbereid bedrijf binnen te komen, is om wat geïnfecteerde USB-sticks bedrukt met het logo van het bedrijf achter te laten op de parkeerplaats,' zegt Michael Goldsmith, een lid van ons onderzoeksteam en een associate director van het Cyber Security Centre in Oxford. Zijn opmerking verwijst naar iets wat in 2012 gebeurde bij het Nederlandse chemiebedrijf DSM. 'Er is altijd wel een medewerker die gaat kijken wat er op staat.'

In de media is ook breeduit gerapporteerd dat onder de deelnemers van de G20-top bij Sint-Petersburg in 2013 USB-sticks en opladers voor mobiele telefoons werden uitgedeeld, allemaal geladen met *malware* bedoeld om informatie te stelen. Ook de Stuxnet-computerworm, waarmee in 2008-2010 een Iraanse fabriek voor uraniumverrijking is gesaboteerd, zou via USB-sticks zijn 'geïnjecteerd' in systemen van die fabriek die niet op internet waren aangesloten. Kortom, alles en iedereen loopt dit risico.

Sociale media zijn explosief gegroeid

De sociale media maken het mogelijk om allerlei informatie te lekken uit een bedrijf en wereldwijd te verspreiden, vaak zonder dat het bedrijf in kwestie er erg in heeft. Met de sociale media kunnen ook *insiders* worden geworven om via hen toegang te krijgen tot bedrijfsmiddelen. Bijzonder effectief blijkt de zogeheten 'versiertruc' (*romance scam*): een geraffineerde oplichter doet zich op een datingsite voor als een aanbidder en haalt zo een medewerker over om vertrouwelijke informatie te delen. Een andere praktijk is om medewerkers onder druk te zetten met kennis die over hen is ingewonnen via sociale netwerken: de afperser zegt tegen de medewerker dat hij computerbestanden zal wissen of pornografische afbeeldingen zal plaatsen op zijn/haar pc op het werk als hij de verlangde gevoelige informatie niet krijgt.

MANAGERS WETEN VAN NIETS

We vroegen tachtig hooggeplaatste managers naar hun kennis omtrent het gevaar van informatielekken van binnenuit en vulden dit aan met diepgaande case-study's van daadwerkelijke incidenten. Dit is, samengevat, wat we tegenkwamen:

- In alle landen en de meeste bedrijfstakken (behalve banken en energiebedrijven) zijn managers grotendeels onwetend over de bedreigingen van binnenuit
- Informatiebeveiliging beschouwen zij meestal als de verantwoordelijkheid van een ander – meestal de afdeling IT
- Maar weinig managers onderkennen dat het belangrijk is om alert te zijn op ongewoon gedrag van medewerkers – bijvoorbeeld bezoek aan extremistische websites of kantoorbezoek op ongebruikelijke tijdstippen – om risico's tijdig in het vizier te krijgen
- Voor bijna twee op de drie in- en externe beveiligingsspecialisten blijkt het heel moeilijk te zijn om bij directies gehoor te krijgen voor de risico's die een organisatie loopt wanneer onvoldoende aandacht wordt besteed aan het gevaar van binnenuit
- IT-afdelingen wordt zelden verteld welke informatie bij uitstek moet worden beschermd, wat aanvaardbare risico's zijn of hoeveel moet worden geïnvesteerd om aanvallen te voorkomen.

WAAROM DOEN ZE HET?

Uit diverse onderzoeken bij de overheid en particuliere instanties blijkt dat insiders die willens en wetens deelnemen aan cyberaanvallen daarvoor uiteenlopende motieven hebben: financieel gewin, wraak, een zucht naar erkenning en macht, reactie op chantage, loyaliteit aan anderen in de organisatie en politieke overtuigingen.

Een voorbeeld dat we in ons onderzoek tegenkwamen betrof een aanval eerder dit jaar (2014) op een klein maar groeiend bedrijf in virtuele training. De dader was een systeembeheerder die verliefd was geworden op een manager bij het bedrijf. Hij had hem bloemen op het werk laten bezorgen en ongepaste sms-berichten gestuurd en was veelvuldig langs zijn huis gereden. De manager had zich beklaagd bij de meerdere van de systeembeheerder.

Toen de systeembeheerder begreep dat hij echt afgewezen was, beschadigde hij de databank met trainingsvideo's van het bedrijf en maakte de backups ontoegankelijk. Het bedrijf ontsloeg hem. De systeembeheerder wist echter dat zijn schuld niet kon worden bewezen en chanteerde het bedrijf: hij eiste enkele duizenden euro's, anders zou hij bekend maken hoe slecht het gesteld was met de beveiliging. Die publiciteit had heel schadelijk kunnen zijn voor dat bedrijf, want het zou naar de beurs gaan. Dit schadelijke incident werd, zoals zovele andere, niet gemeld.

Het komt steeds vaker voor dat mensen uit organisaties zich inlaten met georganiseerde misdaad en actiegroepen. In veel landen zijn inmiddels noodteams opgericht (*computer emergency readiness teams*, CERT's) om bescherming te bieden tegen dergelijke en andere soorten aanvallen. Het CERT Insider Threat Center van Carnegie Mellon University publiceerde in 2012 een rapport over 150 zaken die het had onderzocht (*Spotlight On: Malicious Insiders and Organized Crime Activity*). In zestien procent daarvan was de georganiseerde misdaad betrokken.

Bij een van die zaken, in 2012, stal een Russische bende de gegevens van 3,8 miljoen niet versleutelde bankrekeningen en bijna vier miljoen belastingaangiften van de belastingdienst in de Amerikaanse staat South Carolina. Uit het forensisch onderzoek bleek dat die aanval mogelijk was gemaakt doordat een medewerker een link in een e-mail had aangeklikt, waarna de bende zijn persoonsgegevens kon stelen en zo toegang had gekregen tot de dataservers.

Een van de leden van ons team was Monica Whitty, psychologe aan de universiteit van Leicester. Zij meent, en anderen met haar, dat *insiders* die bewust een cyberaanval plegen of mogelijk maken lijden aan een of meer condities uit de 'duistere driehoek' van machiavellisme, narcisme en psychopathie. Die mening wordt ondersteund door een studie uit 2013 van de CPNI. Daarin werd geconcludeerd dat aanvallers van binnenuit veelal een bepaalde combinatie hebben van de volgende persoonlijkheidskenmerken: onvolwassenheid, laag zelfbeeld, gewetenloosheid of gebrek aan ethisch normbesef, oppervlakkigheid, neiging tot fantaseren, rusteloosheid en impulsiviteit, gebrek aan nauwgezetheid, manipulatief gedrag en onevenwichtigheid.

Roger Duronio, een systeembeheerder bij vermogensbeheerder UBS Wealth Management veroordeeld voor sabotage van het computernetwerk van dat bedrijf in 2006 met een *logic bomb*, vertoonde een aantal van deze eigenschappen. Duronio was onzeker over zijn baan en werd razend toen hij een bonus kreeg van 32.000 dollar in plaats van de 50.000 dollar die hij had verwacht. Hij nam *short*-posities in de aandelen van het bedrijf en zette de bom in werking. Zo'n tweeduizend servers vielen uit in kantoren van UBS verspreid over heel de Verenigde Staten; sommige kantoren konden een aantal weken geen transacties doorgeven. Het bedrijf leed 3,1 miljoen dollar schade aan directe kosten en voor nog eens miljoenen extra aan niet bekend gemaakte specifieke verliezen. Duronio werd veroordeeld tot 97 maanden gevangenis voor zijn daad.

VEEL VOORKOMENDE BEVEILIGINGSMETHODEN WERKEN NIET

De meest gangbare beveiligingsmaatregelen op het gebied van informatiebeheer zijn veel minder effectief tegen *insiders* dan tegen buitenstaanders:

- *Toegangsbeleid* – Een verbod op het gebruik van apparatuur van de werkgever voor persoonlijke zaken weerhoudt mensen er niet van gegevens te stelen
- *Toegangsbewaking* – Met beveiligingspatches en antivirusprogramma's worden inbraken door geautoriseerde maar kwaadwillende werknemers, of door derden met gestolen autorisatiegegevens, niet voorkomen en ook niet gesignaleerd
- *Afscherming* – Plaatsing van kritieke bedrijfsmiddelen in een extra beveiligd gebied voorkomt geen diefstal door mensen die toegang hebben tot de beveiligde systemen
- *Wachtwoordbeleid* – Als medewerkers ingewikkelde wachtwoorden moeten bedenken of vaak van wachtwoord moeten veranderen, schrijven ze die vaak op briefjes die gemakkelijk kunnen worden gestolen
- *Bewustwordingsprogramma's* – Veiligheidsbewustzijn wordt niet opgebouwd door medewerkers enkel de handleiding voor IT-beveiliging te laten doornemen, en evenmin is dit een remedie tegen doelbewust schadelijk handelen door medewerkers.

DE BENADERING VAN HET PROBLEEM

Het managen van het risico van cybercriminaliteit (met hulp) van binnenuit is verwant aan kwaliteit- en veiligheidsmanagement. Al dit soort zaken was ooit de verantwoordelijkheid van een gespecialiseerde afdeling. Maar de technologische omgeving is zo complex geworden en verandert zo snel dat organisaties niet langer elk risico van te voren kunnen inschatten. Dat betekent dat het topmanagement van de organisatie, ongeacht hoe groot of klein die ook is, zich hier direct mee moet bemoeien. De volgende vijf stappen moeten onmiddellijk worden genomen:

Voer een krachtig *insider*-beleid in

Dit beleid moet duidelijk maken wat mensen moeten doen en laten om te voorkomen dat *insiders* de organisatie door onvoorzichtigheid, nalatigheid of fouten in gevaar brengen. Het beleid moet beknopt worden geformuleerd en moet gemakkelijk te begrijpen, na te lezen en na te leven zijn – voor iedereen, niet alleen voor deskundigen op gebied van veiligheid en technologie. De regels moeten gelden voor alle niveaus van de organisatie, ook het topmanagement. Een raamwerk gepubliceerd door de Amerikaanse staat Illinois biedt een model – zie www.illinois.gov/ready/SiteCollectionDocuments/Cyber_SOSSamplePolicy.pdf

Geef medewerkers ook instrumenten die hen helpen zich te houden aan het beleid. Systemen kunnen bijvoorbeeld zo worden ontworpen dat er een waarschuwingsbericht gaat knipperen op het beeldscherm wanneer iemand probeert in te loggen op een deel van het systeem waar gevoelig materiaal opgeslagen ligt. Het systeem zou kunnen vragen of de persoon in kwestie daartoe bevoegd is en zou iedereen die dat niet is moeten registreren en volgen.

Overtredingen moeten beboet worden. Een medewerker die een ernstig misdrijf pleegt, zoals het verkopen van persoonsgegevens van klanten of bewust *malware* injecteren in bedrijfssystemen, moet natuurlijk worden ontslagen en gerechtelijk worden vervolgd. Voor een minder ernstige eerste overtreding, zoals het delen van wachtwoorden om collega's die te vertrouwen zijn toegang te geven tot bedrijfssystemen, kan een waarschuwing worden gegeven aan de medewerker, die wordt opgenomen in zijn/haar dossier.

Ook is het belangrijk medewerkers duidelijk te maken wat het precies betekent om hun dagelijks werk op een veilige manier te doen. Het beleid moet regelmatig worden bekrachtigd met informatiebijeenkomsten en interne communicatiecampagnes, bijvoorbeeld ook met posters die op de werkplek worden opgehangen. Sommige bedrijven laten met behulp van videofilms zien hoe cyberaanvallen mogelijk worden gemaakt doordat medewerkers zich niet aan de regels houden, en hoe ze kunnen worden voorkomen door veiliger te werken.

WAT KUNT U DOEN?

Het algemeen management moet onder meer de volgende eisen stellen aan de afdeling IT:

- Bewaak al het uitgaande verkeer van enterprisenetwerken via internet of draagbare media en meld ongebruikelijke zaken en overtredingen van beleid onmiddellijk
- Houd bij wat de *best practices* zijn op het gebied van ondersteuning van de strategie en het beleid voor cyberveiligheid
- Houd strak de hand aan procedures en protocollen voor netwerkbeveiliging waarin rekening wordt gehouden met de operationele prioriteiten
- Beheer gebruikersaccounts actief om ervoor te zorgen dat medewerkers nooit meer toegang hebben tot gevoelige computersystemen dan absoluut noodzakelijk is
- Voer geregeld een risico-evaluatie uit en rapporteer hierover aan de bedrijfsleiding.

WERK AAN BEWUSTZIJN

Wees open over mogelijke bedreigingen, zodat medewerkers die signaleren en zij op hun hoede kunnen zijn voor iedereen die probeert via hen in te breken. Geef medewerkers gericht training, kijkend naar het soort aanvallen waarmee zij specifiek bij hun werkzaamheden te maken kunnen krijgen. *Phishing* is een veel gebruikte tactiek: misleidende e-mails brengen medewerkers ertoe om persoonlijke gegevens af te staan of een link aan te clicken die vervolgens *malware* downloadt. (Veel mensen

realiseren zich niet dat het adres van de afzender in een e-mail gemakkelijk kan worden vervalst.) Medewerkers kunnen worden getest op hun kwetsbaarheid voor dergelijke aanvallen. Dat kan een onderneming zelf doen of laten doen door een externe beveiligingsdienst.

Ook dan blijft het moeilijk om eigen mensen te verdedigen tegen een vastberaden buitenstaander. In april 2013 was een Franse multinational het slachtoffer van een bijzonder sluwe aanval. De secretaresse van een van de directieleden kreeg een e-mail met een verwijzing naar een factuur opgeslagen in een gezamenlijke beheerdienst in de Cloud. Ze was zo verstandig het bestand niet te openen, maar enkele minuten later kreeg ze een telefoontje van iemand die zich (met succes) voordeed als een ander directielid en haar instrueerde de factuur te downloaden en in behandeling te nemen. Dat deed ze, en daarmee haalde ze onbewust een 'paard van Troje' binnen waarmee criminelen (naar verluidt opererend vanuit Oekraïne) de controle kregen over haar PC. Zo konden ze haar toetsaanslagen registreren en intellectuele eigendom van de onderneming stelen.

Stimuleer medewerkers om melding te maken van ongebruikelijke of verboden zaken. Dat kan technologie zijn – bijvoorbeeld een draagbare harde schijf die wordt aangetroffen in een kantoor waar medewerkers doorgaans alleen via het netwerk gegevens en software ophalen. Het kan ook gedrag zijn – bijvoorbeeld een medewerker of leverancier die naar vertrouwelijke bestanden vraagt waarvoor hij of zij geen bevoegdheid heeft. Medewerkers moeten hier even alert op zijn als passagiers dat moeten zijn op onbeheerde bagage in de vertrekhal van een luchthaven.

Kijk bij werving en selectie naar risico's

Het is nu belangrijker dan ooit om bij werving en selectie procedures en interviewtechnieken te gebruiken waarmee de eerlijkheid van sollicitanten kan worden ingeschat. Er kan worden nagegaan of iemand een strafblad heeft. Let op een verkeerde voorstelling van zaken in het cv. Stel in het sollicitatiegesprek vragen waarmee het 'moreel kompas' van een kandidaat kan worden gepeild. Ons team ontwikkelt testen waarmee werkgevers kunnen bepalen of sollicitanten riskante persoonlijkheidskenmerken hebben, zoals die welke het CPNI in kaart heeft gebracht.

Ook in het sollicitatiegesprek moet besef van informatie- en systeembeveiliging een aandachtspunt zijn. Weet de kandidaat wat de dreiging van binnenuit inhoudt? Zou hij wachtwoorden delen met een teamlid? Onder welke omstandigheden zou hij teamleden toestaan zijn computer te gebruiken met zijn identiteit? Een kandidaat die het ontbreekt aan het benodigde besef hierover kan worden aangenomen als hij of zij verder aan de eisen voldoet. Maar dan moet die nieuwe medewerker wel meteen wegwijs worden gemaakt in het beleid en de aanpak voor cyberveiligheid. Gaat het om een baan in een uiterst gevoelige omgeving? Dan is het nog maar de vraag of iemand met een tekortschietend risico- en veiligheidsbewustzijn wel in dienst moet worden genomen.

Hanteer strenge regels ten aanzien van onderaannemers

Zoals de inbraak bij winkelketen Target laat zien, is het belangrijk ervoor te zorgen dat de organisatie niet in de problemen wordt gebracht door leveranciers of distributeurs. Al het mogelijke moet worden gedaan om, bijvoorbeeld, te voorkomen dat een medewerker van een externe IT-leverancier een 'achterom' creëert in de systemen. Als het risico op een storing of inbraak bij een leverancier veel kleiner is dan bij de eigen organisatie, dan let die leverancier misschien ook minder streng op IT-beveiliging. Zoek partners en leveranciers met een vergelijkbare risicobereidheid en -cultuur als bij de eigen organisatie, zodat er meer kans is op een gemeenschappelijke aanpak op het gebied van cyberveiligheid.

Vraag potentiële leveranciers in de oriënterende gesprekken hoe zij omgaan met het *insider*-risico. Komt het tot een overeenkomst, controleer hen dan regelmatig om na te gaan of ze ook werkelijk zo (blijven) werken als ze hebben gezegd. Maak duidelijk dat u audits zult uitvoeren, en specificeer wat die zullen inhouden. Ook kan een onderneming leveranciers vragen dezelfde controles uit te voeren die ze zelf ook doet: verificatie van de achtergrond van sollicitanten (is er een strafblad, klopt het opgegeven arbeidsverleden?), bewaking van toegang tot gegevens en toepassingen om eventuele ongeoorloofde activiteiten tijdig te signaleren, en indringers weren uit gevoelige gebouwen of delen daarvan.

Houd toezicht op medewerkers

Maak medewerkers duidelijk dat de organisatie toezicht kan en zal houden op hun doen en laten met informatiesystemen voor zover de wet dit toestaat. De beveiliging van computersystemen kan niet volledig worden overgelaten aan deskundigen. De organisatie zal ook zelf scherper moeten toezien op binnenkomende en uitgaande gegevens. Eigen beveiligingsteams of dienstverleners moeten dus regelmatig risicobeoordelingen maken. Daarin moeten onder meer worden benoemd: bronnen van mogelijke bedreigingen, kwetsbare werknemers en netwerken, en de mogelijke gevolgen indien het risico werkelijkheid wordt. Ook is het belangrijk om risicowerend gedrag te meten, zoals responstijden bij waarschuwingen.

Routers of firewalls kunnen vaak uitgaande kanalen bewaken, maar een dergelijke functionaliteit moet wel worden geactiveerd. Beschikt de organisatie niet over de benodigde apparatuur om uitgaand verkeer te controleren, schaf die dan aan. Ook andere vormen van datavervoer moeten worden geregistreerd en gecontroleerd; denk aan USB-sticks en andere draagbare opslagmedia, afdrukken op papier enzovoort. Dit toezicht kan bestaan uit onaangekondigde controles op locaties of zelfs een permanente controle van iedereen die een gebouw betreedt of weer verlaat, net zoals op luchthavens gebeurt (General Electric en Wipro doen dit in Bangalore).

Wil bewaking doeltreffend kunnen zijn, dan moeten de privileges van alle werknemers scherp worden beheerd – ook degenen met het allerhoogste niveau aan toegangsrechten tot bedrijfssystemen, want zij zijn vaak de aanstichters van *insider*-aanvallen. De lijst van medewerkers met bij uitstek verreikende toegangsrechten moet met regelmaat worden uitgedund. Houd degenen die overblijven goed in de gaten om te zien of ze het vertrouwen inderdaad verdienen. Zoek naar systemen waarmee concrete insider-dreigingen kunnen worden opgespoord, zowel om mogelijk bedreigende handelingen te voorkomen als om ze op te sporen als ze toch hebben plaatsgevonden. Met behulp van Big Data kunnen aanwijzingen met elkaar in verband worden gebracht en waarschuwingen worden afgegeven.

Software om *malware* op te sporen kan nuttig zijn. Vooral wanneer externe partijen samen met iemand van binnenuit aan gegevens proberen te komen, is een belangrijke eerste stap vaak om *malware* te injecteren in het netwerk. Wordt er malware aangetroffen, wees dan bedacht op interne daders of medeplichtigen. Onderzoek wat de malware precies zou aanrichten in de systemen; dat kan aanwijzingen opleveren omtrent de identiteit en het uiteindelijke doel van de aanvaller.

Met een bewaking en toezicht van deze orde neemt de werkdruk natuurlijk voor iedereen toe. Daar staat echter tegenover dat de organisatie weerbaarder wordt en haar risico verkleint.

———

Wat is de meest effectieve strategie tegen cybercriminaliteit van (of met medeplichtigheid van) binnenuit? Natuurlijk is het belangrijk om alle beschikbare beveiligingstechnologie in te zetten. En natuurlijk moeten ook de zwakke plekken in technologie en systemen worden aangepakt. Maar het is vooral ook zaak dat alle *insiders* zich gedragen op een manier die de onderneming veilig houdt. Mensen moeten weten welk gedrag aanvaardbaar of onaanvaardbaar is. Het management kan hen duidelijk maken dat zij daarmee niet alleen de organisatie beschermen, maar ook hun eigen baan.

Over de auteurs

David M. Upton is hoogleraar Operations Management aan Said Business School van de universiteit van Oxford. Sadie Creese is hoogleraar cybersecurity in Oxford en leidt er ook het Global Cyber Security Capacity Centre. Upton en Creese leiden het onderzoeksprogramma *Corporate Insider Threat Detection* (Opsporing interne beveiligingsrisico's).

Translated and reprinted by permission of Harvard Business Review. This article was originally published under the English title 'The danger from within', by David M. Upton and Sadie Creese, in the September 2014 issue of the Harvard Business Review, vol. 92, issue 9, pp. 95-101. © 2014 Harvard Business School Publishing Corp. (Distributed by The New York Times Syndicate); all rights reserved. This translation, © 2014 Harvard Business School Publishing Corp. (Distributed by The New York Times Syndicate). Vertaling: Raymond Gijsen.