Malware: geautomatiseerde bedreigingen

Penninx, Wim

Publication date
2009

Published in
ICT Security in de praktijk

Citation (APA)
Penninx, W. (2009). Malware: geautomatiseerde bedreigingen. In A. Smulders, P. Verhagen, B. Jutte, & B. Jansse (Eds.), *ICT Security in de praktijk: voorbeelden en aanbevelingen van deskundigen* (pp. 63-68).

ICT Security in de praktijk

VOORBEELDEN EN AANBEVELINGEN VAN DESKUNDIGEN

ICT Security in de praktijk

VOORBEELDEN EN AANBEVELINGEN VAN DESKUNDIGEN

Colofon

Initiatiefnemer: ICT-Kring Delft
Uitgever: Mantaba Publishing
Sponsors: OGD, TNO, LBVD en ICT-Kring Delft
Ontwerp en vormgeving: Sjansen Design BNO
Druk: Thieme Print4U, Apeldoorn
ISBN/EAN: 978-90-814070-3-8
www.ictkring-delft.nl
info@ictkring-delft.nl

Voorwoord

Beste lezer,

U leest de eerste pagina van het ICT-securityboekje. Dit boekje biedt u de informatie om op een praktische manier de ICT-beveiliging van uw bedrijf te verbeteren. Het combineert de kennis van een groot aantal deskundige ICT-bedrijven en -organisaties die lid zijn van de ICT-Kring Delft. Deze organisatie heeft als doel om het netwerken tussen ICT-bedrijven te bevorderen en daarbij de kennis en kunde m.b.t. ICT te vergroten. Dit boekje is daar een mooi resultaat van.

Het gebruik van ICT is stevig ingebed in samenleving. Steeds meer worden bedrijfs- en productieprocessen afhankelijk van ICT, ook binnen het mkb. Dat heeft overduidelijk grote voordelen. Maar de gebruikers zijn zich nog weinig bewust van de kwetsbaarheid van ICT. Deze praktische handleiding kan aan dat bewustzijn bijdragen. Dat geeft de ondernemer uiteindelijk houvast bij het nemen van eventuele beveiligingsmaatregelen.
Intussen gaan de ontwikkelingen in ICT razendsnel door. En terwijl regelgeving uit Den Haag en Brussel snel achterop raakt bij de ontwikkeling van de techniek, wilt u kunnen blijven ondernemen. Ook MKB-Nederland & VNO-NCW spannen zich daarom, bij het ter perse gaan van dit boek, in de eerste plaats in om de administratieve lasten voortkomend uit de Wet bescherming persoonsgegevens (Wbp) zoveel mogelijk in te dammen. Denk aan het schrappen van schijnzekerheden, overbodige verplichtingen en nalevingkosten.

Tegelijkertijd loopt er een evaluatie van dezelfde Wbp en de Europese Privacy Richtlijn. De ondernemingskoepels zetten in op goede, heldere regelgeving op basis van risicomanagement en uitvoerbaarheid voor ondernemers.
Een boekje als dit komt niet zonder slag of stoot tot stand. Het werven van auteurs en het op elkaar afstemmen van de verschillende bijdragen is geen eenvoudige klus geweest voor de redactieleden. Zij deden dit werk bovendien naast hun drukke baan als ondernemer of ICT-specialist. Hierbij wil ik dan ook hartelijk danken voor hun inzet. Verder gaat mijn dank natuurlijk uit naar de auteurs die hun deskundigheid in een paar A4-tjes zo toegankelijk hebben opgeschreven. Hun tips en ervaringen zullen u zeker van pas komen. Als laatste gaat mijn dank uit naar de sponsors van het ICT-securityboekje, OGD, LBVD, TNO en de ICT-Kring. Zij hebben het mogelijk gemaakt om het boekje te drukken op papier, een medium dat toch nog steeds gebruikt wordt, en de auteurs te laten ondersteunen door een taaldeskundige.
Met de persoonlijke ervaringen, kennis en aanbevelingen die de experts in dit boek met u delen, kunt u zelf aan de slag om op een praktische manier met security om te gaan.

Ik wens u veel leesplezier,

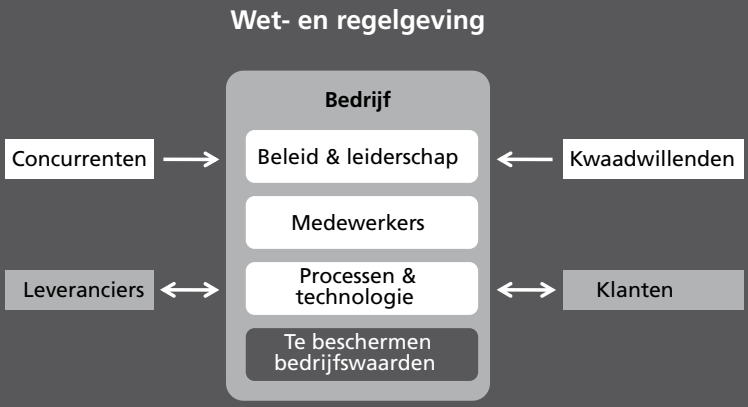
Leendert Jan Visser
Directeur MKB-Nederland

Inleiding

Het belang van de beveiliging van ICT-systemen neemt steeds verder toe. Niet alleen breidt het aantal technische mogelijkheden uit, maar ook neemt de hoeveelheid gevoelige gegevens die bedrijven opslaan steeds verder toe. Zo hebben tegenwoordig bijna alle bedrijven een uitgebreid relatiebeheersysteem en zijn de smartphones en PDA's met al hun mogelijkheden niet meer weg te denken uit het bedrijfsleven.
Dit boekje heeft als doel om systeembeheerders in het Midden- en Kleinbedrijf te helpen hun IT-systemen veiliger te maken. Het boekje is ook interessant voor managers en directeuren, omdat ook beveiligingsbeleid en het invoeren van veiligheidsmaatregelen in een bedrijf aan bod komt, een typische taak voor leidinggevenden. Het boekje is opgebouwd uit een paar grote onderdelen:

- *Beleid en Leiderschap:* hoe ziet ICT-securitybeleid eruit, hoe geeft u het vorm en hoe draagt u het uit?
- *Medewerkers:* hoe maakt u medewerkers bewust van beveiligingsrisico's en hoe voorkomt u incidenten?
- *Processen en Technologie:* welke processen en technologie heeft u en waarmee moet u rekening mee houden vanuit ICT-security oogpunt?

Belangrijk is dat het beveiligingsbeleid zich richt op de bescherming van zaken die waardevol zijn voor een bedrijf. Deze moeten zo goed mogelijk worden beschermd tegen de verschillende risicobronnen: concurrenten, kwaadwillenden, klanten en leveranciers. Daarnaast moet een bedrijf natuurlijk ook werken in overeenstemming met de wet-en regelgeving.



Visualisatie bedrijfsbeveiliging

Een groot aantal auteurs die lid zijn van de ICT-Kring Delft hebben een bijdrage geschreven voor dit boekje. Dit betekent dat u profiteert van de praktische ervaring van deze ICT-deskundigen. De opbouw van de verschillende bijdragen is gelijk. U krijgt altijd een overzicht van de problemen in een bepaald deelgebied van ICT security en u kunt lezen welke maatregelen u kunt nemen. Elk verhaal bevat bovendien een case-study van een fictief bedrijf waarin Ronald, de ICT systeembeheerder, een praktijkprobleem moet oplossen. De auteurs van het boekje hebben allen hun artikel geschreven op persoonlijke titel en onder de Creative Commons licentie. Succes en plezier met het lezen van dit ICT-securityboekje. Wij hopen, en verwachten, dat het de ICT-systemen van uw bedrijf veiliger maakt.

De redactie van *ICT security in de praktijk*
Andre Smulders, Pieter Verhagen, Bart Jutte en Birger Jansen

Inhoudsopgave

Ir. André Smulders (CISSP) - Senior Consultant Security - TNO ICT - www.tno.nl - andre.smulders@tno.nl

André is na zijn studie Technologie Management aan de TU Eindhoven in 1996 gestart in het werkveld van innovatie en ICT en specialiseert zich sinds 2000 in informatiebeveiliging. In zijn huidige rol als adviseur en projectleider heeft hij te maken met informatiebeveiligingsprojecten variërend van technologisch tot strategisch niveau.

Bewust risico nemen

Het belang van een risicoanalyse

Beveiligen is belangrijk, en u wilt uw eigen organisatie ook beveiligen. Maar waartegen? En hoe groot zijn de risico's die u loopt? Een goede beveiliging hangt samen met een juiste inschatting van wat waardevol is voor uw bedrijf en welke risico's u loopt. Dit vraagt om antwoorden op lastige vragen die daarom vaak worden genegeerd.
Inzicht in de risico's voor uw organisatie biedt handvatten om de juiste en doeltreffende maatregelen te nemen. Maatregelen hebben als doel om risico's te beperken. Het zomaar nemen van maatregelen leidt vrijwel altijd tot onnodige kosten en biedt vaak geen vermindering van de risico's. Met een beperkt aantal stappen is het mogelijk om deze impasse te doorbreken. Het doel is simpel. Maak de overstap van onbewust risico lopen naar bewust risico nemen.

Bepalen van risico's

Er zijn verscheidene methoden om vast te stellen welke risico's relevant zijn. Zo'n methode noemen we een risicoanalyse. Er bestaan veel verschillende risicoanalyses en minstens zoveel tools die deze ondersteunen. In essentie komen ze allemaal neer op de volgende stappen:

1. Bepalen wat van waarde is voor uw organisatie. Dit is eigenlijk een vraag die iedere ondernemer moet kunnen beantwoorden. Wat maakt u als ondernemer bijzonder en wat heeft u nodig om dit te behouden? Denk hierbij aan specifieke kennis, belangrijke productiemiddelen of sleutelpersonen binnen uw organisatie. We noemen dit assets.

2. Bepalen wat de impact is op uw organisatie als er wat misgaat met belangrijke assets. Denk hierbij aan de aspecten:
   - Vertrouwelijkheid (de asset wordt onbedoeld toegankelijk voor derden)
   - Beschikbaarheid (de asset is niet meer beschikbaar voor uw organisatie)
   - Integriteit (de asset werkt niet naar behoren)
3. Bepalen wat relevante risico's zijn. Welke assets zijn daadwerkelijk van belang en tegen welke gebeurtenissen wilt u zich beschermen? U dient vast te stellen aan welke gebeurtenissen u echt wat kunt en wilt doen. Vaak kunnen collega's u hierbij helpen. Misschien zijn er in de organisatie al zaken geregeld om de door u onderkende risico's te verminderen.
4. Actie ondernemen om maatregelen te treffen voor de risico's die u aan wilt pakken. Het is essentieel om daadwerkelijk actie te ondernemen om de geïdentificeerde risico's te beperken. Zo voorkomt u schade. Het kan gebeuren dat activiteiten heel veel tijd kosten of te duur zijn. Het is dan een goede keuze om een risico te accepteren in plaats van actie te ondernemen.

De risicoanalyse - 1

>> Martin van Rossem, directeur en eigenaar van een mkb-bedrijf, maakt zich zorgen. Hij hoort steeds vaker dat ICT-beveiliging belangrijk is, maar weet zelf erg weinig van ICT. Hij overweegt daarom om systeembeheerder Ronald de opdracht te geven de ICT-systemen veilig te maken. Het lastige is dat Martin niet kan beoordelen of Ronald onnodig geld besteedt aan maatregelen.

Een bevriende ondernemer geeft Martin de tip om na te denken over wat voor zijn bedrijf belangrijk is en waar zijn marktpositie van afhankelijk is. Daar heeft Martin uiteraard wel verstand van, hij heeft zijn onderneming tenslotte eigenhandig uit de grond gestampt en gemaakt tot het succesvolle bedrijf dat het nu is. Martin schrijft op Post-its de onderwerpen die voor het voortbestaan van zijn bedrijf belangrijk zijn – scherpe prijzen, snelheid van leveren en een positie als betrouwbare zakenpartner.

Martin weet uit ervaring dat de snelheid van leveren vaak de doorslag gegeven heeft bij het verwerven van opdrachten. Hij heeft hiermee in de markt een sterke reputatie opgebouwd. Deze snelheid kan echter op een aantal plekken in de organisatie in gevaar komen. Het probleem

kan zijn dat de opdrachten niet op tijd bij de productielijn aankomen. Ook kan de productielijn zelf uitvallen of er kan een verstoring optreden in het logistieke proces. Dat opdrachten niet op tijd bij de productielijn komen, is eigenlijk geen risico. Frits is een uitstekende verkoper en doet er absoluut alles aan om opdrachten in gang te zetten. Daarnaast heeft hij zijn laptop met internetverbinding en kan hij per telefoon of fax opdrachten doorgeven. Martin besluit dan ook hieraan geen extra aandacht te schenken. Verstoring van het productieproces is een waarschijnlijker probleem. Ronald heeft al eens opgemerkt dat een aantal systemen dat de productie aanstuurt sterk verouderd is. Gelukkig zijn die systemen nog nooit uitgevallen, maar Martin ziet wel in dat Ronald met een analyse moet komen wat de potentiële problemen en mogelijke oplossingen kunnen zijn. Hij besluit productiemanager John, die goed inzicht heeft in de werking van de productielijn, te vragen om Ronald te assisteren. Zo worden onnodige maatregelen voorkomen. Voor het logistieke proces voorziet Martin niet echt problemen. Naast zijn bedrijf zit een verhuurbedrijf dat busjes levert. Zijn zwager heeft een uitzendorganisatie die onder andere chauffeurs onder contract heeft. Mochten er problemen zijn met de distributie, dan is daar in zeer korte tijd wel een mouw aan te passen. Tevreden over zijn analyse en de stappen die hij bedacht heeft, leunt Martin achterover. Morgen kunnen Ronald en John tot actie overgaan. <<

Maatregelen

Om op de hoogte te zijn en te blijven van de risico's die uw organisatie loopt, is het aan te raden om net als Martin periodiek, bijvoorbeeld twee keer per jaar, na te denken over mogelijke risico's. Op het eerste gezicht lijkt dat ingewikkeld, maar het valt in de praktijk vaak mee. Er is geen enkele organisatie waar niets misgaat. Gebruik een incident dan ook om inzicht te krijgen in de risico's die u als ondernemer loopt. Stel daarbij de volgende vragen: wat ging er mis? Hoe erg was dat voor uw organisatie? Zijn de gevolgen beperkt omdat er maatregelen getroffen zijn of had u gewoon geluk dat het allemaal meeviel? Deze vragen komen in feite op hetzelfde neer als het stappenplan van de risicoanalyse. Het voordeel is dat u bij een incident een concreet voorbeeld heeft van wat er mis kan gaan.

Het uitvoeren van de eerste risicoanalyse is vaak het lastigst. De volgende keer dat u zo'n analyse uitvoert, kunt u zich richten op de

zaken die nieuw zijn voor uw organisatie. Zijn er wijzigingen in uw diensten of producten sinds de vorige keer? Stellen uw klanten andere eisen? Is het productieproces gewijzigd?

De risicoanalyse – 2

>> Hoe het is gebeurd, snapt Ronald nog steeds niet, maar eindelijk lijkt zijn directeur Martin het licht te hebben gezien. Hij had hem al vaker aangegeven dat de belangrijkste server verouderd was. Vervanging was noodzakelijk, maar tot nu toe was daar geen aandacht voor. Achteraf gezien ziet Ronald wel in dat hij nooit de link heeft gelegd met de potentiële impact voor het productieproces, zoals de directeur gisteren wel deed. Ronald maakt een afspraak met productiemanager John om samen na te gaan wat de risico's zijn bij het vervangen van de server.

"John, kun je me helpen om de risico's voor het productieproces in kaart te brengen?"

"Natuurlijk, en dan bekijken we daarna nog een aantal ideeën om een deel van het productieproces handmatig op te kunnen vangen."

Na een uur brainstormen zijn de belangrijkste risico's in kaart gebracht en is vastgesteld welke maatregelen ze moeten treffen om deze risico's te beperken. Gelukkig heeft John een gedetailleerd inzicht in de werking van het productieproces en komt hij met praktische oplossingen. Ronald werkt de maatregelen uit in een stappenplan voor het vervangen van de server. John heeft beloofd om het plan vervolgens kritisch te bekijken, zodat ze geen belangrijke risico's over het hoofd zien. Na het akkoord van John kan het plan naar Martin. Hopelijk keurt hij het vervangen van de server goed. <<

Meer weten

Even geen inspiratie of geen idee welke risico's u als organisatie op het gebied van ICT loopt? Kijk dan eens op sites met security-nieuws. Bekende websites zijn:

- http:// www.security.nl
- http:// www.securityfocus.nl

Alleen al het scannen van de koppen van de artikelen geeft u een goed idee van de mogelijke risico's voor uw organisatie.

Arthur de Jong - Software Engineer - West Consulting BV - www.west.nl - arthur@west.nl
Arthur is bij West Consulting BV onder andere verantwoordelijk voor het beheer van de technische infrastructuur, waarbij security een belangrijke rol speelt. Naast zijn werk is hij actief als Debian-ontwikkelaar waar hij een aantal open source tools onderhoudt.

Nico Plat - Technisch Directeur - West Consulting BV - www.west.nl - nico@west.nl
Nico studeerde informatica aan de TU Delft en promoveerde aan deze universiteit. Zijn professionele interesses richten zich - naast security - op formele methoden voor softwareontwikkeling en op bedrijfsarchitecturen.

Veilige webapplicaties

KWETSBAARHEIDSCANS ALS MANIER OM BEVEILIGINGSPROBLEMEN OP TE SPOREN

Inleiding

Tegenwoordig gebruikt iedereen internet. Consumenten boeken hun reizen via internet en bankieren online. Bedrijven bieden hun producten en diensten te koop aan en bieden hun klanten de gelegenheid om vragen te stellen of rapporten op te vragen.

Aan de voorkant is dit alles misschien de normaalste zaak van de wereld, maar aan de achterkant zorgt een complexe combinatie van software voor de dienstverlening. De gegevens van producten en klanten worden via het internet verstuurd en bewaard buiten het zicht van de eigenaren. Dit gebeurt met algemeen bekende constructies. Deze zijn gevoelig voor mensen die op zoek zijn naar de zwakke plekken om daarmee hun voordeel te behalen. Misbruik kan milde gevolgen hebben (enkele gebruikers ondervinden hinder en de beheerafdeling heeft extra werk om de problemen op te lossen) maar de consequenties kunnen net zo goed groot zijn. Privacygevoelige informatie kan op straat komen te liggen of een bedrijfskritische dienst is plotseling niet meer beschikbaar. Ook is het mogelijk dat er reputatieschade ontstaat door het publiek worden van vertrouwelijke informatie.

Dit hoofdstuk laat zien hoe dergelijke risico's te beperken zijn, met een minimum aan beheersinspanning en met oog voor continuïteit. Want de wereld staat niet stil en nieuwe kwetsbaarheden dienen zich continu aan...

Om een webapplicatie te beschermen tegen kwaadwillenden is het belangrijk om op de hoogte te blijven van kwetsbaarheden die zijn ontdekt. Vervolgens kun je de kwetsbaarheden verhelpen door het installeren van de beschikbaar gestelde 'security patches' of het opvolgen van de aanwijzingen van de leverancier. Voor veel software op client-pc's komen beveiligingsupdates beschikbaar die automatisch worden geïnstalleerd (denk aan Windows-updates). Voor server-software is dit minder vaak het geval. Daarom is het noodzakelijk om op de hoogte te blijven van de nieuwste beveiligingsproblemen, vooral bij systemen die via het internet toegankelijk zijn.

Organisaties die kunnen helpen om op de hoogte te blijven van ontdekte kwetsbaarheden in software zijn:

- CERT (http://www.cert.org/)
- SecurityFocus (http://www.securityfocus.com/)
- The SANS Institute (http://www.sans.org/)
- GOVCERT.NL van de Nederlandse overheid (http://www.govcert.nl/)
- Waarschuwingsdienst.nl (http://www.waarschuwingsdienst.nl/)

Een traditionele, maar ook arbeidsintensieve (lees: dure), manier om te controleren of de systeembeveiliging afdoende is, is het uitvoeren van een penetratietest. Dit is een gerichte aanval op een systeem door een deskundige, die specifiek op zoek gaat naar veiligheidsproblemen. Vaak is dit echter een eenmalige actie die niet meer dan een momentopname van de systeemveiligheid biedt.

Een alternatief is het gebruik van scanningtools voor kwetsbaarheid. Dergelijke tools zoeken naar bekende beveiligingsproblemen in veelgebruikte software, door te testen of de kenmerken van het beveiligingsprobleem in de onderzochte sofware terug te vinden zijn. Aanvallers gebruiken deze tools vaak om slecht beveiligde systemen te vinden.
Voor het controleren van systemen op bekende beveiligingsproblemen zijn tal van scanningtools beschikbaar, bijvoorbeeld:

- Nessus (http://www.nessus.org/nessus)
- OpenVAS (http://www.openvas.org/)
- Metasploit (http://www.metasploit.com/)
- Nmap (http://nmap.org/)
- Nikto (http://www.cirt.net/nikto2)

Deze tools leveren een schat aan informatie over zwakheden in configuraties en potentiële problemen met applicaties. Ook kunnen ze controleren of het systeem niet al gehackt is of dat er een 'backdoor' (toegangsmechanisme voor een aanvaller) geïnstalleerd is. Het vinden van de juiste tools en het installeren, configureren en uitvoeren ervan vergt echter veel tijd. Daarna moeten de resultaten nog geëvalueerd worden en dient gekeken te worden of er sprake is van meldingen die veilig te negeren zijn. Voor dit alles is specialistische kennis nodig.

Het uitvoeren van een kwetsbaarheidscan is bovendien geen eenmalige actie. Regelmatig worden er nieuwe fouten in de basissoftware gevonden. Het aantal nieuw ontdekte kwetsbaarheden stijgt nog jaarlijks en bedroeg in 2008 ruim 7400 (bron: IBM X-Force). Ook is een website niet statisch; installatie van nieuwe applicatieversies vindt plaats, configuraties worden aangepast, een applicatie wordt verwijderd maar blijft toch achter op de website (alleen verborgen) enzovoort. Regelmatig zo'n scan herhalen is dus noodzakelijk. Ook hier geldt dat de geïnvesteerde tijd, geld en energie moeten worden afgewogen tegen de risico's: zijn het risico en de potentiële schade zo groot dat het dit alles rechtvaardigt?

Webapplicaties beveiligen - 1

>> Martin surft al jaren regelmatig op het internet en zijn bedrijf heeft een website. Dat tegenwoordig veel meer mogelijk is, is ook hem niet ontgaan. Eigenlijk is het collega Jantine geweest die hem de ogen heeft geopend. Neem nou de organisatie van het zo succesvolle bedrijfsfeest in de Balkan. Daar was geen reisbureau meer aan te pas gekomen: de vliegreis, het hotel, en de skipassen waren allemaal via internet door Jantine geregeld en ook de betalingen waren via internet verricht. Gemak dient de mens. Daarna

ging het voor hem in een razend tempo. Als het even kan, koopt hij tegenwoordig via het internet en ook zijn bankzaken en verzekeringen regelt hij online. De volgende stap was snel gezet: ook het bedrijf moet toch van de nieuwe mogelijkheden van internet kunnen profiteren? De efficiënte IT-inzet zou de groei van het bedrijf ook vast ten goede komen. Tijdens een vrijdagmiddagborrel had Martin hier met salescollega Frits over gefilosofeerd en die begreep hem direct. Een veelgehoorde wens die Frits van hun klanten had opgepikt, was de mogelijkheid tot snel inzicht in de afgenomen producten en in de status van de bijbehorende servicecontracten. Een wens die perfect via het internet was te realiseren, vond zowel Martin als Frits. Ronald had het nieuwe initiatief positief benaderd, maar wat zijn eigen werk betreft was hij niet echt gerust. Hij moest nog denken aan een pas ontdekt probleem met Joomla, het bekende contentmanagementsysteem waarmee het bedrijf werkt. Een fout in de Joomla-software maakte het mogelijk dat kwaadwillenden via het account-activatiemechanisme het wachtwoord van de administrator konden aanpassen. Ronald was zich doodgeschrokken, toen hij bij toeval achter het bestaan van dit probleem kwam. Weer een nieuwe webapplicatie in huis betekende een grotere kans op beveiligingsproblemen. Als één van de concurrenten een dergelijk beveiligingsgat zou kunnen misbruiken en zichzelf zo toegang kon verschaffen tot product- en klantinformatie, dan is de ramp niet te overzien. En Ronald is hiervoor verantwoordelijk. Ronald besloot om deze reden vanaf nu nauwkeurig alle publicaties over ontdekte beveiligingslekken bij te houden en de adviezen om ze te verhelpen op te volgen. Een tijdrovend karwei. Misschien zou hij eens moeten voorstellen om een tweede systeembeheerder aan te stellen. Maar is er geen slimmere oplossing? <<

Maatregelen

Een bedrijf dat meer zekerheid wil hebben of de beveiliging van de via het internet beschikbare systemen op het juiste niveau is, kan er voor kiezen zelf de expertise in huis te halen en kwetsbaarheidscans uit te voeren. Voor het mkb is het echter veelal niet haalbaar om dit zelf te doen. Uitbesteden is dan een goede optie. Het voordeel daarvan is ook dat je relatief goedkoop toegang krijgt tot specialistische ken-

nis. De resultaten van zo'n scan zijn over het algemeen ook begrijpelijk weergegeven in de vorm van een rapport en vaak ontdaan van 'false positives' (ontdekte kwetsbaarheden die na onderzoek geen kwetsbaarheden blijken te zijn). De meeste rapporten geven ook informatie over de verschillen tussen opeenvolgende scans: nieuw ontdekte en opgeloste problemen. Voor het management wordt inzichtelijk hoe de beheerders de voorgestelde maatregelen opvolgen.

Wat deze opvolging betreft: ook hier zijn afwegingen te maken. Het kan best zijn dat er een probleem gevonden wordt dat in omvang beperkt is, maar waarvoor veel inspanning nodig is om het te verhelpen. Het kan heel goed zijn dat het niet de moeite loont om tijd (geld) aan het oplossen van een probleem te besteden.

Het laten uitvoeren van een kwetsbaarheidscan dekt een groot gedeelte van de risico's die webapplicaties met zich meebrengen af. Toch is het zaak een vals gevoel van veiligheid te vermijden. En wel om de volgende redenen:

- Kwetsbaarheidscans voeren alleen tests uit op basis van *bekende* beveiligingsproblemen. Er is dus altijd een achterstand op kwaadwillenden. Frequent scannen en de scans laten uitvoeren door een leverancier die zijn testset actueel houdt, kan dit risico verminderen.
- Webapplicaties maken niet alleen gebruik van generieke basissoftware (besturingssysteem, applicatieserver et cetera) maar ook van specifieke softwarecomponenten, zoals een data-warehouse-oplossing van een kleine leverancier. Kwetsbaarheidscans zullen over het algemeen geen tests uitvoeren die controleren op kwetsbaarheden in deze laatste categorie. Daarom worden deze vaak niet op deze manier ontdekt, ook al zijn ze wél bekend.
- Een scan is zo goed als de uigevoerde tests: je bent altijd afhankelijk van de kwaliteit van de leverancier.

Het uitvoeren van een kwetsbaarheidscan vindt bij voorkeur plaats in een rustige periode, zodat het dagelijks gebruik van de webapplicatie hier minimale hinder van ondervindt. Zeker na de eerste scan is het verstandig om te controleren of het gehele systeem nog naar behoren werkt. Overbelasting van servers of netwerkcomponenten is namelijk mogelijk (áls dat zo is, is dat uiteraard op zichzelf meteen een beveiligingsprobleem). Verder zijn er wellicht nog zaken als statistieken waar je rekening mee moet houden, zodat het na een scan het niet ineens lijkt of veel nieuwe bezoekers de site hebben bezocht.

Webapplicaties beveiligen – 2

>> Ronald had met een lichte vorm van ongerustheid uitgekeken naar de resultaten van de eerste scan. Er was hem verzekerd dat er niets mis kon gaan. Maar is uiteindelijk wel verantwoordelijk voor het gehele bedrijfsnetwerk. De ochtend na het uitvoeren van de scan kwam hij op kantoor en constateerde tot zijn genoegen dat er niets aan de hand was en dat alle systemen normaal functioneerden. Hij ging direct bij Jantine een kopje koffie drinken om haar deelgenoot te maken van de goede afloop, hoewel zij enthousiaster leek te zijn over de plannen voor een nieuw bedrijfsuitje. Een paar dagen later ontving Ronald het rapport met de bevindingen van de eerste scan. De uitkomst viel niet tegen, maar verraste Ronald wel: er waren drie kwetsbaarheden ontdekt die in de categorie 'ernstig' vielen. Eentje daarvan had betrekking op de Apache-webserver die het bedrijf al jarenlang voor zijn eigen website gebruikt. Ronald had met Martin afgesproken dat ze de uitkomst van de eerste scan samen zouden bespreken. Martin had het rapport van te voren doorgebladerd, maar begreep er weinig van. Wel triggerde het woord 'severe vulnerabilities' hem. Ze spraken daarom af dat Ronald met spoed de voorgestelde maatregelen zou uitvoeren. <<

Meer weten

Achtergrondinformatie over de in de case study genoemde kwetsbaarheid in Joomla:

- http://developer.joomla.org/security/news/241-20080801-core-password-remind-functionality.html
- http://www.compassdesigns.net/joomla-blog/Admin-Password-Reset-Vulnerability-in-Joomla-1.5.html
- http://www.milw0rm.com/exploits/6234

Er zijn veel tools beschikbaar voor het zelf uitvoeren van kwetsbaarheidscans. De kwaliteit ervan is wisselend, maar de website http://sectools.org/ is een goed startpunt om zo'n tool te vinden.

Voor meer algemene informatie over security-scanproducten:

- http://en.wikipedia.org/wiki/Web_Application_Security_Scanner
- http://en.wikipedia.org/wiki/Vulnerability_scanner
- http://netsecurity.about.com/cs/hackertools/a/aa030404.htm

Ten slotte, aanbieders van scanoplossingen zijn te vinden op:

- https://www.pcisecuritystandards.org/pdfs/asv_report.html
- http://cve.mitre.org/compatible/vulnerability_management.html

Alf Moens (MISM) - Corporate Information Security Officer - Delft University of Technology - www.tudelft.nl - a.t.g.moens@tudelft.nl

Sinds 2002 is Alf verantwoordelijk voor de informatiebeveiligingstrategie van de TU Delft. Daarnaast is hij programmamanager informatiebeveiliging bij SURFfoundation en voorzitter van SURFibo (de samenwerkende informatiebeveiligers van het Hoger Onderwijs). Alf heeft een bijzondere interesse in het meten van (de volwassenheid van) informatiebeveiliging en in bedrijfscontinuïteitsvraagstukken. In 2007 behaalde hij als eerste in Nederland de master titel in Information Security Management.

Security-beleid

WAT IS HET EN HOE MAAK JE HET?

Inleiding

Bedrijven en organisaties werken met informatie. Een modern bedrijf kan niet zonder informatie en ICT-apparatuur. En als wat mis gaat, zijn de gevolgen vaak ernstig. Hoe goed is een bedrijf hier op voorbereid? Wat kan en mag wel en wat niet? Zijn de gegevens beschermd tegen diefstal door fysieke inbraak en via internet? Mogen de medewerkers gebruikmaken van internet, en zo ja waarvoor? Mag ICT-apparatuur het bedrijfspand uit, is gebruik van usb-sticks toegestaan? Hoe voorkom je dat een kwaadwillende via een valse website jouw klanten oplicht?
Een security-beleid maakt duidelijk wat wel en niet kan en mag. Security-beleid helpt om de gevolgen van een calamiteit (brand, virusaanval, diefstal, grote stroomstoring, verlies van usb-stick) binnen de perken te houden, doordat vooraf al nagedacht is over dit soort problemen.

Uitgangspunten voor beleid

Het security-beleid omvat een aantal afspraken en uitgangspunten:

Welke informatie en welke ICT-systemen zijn belangrijk voor het bedrijf?
Wanneer je weet wat belangrijk is voor het bedrijf, kun je dit op de juiste manier beschermen. Je kunt dan beschermende maatregelen nemen om de gevolgen van een calamiteit te beperken. Het maken van een back-up en back-uppen op een andere plek maken het mogelijk na

een brand of diefstal weer snel de draad op te pakken. Bij het bepalen van het belang van informatie, wordt gekeken naar de belangrijkste bedrijfsprocessen en de rol die gegevens en informatiestromen daar in spelen. Als duidelijk is wat het belang van informatie is voor het bedrijf dan is het mogelijk passen maatregelen te bepalen om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie zeker te stellen. Gebruik een methode zoals in het hoofdstuk "Bewust Risico Nemen" is beschreven om hierin een juiste afweging te maken.

Wie is verantwoordelijk voor de beveiliging?
Het is niet zo dat één verantwoordelijke alles moet doen. Beveiliging is een zaak van iedereen; alle medewerkers en alle gasten. De verantwoordelijke persoon ziet toe dat iedereen zich aan de regels houdt en zorgt ervoor dat alles beschikbaar is om aan die regels te voldoen. Wanneer is afgesproken dat er altijd een virusscanner op de pc's moet draaien, dan zorgt de security-verantwoordelijke ervoor dat de software beschikbaar is.

Bestaat er specifieke wet- of regelgeving waar rekening mee gehouden moet worden? Stelt de overheid eisen?
Afhankelijk van de bedrijfstak kunnen dat er meer of minder zijn. Voor ieder bedrijf geldt de bewaarplicht van financiële gegevens. De Wet op de Persoonsgegevens (Privacywet) stelt eisen aan iedere database waar persoonsgegevens in staan: een klantenbestand, abonneeregistratie, een ledenadministratie, een datingsite. Vraag zo nodig na bij de branchevereniging of de Kamer van Koophandel welke regels voor uw organisatie van toepassing zijn.

Wat zijn de basisregels?
Hierin staat alles over het gebruik van firewalls, virusscanners, wachtwoorden, het niet delen van gebruikersnamen en onder welke voorwaarden thuiswerken toegestaan is.

Hoe houden we bij wat mis ging?
Door missers en bijna missers bij te houden, is te controleren of de opgestelde regels afdoende zijn. Als ondanks de virusscanner toch een pc gehackt is, dan dienen er aanvullende maatregelen genomen te worden om herhaling te voorkomen.

Hoe staat het met het beveiligingsbewustzijn?

Een security-beleid is waardeloos als het alleen maar in de la ligt. Alle betrokkenen moeten weten wat kan en mag. Breng het security-beleid geregeld onder de aandacht. Dat kan door de belangrijkste regels op een paar posters te zetten of op de schermachtergrond van de pc's.

Problemen met de virusscanner – 1

>> De licentie voor de virusscanner-updates is al een tijdje verlopen. Het is nodig een nieuwe aan te schaffen, maar het bedrijf loopt flink achter. Frits heeft weer eens een nieuwe softwaregimmick gevonden en op zijn laptop gezet. Nu krijgt hij om de haverklap pop-ups, waarin hem van alles te koop wordt aangeboden. Systeembeheerder Ronald zucht een paar keer diep en stapt bij de directeur naar binnen. Hij weet al dat het een moeilijke discussie gaat worden.

"We zijn weer toe aan een nieuwe jaarlicentie voor de virusscanner. Mag ik je handtekening onder deze bestelopdracht?", vraagt Ronald.

"Voor dit soort zaken heb ik nu geen tijd. Bovendien heb ik nooit virussen."

"Jij toevallig niet, maar bij Frits heb ik vorige week weer twee virussen verwijderd, omdat hij weer wat had gedownload. Zijn hele systeem was naar de Filistijnen. Met deze nieuwe versie van de virusscanner was dit niet gebeurd".

Martin zet zijn handtekening en Ronald kan voorlopig wat gaatjes dichten met de nieuwe virusscanner. <<

Het security-beleid legt de afspraken in grote lijnen vast. Dit kan aangevuld worden met meer detaillistische afspraken over:

- het internetgebruik.
- het gebruik van wachtwoorden.
- het maken van back-ups, ook voor laptops.
- het gebruik van (bedrijfs-)e-mail.

Voor de systeembeheerder geeft het beveiligingsbeleid heldere richtlijnen over wat wel en niet mag op de computersystemen:

- Wie krijgt toegang en met welke rechten?
- Wanneer voeren we software-updates uit?
- Hoe vaak maken we een back-up?
- Mogen er kopieën van het klantenbestand op laptop of usb-stick meegenomen worden?

Bij brancheverenigingen en op internet zijn veel voorbeelden te vinden van security-beleid. Een beleidstuk werkt echter pas als het van het bedrijf zelf is en daarop toegesneden. Al die voorbeelden kunnen goed dienen om ideeën op te doen en om stukken uit over te nemen. Het bedrijf zal zelf hieruit bewust keuzes moeten maken.
De opzet en implementatie van een security-beleid kent een aantal stappen. Het hier gepresenteerde stappenplan is gebaseerd op het stappenplan dat Digibewust voor het mkb ontwikkelde:

Stap 1: Voorbereiding
Maak in het bedrijf bekend wat er staat te gebeuren. Bepaal of er voldoende kennis beschikbaar is of dat hulp geboden is. Spreek af wie de verantwoordelijkheid op zich neemt voor de invoering en controle van de beveiliging.

Stap 2: Inventarisatie
Bepaal welke informatie en welke apparatuur beschermd moeten worden, denk hierbij ook aan software, speciale hardware zoals printers en scanners en de documentatie en procedures. Ga na welke bedreigingen een rol kunnen spelen en welke maatregelen reeds genomen zijn. Stel een prioriteitenlijst op van te beveiligen zaken. Een methode om deze inventarisatie te doen is beschreven in het hoofdstuk 'Bewust Risico Nemen'.

Stap 3: Plannen maken
Als bekend is wat beschermd moet worden en op welke manier, dan is de volgende stap om te kijken wat er moet gebeuren. Elk bedrijf heeft al enige beveiliging. Kijk in deze stap of de beveiliging afdoende is en maak een lijstje van waar de gaten zitten.

Stap 4: Uitvoeren

Voer de plannen uit in de volgorde zoals bepaald in de prioriteitenlijst van stap 2. Communiceer dit met alle betrokkenen en verzorg trainingen, voorlichting of opleidingen. Kies in het begin vooral verbeteringen die snel te realiseren zijn zodat snel resultaat zichtbaar is. Dan blijft iedereen enthousiast.

Stap 5: Controleren

Check geregeld wat de voortgang is en hoever je bent ten opzichte van het oorspronkelijke plan. Controleer of de verbeteringen ook het gewenste effect hebben en leg dit vast, dat zijn successen. Als je echt moet aantonen dat de beveiliging in orde is, kun je een audit laten doen. Controleer in elk geval bij de afronding van ieder plan of de vorige stappen het gewenste effect hebben.

Stap 6: Herhalen

Hanteer als stelregel om tenminste eenmaal per jaar de inventarisatie uit stap 2 te herhalen. In een jaar tijd kan veel veranderen, zowel in de bedreigingen van buitenaf als in de ontwikkeling van de bedrijfsactiviteiten: nieuwe klanten, nieuwe apparatuur of programmatuur, nieuwe producten of dienstverlening.

Problemen met de virusscanner – 2

>> Ronald heeft in het security-beleid laten vastleggen dat alle pc's en laptops altijd een up-to-date virusscanner moeten hebben. Ook mogen de bedrijfs-pc's niet voor privézaken gebruikt worden, zoals het downloaden van muziek en films. Martin vond het een goede zaak om dit soort dingen structureel te regelen en niet telkens ad hoc brandjes te hoeven blussen. Ronald heeft op basis van het beveiligingsbeleid een jaarlijks budget gekregen voor beveiligingszaken. Hiermee kan hij zelf virusscanners en andere tools aanschaffen die nodig zijn om de beveiliging up-to-date te houden. Hij heeft nu zelf de controle en kan zo voorkomen dat virusscanners verouderd raken en onvoldoende bescherming bieden. <<

Meer informatie?

- http://www.digibewust.nl/Bescherm_je_bedrijf
- http://www.ibpedia.nl
- http://www.pvib.nl

Ferdinand Helmann - Directeur - Porter Novelli - www.porternovelli.nl - fhelmann@porternovelli.nl

Ferdinand is directeur van de Nederlandse vestiging van het internationale communicatieadviesbureau Porter Novelli. Hij adviseert bedrijven en organisaties over vraagstukken op het gebied van reputatie, crisiscommunicatie, issues en public affairs. Hij is medeauteur van het boek 'Issuesmanagement, een Stappenplan', dat in 2007 is verschenen bij Uitgeverij Boom Onderwijs.

Reputatiemanagement

HOE EEN ONSCHULDIG TECHNISCH PROBLEEM KAN LEIDEN TOT EEN REPUTATIEDRAMA

Inleiding

Grote organisaties komen vaak negatief in het nieuws als een functionaris zijn usb-stick verliest of zijn computer bij het grofvuil zet. Ook kleine organisaties kunnen speelbal worden van de media. Als u niet oppast liggen uw bedrijfsgegevens (of nog erger uw klantgegevens) op straat. Wat moet u doen als de media nieuwswaarde ziet in de fouten die u heeft gemaakt, maar waar u geen erg in had? Keldert dan het imago van de onderneming waar u voor werkt? Is de negatieve meningvorming nog om te buigen en is van de nood een deugd te maken?

Dit hoofdstuk behandelt de risico's die kleven aan het onzorgvuldig omgaan met klantgegevens. Soms heeft een bedrijf geen weet van dit risico als het in goed vertrouwen taken delegeert aan andere organisaties.

Wat is reputatiemanagement?

Reputaties van mensen en bedrijven zijn gevoelige dingen. U kunt op het ene moment zeer goed bekend staan en op het volgende moment door de hele wereld verguisd worden. Als uw reputatie onder druk staat, kan de impact op de bedrijfsvoering enorm zijn. Reputatiemanagement is het bewust sturen op het realiseren van een reputatie bij in- en externe doelgroepen, die overeenkomt met de – gewenste – identiteit van de orga-

nisatie. Dat heeft betrekking op vele aspecten, zoals aantrekkingskracht van het merk, kwaliteit van producten of diensten, goed werkgeverschap, goede financiële positie, innovatiekracht, maatschappelijke betrokkenheid en duurzaam ondernemen, ethiek en leiderschap. Reputatie is een middel om u te onderscheiden van uw concurrenten, maar het is vooral ook een basis voor het vertrouwen dat de buitenwereld in u stelt.

Vaak kunt u rustig en weloverwogen bouwen aan de reputatie die u graag wilt hebben. Maar soms kan door een incident in één aspect van de bedrijfsvoering een groot probleem voor uw reputatie ontstaan. Bijvoorbeeld als er een lek in de ICT-beveiliging zit. Dan is sprake van een reputatiecrisis en komt crisiscommunicatie om de hoek kijken. Dat wil zeggen zodanige maatregelen nemen naar aanleiding van een plotselinge gebeurtenis, dat uw reputatie zo weinig mogelijk schade ondervindt of zo snel mogelijk herstelt.

De informatie ligt op straat – 1

>> Dinsdag 9 november 10.00 uur
Martin zit rustig achter zijn bureau met een kopje koffie. De verkopen gaan goed en de laatste tijd heeft hij producten kunnen leveren aan een aantal bekende Nederlanders, waaronder televisiepersoonlijkheden en bestuursleden van grote Nederlandse ondernemingen. Dat waren grote opdrachten. Het ging eigenlijk heel snel. Via een presentator van een bekend tv-programma ging het balletje rollen. Het bedrijf had bij hem thuis producten geleverd en geïnstalleerd en kennelijk naar tevredenheid. Want door mond-tot-mondreclame kwam hij toen terecht bij andere beroemdheden. Jammer eigenlijk dat hij dit in zijn reclame nooit zou kunnen gebruiken. In de contracten hebben de klanten dit punt van vertrouwelijkheid dan ook nadrukkelijk vast laten leggen.

Dinsdag 9 november 11.00 uur
Ronald is net met het onderhoud van de server bezig als hij wordt gebeld door Martin – in totale paniek. Een minuut later zit hij bij Martin op de kamer. Vriendelijkheden worden achterwege gelaten. "Hoe is het in vredesnaam mogelijk dat mensen zo maar van buitenaf in ons systeem kunnen", luidt de vraag van Martin.

"Maar dat kan helemaal niet", zegt Ronald verbijsterd. Toch had Martin net een zeer gerenommeerde klant aan de telefoon die beweert van wel. Die klant is gebeld door een journalist van een roddelblad. Die zegt dat hij zwart op wit heeft dat de klant producten van het bedrijf in zijn huis heeft laten installeren. En dat terwijl deze persoon altijd publiekelijk heeft beweerd dat hij dat niet wil. De journalist claimt dat hij de informatie uit het boekhoudsysteem van het bedrijf heeft kunnen halen… en die informatie klopt.

Dinsdag 9 november 11.10 uur
Iemand van het roddelblad belt op. De journalist wil graag wat informatie over producten die het bedrijf heeft geïnstalleerd bij verschillende bekende Nederlanders. Vooral in de beweegredenen en speciale wensen is hij geïnteresseerd. Martin handelt het telefoontje onhandig af door te zeggen dat hij geen commentaar heeft en hij hangt direct op.

Dinsdag 9 november 11.15 uur
"Dit wordt een ramp", zegt Martin tegen Ronald. "Hoe kan die journalist in ons systeem gekomen zijn?"
"Het enige wat ik kan bedenken is dat er iets mis is bij onze leverancier. Ze hebben hun boekhoudprogramma uitbesteed. Ik zal alles uitzoeken", belooft Ronald.

Dinsdag 9 november 11.30 uur
Opnieuw gaat de telefoon bij Martin. Het is een van de belangrijkste financiële dagbladen van Nederland. Zij hebben op de website van het roddelblad gezien dat een journalist daar vertrouwelijke gegevens over klanten uit het systeem van het bedrijf heeft kunnen halen. Ze gaan dit als case gebruiken voor een artikel over de kwaliteit van gegevensbeveiliging in Nederland. Ze hebben ook het College ter Bescherming van Persoonsgegevens en een aantal Tweede Kamerleden om commentaar gevraagd, evenals de brancheorganisatie waar het bedrijf lid van is en de ICT-Kring Delft. Ze willen graag een toelichting van Martin op het gebeurde en zijn ook benieuwd welke beveiligingen en ICT-gedragscodes het bedrijf hanteert om dit soort zaken te voorkomen. In verband met de deadline van de krant moet hij binnen een kwartier reageren. Martin belt Ronald. Maar Ronald weet het ook niet zo uit z'n hoofd.
"Ik moet het echt even uitzoeken. Over een uurtje weet ik meer", zegt hij. Maar over een uurtje is te laat… <<

Een crisis kan ook leiden tot een publiek debat. Dat gebeurt als het onderwerp van de crisis te maken heeft met een groter maatschappelijk vraagstuk. Bijvoorbeeld de vraag of wij in onze samenleving uit oogpunt van privacy kritisch genoeg omgaan met gegevensopslag. Dan kan de uitdaging voor een organisatie zijn om een zekere invloed te hebben op die maatschappelijke discussie. Maar meestal is dat het werkterrein van grote ondernemingen of brancheorganisaties.

Maatregelen

Natuurlijk is het in de case study te laat voor Martin want de media wachten niet. Dus kan zijn bedrijf behoorlijk negatieve publiciteit verwachten met alle mogelijke gevolgen van dien voor de business. En het is eigenlijk heel onnodig. Incidenten kunt u weliswaar niet altijd voorkomen, maar u kunt het vertrouwen van de markt wel behouden als u de oorzaak uitlegt en adequate maatregelen laat zien. Snelle communicatie is daarbij een sleutelbegrip. Dat wil zeggen: ervoor zorgen dat u een verhaal heeft en dat u de kanalen heeft om dat verhaal te vertellen.

Wat Martin's bedrijf in dit geval paraat had moeten hebben, is een uitleg hoe de procedures werken. Bijvoorbeeld een gedragscode voor eigen medewerkers over hoe om te gaan met vertrouwelijke klantgegevens en de interne maatregelen om de naleving van die code te waarborgen. En in dit geval misschien nog belangrijker: harde afspraken ter waarborging van gegevensbescherming bij de leveranciers aan wie u een deel van de bedrijfsvoering uitbesteedt. Daarnaast is het belangrijk om snel een overzicht van media en belangrijke externe stakeholders beschikbaar te hebben met wie u desgewenst contact kunt opnemen.

Als Martin onmiddellijk over dit soort gegevens had beschikt, was hij beter in staat geweest om adequaat en snel te reageren naar klanten, media en andere externe belanghebbenden. Wat hij in dit stadium tegen de krant had kunnen zeggen, is dat de gebeurtenis volstrekt in strijd is met het beleid van zijn organisatie. Hij had kunnen toelichten welke waarborgen het bedrijf in acht neemt, dat er direct een onderzoek gestart zou worden en dat hij onmiddellijk adequate maatregelen

zou nemen ter voorkoming van verdere schade. Daarna had hij direct contact kunnen opnemen met de klanten die in de publiciteit zouden komen en met andere belangrijke relaties. Daarmee had hij de negatieve impact niet voorkomen maar zeker wel beperkt.

De informatie ligt op straat – 2

>> Dinsdag 16 november 15.00 uur
Een week later. Martin en Ronald zitten weer bij elkaar. De hele zaak is inmiddels duidelijk. Het bedrijf aan wie het boekhoudprogramma is uitbesteed, had een fout in de beveiliging gemaakt. De fout was snel gevonden en hersteld. Martin heeft de krant gebeld en alle organisaties die zich in het krantenartikel nogal smalend hebben uitgelaten over zijn bedrijf. Ook heeft hij een brief met excuses geschreven naar de gedupeerde klanten. De zaak is met een sisser afgelopen, maar dat was eigenlijk meer geluk dan wijsheid. Inmiddels heeft Ronald een interne ICT-gedragscode ontwikkeld en een code voor externe leveranciers, die aan de contracten gekoppeld is. Martin heeft al deze gegevens in zijn bureau, evenals de namen en adressen van belangrijke mensen en organisaties op het gebied van ICT en ICT-beveiliging. Als zoiets weer gebeurt is het vervelend, maar zou het wel voor minder paniek zorgen. <<

Meer weten

- www.businessissues.nl (artikelen en info)
- www.porternovelli.nl (adviesbureau)

Mark Krul - ICT-lawyer - GMW Advocaten - www.gmw.nl - m.krul@gmw.nl

Mark studeerde rechten aan de Universiteit van Leiden. Momenteel is hij ICT-jurist bij GMW Advocaten. Hier houdt hij zich bezig met ICT-recht, advisering van ICT-ondernemers op het gebied van ICT-contracten, e-commerce, privacy en het voeren van procedures.

Compliance wet- en regelgeving: privacygevoelige gegevens

BESCHERMING VAN PRIVACYGEVOELIGE GEGEVENS

Inleiding

Iedere ondernemer beveiligt in meer of mindere mate zijn bedrijfsgegevens. Denk aan klantgegevens die niet in handen mogen komen van de concurrentie. Waar bedrijven soms niet bij stilstaan, is dat de klantgegevens ook persoonsgegevens bevatten. Als dat zo is, dient te worden voldaan aan de verplichtingen uit de Wet bescherming persoonsgegevens (Wbp). Over die verplichtingen gaat dit hoofdstuk. Wij besteden daarbij aandacht aan de eisen die de Wbp stelt aan een deugdelijke beveiliging.

Het College bescherming persoonsgegevens
De instantie die toezicht houdt op de naleving van de regels is het College bescherming persoonsgegevens (Cbp). Het college kan handhavend optreden tegen een ieder die zich niet houdt aan de Wbp. Zo heeft het college de mogelijkheid bestuursdwang toe te passen en boetes op te leggen.

Op wie legt de wet verplichtingen?
De Wbp is van toepassing op een ieder die persoonsgegevens verwerkt. Daarbij rusten de meeste verplichtingen op de 'verantwoordelijke'. Dit is de medewerker binnen een onderneming die bepaalt welke persoonsgegevens worden gebruikt en voor welk doel. Wat zijn nu persoonsgegevens en wanneer is sprake van een verwerking?

Persoonsgegevens

Persoonsgegevens zijn alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon. Voorbeelden van persoonsgegevens zijn iemands naam of geboortedatum. Maar het gaat verder dan dat. Het gaat om alle gegevens op basis waarvan een natuurlijk persoon te herleiden is. Ook een IP-adres is een persoonsgegeven omdat aan de hand daarvan een individueel persoon door bijvoorbeeld een internetserviceprovider is te identificeren. Denk ook aan de profielgegevens op websites als Hyves en LinkedIn. U moet onthouden dat er al snel sprake is van een persoonsgegeven in de zin van de Wbp.

Gegevens over ondernemingen of organisaties zijn in de regel geen persoonsgegevens. Indien in uw klantenbestand alleen ondernemingen voorkomen, dan bevat deze geen persoonsgegevens. Als u informatie opneemt over uw vaste contactpersoon bij die ondernemingen, dan is er wel sprake van persoonsgegevens en moet u voldoen aan de eisen die de Wbp stelt.

Verwerking persoonsgegevens

Ook van een verwerking is snel sprake. Dit is bijvoorbeeld het verzamelen, vastleggen en ordenen van gegevens, maar ook het bewaren, bijwerken en wijzigen daarvan. Eigenlijk is elke geautomatiseerde handeling met een persoonsgegeven een verwerking.

Door de snelle ontwikkelingen op ICT-gebied ontstaan bovendien steeds nieuwe manieren van verwerking van persoonsgegevens. Denk bijvoorbeeld aan RFID, sociale-netwerksites en zoekmachines. Bij nieuwe toepassingen is vaak niet direct duidelijk hoe de wettelijke regels moeten worden toegepast. Uitgangspunt is dat de offline privacyregels ook online gelden.

Meldingsplicht

Een belangrijke verplichting is de meldingsplicht. Indien u persoonsgegevens verwerkt, dient u de verwerking te melden bij het Cbp. De melding moet plaatsvinden voordat u begint met de verwerking. Op de website van het Cbp (www.cbpweb.nl) staat vermeld op welke wijze u de verwerking kunt melden. Als u de verwerking niet meldt, kan het Cbp u een boete opleggen.

De meldingsplicht geldt overigens niet voor alle soorten van verwerking. Als de verwerking valt onder de vrijstellingsregeling hoeft die niet te worden gemeld. Onder de vrijstellingsregeling vallen bijvoorbeeld verwerkingen van klant- en personeelsgegevens, maar ook verwerkingen ten dienste van het interne beheer van uw organisatie, zoals verwerkingen met betrekking tot netwerk- en computersystemen, communicatieapparatuur en toegangscontrole. De vrijstellingsregeling is te vinden op de website van het Cbp. Ook als u geen meldingsplicht heeft moet u voldoen aan de eisen uit de Wbp.

Wat zijn de wettelijke eisen?
De hoofdregel van de Wbp is dat de verwerking van persoonsgegevens behoorlijk en zorgvuldig en in overeenstemming met de wet moet zijn. Dat betekent onder andere dat u persoonsgegevens alleen mag verwerken voor een vooraf door u gedefinieerd doel. U zult voordat u begint met de verwerking van persoonsgegevens op papier moeten zetten voor welk doel u de persoonsgegevens wilt verwerken. Daarbij moet u zich afvragen of u niet met minder gegevens of zelfs met anonieme gegevens kunt volstaan.

Het doel van de verwerking moet gerechtvaardigd zijn. Daarvan is onder andere sprake als voor de verwerking toestemming verkregen is van degene waarop de persoonsgegevens betrekking hebben (de betrokkene) of als de verwerking nodig is om een overeenkomst uit te voeren. De verwerking van bijvoorbeeld personeelsgegevens en klantgegevens zullen in het algemeen terug te voeren zijn op een rechtvaardigingsgrond.

Indien u een doel heeft om persoonsgegevens te verwerken en u een rechtvaardigingsgrond heeft voor de verwerking, zult u vervolgens moeten voldoen aan de overige wettelijke eisen. Die eisen zijn onder meer dat u iedere betrokkene inzage moeten geven in zijn persoonsgegevens als hij daarom verzoekt en u gegevens actueel dient te houden. Als u niet aan deze verplichtingen voldoet, kan de betrokkene een klacht tegen u indienen bij het Cbp. Het Cbp kan u dan vervolgens bestuursdwang aanzeggen of een boete opleggen.

Belangrijke eis: verplichte beveiliging

Een belangrijke verplichting is de plicht van beveiliging (artikel 13 Wbp). Deze verplichting houdt in dat u passende technische en organisatorische maatregelen moet nemen om het verlies van gegevens of onrechtmatig gebruik tegen te gaan.

Onder technische maatregelen wordt in ieder geval verstaan de logische en fysieke maatregelen in en rondom de informatiesystemen, zoals toegangscontroles en gegevensversleuteling. De organisatorische maatregelen kunnen bijvoorbeeld inhouden dat maar een beperkt aantal personen toegang heeft tot uw computersysteem, al dan niet met gebruikmaking van wachtwoorden.

Wat precies moet worden verstaan onder 'passende' maatregelen blijkt niet uit de wet. De wet geeft slechts een algemene beschrijving. In de Handleiding voor verwerkers van persoonsgegevens - te vinden op de website van het Cbp - staat wel een toelichting, maar ook die is vrij algemeen. De reden hiervan is dat het afhangt van specifieke omstandigheden welke mate van beveiliging 'passend' is. Voor iedere verwerking van persoonsgegevens zult u dus moeten inventariseren welke technische en organisatorische maatregelen u dient te nemen om een passend beveiligingsniveau te bereiken. Bij die inventarisatie zult u de risico's van de verwerking en de aard van de te beschermen gegevens mee moeten wegen. Uitgangspunt is dat hoe gevoeliger de gegevens zijn, hoe zwaarder de beveiliging moet zijn die u toepast . U moet ook rekening houden met de stand van de techniek en de kosten van de maatregelen. Dat betekent ook dat u periodiek moet nagaan of uw systeem aanpassing behoeft, bijvoorbeeld omdat er nieuwe ICT-mogelijkheden beschikbaar zijn.

In de andere hoofdstukken in dit boek wordt al vrij gedetailleerd aangegeven welke beveiligingsmaatregelen u kunt nemen. U weet nu waarom het belangrijk is dat u uw gegevens beveiligd. Niet alleen om gevoelige gegevens te beschermen tegen concurrenten maar ook om te kunnen voldoen aan de eisen van de Wet bescherming persoonsgegevens.

De verdwenen laptop – 1

>> Frits, de topverkoper van het bedrijf van Martin, is blij, erg blij. Hij heeft net de deal van het jaar gesloten met een grote klant. Hij loopt naar zijn auto en zijn gezicht betrekt. De ruit van zijn nieuwe auto ligt aan diggelen. En wat nog erger is, zijn laptop – met daarop alle klantgegevens – is van de achterbank verdwenen. Gelukkig heeft hij de usb-stick nog met een back-up van die gegevens. Hij zoekt in zijn jaszak en constateert dat er een klein gat in zit. Weg usb-stick. Frits rijdt terug naar kantoor. Zijn feeststemming is behoorlijk getemperd, maar hij weet zich gesterkt door de wetenschap dat de klantgegevens ook op zijn kantoorcomputer staan.

Martin, na drie weken nog steeds zeer blij met de nieuwe topklant, krijgt de schrik van zijn leven. De directeur van een zeer gerenommeerde klant belde zojuist met de mededeling dat hij door een concurrerend bedrijf was gebeld. Die had een uitermate voordelig aanbod gedaan. Bovendien beschikte dit bedrijf ook nog eens over vertrouwelijke omzetgegevens van de klant en de namen van contactpersonen. Op die manier was de concurrent uitstekend in staat een zeer voordelig aanbod te doen. Martin biedt de klant zijn excuses aan en onderneemt direct actie om een herhaling te voorkomen. <<

Maatregelen

Deze casus onderstreept het belang van een beleid gericht op de omgang met persoonsgegevens. Het gaat niet alleen om commerciële belangen, maar ook om privacybelangen. Door het opslaan van namen van contactpersonen van de betreffende klant speelt de Wbp ineens een grote rol. Het verwerken van deze gegevens is toegestaan omdat de verwerking van klantgegevens onder de vrijstellingsregeling van de Wbp valt. Het gebruik van deze gegevens dient echter te voldoen aan de eisen van de Wbp. Martin zal als directeur aangemerkt moeten worden als verantwoordelijke in de zin van de Wbp. Zodoende is hij verplicht technische en organisatorische maatregelen te nemen om de gegevens te beschermen en situaties als in de case study te voorkomen.

De verdwenen laptop – 2

>> Martin heeft inmiddels maatregelen genomen. Er is beleid gemaakt over de omgang met persoonsgegevens. Niet iedereen heeft nu zomaar toegang tot de klantgegevens. Alleen de personen die voor de uitvoering van hun werk moeten kunnen beschikken over de klantgegevens hebben die mogelijkheid. Bovendien heeft systeembeheerder Ronald ervoor gezorgd dat alleen na invoering van een wachtwoord de klantgegevens te zien zijn. Het gebruik van usb-sticks buiten het bedrijf is verboden. Ook zijn strenge eisen gesteld aan het gebruik van laptops met daarop bedrijfsgegevens. <<

Hans Baars CISSP, CISM - Security Architect - Enexis BV - www.enexis.nl - j.h.baars@blixt.nl

Sinds 1999 is Hans werkzaam geweest als informatiebeveiligingfunctionaris en intern auditor bij het Korps landelijke politiediensten. Daarna heeft hij twee jaar als (senior) consultant bij 3-Angle Software & Services in Amstelveen gewerkt en een jaar als senior consultant bij Strict BV te Vianen. Vanaf september 2009 is Hans security-architect bij Enexis BV te Rosmalen.

Factor mens

Inleiding

De factor 'mens' is de meest onberekenbare factor binnen een bedrijf. Het maakt daarbij niets uit of we het hebben over een multinational met tienduizenden werknemers, of een bedrijf met vijftien medewerkers. Een enkele uitzondering daargelaten – waar medewerkers een vooropgezet plan hebben om informatie te verzamelen en naar buiten te smokkelen (bedrijfsspionage) – komen eigenlijk alle medewerkers met de beste bedoelingen bij hun nieuwe baas werken.

Omstandigheden kunnen echter veranderen. De relatie tussen chef en medewerker wordt verstoord of een medewerker krijgt geldnood, waardoor het aanbod van iemand om informatie te verkopen interessant wordt. Reorganisaties kunnen ertoe leiden dat een medewerker er op achteruit gaat, of ontslagen wordt. Kortom: allerlei omstandigheden kunnen ervoor zorgen dat de houding van de eens zo loyale medewerker verandert.

Dit hoofdstuk gaat over de factor mens als factor die bewust schade aanricht aan een organisatie en wat u kunt ondernemen om die schade te voorkomen. Het gaat zoals gezegd om bewust aangerichte schade. Onbewust aangerichte schade valt onder de categorie 'bewustwording', dat in een afzonderlijk hoofdstuk behandeld wordt.

De factor mens, de meest onberekenbare factor

Een mkb-bedrijf krijgt met alle factoren te maken die ook in grote bedrijven voorkomen. Wat informatiebeveiliging betreft, maakt het echt niet uit of je in een bedrijf met tien medewerkers werkt of in een groot bedrijf met honderden, zo niet duizenden medewerkers. Deels zijn problemen op dit gebied op te lossen door ervoor te zorgen dat de medewerkers beveiliging als een logisch onderdeel van hun werkzaamheden beschouwen. Anderzijds maakt het ook uit met wat voor informatie gewerkt wordt. Bij het bedrijf uit de case study is, ondanks het beperkte aantal medewerkers, veel gevoelige informatie aanwezig. Die informatie heeft betrekking op de privacygegevens van klanten, technische tekeningen van zelf ontworpen en gepatenteerde producten en gegevens over de financiële stand van zaken binnen het bedrijf. Directeur Martin heeft informatiebeveiliging altijd als een ICT-aangelegenheid beschouwd. Informatiebeveiliging gaat immers over het instellen van de firewall en het installeren van een virusscanner. Daarom heeft hij Ronald, de systeembeheerder en diens voorganger, de verantwoording over informatiebeveiliging gegeven.

Toch is er wat veranderd sinds de komst van Ronald. Martin heeft ondervonden dat de mens van de ene dag op de andere kan veranderen. Mensen blijken dan plotseling anders te zijn dan je denkt en verwacht. Door informatiebeveiliging op de juiste manier in een organisatie in te richten komt men tot een paar ontdekkingen…

Informatiebeveiliging gaat over meer dan alleen een goed werkende firewall en virusdetectie voor e-mail. Het zorgt er ook voor dat de medewerker die plotseling meer wil dan goed is voor het bedrijf tijdig wordt ontdekt. En nog beter: het voorkomt dat een medewerker zijn loyaliteit laat varen.

De logic bom-1

>> Ronald is nog maar kort in dienst bij Martin. Hij werkt er nu drie maanden en iedere keer dat hij vraagt waar de vorige systeembeheerder is gebleven, wordt er wat onduidelijk gedaan en krijgt hij te horen dat die nogal onverwacht vertrokken is. Ronald vraagt het zich om diverse redenen af. De eerste en belangrijkste reden is informatie over bepaalde netwerkconfiguraties; beslissingen die genomen zijn bij de inrichting van het totale computersysteem. De tweede reden is de wantrouwigheid die hij bij Martin voelt, als hij het heeft over zijn werk en de mogelijkheden die hij binnen het computersysteem heeft.

Op een goede maandagochtend besluit hij het onderwerp aan te snijden. Hij vraagt Martin op de man af waarom hij geen contact kan opnemen met zijn voorganger. Martin denkt even na en zegt dan dat hij na de koffie maar even in zijn kantoor moet komen.

Meteen na de koffie gaan beiden naar het kantoor van Martin waar het hoge woord er uit komt. Na een korte periode waarin de systeembeheerder Jan en Martin het goed met elkaar hadden kunnen vinden, had Jan om een salarisverhoging gevraagd. Martin had die salarisverhoging geweigerd. Zijn reactie was gebaseerd op het feit dat Jan pas twee maanden voor hem werkte en hij van mening is dat salarisverhogingen pas na een jaar bespreekbaar zijn. Hierop was Jan boos het kantoor uitgegaan. Vanaf dat moment was hun verhouding slecht geworden. Jan liet alles liggen wat hij moest doen. Nieuwe medewerkers moesten dagen op een account wachten en twee maal ging data verloren omdat er door een fout geen back-up bleek te zijn. De problemen liepen zo hoog op dat, ook na een indringend gesprek tussen Martin en Jan, het besluit viel om de proeftijd niet te verlengen. Martin had Jan van het besluit op de hoogte gesteld. Hij had nog drie weken te werken voor het contract af liep.

De volgende dag kwam Jan niet op kantoor en was ook niet bereikbaar. Na drie dagen kwam Frits geschrokken bij Martin binnen. Hij was in een verkoopgesprek geweest en wilde productinformatie opvragen. Op geen enkele zoekopdracht kwam de gezochte informatie naar voren. Hij had ook financiële informatie over de klant waarmee hij in gesprek was nodig, maar het CRM-systeem startte niet op. Hij had het gesprek afgerond en was daarop naar Martin gegaan omdat Jan niet aanwezig bleek te zijn.

Terwijl Martin en Frits in gesprek waren, kwam Jantine binnen lopen. Ook zij had geen toegang meer tot de CRM-applicatie.

Na uitvoerig overleg werd besloten de leverancier van de CRM-applicatie te benaderen en daar het probleem voor te leggen. De leverancier was bereid om een van de ontwikkelaars te laten komen om uit te zoeken waar het probleem lag. Na vele uren zoekwerk werd duidelijk wat er gebeurd was. Jan had een zogenaamde logic bomb in het systeem geplaatst. Een logic bomb is software die als een soort bom op een van te voren ingesteld moment (tijdstip of handeling in het systeem) tot ontploffing komt en op dat moment grote schade aan het systeem aanbrengt.

De ontwikkelaar kon aan de hand van door hem ingebouwde logging, waarin alle handelingen van systeembeheerders worden vastgelegd, aantonen dat Jan de logic bomb had geplaatst. De bom was geactiveerd door het inloggen van Frits en had op dat moment alle gebruikersnamen en de inhoud van de database gewist. Hierdoor was het niet meer mogelijk in het systeem in te loggen. Was dat wel mogelijk geweest, dan had de ingelogde medewerker geen gegevens meer in het systeem aangetroffen.

Gelukkig was de CRM-applicatie pas enkele maanden in gebruik en werd er dagelijks, in de nachtelijke uren een back-up gemaakt. De ontwikkelaar kon de logic bomb verwijderen en vervolgens een goede back-up terug plaatsen, waarna de CRM-applicatie weer beschikbaar was. <<

Maatregelen

Insiders kunnen vanuit informatiebeveiligingsoogpunt dus veel schade aanrichten. Medewerkers kennen de organisatie en dus ook de zwakke plekken. Zij weten waar vitale informatie te vinden is. Is de directeur afwezig, dan kun je ongemerkt zijn kamer inlopen en in de lades en het postbakje kijken. In het hoofdstuk bewustwording is al het nodige gezegd over het beveiligingsgevoel van medewerkers en hoe daarmee om te gaan. Bewustwording is echter voornamelijk gericht op de goedwillende medewerker. Heeft u te maken met medewerkers die bewust schade willen aanrichten, dan is het moeilijk om u daar tegen te wapenen. Toch zijn er zaken die geregeld kunnen worden om de kans op bewust aangerichte schade in ieder geval in te perken.

Maatregelen tegen misbruik insiders

Een bedrijf kan de volgende beveiligingsmaatregelen nemen om risico's tegen bewust misbruik te voorkomen.

1. Beperk het aantal medewerkers dat u echt vertrouwt. Hiermee wordt bedoeld dat u het aantal medewerkers dat alle rechten op de informatiesystemen heeft, zo beperkt mogelijk moet houden. Medewerkers met alle systeemrechten kunnen veel schade aanrichten.
2. Zorg ervoor dat medewerkers in een functie die veel vertrouwen nodig hebben, ook werkelijk betrouwbaar zijn. Dit is het idee achter screening of het overleggen van een Verklaring van Onbesproken Gedrag, dat bij het ministerie van Justitie door tussenkomst van de gemeente wordt afgegeven. Ook navraag bij de vorige (huidige) werkgever kan bijdragen aan het gevoel van veiligheid.
3. Beperk de hoeveelheid rechten die iedere medewerker heeft. Dit wordt compartimentering genoemd. Dit betekent dat de medewerker, als hij schade aan wil richten, maar een beperkte schade aan kan richten. Zorg er daarom voor dat medewerkers sleutels krijgen waarmee zij alleen hun kantoor kunnen openen, wachtwoorden waarmee zij alleen hun account kunnen activeren en binnen dat account alleen over de informatie beschikken die voor hun taak van belang is. Dit laatste wordt ook wel het need-to-know-principe genoemd.
4. Geef medewerkers overlappende rechten. Het gaat hier om het zogenaamde vier-ogen-principe. Hierbij vindt controle op elkaars werkzaamheden plaats. Gebruikelijk is bijvoorbeeld dat een administratieve (financiële) medewerker bepaalde bedragen ongecontroleerd over mag maken. Wanneer ze echter hoge bedragen moeten overmaken, dan is er een controle door een collega nodig die vervolgens de overboeking moet accorderen. Hiermee wordt voorkomen dat een collega de bankrekening van het bedrijf naar de Kaaimaneilanden overboekt en er zelf een enkele reis achteraan neemt. Hierbij is het zaak niet over het hoofd te zien dat het overboeken van vele (zeer) lage bedragen ook niet de bedoeling is. Hetzelfde geldt voor systeembeheerders die zeer schadelijke acties op systemen kunnen uitvoeren. Bouw ook hier een vier-ogen-principe in. Dan kan een logic bomb zoals Jan in het systeem plaatste niet, of veel moeilijker, worden geplaatst. Vaak is

een langere vakantieperiode, waarbij het werk van een frauderende medewerker door een collega over wordt genomen, het juiste moment om te ontdekken wat er binnen het bedrijf gebeurt.

5. Ontdek een barst in de beveiliging in een zo vroeg mogelijk stadium en besteedt er direct aandacht aan. Bouw daarom zoveel mogelijk controlemogelijkheden in om te signaleren wanneer er risicovolle acties in het systeem plaatsvinden. Wanneer een vergrijp ernstig genoeg is, schakel dan de politie in. Dit is meteen een signaal naar andere medewerkers met kwade bedoelingen. U neemt het serieus en accepteert dit soort inbreuken niet. U heeft vertrouwen in de medewerkers en wilt dat vertrouwen immers niet beschaamd zien.

Het monitoren van systemen en regelmatige controles (audits) brengen beveiligingsinbreuken vaak in een vroeg stadium aan het licht.

De logic bom – 2

>> Het gevolg van de sabotage van de vorige systeembeheerder was dat Martin erg wantrouwig is geworden naar de nieuwe systeembeheerder. Hij weet immers welke macht die medewerker binnen zijn bedrijf kan uitoefenen. Hij vertelt dat hij Ronald alle vertrouwen wil schenken, maar dat dat wel heel veel moeite kost.

Voor Ronald is nu veel duidelijk geworden. De vreemde momenten waarop Martin zijn werkkamer binnen komt vallen en dan duidelijk met een smoesje vraagt wat hij aan het doen is. Hij weet echter het vertrouwen van Martin te winnen door zelf met een voorstel te komen.

Hij zal, met toezicht van een door Martin aan te wijzen expert, waarborgen in het systeem inbouwen. Deze zorgen ervoor dat hij geen grote schade aan het systeem kan aanrichten. Hij zal bovendien een logging- en monitoringsysteem aanbrengen dat een alarmering geeft wanneer er ergens binnen het systeem risicovolle handelingen worden verricht. Dit levert meteen ook beveiliging voor inbreuken van buitenaf op.

Tot slot stelt hij voor een risicoanalyse op de totale informatiehuishouding binnen het bedrijf uit te laten voeren, waarna beveiligingsmaatregelen op basis van ISO 27002, de algemeen

geaccepteerde Code voor Informatiebeveiliging, geïmplementeerd worden. Samen met de net behaalde ISO 9001-certificering voor kwaliteitsbeheersing, voldoet Martin's bedrijf dan aan de beste beveiligings- en kwaliteitsstandaarden die er zijn.

Een tijd later praten ze verder over continuïteitsbeheer, weliswaar onderdeel van de Code, maar toch wel een vak apart. Hiermee is te voorkomen dat, zoals dus eerder gebeurd is, de organisatie stil komt te liggen door uitval van haar CRM-systeem. <<

Meer weten:

- http://www.schneier.com/blog/archives/2009/02/insiders.html
- www.ibpedia.nl
- http://www.ibpedia.nl/index.php?title=Categorie:IBpedia-NL
- http://www.ibpedia.nl/index.php?title=Boekbesprekingen_over_informatiebeveiliging
- http://www.ibpedia.nl/index.php?title=ISFS
- Informatiebeveiliging onder controle 2e Editie, Paul Overbeek, Edo Roos Lindgreen, Marcel Spruit
- ISBN-13: 9789043006927 / ISBN-10: 9043006920

Bart Jutte - directeur en adviseur - Concilio - www.concilio.nl - bart.jutte@concilio.nl

Bart Jutte ondersteunt als adviseur bedrijven met het succesvoller maken van hun projecten door het toepassen van risicomanagement. Hij is auteur van het Handboek Projectrisico's.

Veilig uitbesteden

ICT UITBESTEDEN – VLOEK OF ZEGEN?

Inleiding

Als klein bedrijf kunt en wilt u niet alles zelf doen op ICT-gebied. Sommige ICT-diensten zijn te ingewikkeld geworden, andere diensten zijn goedkoper bij specialisten in te kopen. Uitbesteden brengt risico's met zich mee: als een leverancier slecht werk levert of failliet gaat, zit u met de problemen. Uw eigen dienstverlening wordt onmogelijk of lukt alleen met kunst- en vliegwerk. Ook kunnen gevoelige bedrijfsgegevens in handen komen van derden. Dit hoofdstuk gaat over de belangrijkste beveiligingsrisico's bij het uitbesteden van ICT-diensten en -producten en hoe u dat aan kunt pakken.

Uitbestedingrisico's

Er zijn veel ICT-onderdelen die u kunt uitbesteden. Ze variëren van de ICT-infrastructuur (netwerkbeheer, telefooncentrale) tot en met complete bedrijfsprocessen zoals de levering van goederen. Een trend die nu sterk toeneemt, is het afnemen van software als een dienst via internet (SaaS). Bekende voorbeelden zijn boekhoudsoftware, e-mailprogramma's en projectsoftware. Uitbesteding van ICT brengt beveiligingsrisico's met zich mee. Hieronder zijn de belangrijkste opgesomd:

- Verlies vertrouwelijkheid informatie: financiële gegevens of klantgegevens kunnen door uitbesteding terechtkomen op plaatsen buiten uw bedrijfsnetwerk.

- Bij uitbesteed beheer krijgen medewerkers van buiten het bedrijf toegang tot uw bedrijfsinformatie.
- Beschikbaarheid van informatiesystemen: bij uitbesteding van software of bedrijfsprocessen hangt de beschikbaarheid van ICT-diensten af van de kwaliteit van de leverancier. Als er koppelingen zijn met het eigen IT-systeem, betekent dit dat het geheel storingsgevoeliger is.
- Integriteit gegevens: data die buiten uw bedrijf worden verwerkt en opgeslagen, kunnen daar mogelijk worden aangepast, zodat ze niet meer kloppen.

Haperende boekhouding – 1

>> Ronald baalt, hij heeft net een telefoontje gehad van Jantine van de administratie, dat het boekhoudpakket het niet doet. Een vervelend probleem, want dit is net de laatste dag waarop de financiële resultaten van dit kwartaal worden samengesteld. Als het probleem niet snel is opgelost, krijgen ze problemen met de investeerders, accountant en de Belastingdienst. Het meest lastige aan het hele verhaal is nog dat Ronald zelf weinig invloed heeft op het probleem. Sinds een half jaar wordt het boekhoudpakket namelijk als dienst ingekocht bij een externe leverancier. Het programma draait nu niet meer op het bedrijfsnetwerk, maar is via internet te benaderen met een wachtwoord en gebruikersnaam. Handig voor de boekhouder die wel eens thuis werkt, maar nu zit hij met een probleem. Gelukkig biedt een telefoontje uitkomst. De leverancier vertelt dat zij een probleem met hun netwerk hadden en dat ze bezig zijn om hun back-updatacenter te activeren. Hij verwacht dat alles binnen een kwartier weer up-and-running zal zijn en dat maximaal een half uur aan gegevens verloren gaat. Ronald haalt opgelucht adem, hij belt Jantine en vertelt dat het probleem binnen een kwartiertje verholpen is. De leverancier houdt zijn woord en binnen een kwartiertje werkt de applicatie weer. Ronald prijst zich gelukkig met de zorgvuldige uitbesteding aan een professionele leverancier. <<

ICT-uitbesteding brengt ook een aantal algemene bedrijfsrisico's met zich mee. Deze kunnen op termijn de kwaliteit van de dienstverlening verminderen en zo uw bedrijf in problemen brengen:

- Te grote afhankelijkheid van één leverancier
- Vermindering vakkennis
- Hoge kosten van de uitbesteding
- Verlies controle over kernprocessen
- Doorvoeren wijzingen duurt lang
- Geen zeggenschap over gewenste ICT-uitbreidingen

Maatregelen

Vertrouwen in uw toekomstige toeleverancier is cruciaal als u ICT gaat uitbesteden. Dit vertrouwen is niet alleen een gevoel, maar moet zijn onderbouwd met feiten en resultaten. Neem daarom de volgende maatregelen:

- Bouw kennis op over uitbesteden (contracten) en het product dat u wilt inkopen.
- Win informatie in over mogelijke leveranciers: wat is hun reputatie bij andere klanten, welke cijfers hebben zij beschikbaar over uptime, levertijden en andere punten die voor uw bedrijf van belang zijn.
- Hoe zit hun systeem technisch in elkaar en welke zwakheden zijn hiervan bekend?
- Stem met de bedrijfsleiding af wat u wel en niet wilt uitbesteden en wie welke rol heeft in de contractfase en bij het beheer.
- Controleer zelf met (eenvoudige) testjes of de beveiliging goed in elkaar zit of niet.
- Zorg voor een plan B, een alternatief dat u kunt gebruiken als de uitbesteding bij de leverancier mislukt.

Haperende boekhouding – 2

>> Waarom Ronald koos voor uitbesteding van het boekhoudpakket? Martin had een half jaar geleden zijn eisen op tafel gelegd: "Ronald, dat boekhoudpakket dat wij nu hebben is ronduit onhandig. Je weet dat wij een nieuwe boekhouder nodig hebben en met veel moeite heb ik nu een geschikte kandidaat gevonden. Het probleem is dat die een dag per week thuis wil werken. Dat moet toch technisch op te lossen zijn? Bovendien wil ik ook vanaf thuis de financiële cijfers kunnen bekijken."

Ronald zet de zaken op een rijtje. Op dit moment is het boekhoudpakket geïnstalleerd op één pc. Hij heeft twee opties: een VPN-verbinding maken, waardoor medewerkers van buiten bij het bedrijfsnetwerk kunnen om zo de administratie te benaderen òf het boekhoudpakket als service afnemen via internet. Dat laatste kan lastig zijn als het pakket moet worden geïntegreerd met andere applicaties zoals het relatiebeheer. Ronald werkt de twee alternatieven uit, probeert wat software via internet en belt met leveranciers en een paar van hun klanten om inzicht te krijgen in de kosten, contractvormen en service die ze bieden. Een week later zitten Ronald en Martin weer bij elkaar. Ronald spreekt zijn voorkeur uit voor de webvariant, een keuze die ook de accountant ondersteunt; die krijgt hiermee direct inzicht in de boekhouding. Op termijn is deze oplossing wel duurder dan een bestaand pakket, maar Martin vindt dit geen bezwaar: "Als dit helpt om de nieuwe boekhouder vast te houden en sneller te laten werken, dan is die paar honderd euro snel terugverdiend! Goed werk Ronald, schaf die software maar aan." <<

Meer weten

Over het uitbesteden van ICT is veel kennis beschikbaar. De volgende websites en artikelen zijn goede startpunten:

- http://ictcoordinator.veilig.kennisnet.nl/uitbesteden
- http://www.managementkennisbank.nl/NL/ict-telecommunicatie-advies/ict-outsourcing-ict-uitbesteden-automatisering/

Hans Baars CISSP, CISM - Security Architect - Enexis BV - www.enexis.nl - j.h.baars@blixt.nl

Sinds 1999 is Hans werkzaam geweest als informatiebeveiligingfunctionaris en intern auditor bij het Korps landelijke politiediensten. Daarna heeft hij twee jaar als (senior) consultant bij 3-Angle Software & Services in Amstelveen gewerkt en een jaar als senior consultant bij Strict BV te Vianen. Vanaf september 2009 is Hans security-architect bij Enexis BV te Rosmalen.

Bewustwording

Inleiding

Bewustwording, wat bedoelen we daarmee? Eigenlijk is dat heel eenvoudig: wanneer bewustwording is bereikt, is informatiebeveiliging een normaal onderdeel van de dagelijkse werkzaamheden geworden. Zo normaal, dat de medewerkers zonder daar over na te denken beveiligingsbewust met bedrijfsinformatie omgaan. Informatiebeveiliging 'zit tussen de oren'. Dit is een belangrijke kwaliteitsstap, omdat informatiebeveiliging uiteindelijk zorgt voor een kwalitatief goed functionerende organisatie. In dit hoofdstuk wordt uitgelegd hoe bewustwording in een bedrijf tot stand komt en tegen welke problemen de directeur aanloopt als medewerkers onbewust risico lopen en nemen.

Bewustwording – de zin en onzin

Het bedrijf uit de case study is een mkb-bedrijf. Klein, maar de groei zit er goed in. In dit soort bedrijven is geen speciale security officer aanwezig. Beveiliging, als er al iemand voor is, is een deeltaak van een van de medewerkers. In de case is dat ook het geval. Beveiliging is, zo denkt directeur Martin, een ICT-aangelegenheid en hij heeft systeembeheerder Ronald dan ook de verantwoordelijkheid over informatiebeveiliging gegeven. Wil informatiebeveiliging een succes worden dan is het allerbelangrijkste om een zogenaamde top-down benadering te kiezen. Je kunt als beveiliger nog zoveel van de medewerkers verwachten, als het management het goede voorbeeld niet geeft, dan zullen de medewerkers het nut er niet van inzien.

Het begint dus allemaal met de voorbeeldfunctie van leidinggevenden. Het starten van een bewustwordingscampagne kan dan ook het beste gesteund worden door bijeenkomsten waar de directie of een hooggeplaatste medewerker namens de directie de opening verzorgt.
In grote organisaties heb je verschillende afdelingen die weinig of geen directe raakvlakken met andere afdelingen hebben. Het 'wij-gevoel' mag dan meer aan bod komen. Belangrijk is dat medewerkers zich herkennen in de aangesneden onderwerpen. Het heeft immers geen zin om in te gaan op het risico van vertrouwelijke bedrijfsinformatie via e-mail als je spreekt met medewerkers zonder e-mailadres van het bedrijf.

Nadat de directie te kennen heeft gegeven informatiebeveiliging belangrijk te vinden, is het tijd om uit te leggen wat informatiebeveiliging zoal inhoudt. Een mooie methode is het vertonen van een filmpje van ongeveer tien minuten waarin een aantal herkenbare situaties aan bod komen waarbij iedereen een gevoel heeft dat er dingen gebeuren die eigenlijk niet kunnen of zouden mogen gebeuren. Na dit filmpje is er tijd voor discussie over wat er getoond is. De bewustwordingsessie eindigt met een evaluatie om het gevoel van de medewerkers bij deze sessie te peilen en duidelijk te maken dat voor vragen de deur altijd open staat.
Na deze bewustwordingssessie waarin slechts een aantal facetten van informatiebeveiliging wordt belicht, is het tijd om het stokje over te dragen aan de direct leidinggevenden van de afdelingen. Zij hebben inmiddels een wat diepgaander cursus achter de rug en nemen informatiebeveiliging op in het werkoverleg en jaargesprekken met de medewerkers. Zij zorgen ervoor dat ze openstaan voor beveiligingsrisico's die medewerkers signaleren. Zij vormen de schakel tussen de security officer en de medewerkers. Bij het bedrijf uit de case waar slechts enkele mensen werken, is de lijn natuurlijk kort en loopt iedereen gewoon bij Ronald binnen als ze wat te vragen hebben.

Social engineering – 1

>> Martin zit eens rustig na te denken over de toekomst van zijn bedrijf. De kredietcrisis heeft gelukkig nog geen vat op hem gekregen en de zaken lopen als een trein. Hij heeft deze middag met Jantine besloten dat zij handen tekort komen en nog drie vacatures gaan plaatsen.

Plotseling komt Ronald aangeslagen de kamer binnen en vertelt dat hij die middag is gebeld door iemand waarvan hij dacht dat het de leverancier van de CRM-applicatie was. De man, wiens stem hem wel bekend voorkwam, maar waar hij nu niet zeker meer van was, vroeg hem om de cd met de applicatie. Zij hadden een methode bedacht om de veilige verbinding met het incassobureau op te zetten, maar hadden daarvoor de cd nodig. In zijn enthousiasme voor een snelle oplossing van het door hem gesignaleerde probleem, had Ronald de man gezegd dat hij maar moest komen en dat hij de cd klaar zou leggen bij de receptie. Een paar minuten geleden had de receptie Ronald gebeld en gezegd dat de cd opgehaald was. De receptioniste vond het vreemd hoe de man met zonnebril zich gedroeg. Hierop belde Ronald de softwareleverancier. Die weet van niets.
"Waarom zouden wij die cd ophalen?", had de leverancier gezegd. "Wij hebben de software immers zelf, en voor die koppeling hebben wij de software niet nodig. Dat is een netwerkkoppeling die jullie moeten maken."
Het lijkt erop dat iemand zich eerst van de nodige informatie heeft voorzien en toen met valse voorwendsels de meest vertrouwelijke bedrijfsinformatie heeft gestolen. <<

Maatregelen

Een goede beveiligingstraining kan de risico's inperken:

- Maak medewerkers bewust van het feit dat er altijd mensen kunnen zijn die op bedrijfsinformatie uit zijn. Vertrouw nooit zomaar iemand die zegt dat ze namens een bekende informatie op komen halen.
- Geef nooit het persoonlijke wachtwoord af omdat er zogenaamd een update moet worden geïnstalleerd. Systeembeheerders kunnen altijd met een eigen account inloggen om dit soort werkzaamheden uit te voeren.
- Laat altijd de beveiliging op laptops en PDA's staan. Bij verlies of diefstal wordt het in ieder geval moeilijker om de vertrouwelijke informatie op het apparaat te bemachtigen.
- Zet vertrouwelijke informatie die niet echt op een laptop of PDA hoeft te staan, er ook niet op. Hoe minder risico hoe beter.
- Praat buiten je werk niet met vreemden en bekenden, over vertrouwelijke zaken over je werk. Ook mensen die je vertrouwt, kunnen soms met jouw informatie pronken omdat het zo interessant was... En wie hoort het dan weer? Dat heb je niet in de hand.

Het gegeven voorbeeld wordt met de Engelse benaming 'Social Engeneering' beschreven. Het gaat om mensen die zich met een vlotte babbel voordoen als een ander. Om een bepaald doel te bereiken onderzoeken zij een bedrijf. Soms worden mensen in hun privéomgeving aangesproken en door middel van mooie, vriendschappelijke praatjes uitspraken ontlokt. Deze zijn te gebruiken om een bedrijf binnen te komen en om informatie los te krijgen. In dit geval was de dader op de hoogte van het bestaan van de cd met CRM-informatie. Belangrijk is ook het gegeven dat hij weet dat er een koppeling met een incassobureau gemaakt moet worden en dat daar een probleem mee is.

Social engineering – 2

>> Nadat Ronald zijn verhaal heeft verteld, valt het stil in de kamer. Jantine stormt nu ook de kamer binnen om te vertellen dat de pda van Frits uit zijn cabrio gestolen is. Frits had tot overmaat van ramp de beveiliging van zijn pda verwijderd. Op de vraag wat er dan allemaal op de pda aanwezig was, bleek dat Frits in verband met de CRM-applicatie de volledige klantendatabase op de pda had gezet, alle debiteuren- en crediteurengegevens had gekopieerd en ook alle productinformatie met de bijbehorende prijzen op de pda had staan. De schade voor het bedrijf kan enorm zijn. Hun deels vertrouwelijke bedrijfsinformatie kan in verkeerde handen vallen, alle financiële gegevens zijn bekend en de privacy van klanten is in gevaar. De vraag is of er bovendien sprake is van een gecombineerde actie tussen de man die de cd heeft opgehaald en de diefstal van de pda. <<

Meer weten

- www.ibpedia.nl
- http://www.ibpedia.nl/index.php?title=Categorie:IBpedia-NL
- http://www.ibpedia.nl/index.php?title=Boekbesprekingen_over_informatiebeveiliging
- http://www.ibpedia.nl/index.php?title=ISFS
- Informatiebeveiliging onder controle 2e Editie, Paul Overbeek, Edo Roos Lindgreen, Marcel Spruit ISBN-13: 9789043006927 / ISBN-10: 9043006920

André van Soest - Adviseur Informatiebeveiliging LBVD Informatiebeveiligers - www.lbvd.nl - andre.van.soest@lbvd.nl

André is betrokken bij het managen en uitvoeren van projecten op het gebied van informatiebeveiliging met een uiteenlopend karakter, waaronder IB-onderzoeken en -verbetertrajecten en Mystery Guest-acties.

Inhuren van personeel: lust of last?

Inleiding

Een bedrijf dat groeit heeft op een bepaald moment behoefte aan nieuwe medewerkers. Vaak kijken medewerkers binnen hun eigen vrienden- en kennissenkring naar nieuwe collega's. Het plaatsen van advertenties in dag- en weekbladen of via internet om de juiste persoon binnen te halen kan ook het gewenste resultaat leveren. Soms heeft u wellicht de behoefte om tijdelijk wat extra handen tot uw beschikking te hebben voor het realiseren van een project of heeft u specialistische kennis nodig omdat u die zelf niet in huis heeft. Ook als een bedrijf voldoende mensen heeft, kunnen er situaties ontstaan waarop er extra mensen nodig zijn, bijvoorbeeld wanneer iemand met zwangerschapsverlof gaat of iemand een jaar sabbatical opneemt. Op dat moment kunt u ook besluiten om personeel in te huren via een uitzendorganisatie of een detacheringbureau.

Personeel inhuren zorgt echter voor extra risico´s. Dit hoofdstuk gaat nader in op de aspecten waar u als bedrijf aan moet denken wanneer u mensen tijdelijk inhuurt.

Risico's bij het inhuren

Voor medewerkers die in dienst komen bij een bedrijf is een aantal zaken standaard geregeld. Dit begint al bij de werving en selectie van

kandidaten. Voor bepaalde functies vindt screening (verificatie van de achtergrond van een persoon) plaats. Zodra een medewerker in dienst treedt, zal hij of zij de arbeidsovereenkomst en eventueel een geheimhoudingsverklaring moeten ondertekenen. Soms benoemt de personeelsfunctionaris ook mogelijke disciplinaire maatregelen indien men zich niet houdt aan de regels en procedures.

Vaak krijgen nieuwe medewerkers een handboek waarin beschreven is wat zij wel en niet mogen. U kunt hierbij denken aan internetgebruik, hoe om te gaan met e-mail, het behandelen van vertrouwelijke informatie enzovoorts. Als een medewerker een laptop krijgt, zal facilitaire zaken of een andere afdeling vaak een aparte gebruikersovereenkomst opstellen die de medewerker dient te ondertekenen.

Om daadwerkelijk aan het werk te gaan, zal men voorzieningen als een toegangspas of sleutel, een werkplek, een computer en toegang tot het netwerk moeten regelen.

De uitzendorganisatie of een detacheringbureau zal voor de medewerkers veel van bovengenoemde zaken zelf regelen. De medewerker is in dienst van de organisatie of het bureau en heeft daarmee een arbeidsrelatie (dus ook een arbeidsovereenkomst). Als bedrijf sluit u daarom een (detacherings)overeenkomst af met de uitzendorganisatie of een detacheringbureau en niet rechtstreeks met de ingehuurde medewerker zelf.

Contractueel

Als u eigen medewerkers in (tijdelijke) dienst neemt, regelt u de arbeidsvoorwaarden zelf. Omdat een externe medewerker niet bij u in dienst komt, zult u een aantal (juridische) zaken met de uitzendorganisatie of het detacheringbureau moeten regelen. Vaak hebben deze bureaus de zaken goed voor elkaar, maar soms stelt u specifieke eisen die u contractueel vastgelegd wilt hebben.

U wilt in ieder geval zeker weten dat alles geregeld is. Denk hierbij aan de volgende zaken:

- Is er iets geregeld op het gebied van geheimhouding en het houden aan regels?
- Heeft de derde partij een aansprakelijkheidsverzekering afgesloten en dekt deze verzekering alle schade of blijft u zelf nog met hoge kosten zitten?
- Is de medewerker voldoende gescreend, waardoor het bedrijfsrisico minimaal is?
- Hoe gaat u om met een medewerker die na afloop van de inhuurperiode gaat werken bij een concurrent? Is hiervoor iets geregeld?

Voorzieningen

Alles is contractueel geregeld met de uitzendorganisatie of het detacheringbureau en de medewerker komt uw bedrijf ondersteunen. Als bedrijf moet u dan onder andere de volgende zaken geregeld hebben zodat de medewerker direct aan de slag kan:

- Toegang tot het gebouw en afdeling: verstrekken van een toegangspas of sleutel. Denk erover na of deze medewerker volledige toegang tot alle ruimtes krijgt of alleen tot de plekken die voor de functie noodzakelijk zijn.
- Toegang tot het netwerk en applicaties: wilt u dat de medewerker dezelfde rechten krijgt als een eigen medewerker en beschikking heeft over alle informatie of maakt u een selectie?
- Bedrijfsmiddelen: krijgt de medewerker een pc of mag hij gebruikmaken van een eigen laptop? Vaak hebben medewerkers van een consultancybureau een eigen laptop, waardoor zij niet per se een pc van het bedrijf nodig hebben. Als klein bedrijf lijkt dit erg handig omdat u geen extra pc hoeft aan te schaffen. Het toestaan van een eigen laptop brengt echter wel een aantal risico's met zich mee, die u als bedrijf niet geheel kunt afdekken. De medewerker kan namelijk eenvoudig complete mappen van het netwerk naar zijn laptop kopiëren. Wanneer deze informatie op straat komt te liggen doordat de medewerker de laptop verliest of doordat iemand de laptop steelt, kan dit grote schade betekenen

voor het bedrijf. Daarnaast weet u niet of de medewerker privé bepaalde websites bezoekt, waardoor er virussen op de laptop terechtkomen die op het bedrijfsnetwerk kunnen belanden. Ook weet u niet of de medewerker de laptop gebruikt voor het versturen van zakelijke en privé e-mails. Een andere vraag is of de laptop voorzien is van een goed antivirusprogramma en of alle software-updates zijn geïnstalleerd.

De juiste man voor de juiste klus – 1

>> Jantine kan door de snelle groei van het bedrijf alle administratieve en personele taken niet goed meer aan met haar team. Een van haar medewerkers doet het functioneel beheer van het Personeel en Administratie Informatie Systeem (PAIS), maar heeft haar baan opgezegd. Jantine zoekt daarom op korte termijn een nieuwe medewerker die ervaring heeft met deze werkzaamheden. Er is tenslotte niet voldoende tijd om iemand goed in te werken. Er is een vacature in de landelijke dagbladen geplaatst en ook op de bekende vacaturesites is geadverteerd. Dit heeft genoeg reacties opgeleverd, maar niemand heeft ervaring met PAIS.

Jantine besluit om Ronald, waarvan ze vermoedt dat hij een oogje op haar heeft, te vragen mee te denken over een oplossing.

"Ronald, ik zit met een probleem en ik zou het heel erg lief van je vinden als je mij daarmee kunt helpen. Mijn functioneel beheerder gaat binnenkort weg. Ik heb advertenties geplaatst, maar iedereen die reageert, heeft geen ervaring met PAIS. Weet jij hoe ik dit moet oplossen?"

"Daar moet ik even over nadenken" zegt Ronald die zich vereerd voelt dat Jantine bij hem komt.

"Bij mijn vorige werkgever heb ik dit wel eens meegemaakt. Toen huurden wij een tijdelijke consultant in totdat onze afdeling zelf een medewerker had gevonden. De interimmer heeft de nieuwe medewerker vervolgens opgeleid en ingewerkt."

"Weet je een betrouwbaar bureau dat dit zou kunnen?"

"Ja, Consultancy & Co. Zal ik een afspraak met ze maken?"

"Heel graag", zegt Jantine met een brede glimlach die Ronald doet blozen.

Ronald belt met Consultancy & Co en maakt voor dezelfde week nog een afspraak. In de tussentijd gaat hij de standaard inhuur-

contracten na, om er zeker van te zijn dat alles contractueel is afgedekt op het gebied van geheimhouding, concurrentiebeding et cetera. Ronald heeft bij een andere werkgever meegemaakt dat dit niet goed geregeld was, wat resulteerde in een rechtszaak en dat wil hij te allen tijde voorkomen. Ronald vindt in het standaardcontract nog een hiaat en laat dat door de juridische afdeling rechtzetten. Ronald is tevreden en gaat vol vertrouwen het gesprek met Consultancy & Co in. <<

Maatregelen

Om de continuïteit van bedrijfsprocessen te waarborgen is het, afhankelijk van de omstandigheden, een goede optie om personeel in te huren. In het contract met een bureau (of leverancier) dient uw bedrijf in ieder geval zaken te regelen die niet (voldoende) afgedekt zijn door de wet- en regelgeving, zoals geheimhouding en intellectueel eigendom. Om de risico's zo klein mogelijk te houden dient uw bedrijf een aantal zaken contractueel af te dekken. Niet alle genoemde punten zijn even relevant voor elke inhuur, maar het is van belang dat u hier wel bewust mee omgaat:

- Win informatie in via uw netwerk; heeft iemand ervaring met bepaalde bureaus?
- Als u zelf een bureau heeft gevonden, vraag dan naar referenties en check deze.
- Zorg ervoor dat u een standaardcontract heeft of dat u minimaal kunt beoordelen wat in een contract met derden aan aanvullende eisen opgenomen moet zijn. Vraag naar de aansprakelijkheidsverzekering van de leverancier.
- Bepaal welke functies u wilt uitbesteden en welke niet. Dit kan te maken hebben met (verregaande) bevoegdheden, vertrouwelijkheid, de continuïteit die u zelf in de hand wilt hebben of een vast aanspreekpunt dat u wilt behouden.
- Het contract met het bureau dient duidelijke bepalingen te bevatten over de verantwoordelijkheden met betrekking tot het screenen van personeel.

- Stel voor belangrijke functies ook een aparte geheimhoudingsverklaring op en laat deze door de medewerker tekenen, ondanks dat dit al is geregeld in de arbeidsovereenkomst met hun werkgever. Neem in het contract met het bureau op welke eisen u specifiek aan de geheimhoudingsverklaring stelt.
- Leg contractueel vast wanneer u gerechtelijke stappen onderneemt tegen de externe medewerker of zijn werkgever. Dit is zeker van belang wanneer de concurrent de externe medewerker later ook inhuurt.
- Zorg ervoor dat de primaire bedrijfsprocessen niet te veel afhankelijk worden van een derde partij.
- Het management dient informatiebeveiliging ook naar externe medewerkers uit te dragen, waardoor het bewustzijn met betrekking tot informatiebeveiliging bij hen gemeengoed wordt of blijft. Naast interne medewerkers dienen ook externe medewerkers in beveiligingsprocedures en -technieken getraind te zijn.
- Ondanks dat alles contractueel is vastgelegd, is het toch mogelijk dat uw bedrijf gerechtelijke stappen moet ondernemen tegen een externe medewerker of zijn werkgever. Bedenk van tevoren welke stappen u moet ondernemen om mogelijk bewijsmateriaal te verzamelen. Leg van tevoren procedureel vast wie binnen het bedrijf welke acties onderneemt.
- Denk niet alleen na over zaken die u met de uitzendorganisatie of het detacheringbureau moet regelen, maar kijk ook welke maatregelen u moet treffen zodat de externe medewerker zijn of haar werk bij uw bedrijf kan uitvoeren. Misschien ligt dit voor de hand, maar het is te allen tijde belangrijk dat alle systemen voorzien zijn van de juiste software updates, patches en dat antivirussoftware is geïnstalleerd en actief is.
- Zorg dat de externe medewerker een tijdelijke account krijgt. Zo voorkomt u dat u vergeet om het account nadien te blokkeren of te verwijderen. Geef niet automatisch volledig toegang tot alle systemen, maar ga na welke rechten de tijdelijke medewerker nodig heeft om te kunnen werken.
- Laat geen vreemde laptops toe op het bedrijfsnetwerk. Indien het toch noodzakelijk is dat een externe medewerker een vreemde laptop op het bedrijfsnetwerk aansluit, moet u een aantal

maatregelen treffen. Plaats de vreemde laptop bijvoorbeeld in een apart netwerk (een subnet) dat voorzien is van een router/firewall die op de juiste wijze is geconfigureerd. Het bedrijfsnetwerk is daardoor alleen via de router te bereiken. De router kan verbindingen analyseren, filteren en loggen. Ook voorkomt u hiermee dat een externe medewerker toegang krijgt tot systemen waarvoor hij/zij niet bevoegd is.

- Als blijkt dat er toch een virus via de vreemde laptop op de server terecht is gekomen en schade heeft veroorzaakt, zult u dat bij het bureau van de externe medewerker moeten verhalen. Zorg ervoor dat dit contractueel is vastgelegd.

De juiste man voor de juiste klus – 2

>> Het bedrijf heeft een uitbreiding op PAIS gekocht en Ronald heeft ondersteuning nodig om het financiële deel van het pakket in te richten. Hij heeft in de investeringsaanvraag voldoende kosten gereserveerd om voor twee maanden een specialist in te huren. Willem is specialist op het gebied van PAIS en werkt voor een consultancybureau. Hij komt Ronald ondersteunen bij het inrichten van PAIS. Willem heeft een eigen laptop en vindt het wel makkelijk om zijn laptop op het netwerk aan te sluiten. Ronald vindt dat prima, want er is geen pc beschikbaar. Hij maakt een account voor Willem aan, zodat hij toegang krijgt tot de server waar hij de personele en financiële gegevens kan benaderen. Ook zorgt hij ervoor dat Willem internettoegang heeft.

Martin belt Ronald op, omdat hij er een viruswaarschuwing op zijn beeldscherm verschijnt, en hij heeft niets vreemds gedaan. Ronald heeft allerlei maatregelen getroffen zodat het haast onmogelijk is om virussen of andere malware binnen te halen. Bij de directeur aangekomen ziet Ronald dat het inderdaad een virus is en hij verwijdert het direct. Ronald vraag aan de directeur wat hij exact gedaan heeft om na te gaan hoe het virus binnen is gekomen. De directeur zegt dat hij alleen een bestandje met de investeringen van dit jaar heeft geopend en dat toen de melding kwam. Ronald kan dit niet plaatsen en gaat het uitzoeken.

Ronald begrijpt er niets van en loopt naar zijn kantoor om eens goed na te denken hoe het virus op het netwerk is gekomen. De medewerkers hebben geen toegang tot bepaalde sites waardoor zij een virus zouden kunnen oplopen. Medewerkers kunnen software niet zomaar installeren en e-mailverkeer wordt gescand. De laatste updates van het antiviruspakket zijn geïnstalleerd en externe opslagmedia als een usb-stick of harddisk, kan men niet op de pc aansluiten. Alles is dichtgezet. Ronald vraagt zich af wat het kan zijn. Hij komt er niet uit en loopt naar Willem om te vragen hoe het gaat met het inrichten van PAIS. Op dat moment ziet Ronald de laptop en er gaat een lichtje branden.

Willem bezocht de avond ervoor een forum waar bepaalde tools werden besproken. Een van de forumleden raadde Willem aan om een programmaatje te installeren waarmee hij de snelheid van zijn laptop kon verbeteren. Zijn laptop was inderdaad wat traag, dus Willem kon wel wat snelheid gebruiken en downloadde het programmaatje. <<

Meer weten

- Hoofdstuk 6 en 8 van de ISO-standaard ISO27002:2007 (Code voor Informatiebeveiliging). te verkrijgen via www.nen.nl
- www.ibpedia.nl
- www.ibpedia.nl/index.php?title=ISFS

Wim Penninx - ICT Architect - TU Delft - www.tudelft.nl - w.h.penninx@tudelft.nl

Na zijn opleiding en werk als astronoom aan de Universiteiten van Groningen, Amsterdam en het MIT is Wim begin jaren negentig in de ICT gaan werken. Sinds 2004 is hij ICT-projectleider en ICT-architect op de TU Delft waar hij zich bezig houdt met onderwerpen als infrastructuur, Federated Identity Management en security.

Malware: geautomatiseerde bedreigingen

Inleiding

Inbreken via internet is een fact of life geworden. Eén van de uitdagingen voor de ICT-beveiligers is dat nieuwe inbraaktechnieken zeer snel hun weg vinden naar elke internettoegangsdeur. Professionele internetcriminaliteit is geen toekomstige bedreiging; het is volop aanwezig. Inbraaksoftware wordt in eerste instantie vaak gemaakt door intelligente ICT'ers, soms voor wetenschappelijk belang, soms als 'uitdaging voor de hobbyist'. Deze soms zeer professionele tools zijn in toenemende mate toegankelijk voor technische knutselaars (scriptkiddies). Deze gebruiken het voor inbreken als kick, of verkopen het door aan internetcriminelen die deze tools uitbuiten, vaak voor geldelijk gewin. In dit hoofdstuk schetsen we de varianten van malware, en vertellen we hoe u zich er tegen kunt wapenen.

De bedreigingen

Malware is de verzamelnaam voor kwaadaardige en/of schadelijke software. Het is een Engelse samenvoeging van MALicious softWARE. De meeste gebruikers zullen het eenvoudig computervirussen noemen. Er zijn verschillende malware-varianten; ieder met hun eigen technieken, bedreigingen en beschermingsvormen. Doordat het aantal varianten malware snel toeneemt, zijn de definities van malware-typen nog vaak onderwerp van discussie.

- Computervirus: de meeste virussen kunnen zichzelf niet zelfstandig verspreiden, maar gebruiken een medium voor verspreiding. Media die veel gebruikt worden zijn: e-mailprogramma's, waarbij e-mailadressen die uit de mail gehaald worden, of een cd of usb-stick.
- Computerworm: een worm verspreidt zich zelfstandig, zonder gebruik te maken van een medium. Veel van deze wormen verspreiden zich doordat ze zwakheden in het besturingssysteem gebruiken; soms proberen ze verbindingen te maken met IP-nummers die in de buurt zitten van het eigen IP-nummer.
- Spyware: 'spionagesoftware' geeft informatie over de gebruikers-activiteiten door aan een computer op internet, zonder dat de gebruiker zich hiervan bewust is. De grens tussen spyware en het doorgeven van informatie aan de maker om het product te verbeteren of om het gebruikersgedrag van een grote groep te analyseren is niet altijd helder. Op deze wijze is het doorspelen van creditcardinformatie mogelijk.
- Adware: 'advertentiesoftware'. Dit is soms in overeenstemming met de acceptatievoorwaarden van software (daarmee genereert de maker soms wat inkomsten), maar het kan ook ongewenst geïnstalleerd worden. In een professionele omgeving wordt dit nagenoeg nooit bewust geaccepteerd.
- Trojan horse: deze software is vernoemd naar het klassieke verhaal uit het oude Griekenland. De Grieken belegerden tien jaar de stad Troje zonder binnen te komen. Uiteindelijk bouwden ze een groot houten paard en gaven dit aan de Trojanen. Deze haalden het paard binnen, en eenmaal binnen in de stad, bleek dat in het grote houten paard het leger van de Grieken te zitten, die zo de stad veroverden. Bij een Trojan horse kan er een lading meegedragen worden van allerlei soorten. Zo kan ongemerkt software op de pc binnenkomen waarmee iemand van buiten acties kan starten op de pc. Deze worden soms gebruikt als tussenstation voor een aanval. Als een aanvaller zo de beschikking heeft over honderd pc's met een Trojan horse, heeft hij ruime mogelijkheden voor een aanval: hij kan met veel bandbreedte een gezamenlijke aanval doen. De afkomst van de aanvaller is niet zichtbaar, aangezien de Trojan horse geen informatie achterlaat. Een chatsessie van Prinses Maxima met Nederlandse burgers werd ooit zo via een DDOS platgelegd.

- Rootkit: een set van tools om 'root' te worden. Root is binnen Unix het centrale account dat alle rechten heeft en alle rechten verdeelt, bij Windows-systemen is dit de administrator. Indien een aanvaller doordringt tot de kern van een systeem, kan hij een rootkit installeren. Een rootkit nestelt zich meestal zeer diep in een systeem. Verwijderen van een component zorgt er vaak voor dat via een andere component de inbreker alsnog volledig toegang heeft. Van een rootkit wordt niet altijd direct misbruik gemaakt. Het kan sluimerend aanwezig zijn, waarna plotseling het misbruik kan toeslaan.
- Boot sector-virus: nestelt zich in het opstartonderdeel van het systeem. Nog voor een gebruiker bij de omgeving kan, is het virus reeds actief. De term wordt tegenwoordig minder gebruikt; het concept dat malware reeds actief is voordat een gebruiker iets doet op een machine is gebruikelijker.

Malware kan op twee manieren op een pc komen:

- De pc staat aan en kwaadwillenden plaatsen via een beveiligingslek op afstand software.
- Installatie van software door activiteit van een gebruiker; er zijn veel verschillende activiteiten die een gebruiker kan uitvoeren, waardoor dit gebeurt:
  - Aanklikken van een normale website, waarop informatie staat, maar ook inhoud die malware toevoegt op de pc (drive by-infectie);
  - Aanklikken van iets in een e-mail, zoals een filmpje;
  - Aanklikken van software op een cd, dvd of usb-stick.

Het beschermen tegen deze twee categorieën behoeft twee verschillende aanpakken. Hierop komen we in de paragraaf over de maatregelen terug.

De bedreigingen door de jaren heen

In de werkwijze voor hackers zien we een duidelijke ontwikkeling door de jaren heen. Een aantal jaar geleden waren de security-gaten groot en bestonden er veel virussen die op deze wijze de wereld veroverden. De reparaties van de security-openingen verlopen nu beter door de verbe-

terde updateservices van met name Windows. Het verleiden van gebruikers tot het aanklikken van niet betrouwbare sites is dan ook toegenomen. Gebruikers ontvangen een bericht waarvan ze denken dat ze de inhoud kunnen vertrouwen. Dit wordt phishing genoemd. Voorbeelden zijn een e-mail waar de afzender een betrouwbare organisatie of bekende lijkt. Kwaadwillenden hebben deze verkregen via Instant Messaging, LinkedIn of mailinformatie op andere sociale-netwerksites.

De vertragende factor – 1

>> Ronald heeft regels ingesteld om de beveiliging van de pc's op orde te houden. Medewerkers mogen zelf geen software installeren. Na wat discussies kan de directeur zich hierin vinden. Al vrij snel blijkt dat Frits verschillende software gebruikt om efficiënt zijn mooie overzichten aan de directeur te tonen. Martin maakt dan ook een uitzondering voor Frits; hij mag zijn eigen software installeren. De andere medewerkers krijgen geen rechten om software op de eigen pc te installeren. Voor Ronald was dit nog steeds geen wenselijke oplossing, maar hij weet dat een discussie met de directeur hierover weinig zin heeft, dus hij laat het zo. Op een maandagmiddag meldt Jantine dat haar pc erg traag is. Hij twijfelt wel of haar pc niet wat langzamer is dan zijn eigen vanwege de leeftijd van haar computer. Later merkt hij zelf dat ook zijn pc wat aan de trage kant is. Even later blijkt dat alle bedrijfscomputers helemaal niet meer soepel werken. Ronald gaat op zoek en besluit de internetverbinding er uit te halen. De pc's lijken daarna weer goed te werken. De internetverbinding wordt vervolgens weer aangezet en het probleem keert terug. Vervolgens worden de router en de switch herstart, maar niets helpt. Hij sluit dan de pc van Jantine af om te zien of dat het probleem oplost; zij was tenslotte de eerste die het probleem meldde. Ook dit blijkt het probleem niet op te lossen. Vervolgens zet hij stapsgewijs alle pc's aan en uit om te zien of het iets uitmaakt. Een paar uur later, als de directeur al een paar keer gevraagd heeft of hij niet een gespecialiseerd bedrijf moet bellen, komt Ronald er achter dat het aan de pc van Frits ligt. Frits moet een andere computer gebruiken, totdat Ronald het probleem echt op kan lossen. <<

Maatregelen

Er zijn maatregelen nodig om geautomatiseerde aanvallen te kunnen weerstaan. In het beveiligen tegen malware is het altijd nodig om naast preventieve maatregelen te treffen, ook te kunnen reageren bij incidenten met reactieve maatregelen.

- Preventief technisch
  - Zorg ervoor dat alle security patches snel en gecontroleerd geïnstalleerd worden. Dit geldt voor alle onderdelen, dus ook de servers, routers, firewalls, clients, besturingssystemen en applicaties. Elk beveiligingsgat wordt tegenwoordig snel misbruikt.
  - Zorg ervoor dat de antivirusprogramma's op de werkplek én op de client actief zijn. Door het gebruik van webmail, waarmee ook bijlagen direct op de werkplek geopend kunnen worden, zijn ook de antivirus-tools op de clients belangrijk.
  - Indien de organisatie niet al te groot is en er beperkte mogelijkheden zijn om kennis bij de systeembeheerders op vereist niveau te houden, maak dan gebruik van externe diensten van gespecialiseerde organisaties.
  - Kies voor geïntegreerde management/security-tools, met geautomatiseerde en geïntegreerde security auditing.
- Preventieve bewustwording: naast de taken van systeembeheer is de belangrijkste preventieve activiteit bewustwording. Aangezien de aanvallen steeds subtieler worden, zijn ook kennis en bewustzijn bij de mkb-medewerkers van belang. Laat eens op een bijeenkomst het risico zien van een e-mail die lijkt alsof hij door een bank verstuurd is. Of het risico van een afwijkend MSN-bericht van een goede kennis die je naar een kwaadaardige website lokt. Een goede bewustwording van medewerkers is de belangrijkste manier om tegenwoordig risico's te verminderen.
- Reactief bij incidenten: mocht er een incident optreden en er zijn machines besmet, zorg dat er snel actie genomen wordt zodat het probleem niet uitbreidt. Sluit de internetverbinding af, haal pc's van het interne netwerk af. Als het hele interne netwerk plat ligt en de probleemoorzaak niet is te achterhalen, is wellicht hulp van buiten nodig. Dit is af te dekken met supportcontracten.

De vertragende factor – 2

>> Frits was zich de vrijdag voor het incident aan het voorbereiden op de verjaardag van zijn vrouw. Hij gebruikt de pauze om op internet een leuk cadeau voor haar te zoeken. Hij vindt een roze smartphone. Als extraatje denkt hij er aan om een cd te branden met haar favoriete muziek. Hij zoekt in nieuwsgroepen en via Limewire naar muziek voor haar. Dit gaat op kantoor sneller dan thuis. Omdat het downloaden nog wat sneller gaat als hij de virusscanner tijdelijk uitzet, doet hij dit. In de loop van de middag kwam hij erachter dat hij de virusscanner niet direct na de lunch weer aangezet heeft en deed dat dus later die vrijdagmiddag. Achteraf blijkt dat hij bij het downloaden een mp3.exe die er uitzag als een mp3-bestand gedownload heeft. Hij had hem aangeklikt, waardoor zijn pc met een trojan horse geïnfecteerd raakte. De maandag erop werd deze actief. Waarschijnlijk had de maker van de trojan horse deze ingezet voor de aanval op de website van een ander bedrijf. Hierdoor raakte de firewall en het interne netwerk overbelast, waardoor niemand meer normaal kon werken. Ronald kan dit voorval in de toekomst gebruiken als Martin weer keuzes maakt die nadelig zijn voor hem en het bedrijf. <<

Meer weten

Kijk voor meer informatie bij Wikipedia-informatie als:

- http://en.wikipedia.org/wiki/Malware.

Voor het up-to-date zijn van de pc-beveiliging zal er steeds meer gebruik gemaakt worden van OVAL (Open Vulnerability and Assessment Language). Zie:

- http://en.wikipedia.org/wiki/Open_Vulnerability_and_Assessment_Language.

Rein de Vries - Directeur en Adviseur - LBVD Informatiebeveiligers - www.lbvd.nl - rein.de.vries@lbvd.nl

Rein is medeoprichter van het Delftse adviesbureau LBVD Informatiebeveiligers en is voor het overgrote deel van zijn tijd uitvoerend betrokken bij IB-onderzoeken en -verbetertrajecten. Begin jaren negentig kwam hij voor het eerst in aanraking met (netwerk)beveiliging. Door een brede interesse is hij gegroeid naar allround informatiebeveiliger.

Beveiligen tegen gevaren van buiten

DE FYSIEKE KANT VAN ICT-SECURITY

Inleiding

Waarom zou je via internet inbreken op systemen als je ook gewoon een laptop of usb-stick met bedrijfsinformatie kan 'lenen'? Of kans ziet om back-uptapes te bemachtigen?

Vaak staat men bij het beveiligen van computers vooral stil bij de softwaretechnische kant: authenticatie, versleuteling, back-ups, het verhelpen van security-lekken, enzovoorts. Er is echter ook een fysieke kant die zeker zo belangrijk is: hoe zorgen we ervoor dat alleen degenen die dat mogen fysiek toegang krijgen tot de voor hen bedoelde informatie of informatiesystemen? Dit hoofdstuk gaat nader in op deze vraag.

Fysieke bedreigingen en risico's

Gevaren van buitenaf kunnen ervoor zorgen dat informatie of informatiesystemen niet langer beschikbaar zijn, dat vreemden kennisnemen van gevoelige bedrijfsinformatie of dat de correctheid van informatie niet gegarandeerd is. Als de schade die in dat geval ontstaat niet acceptabel is, moet u maatregelen treffen, om de kans op incidenten te verkleinen of om de schade te beperken indien een verstoring optreedt.

Daarbij gaat het vooral om het beschermen van informatie en informatiesystemen als belangrijke bedrijfsmiddelen. Dit vraagt om een andere kijk dan wanneer u bijvoorbeeld waardevolle objecten, zoals kunstwerken, fysiek wilt beveiligen tegen diefstal of beschadiging.

Bedreigingen heb je in verschillende soorten. Naast puur fysieke bedreigingen, zoals brand en natuurgeweld, vormt de mens ook een wezenlijk gevaar. Mensen kunnen zich vergissen, ontwetend of onoplettend zijn. Kwalijker is het wanneer opzet in het spel is. Denk hierbij aan diefstal, vandalisme en sabotage.

Bij bedrijven is meestal een facilitair medewerker, manager of een facilitaire afdeling verantwoordelijk voor fysieke beveiliging. Deze is echter vaak druk met andere zaken zoals catering, schoonmaak, klimaatbeheersing of onderhoud en beveiligt veelal vanuit eigen (bouwkundige) principes die los staan van ICT-security. Een kritische blik vanuit ICT kan dus geen kwaad.

De nieuwe serverruimte – 1

>> Vanwege groei moet het bedrijf van Martin verhuizen. Martin is persoonlijk betrokken bij het verhuisplan en beslist mee over waar de nieuwe serverruimte moet komen: in de kelder. Zo heb je het minst geluidsoverlast en blijft elders meer ruimte over voor werkplekken. En daglicht is in een serverruimte niet nodig. De plannen zijn bijna klaar als Ronald hier weet van krijgt. Net op tijd schiet hij Martin aan.

"Het is niet zo slim om de systemen in de kelder te plaatsen, die zou wel eens vol kunnen lopen met water. Als we al geen last krijgen van het grondwater of van een overstroming door hevige regenval, dan kan bij een brand al het bluswater de kelder inlopen."

"Daar zit wat in", antwoordt Martin. "Goed, dan heb ik boven op de eerste etage aan de buitenzijde nog wel een kamer vrij."

"Geen goed plan", sputtert Ronald tegen. "Bij storm kan het raam het begeven, waardoor alles blootstaat aan wind en regen. Of een laddertje tegen de muur en hup, een dief is een hoop leuk speelgoed rijker."

"Oke, oke", zucht Martin. "Dan offer ik mijn hok in het midden van de eerste wel op, jij je zin …" <<

Maatregelen

Maatregelen om de fysieke kant van ICT-security in te vullen zijn er genoeg. We volstaan hier met een opsomming van de belangrijkste zaken (bedenk dat er veel meer mogelijk is):

Risico's en zones

- Bedenk goed waartegen u beveiligt. Wie is de vijand, wat zijn de risico's? Zorg voor een balans tussen risico en maatregelen.
- Denk in risicogebieden. Plaats de meest waardevolle zaken in een extra beveiligde zone. Alle systemen waar belangrijke toepassingen op draaien – maar ook testsystemen – horen bijvoorbeeld thuis in de serverruimte. Minimaliseer de activiteiten in kritische ruimtes.
- Voorzie iedere zone van een eigen toegangsbeveiliging. Dit kan ook een portier bij een deur zijn. Denk ook aan het (niet) kunnen openen van ramen en een inbraakalarm.
- Bij laden en lossen hebben medewerkers van derden mogelijk toegang tot plekken in het gebouw waar u ze eigenlijk niet wilt hebben. Voorkom dit.
- Buiten (rondom het pand) is ook een zone. Is een hoog hek nodig? Buitenverlichting met bewegingsdetectie? Een juridische afscherming in de vorm van een waarschuwing is een alternatief.
- Zijn camera's nodig? Deze hebben een afschrikkende werking. Bedenk echter wel dat, als u opnames maakt, u rekening moet houden met privacy en wet- en regelgeving.

Toegang tot ruimtes

- U kunt ruimtes met deursloten beveiligen. U kunt de toegang in dat geval echter slecht beheersen. Immers, iedereen die over een sleutel kan beschikken, heeft in principe onbeperkt toegang. Een elektronisch toegangssysteem is een betere keuze. U kunt deze vergelijken met logische toegangsbeveiliging. Iedere gebruiker heeft een eigen elektronische sleutel. Het gebruikersniveau bepaalt wie wanneer waar naar binnen mag. Via een logging kunt u zien wie wanneer ergens binnen is geweest.
- Deuren zijn ideaal voor buitenstaanders om naar binnen te glippen, zelfs als ze voorzien zijn van elektronische sloten. Via 'tailgating', het meeliften met iemand die net naar binnen of buiten gaat, kunnen kwaadwilligen binnenkomen. Wilt u dit uitbannen, dan moet u uw toevlucht nemen tot tourniquets – draaipoortjes – waarbij dit menselijke manco op technische wijze is verholpen. Wel een dure oplossing overigens. Rokers hebben veelal de neiging om bij een achteringang te roken. Dit is voor kwaadwilligen ook een prima plek om via social engineering binnen te sluipen. Een alarm op een deur die puur bedoeld is als nooduitgang, kan geen kwaad.
- Fysieke en logische toegangsbeveiliging zijn ook prima te combineren. Er zijn oplossingen verkrijgbaar waarbij je met dezelfde token (bijvoorbeeld een smartcard) toegang kan krijgen tot zowel ruimtes als pc's. Een belangrijk pluspunt is dat gebruikers hun pc zelf automatisch vergrendelen wanneer ze aan de wandel gaan: ze hebben daarbij immers hun token nodig.
- Het kan zijn dat onderhoudsmonteurs van derden werkzaamheden in kritische ruimtes moeten uitvoeren. Bijvoorbeeld aan de airco of UPS in de serverruimte. Door deze personen continu te (laten) begeleiden voorkomt u 'rare dingen'.

Toegang tot gegevensdragers

- Ladeblokken en dossierkasten zijn veelal vrij gemakkelijk open te breken. Kluizen zijn meer geschikt voor gevoelige informatie. De binnenkant van een kluis kunt u ook zien als een zone. Bedenk bij de aanschaf van een kluis of deze vooral brandwerend moet zijn (zodat de inhoud beschikbaar blijft) of braakwerend (gericht op behoud van vertrouwelijkheid en/of integriteit).

- Nog steeds staat veel informatie op papier. Ook gevoelige informatie. Bijvoorbeeld handboeken voor de beheerder, systeemdocumentatie en de lijst met systeemwachtwoorden. Waar bergt u deze op? Wie kan erbij? Wanneer gevoelige documenten niet meer nodig zijn, moeten medewerkers ze op een correcte wijze kunnen afdanken. Denk hierbij aan versnipperaars en aan speciale papiercontainers. Versnipperaars weten veelal ook wel raad met cd's en dvd's.
- Voed gebruikers op. Leer ze gegevensdagers zoals usb-sticks, smartphones, waardevolle papieren, maar ook (mini-)laptops niet onbeheerd achter te laten. Breng ze het 'clear desk'-principe bij en geef natuurlijk zelf het goede voorbeeld.

En verder …

- Besteed aandacht aan bekabeling. Voorkom storingen en meeluistermogelijkheden.
- Zet IT-systemen vast. Zo voorkomt u valschade.
- Overweeg versleuteling van opgeslagen informatie. Zo blijft bij diefstal de schade beperkt tot de (straat)waarde van het apparaat.
- Een UPS, Uninterruptable Power Supply, beschermt niet alleen tegen stroomuitval, maar ook tegen 'vuile' stroom. Spanningspieken op het elektriciteitsnet vormen ook een gevaar van buiten.

De nieuwe serverruimte – 2

>> Het is Ronald opgevallen dat bij de printers vaak afdrukken rondslingeren. Zo heeft hij wel eens een cv gevonden van iemand die naar een hoge functie solliciteerde, maar ook een ingevuld beoordelingsformulier (van hemzelf nota bene) en een marketingplan met een nieuwe strategie. Omdat dit niet de bedoeling kan zijn, stapt Ronald meestal op de boosdoener zelf af. Het blijft echter gebeuren en die 'menselijke factor' begint Ronald flink te storen. Bij toeval valt zijn oog op een artikel over beveiligd printen: de gebruiker moet eerst een code intoetsen of een token gebruiken voordat de printer documenten afdrukt. Menselijke onvolkomenheid uitbannen via techniek dus. Een prima, maar wel duurdere keuze. Beveiliging heeft een prijs, maar levert ook wat op. Jammer dat dit niet altijd even zichtbaar is. <<

Meer weten

Over fysieke beveiliging is veel informatie beschikbaar. De volgende websites en boeken helpen u verder:

- Hoofdstuk 9 van de ISO-standaard ISO27002:2007 (Code voor Informatiebeveiliging). Te verkrijgen via www.nen.nl
- Fysieke beveiliging, delen 1, 2 en 3. Verschenen in Informatiebeveiliging (september 2004, februari 2005 en april 2005)
- Security Awareness, G.M.H.C. Bongers RSE, Koninklijke Vermande 2005, ISBN: 90 12 108876 4

Ing. Zarco Zwier - Security-coördinator, -consultant en -docent - OGD ICT-diensten - www.ogd.nl - z.zwier@ogd.nl en z.e.zwier@zarco.nl

Zarco is binnen OGD ICT-diensten werkzaam als coördinator van de kenniscel Netwerken en Beveiliging. In deze functie is hij verantwoordelijk voor de borging van kennis in het deelvakgebied netwerken en beveiliging en onderhoudt hij contacten met leveranciers en partners. Daarnaast traint hij collega's op het gebied van beveiliging en geeft hij advies aan klanten over de beveiliging van hun informatiesystemen.

Internetbetalingen

WORD GEEN SLACHTOFFER VAN INTERNETCRIMINALITEIT

Inleiding

De voordelen van betalen via internet zijn duidelijk: 24-uurs beschikbaarheid, gebruiksgemak en snelheid. Vanuit uw huiskamer voert u de gegevens in en binnen enkele seconden is het geld overgeboekt. Als u dat vergelijkt met de traditionele overschrijfkaarten is het moeilijk voor te stellen dat het zo jarenlang in z'n werk ging.

Ondanks dat banken hun uiterste best doen om het systeem veilig te maken, kleven er risico's aan betalen via internet. De financiële transactie vindt immers plaats via een netwerk dat voor iedereen toegankelijk is, ook voor criminelen.

Dit hoofdstuk laat de gevaren zien van betalen via internet en de maatregelen die u kunt nemen om te voorkomen dat u geld verliest door internetbetalingen.

De gevaren van betalen via internet

Wanneer u een betaling via het internet wilt uitvoeren, zijn er onzekerheden waar u mee te maken heeft. Deze onzekerheden zijn in drie categorieën in te delen:

Beschikbaarheid – hebben de gemachtigde personen beschikking over gegevens of middelen op het moment dat zij deze nodig hebben? U vraagt zich misschien af:

- Komt het geld wel bij de begunstigde terecht?
- Is het geld op mijn rekening nog wel veilig?

Integriteit – zijn de beschikbare gegevens correct en volledig? Te denken valt aan:

- Is de begunstigde wel diegene die hij of zij beweert te zijn?
- Komt het geld wel op de gewenste rekening terecht?

Vertrouwelijkheid – zijn de gemachtigde personen de enigen die toegang hebben tot vertrouwelijke informatie? U zou toch niet willen dat:

- Criminelen weten hoe ze een geldige code kunnen maken zoals uw bankcalculator dat doet?
- Een hacker uw ingevoerde bevestigingscode onderschept?

Als een crimineel uw geld kan wegsluizen of een criminele 'verkoper' het product niet levert, dan bestaat het risico dat u uw geld kwijt bent. Om teleurstellingen te voorkomen, is het verstandig om maatregelen te nemen ter beveiliging van uw systemen.

De nieuwe PC – 1

>> Frits is erg content met zijn nieuwe bedrijfs-pc. Ronald heeft vorige week flink z'n handen uit de mouwen gestoken om een nieuwe computer te plaatsen met het nieuwste van het nieuwste; een computer met de allernieuwste versie van Windows. Ronald heeft nog geen virusscanner geïnstalleerd op de nieuwe computer. Hij zou wel willen, maar de virusscanner is helaas niet geschikt voor deze Windows-versie. Na de installatie van de nieuwe computer heeft Ronald de oude pc veilig ontdaan van alle gegevens. Ronald, die duidelijk beveiligingsbewust is, neemt beveiligingsmaatregelen om problemen te voorkomen. Zo zet hij de Windows Firewall aan op de nieuwe computer om toegang van onbevoegde personen en programma's te voorkomen. <<

Maatregelen

Om te voorkomen dat u van uw geld bestolen wordt via het internet, is het aan te raden om de volgende basismaatregelen te nemen:

- Wees zorgvuldig met uw inloggegevens. Geef ze nooit af en bewaar ze niet op papier buiten een kluis.
- Wijzig uw wachtwoorden regelmatig. Gebruik geen onveilige of voor de hand liggende wachtwoorden. Goede wachtwoorden zijn lang en bevatten hoofdletters, kleine letters, cijfers en leestekens.
- Controleer of de betaalwebsite gebruikmaakt van een beveiligde verbinding. Het adres begint met https:// in plaats van http:// Controleer daarnaast of het gebruikte SSL-certificaat ook van de correcte partij is.
- Bescherm uw computers tegen virussen en spyware; installeer een virusscanner. Een spywarescanner komt tegenwoordig ook vaak van pas om vervelende programma's te verwijderen die sommige virusscanners niet kunnen vinden of verwijderen. Wanneer uw bedrijf een verhoogd risico loopt, kunt u aanvullende maatregelen nemen zoals verschillende virusscanners voor e-mail, werkstations en proxy om zo de detectiegraad te verhogen. Geen enkele virusscanner kan 100 procent van alle kwaadaardige software detecteren.
- Wijs één werkstation aan als betalingscomputer; wanneer hier maar een computer voor gebruikt wordt, heeft alleen deze pc extra beveiliging nodig.
  - Scherm deze computer af voor overbodige software; sta alleen toe de benodigde software te gebruiken, dus het besturingssysteem, de internetbrowser en eventueel de banksoftware.
  - Scherm de betalingscomputer af voor overbodige verbindingen; schakel een firewall in op de computer en laat deze binnenkomende verbindingen blokkeren. Geef dit werkstation exclusieve toegang tot de website van de bank. Scherm andere werkstations af. Dit voorkomt misbruik vanaf een ander werkstation.
  - Machtig één persoon om deze computer te gebruiken; door alleen de voor betalingen verantwoordelijke medewerker te machtigen om op deze computer te kunnen inloggen, is het gebruik beter te reguleren.
- Verifieer via de telefoon of de betaling correct is uitgevoerd. Neem contact op met uw bank indien dit niet het geval is.

Deze maatregelen lijken veel werk, maar ze zorgen ervoor dat de computer maar één doel heeft, namelijk betalingen uitvoeren via de eigen bank. Dit minimaliseert het risico op misbruik.

De nieuwe PC – 2

>> Martin is verheugd dat het bedrijf technologisch vooruit gaat, maar omdat het hier om een computer gaat die financiële transacties moet gaan uitvoeren, wil hij er wel zeker van zijn dat het systeem veilig is. Als verantwoordelijke voor de automatisering moet Ronald tekst en uitleg geven aan Martin. Ronald legt uit dat er van hun virusscanner nog geen versie voor deze Windows-variant beschikbaar is. Logischerwijs wil Martin, als eindverantwoordelijke voor het gehele bedrijf, toch wel graag weten of dit wel veilig genoeg is. Ronald geeft aan direct om opheldering bij de leverancier te vragen. Voorlopig geen nieuwe Windows is de conclusie. Het probleem is dat de leverancier pas in het tweede kwartaal van volgend jaar een eerste versie hoopt te hebben. Frits die enthousiast zijn nieuwe pc heeft verkend, loopt binnen bij Ronald.
"Ah, daar ben je!", zegt hij tegen Ronald. "Die nieuwe pc doet een beetje raar…"
Ronald vermoedt dat er een virus of iets dergelijks op de betalingscomputer terecht is gekomen. Hij loopt met Frits mee om te zien wat er aan de hand is. De computer blijkt geïnfecteerd te zijn met het trojaans paard Win32. Ficti.f, dat schermafdrukken, muisbewegingen en toetsenbordaanslagen registreert en doorstuurt naar kwaadwillenden. Ronald formatteert de computer en installeert Windows XP, inclusief antivirussoftware. Gelukkig waren er nog geen betalingen uitgevoerd op de nieuwe computer. <<

Wanneer u slachtoffer bent geworden van internetcriminaliteit, doet u er altijd verstandig aan om aangifte te doen bij de politie.

Meer weten

- Veilig bankieren - http://www.veiligbankieren.nl
- 3x kloppen - http://www.3xkloppen.nl
- Alles over betalen - http://www.allesoverbetalen.nl/bedrijven
- Ius mentis - http://www.iusmentis.com/zakendoen/epayment/internetbetalen
- Kijk ook op website van uw eigen bank.

Ing. Zarco Zwier - Security-coördinator, -consultant en -docent - OGD ICT-diensten - www.ogd.nl - z.zwier@ogd.nl en z.e.zwier@zarco.nl

Zarco is binnen OGD ICT-diensten werkzaam als coördinator van de kenniscel Netwerken en Beveiliging. In deze functie is hij verantwoordelijk voor de borging van kennis in het deelvakgebied netwerken en beveiliging en onderhoudt hij contacten met leveranciers en partners. Daarnaast traint hij collega's op het gebied van beveiliging en geeft hij advies aan klanten over de beveiliging van hun informatiesystemen.

Fysieke beveiliging technische ruimten

HET BELANG VAN HET FYSIEKE VOOR HET ELEKTRONISCHE

Inleiding

Wanneer er over informatiebeveiliging wordt gesproken, wordt het onderwerp fysieke beveiliging nogal eens vergeten. Dit kan u duur komen te staan. Een kwaadwillend persoon kan in het ergste geval met fysieke toegang volledige toegang tot de systemen in de technische ruimtes en dus toegang tot uw informatie verkrijgen. Anderzijds kan overmacht al uw bedrijfsgegevens vernietigen.

In dit hoofdstuk worden de risico's behandeld die een bedrijf kan lopen wanneer men de fysieke beveiliging van de technische ruimtes niet op orde heeft.

Fysieke gevaren voor uw data

Er zijn veel fysieke gevaren die u uw data kunnen kosten. Als niet voldoende maatregelen heeft genomen, kan dit gevolgen hebben voor de beschikbaarheid, integriteit en vertrouwelijkheid van uw data:

- U zou niet willen dat de beschikbaarheid van uw informatie en informatiemiddelen in het gedrang komt. Een mogelijk horrorscenario: buiten kantooruren ontstaat er door lekkage kortsluiting in de serverruimte en er ontstaat brand. Er is geen

automatische gasblusinstallatie geïnstalleerd en alle tapes worden in de serverruimte in een openstaande of alleen brandwerende kluis bewaard. Belangrijke data kan zo verloren gaan.

- Blijft de integriteit van de data intact; zijn de opgeslagen gegevens volledig en correct, zoals u ze heeft opgeslagen? Wanneer een ongeautoriseerd persoon toegang tot de opslagsystemen kan verkrijgen, kan deze persoon mogelijk cruciale data wijzigen in eigen voordeel. Te denken valt aan zaken als rekeningnummers van partijen aan wie u maandelijks geld overmaakt. Wanneer dit geautomatiseerd gebeurt, ontvangen personen geld van u zonder daar recht op te hebben.
- Blijven uw bedrijfsgegevens vertrouwelijk? Heeft u bedrijfsgeheimen opgeslagen op uw systemen? Dan bent u er vast benauwd voor dat deze gegevens in handen van een concurrent komen, wanneer een inbreker een stapel tapes uit de serverruimte meeneemt.

Wanneer gegevens niet veilig bewaard worden en u raakt uw data op de productiesystemen kwijt, dan kan dat in het ergste geval het einde van uw bedrijf betekenen.

Een lek met gevolgen – 1

>> Het bedrijf van Martin is in korte tijd flink gegroeid. Tot voor kort deelden ze hun huidige pand met een vastgoedkantoor. Dit kantoor moest al vrij snel in de kredietcrisis de deuren sluiten, waarna Martin de vrijgekomen ruimte erbij huurde. Nu kon eindelijk gewerkt worden aan een professionele serverruimte. Ronald had een gespecialiseerde aannemer ingehuurd om de serverruimte in te richten toen ze het nieuwe pand betrokken. Deze aannemer legde tevens nieuwe bekabeling en outlets aan en nam de verhuizing van de oude naar de nieuwe ruimte op zich. Het is vrijdag, twee weken na de verhuizing. Afgelopen nacht heeft de airco blijkbaar overuren gedraaid en is daarbij gaan lekken. Vervelend genoeg was er een stopcontact afgemonteerd onder de airconditioning. Vanwege gebrek aan extra stroomvoorziening in de serverkast, hebben de aannemers de telefooncentrale op dit stopcontact aangesloten. De door de lekkage veroorzaakte kortsluiting heeft de voeding van de telefooncentrale opgeblazen en nu zit het hele kantoor zonder telefoon. <<

Fysieke maatregelen om uw data te beschermen

Welke maatregelen kunt u nemen om uw informatie en informatiemiddelen fysiek te beschermen tegen catastrofes en indringers?
Bescherm uw apparatuur tegen de elementen

- Zorg dat lekkages niet kunnen voorkomen of in ieder geval niet uw apparatuur kunnen beschadigen. Dus zorg ervoor dat er geen verwarmingsbuizen of airconditioningunit boven de apparatuur geplaatst zijn.
- Plaats de apparatuur niet in een kelder die onder water kan lopen.
- Installeer een brandalarm en laat deze regelmatig controleren.
- Zorg voor een gedegen en passende brandblusinstallatie, dus geen sprinklersysteem in de serverruimte. Laat de blussystemen periodiek controleren.
- Zorg voor een goede koeling van de ruimte. Laat de airconditioning regelmatig een onderhoudsbeurt ondergaan.
- Bewaar de back-ups niet in de serverruimte, maar in een water- en brandbestendige kluis, liefst op een andere locatie.

Zorg voor toegangsbeveiliging en -registratie

- Is er bekend welke ruimtes extra beveiliging hebben of moeten hebben? Denk ook aan ruimtes waar switches, routers en modems geplaatst zijn.
- Sluit ook kasten in de technische ruimtes goed af, zoals kluizen en serverracks.
- Maak onderscheid in toegangsbeveiliging en -registratie voor het pand en voor de beveiligde ruimtes. Bewaar deze gegevens net zolang als uw financiële gegevens. Mochten er inconsistenties blijken te zijn binnen de financiële bewaartermijn, dan kan er uitgezocht worden of er iemand toegang tot de gegevens had.
- Baseer de toegangsbeveiliging op een elektronisch slot in plaats van een sleutel en maak onderscheid wie toegang tot de verschillende technische ruimtes krijgt.
- Is de beveiligde ruimte ook daadwerkelijk altijd gesloten? Wanneer toch voor een sleutel is gekozen, wordt de sleutel wel uit het slot gehaald?
- Loopt het systeemplafond niet boven de deur door naar de beveiligde ruimtes?

- Is vastgelegd dat er geen etenswaren en vloeistoffen mogen worden meegenomen naar de serverruimte als ze niet afgesloten zijn verpakt? Denk aan drinken, schoonmaakemmers enzovoorts.
- Blokkeer de consoles van alle pc's.
- Zorg voor correct aangesloten apparatuur
- Is de stroomvoorziening voldoende? Liefst eigen groepen voor airconditioning per rack. Gebruik geen verdeeldozen op een enkel stopcontact.
- Worden de elektrische groepen in de serverkast alleen gebruikt voor servers en netwerkapparatuur?
- Is de technische apparatuur alleen aangesloten op de stroomvoorziening in de kast?
- Zijn alle aansluitingen en kabels correct afgewerkt en voorzien van een label? Is de kans groot dat iemand belangrijke aansluitingen ontkoppelt of een stekker verkeerd aansluit?
- Is alle apparatuur op een UPS aangesloten met voldoende capaciteit? Denk ook aan het console. Wordt de UPS regelmatig getest? Hoe oud zijn de batterijen? Is de up-time van iedere UPS bekend?

Een lek met gevolgen – 2

>> Martin ontdekt die vrijdagochtend al vrij snel dat niemand kan bellen. Zodra Ronald binnen komt lopen spreekt hij hem aan.

"Er kan niemand bellen, Ronald! Enig idee waardoor dat kan komen?"

"Momentje, ik ga even kijken", antwoordt Ronald.

Eenmaal in de serverruimte aangekomen, ziet Ronald de lekkage van de airconditioning naar het stopcontact waarop de telefooncentrale is aangesloten.

"Slechte zaak!", laat Ronald Martin weten. "Ik vermoed dat de voeding van de centrale stuk is. Er is lekkage geweest en hij gaat niet meer aan."

Martin is verbaasd en wil weten hoe er lekkage is ontstaan. Waarom zijn er geen maatregelen tegen beschadiging van de apparatuur genomen? Ronald legt uit dat de telefooncentrale

door de aannemer op het betreffende stopcontact is aangesloten wegens gebrek aan stroomvoorziening in de serverkast. Op deze mededeling laat Martin met een boze ondertoon weten, "Ik ga mobiel even contact opnemen met de verantwoordelijken!"

Enige momenten later is hij terug in het kantoor van Ronald. De kosten zijn voor de aannemer, zo laat hij Ronald weten. Allebei beseffen ze hoe blij ze zijn dat er geen brand uitgebroken is. Ronald gaat direct controleren of er geen andere risico's zijn ontstaan bij het inrichten van de serverruimte. Bij een volgende verhuizing doet hij dit uiteraard vooraf. <<

Denk dus goed na over hoe u informatiemiddelen installeert, hoe u de technische ruimtes inricht en beveiligt en hoe u informatie achterlaat.

Meer weten

- Richtlijnenboek Informatiebeveiliging SUWI gemeenten
  http://www.bkwi.nl/fileadmin/informatiebeveiligingsplan/docs/Richtlijnen_html
- Fysieke beveiliging (deel 1)
  https://www.pvib.nl/download/?id=6474504
- Fysieke beveiliging (deel 2)
  https://www.pvib.nl/download/?id=6473494
- Fysieke beveiliging (deel 3)
  https://www.pvib.nl/download/?id=6473529
  Implementing Robust Physical Security
  http://www.sans.org/reading_room/whitepapers/physcial/1447.php (Engels)
- Protect Yourself
  http://www.sans.org/reading_room/whitepapers/physcial/271.php (Engels)

Rudolf van der Heide - Specialist data warehousing en business intelligence - Zelfstandig ondernemer - www.rudolfvanderheide.nl - info@rudolfvanderheide.nl

Rudolf heeft onder andere bij The Vision Web, Delta Lloyd en ING gewerkt als data warehouse-specialist. Sinds 2007 zet hij zijn ruim tien jaar ervaring als zelfstandig specialist in voor diverse opdrachtgevers. Hij is gespecialiseerd in architectuur en performance tuning.

Beveiliging datawarehouses

Inleiding

Naast systemen voor de ondersteuning van de operationele processen van uw onderneming, heeft u behoefte aan mogelijkheden om uw informatie te analyseren en te rapporteren. Dit kan door middel van een datawarehouse voor wat grotere ondernemingen of met eenvoudiger middelen zoals rechtstreekse rapporten op de database van de operationele systemen. De risico's en de beveiligingseisen verschillen aanzienlijk van die van operationele systemen. Dit hoofdstuk gaat over de beveiliging van rapportagesystemen.

Informatie is het enige productiemiddel dat meer waard wordt naarmate je het meer gebruikt. Dit suggereert niet al te veel beveiliging. Eenvoudige toegang tot informatie kan veel opleveren.

De verdachte klant

>> Jantine is bezig met het versturen van betalingsherinneringen. Een vervelend klusje, maar uiteindelijk zeer dankbaar werk als ook het laatste geld binnen is. Terwijl ze bezig is, ziet ze dat een grote klant een forse betalingsachterstand heeft. Ergens vertrouwt ze het niet helemaal. Ze kijkt in het verkoopsysteem en ziet dat deze klant nog steeds hele grote orders plaatst. Omdat het zo'n grote klant is, kunnen ze rechtstreeks orders plaatsen. Een mooie service, maar daardoor is er ook wat minder controle.

Bij de koffieautomaat ziet ze Ronald en spreekt hem aan:

"Ronald, kun je me even helpen?", vraagt ze met haar stralende glimlach.

"Natuurlijk Jantine, wat kan ik voor je doen?", zegt Ronald, die geen weerstand kan bieden aan zo'n verzoek.

"Ik vertrouw het bestelbedrag van een grote klant niet helemaal, maar ik wil ook geen paniek zaaien. Volgens mij is er iets aan de hand."

"Zullen we dan samen wat diepgaander naar hun orders kijken?"

Zo gezegd, zo gedaan. Ronald en Jantine bekijken de orderhistorie van de klant en zien dat deze opvallend meer bestelt dan vorig jaar. Samen gaan ze naar Martin en vertellen over hun zorgen. Vanwege de duidelijke analyse, neemt Martin hun zorgen serieus en gaat er achteraan.

De volgende morgen vertelt Martin aan alle medewerkers dat de klant geen bestellingen meer mag plaatsen, totdat alle achterstallige betalingen binnen zijn. Het lijkt erop dat de klant in grote betalingsproblemen zit en nog snel extra voorraad probeert te bestellen, voordat leveranciers niet meer willen leveren. Martin complimenteert daarop Jantine en Ronald voor hun oplettendheid. <<

Aan de andere kant maken eenvoudige rapportagesystemen het ook gemakkelijker om bijvoorbeeld lijsten met klantgegevens te verspreiden.

Het voordeel van niet beveiligen

Bij veel organisaties wordt een rapportageomgeving 'zo goed mogelijk beveiligd'. Dat wil zeggen, dat je alleen de informatie kan zien, waar je echt toegang toe mag hebben in het kader van je functie. Sommige organisaties gaan zelfs zo ver dat verkopers alleen de informatie over hun eigen klanten mogen zien. Als u het zo aanpakt, zal u als organisatie niet snel een probleem als in de case ontdekken.

Bij operationele systemen is het belangrijk dat medewerkers niet zomaar van alles kunnen, omdat daarmee de dienstverlening in gevaar wordt gebracht. Natuurlijk mag niet iedereen zomaar een order kunnen wijzigen. Bij rapportagesystemen speelt dit veel minder. In principe zijn deze systemen alleen maar om informatie te raadplegen en kun je dus niets wijzigen.

Dit betekent natuurlijk niet dat u maar helemaal niet moet beveiligen. Het is belangrijk om de risico's van niet beveiligen af te wegen tegen de mogelijke opbrengsten. Deze opbrengsten zijn onder meer:

- Fraudedetectie, zie het genoemde voorbeeld.
- Kwaliteit van de informatie, als meer mensen de informatie gebruiken, is er meer noodzaak om de kwaliteit te verbeteren.
- Kennisdeling en samenwerking. Het kan een verkoper op nieuwe ideeën brengen, als hij gegevens kan zien over klanten van andere verkopers.
- Vertrouwen. Heel strikte beveiliging is een blijk van wantrouwen. Wat is het effect daarvan op uw medewerkers?

Redenen om wel te beveiligen

Wat zijn redenen om wel te beveiligen? Achtereenvolgens komen ter sprake: wettelijke eisen en reputatieschade, toegang van externe partijen tot uw systemen, gebruikersvriendelijkheid, lekken.
Voor alle duidelijkheid: we praten hier over systemen voor rapportage en dus met alleen leestoegang. De betrouwbaarheid van de informatie is alleen te garanderen als een rapportagesysteem automatisch gevuld wordt vanuit andere systemen via batchprocessen. Als er al iemand schrijfrechten nodig heeft, gelden hiervoor dezelfde eisen als bij operationele systemen.

Wettelijke eisen en reputatieschade

Bepaalde informatie mag niet zomaar toegankelijk zijn, bijvoorbeeld in het kader van de Wet bescherming persoonsgegevens, maar ook vanwege reputatieschade als ze op straat komen te liggen, bijvoorbeeld creditcardgegevens. Een ander duidelijk voorbeeld zijn financiële gegevens in een beursgenoteerd bedrijf, vanwege mogelijk misbruik van voorkennis.

Zodra u met dit soort informatie te maken hebt, moet u deze afschermen om elke vorm van ongeautoriseerd gebruik te voorkomen. De andere kant van het verhaal is dat deze informatie ook vaak niet nodig is voor analyses. Als u de verkopen van een verzekeringsbedrijf wilt analyseren kunt u volstaan met klantnummer en extra demografische gegevens, zoals leeftijd, gezinssamenstelling en postcode. Heeft iemand de detailgegevens nodig, dan kan hij deze verzekeringsadministratie krijgen aan de hand van het klantnummer, als hij daar de rechten toe heeft.

Toegang van externe partijen tot uw (rapportage)systemen

Geeft u klanten en leveranciers toegang tot uw systemen, zodat ze de status van orders kunnen volgen? In dat geval kunt u het beste te werk gaan zoals bij operationele systemen. Een externe partij mag alleen zien waar hij expliciet recht op heeft. Dit geeft soms tegenstrijdige belangen: enerzijds moet de rapportageomgeving zo open mogelijk zijn voor interne medewerkers, anderzijds is er strikte beveiliging voor externe partijen. Hierdoor is het risico op fouten aanwezig en zijn de eisen vaak niet meer te combineren. Mogelijke oplossingen zijn een apart systeem voor externe partijen of externe partijen die alleen informatie kunnen opvragen via webservices.

Gebruikersvriendelijkheid

Te veel beveiliging roept al snel irritatie op. Er zijn echter situaties waarin beveiliging juist gebruikersvriendelijkheid oplevert. Als u een grote keten heeft met veel verschillende vestigingen, zullen medewerkers juist blij zijn, als ze alleen de klanten of verkopen van hun eigen vestiging te zien krijgen.

Lekken

Zoals we gezien hebben, heeft het grote voordelen om niet al te veel beveiliging te hebben in een rapportageomgeving. Daarmee wordt het gevaar van lekken wel groter. Dit speelt met name als rapportage plaatsvindt in tools als Excel en Access. Veel bedrijven stoppen alle verkoopinformatie in Excel of Access, zodat informatie gemakkelijk te analyseren is. Dat betekent wel dat medewerkers die informatie meenemen op laptops en naar thuis-pc's. En daarmee ligt zomaar het hele bestand op straat.

Probeer dit te voorkomen door een eenvoudig rapportagesysteem te ontwikkelen, waarin medewerkers online de informatie kunnen opvragen die ze nodig hebben, ook buiten het kantoor.

De IT-afdeling

Hoe zit het met de toegang voor beheerders en ontwikkelaars?
Problemen met rapportage en analyse zijn alleen goed op te lossen met productiegegevens. Hetzelfde geldt voor het ontwikkelen van rapportageoplossingen en standaardrapportages. De oorzaak is dat in productiesituaties de gebruiker aan het werk is, praktische oplossingen probeert te vinden en ook gewoon fouten maakt. Ook is het belangrijk dat problemen snel worden opgelost, dus in het productiesysteem. Analyses en rapportages zijn veel minder gestructureerd dan operationele processen, waardoor er ook veel sneller iets mis is.
Vaak heeft de persoon die het handigst is in het analyseren van informatie (een slimme databasebeheerder, een informatieanalist, een assistent controller) geen toegang tot veel productiesystemen en kan daarom anderen niet goed ondersteunen bij hun problemen.
Om die reden is het verstandig beheerders en ontwikkelaars wel toegang te geven tot productiesystemen. Een goede audit-functie heeft dan natuurlijk wel veel preventieve waarde. Maar als u uw medewerkers niet vertrouwt, kunt u ze beter niet aannemen.

Aanbevelingen

- Geef interne medewerkers ruim toegang voor tot het bekijken en analyseren van informatie, zolang ze niets kunnen wijzigen.
- Kijk niet alleen naar de risico's, maar ook naar de (verborgen) opbrengsten van niet te strikt beveiligen.
- Voorkom Excel en Access als rapportagesysteem. Geef in plaats daarvan medewerkers ook buiten kantoor mogelijkheden tot online rapportages.
- Geef beheerders voldoende toegang tot productiedata. Beheerders die geen toegang hebben tot productiegegevens, hebben een negatief effect op bruikbaarheid van de rapportageomgeving en de tevredenheid van uw medewerkers met de rapportageomgeving.

Marcel de Graaf MBCI - senior adviseur informatiebeveiliging - Ministerie van Defensie - www.defensie.nl - marcel@informatiebeveiliging.org
Marcel heeft 25 jaar lang zowel brede als diepgaande ervaring en kennis opgedaan op het terrein van de informatievoorziening en de ICT. Bij informatiebeveiliging begeeft hij zich het liefst op het snijvlak tussen business en ICT.

Rick Zondervan - beheerder Security Management & Control - Ministerie van Defensie - www.defensie.nl - rick@zondervn.nl
Rick is onder andere betrokken geweest bij de verhuizing van een ICT-bedrijf, waar hij een analyse heeft gemaakt van de mogelijke bedreigingen. Rick weet waaraan hij moet denken bij de verhuizing van een ICT-organisatie.

Uitwijkvoorzieningen en verhuizing

Inleiding

Elk bedrijf maakt wel eens een verhuizing mee, bijvoorbeeld omdat het door succes letterlijk uit zijn voegen barst. Bij een bedrijfsverhuizing is informatiebeveiliging natuurlijk uitermate belangrijk. Vragen als 'werkt alles straks weer in het nieuwe pand?', 'wat doen wij als de verhuiswagen een ongeluk krijgt?' en 'waar moeten we op letten op de nieuwe locatie?' moet u beantwoorden. Een verhuizing moet goed worden voorbereid. Nog altijd kan het onverwachte en ongehoopte optreden; er ontstaat een calamiteit. Grote organisaties hebben (als het goed is) een crisisteam dat opgeleid en geoefend is om bij calamiteiten op te treden. Binnen het mkb bestaat hier meestal de mogelijkheid niet voor omdat het simpelweg teveel kost. Dit hoofdstuk beschrijft hoe u, zonder al teveel kosten toch maatregelen kunt nemen, mocht er iets ernstig misgaan. De hoofdpersoon Ronald in de case studies heeft deze kennis en ervaring en weet de problemen op te lossen. Alles gaat dus uiteindelijk goed. Wel even een gewetensvraag: Ronald is een goede en slimme vent, maar is het verstandig om voor uw continuïteit afhankelijk te zijn van uw ICT-beheerder?

Voorbereiding op maatregelen achteraf

De verhuizing van uw bedrijf betekent nogal wat. U moet dan van alles en nog wat regelen. Vergelijk het maar met het verhuizen naar een

nieuwe woning: Wat nemen we mee? Wat kopen we nieuw? Verhuizen we zelf? Willen we na de verhuizing direct overnachten in het nieuwe huis? Als u eenmaal verhuisd bent naar uw nieuwe huis, is het vaak zoeken naar uw spullen. Het zit nog in dozen of heeft een nieuwe plek gevonden. Dit kan helemaal het geval zijn als u een verhuisbedrijf heeft ingehuurd en u heeft geen afspraken gemaakt over de stickers en plekken waar de spullen moeten worden neergezet, et cetera. Daarnaast zullen bepaalde apparaten nog niet aangesloten zijn. Maar goed, u bent verhuisd en dat neemt u dan op de koop toe.
Bij een bedrijfsverhuizing kan hetzelfde gebeuren, alleen kost het u direct geld als u niet meteen aan de slag kunt in uw nieuwe pand. Het is dus verstandig om bij een verhuizing stil te staan bij de risico's en om voorzorgsmaatregelen te nemen. Maar hoe goed alles van tevoren ook geregeld is, er kan natuurlijk altijd iets fout gaan. De praktijk leert ons dat als er dan iets mis gaat, er opeens van alles mis gaat. Meestal komt dit, omdat de organisatie zich hier simpelweg niet op heeft voorbereid. En wat zijn dan de reacties in zo'n situatie? Er ontstaat chaos en soms paniek, zekerheden vallen weg, er is ongeloof, mensen trekken zich terug of vinden dat het wel meevalt, de medewerkers en het management wijzen onderling schuldigen aan en spelen paniekvoetbal. De controle is weg en het wordt van kwaad tot erger.
Natuurlijk kunt u zich niet overal op voorbereiden, maar als u de risico's in kaart heeft gebracht, kunt u afspraken maken over wat te doen als het dan toch mis gaat. Elke organisatie heeft haar eigen kenmerken, maar er bestaan enkele basispunten waar elk bedrijf bij een calamiteit mee te maken krijgt. Hieronder worden deze opgesomd en toegelicht. De lijst is niet volledig, maar het geeft stof tot nadenken en om toe te passen op uw eigen organisatie.

Eerste uren zijn kritiek

Hoe eerder de organisatie onderkent dat er iets ernstig fout is gegaan, hoe groter de kans dat er snel weer controle op de situatie ontstaat. Bij een verhuizing is het daarom belangrijk dat er continu duidelijk is wat er gebeurt. De gouden regel is: eerst denken en dan doen. Te snel en ondoordacht handelen kan weer leiden tot foute inschattingen met alle gevolgen van dien. Hoe goed de bedoelingen van bijvoorbeeld de verhuizers ook zijn bij een probleem: het is uw bedrijf, u beslist wat er gebeurt! Het is daarom

van belang om hier een soort scenario voor klaar te hebben liggen. Bepaal dan ook wie er besluiten mag nemen, mocht er echt wat fout gaan.

Organisatie

Bij een verhuizing kunnen er veel zaken misgaan; zo moeten de meeste organisaties er niet aan denken dat de computersystemen opeens niet blijken te werken. Zorg er daarom voor dat van tevoren is afgesproken wie wat doet als een dergelijke situatie zich voordoet. Het kan enorm helpen als een up-to-date lijst met naw-gegevens voorhanden is, zodat u uw medewerkers van de situatie op de hoogte kunt brengen. Wellicht heeft u een projectteam voor de verhuizing ingesteld. Zorg ervoor dat de teamleden weten hoe ze moeten optreden bij een calamiteit.

Besluitvorming

Een ongeluk komt meestal niet alleen en vaak op een ongewenst moment. Er moet daarentegen wel snel worden besloten welke acties u gaat ondernemen. Het is daarom van levensbelang om slagvaardig te kunnen handelen. Er moet iemand zijn die op het juiste moment de juiste beslissingen kan nemen. Dit hoeft overigens niet altijd iemand van het management te zijn.

Informatie

Als de dingen misgaan, verzamel dan de relevante informatie zoals:

- Wat is er gebeurd?
- Wat kan de oorzaak zijn?
- Wat is de schade?
- Wanneer gebeurde het?
- Wie zijn erbij betrokken?
- Waar vond het plaats?

Communicatie (intern/ extern)

Op het moment dat er besloten is dat er sprake is van een calamiteit, is de kans op verspreiding van foutieve informatie groot. Dit kan weer negatieve invloed hebben op het herstel; er gaat bijvoorbeeld tijd verloren door

onduidelijkheden. Communiceer dus voldoende en helder. Dit geldt zowel voor de medewerkers als voor de buitenwereld. Bij de buitenwereld moet u denken aan politie, brandweer, hulpdiensten, enzovoort. Soms moet u zelfs de pers te woord staan. Wees voorbereid op wat en hoe de organisatie met de pers communiceert. Op welke wijze u ook besluit te communiceren: lieg nooit. Onwaarheden komen over het algemeen uit, waardoor u uw geloofwaardigheid, en dus uw betrouwbaarheid, als organisatie verliest.

Herstel

Als de problemen onder controle zijn, kan het herstel beginnen. Het is dan belangrijk om te weten welke bedrijfsonderdelen weer als eerste operationeel moeten zijn en welke mensen en middelen hiervoor nodig zijn. Wees dus voorbereid ook al denkt u er misschien liever niet over na.

Nazorg en evaluatie

De problemen zijn voorbij en het bedrijf is weer opgestart. Blijf echter communiceren met zowel de medewerkers als de buitenwereld. Laat duidelijk merken dat uw organisatie er (weer) is. Vergeet niet eenieder te bedanken voor de hulp en steun. Draai de situatie om: het klopt dat u een groot probleem had maar u bent in staat gebleken dit goed op te lossen. Evalueer de situatie; breng de goede en verbeterpunten in kaart. Leer ervan.

Een goede voorbereiding is het halve werk – 1

>> Ronald krijgt van Martin te horen dat het bedrijf gaat verhuizen naar een nieuwe locatie en dat Ronald de verhuizing rondom de ICT voor zijn rekening moet nemen. Als Ronald denkt aan het verhuizen van een bedrijf dan blijft het verhaal van een oud-collega in zijn hoofd zitten. Die oud-collega vertelde eens dat het bedrijf waar hij destijds werkte als helpdeskmedewerker ging verhuizen. De verhuizing zou op een zaterdag plaatsvinden zodat het personeel maandag weer aan het werk kon. Helaas liepen de zaken anders dan verwacht. De verhuiswagen met daarin alle systemen kwam in een slip terecht, kantelde en in een oogwenk lag alle kostbare apparatuur in gruzelementen. ‘s Maandags liepen

alle medewerkers verdwaasd rond en wisten ze niet wat ze nu moesten gaan doen. Ook de desktop, die hij nodig had om zijn helpdeskwerkzaamheden uit te voeren was onherstelbaar beschadigd. De nieuwe apparatuur was zeer snel besteld, maar tijdens de drie dagen levertijd konden hij en zijn collega's hun werk niet uitvoeren. Gelukkig had een systeembeheerder nog een maand oude back-up op zijn laptop staan zodat niet alle data weg was. Drie dagen later kon de oud-collega weer aan het werk. Hij had drie dagen gevuld met het terugzoeken van oude back-ups en tafeltennis met zijn collega's. Ronald weet dus ongeveer wat er fout kan gaan bij een verhuizing. Hij wil dat zodra zijn collega's na de verhuizing op hun nieuwe werkplek komen alles gewoon werkt als voorheen. Daarom zal hij goed moeten onderzoeken hoe hij de verhuizing van a tot z aanpakt. <<

Maatregelen vooraf

Is het dan wel mogelijk om goed voorbereid te verhuizen? Natuurlijk. U doet dit door voorzorgsmaatregelen te nemen. Hieronder treft u een aantal maatregelen aan die u kunt gebruiken als voorbeeld. Zo kunt u uw eigen maatregelen gaan vaststellen. Definieer randvoorwaarden voordat u met verhuizen begint: infrastructuur ICT-netwerk moet klaar liggen.
Zo is het bijvoorbeeld erg handig als het nieuwe pand al helemaal klaar is om een compleet netwerk te ontvangen. Zo moet er een infrastructuur klaar zijn met voldoende en goede bekabeling. Dit kan allemaal al voordat de verhuizing plaatsvindt. Door een infrastructuur klaar te hebben, is het bij aankomst van onder andere de servers, routers slechts een kwestie van aansluiten en opstarten.
Zorg voor een goede beveiliging: huur ze in of laat uw meest betrouwbare mensen de meest waardevolle zaken verhuizen.
Alleen voordat alle spullen er zijn, liggen er nog veel risico's op de loer. Zoals in het voorbeeld is het mogelijk dat de spullen nooit aankomen, dit kan komen door een chauffeur met andere plannen, een ongeval of overval. Tegen deze risico's is van alles te doen en te bedenken maar ze moeten wel realistisch en haalbaar zijn. Een politie-escorte aanvragen is een idee, maar hoe groot is de kans dat u die krijgt? Er verhuizen immers elk weekend wel bedrijven en de politie heeft wel betere dingen te

doen. Een andere manier om deze risico's tegen te gaan is om te zorgen dat er een complete back-up is van alle data en deze los van de rest van de systemen te vervoeren. Ook is het mogelijk om nieuwe systemen klaar te zetten op de nieuwe locatie om in het geval dat de systemen niet aankomen de nieuwe systemen in te richten en daar de back-ups op te laden. Op deze manier is zeker gesteld dat medewerkers na de verhuizing meteen weer aan de slag kunnen.

Een goede voorbereiding is het halve werk – 2

>> Ronald staat aan de vooravond van de grote verhuizing. Hij heeft voor het verhuizen verschillende checklists op Google gevonden en op basis hiervan zijn eigen checklist samengesteld. Nog één keer loopt hij zijn checklist na:

• Infrastructuur nieuwe locatie • Back-up klaar om te vervoeren • Systemen staan klaar • Back-upsysteem geregeld • Verhuiswagen geregeld • Hulp geregeld

De volgende ochtend gaat het dan gebeuren. In het nieuwe gebouw is de internetverbinding al opgezet en staan alle routers, firewalls en switches ingesteld zoals afgesproken. Vannacht is een grote back-up gemaakt van het hele serverpark en deze back-up is al op de locatie aangekomen. Tijdens het vervoeren van de servers valt er één server. Deze start niet meer op de nieuwe locatie, dus het vermoeden bestaat dat er een stuk hardware kapot gegaan is. Gelukkig heeft Ronald zijn zaken goed op orde, er zijn namelijk voor de zekerheid verschillende reserveservers gehuurd. Het is nu een kwestie van de harde schijf in de reserveserver vullen met de goede back-up en het systeem draait weer. Maandag na de verhuizing komt het personeel aan op hun nieuwe werkplek. Veelgehoorde opmerkingen zijn 'wat goed dat je er niets van merkt dat we ergens anders werken' en 'zijn de e-mailadressen van iedereen nog wel hetzelfde?'. Een enkele computer heeft de verhuizing niet overleefd, zo blijkt later. Dan is er een netwerkkaart stuk, dan weer een harde schijf. Allemaal geen probleem voor Ronald , want hij heeft genoeg reserveonderdelen. Aan het einde van de eerste week in het nieuwe pand komt Martin Ronald bedanken voor de soepele ICT-verhuizing. <<

ing. Kelvin Rorive MSc CISSP CISA - Senior Security consultant - Strict - www.strict.nl - k.rorive@strict.nl

Kelvin is zijn carriere in de informatiebeveiliging in 1996 gestart als netwerk-beveiligingsexpert bij een grote bank. Daarna heeft hij als consultant uiteenlopende bedrijven ondersteund bij hun informatiebeveiligingvraagstukken. De laatste jaren richt Kelvin zich vooral op het beheersbaar en controleerbaar inrichten van informatiebeveiliging.

Beheersing van informatiebeveiliging

HOE HOUD IK MIJN IT-OMGEVING VEILIG?

Inleiding

In dit boekje wordt uitgebreid beschreven hoe u het beste tot een goed beveiligde IT-omgeving kan komen. Maar een IT-omgeving verandert voortdurend als gevolg van bijvoorbeeld nieuwe ontwikkelingen en organisatorische aanpassingen. Het is een flinke uitdaging de IT-omgeving mee te laten veranderen. Maar wat betekenen deze veranderingen voor de beveiliging van de IT-omgeving? Deze moet natuurlijk ook bijgesteld worden. Maar hoe kunt u dat doen zonder telkens weer een uitgebreide risicoanalyse uit te voeren? In dit artikel wordt beschreven hoe u met zo weinig mogelijk inspanning toch de IT-omgeving aantoonbaar veilig houdt, ondanks de voordurende veranderingen.

Beheersing van Informatiebeveiliging

Hoe vaak komt het niet voor dat uw bedrijf een keuze maakt en de IT-afdeling wordt gevraagd om hiervoor zo snel mogelijk een applicatie te installeren. 'De concurrentie heeft ook deze applicatie en we willen niet achterlopen'. Gevolg is een haastklus waarbij beveiliging 'even' naar achter wordt geschoven. Meestal betekent dit, dat de beveiliging nooit wordt ingevuld. Want het volgende project staat al voor de deur.

Neem een nieuwe financiële applicatie die is geïnstalleerd in de IT-omgeving. Er moet nagedacht worden over hoe er moet worden omgegaan met een calamiteit. Er is waarschijnlijk wel wat geregeld met een back-up. Ook is het van belang dat de database van de applicatie beveiligd is, omdat hierin toevallig de hele financiële boekhouding staat. Zonder de beveiliging werkt de applicatie functioneel prima. Dus de keuze om beveiliging uit te stellen is dan snel gemaakt.

Op deze manier ontstaat een steeds groter wordend gat in de beveiliging. De organisatie wordt daarmee in de loop der tijd steeds kwetsbaarder en er ontstaan onacceptabele risico's.

Idealiter zou u willen dat u bij elke aanpassing in de IT-omgeving ook de noodzakelijke aanpassingen kunt doen in de beveiliging. Zo houdt u de beveiliging van de IT-omgeving op een 'gezond' niveau. Ook voorkomt u zo dat er een kostbare en tijdrovende inhaalslag gemaakt moet worden op het gebied van beveiliging.

Als verantwoordelijke wilt u in een vroeg stadium op de hoogte zijn van aanstaande veranderingen. Zo wilt u bijvoorbeeld vroegtijdig betrokken zijn bij fusiegesprekken. Een dergelijke verandering vereist nogal wat voorbereidingen om de fusie op het gebied van IT en beveiliging vloeiend te laten verlopen.

Het is van belang dat u als verantwoordelijke op de juiste plekken in de organisatie uw invloed kan uitoefenen. Het vooraf meedenken bij de keuze van een nieuw product helpt bij het maken van de juiste beslissingen. Al is het maar om te kunnen inbrengen dat u meer tijd nodig heeft om de voorgenomen wijziging veilig uit te voeren.

Klantinformatie onder handbereik – 1

>> Frits heeft inmiddels honderden visitekaartjes van klanten en potentiële klanten. Het CRM-pakket barst uit zijn voegen en is dusdanig verouderd dat het niet meer ondersteund wordt. Zo heeft Frits geen goed overzicht meer over al deze relaties, waardoor mo-

gelijk verkoopkansen worden gemist. Frits heeft samen met Martin besloten om een nieuw CRM-pakket aan te schaffen waarmee minimaal een goed relatiebeheer is uit te voeren. Een goede vriend van Martin werkt bij een bedrijf dat prima CRM-applicaties levert. Martin heeft samen met Frits besloten om deze applicatie aan te schaffen op basis van de ruime functionaliteit die het heeft.

De bedoeling is dat in dit CRM-pakket op termijn ook gegevens worden bijgehouden zoals afgesloten contracten en de waarde van de producten die zijn afgenomen door de klanten.

De applicatie was oorspronkelijk ontwikkeld voor MS-DOS, maar is met de jaren doorontwikkeld tot een Windows-applicatie. De leverancier gebruikt voor de meeste functies in het CRM-pakket de database, maar er is nog een aantal functies dat het bestandssysteem gebruikt voor opslag van gegevens. Het CRM-pakket gebruikt een eigen authenticatiesysteem en is niet te integreren met een generiek authenticatiesysteem, zoals Active Directory van Microsoft.

Ronald wordt geconfronteerd met de applicatie en wordt verzocht het te installeren en zo snel mogelijk beschikbaar te maken, ook op de pda van Frits. Dan heeft Frits onderweg ook alle noodzakelijke informatie bij de hand.

Ronald krijgt een applicatie die misschien wel functioneel veel te bieden heeft, maar op het gebied van beveiliging nog te wensen overlaat. Ronald besluit onder druk van Martin en Frits de CRM-applicatie zo snel mogelijk beschikbaar te stellen. Via de ingebouwde webinterface kan iedereen met een inlogcode bij de klantgegevens. Dit werkt ook goed met de nieuwe, nu beter beveiligde pda van Frits.

Ronald realiseert zich dat er beveiligingsrisico's zijn die hij nog moet verhelpen. De webpagina is bijvoorbeeld niet beveiligd met SSL, waardoor onbevoegden 'mee kunnen lezen' en het maken van back-ups is nog niet ingeregeld. Ook moet een aantal beveiligingsupdates voor de webinterface van de CRM-applicatie nog geïnstalleerd worden. Het dichttimmeren, ook wel hardenen van de server, is ook maar even naar achteren geschoven omdat Ronald nog niet precies weet wat de gevolgen zijn van het hardenen voor de CRM-applicatie. Voorlopig is de stress uit de lucht en Ronald zal eerdaags de beveiligingszaken gaan regelen. Maar helaas, de volgende verandering staat alweer voor de deur. Er moet een koppeling gerealiseerd worden met het incassobureau voor het geautomatiseerd doorgeven van wanbetalers... <<

Maatregel

In de case wordt duidelijk dat Ronald onvoldoende betrokken is bij belangrijke beslissingen waardoor vooraf invloed uitoefenen niet mogelijk is. Verder zijn de geconstateerde problemen achteraf vrijwel niet op te lossen: je loopt eigenlijk achter de feiten aan. Om beveiliging te beheersen is een proactieve rol van belang. U wilt als systeembeheerder het management een aantal keuzes voorleggen met de bijbehorende consequenties. Bijvoorbeeld een keuze van weinig beveiliging met lage kosten, maar een groot bedrijfsrisico. Of een keuze met hoge kosten, maar wel een goede beveiliging. Het management kan dan uw input meenemen in de afweging. Hierdoor zal de inspanning achteraf, om de zaken veilig te krijgen, aanzienlijk minder zijn. Misschien lijkt de besluitvorming in het begin wat moeilijker te gaan, maar de winst achteraf is veel groter. Nieuwe IT-onderdelen zijn op deze manier vanaf het begin goed beveiligd, conform de voor de organisatie opgestelde beveiligingsstandaard.

Een bedrijf, groot of klein, kan zich laten certificeren volgens ISO 27001. Deze standaard beschrijft hoe een organisatie kan aantonen dat ze 'in control' zijn. Een randvoorwaarde bij deze certificering is dat een organisatie gewend moet zijn om vooraf na te denken over beveiliging.

Om een ISO 27001-certificering te verkrijgen moet een zogenaamd ISMS (Information Security Management System) worden ingericht. Dit systeem zorgt voor een nauwkeurige administratie rond de IT-omgeving en de kwaliteit (lees beveiliging) daarvan. Een certificering kan voor klanten van grote toegevoegde waarde zijn. De klant hoeft zich niet af te vragen of uw organisatie bijvoorbeeld wel veilig omgaat met zijn gegevens. Een certificering kan een ingrijpend traject zijn, maar verdient op lange termijn zijn investering ruimschoots terug.

Klantinformatie onder handbereik – 2

>> Ronald heeft de installatie-cd van de CRM-applicatie nog niet opgeborgen of hij wordt gevraagd de koppeling te realiseren met het incassobureau voor het doorgeven van wanbetalers. Ronald wil niet nog een keer in de valkuil stappen en vraagt een gesprek aan met Martin. Ronald legt Martin het beveiligingsplan voor dat destijds is opgesteld. Ronald geeft aan dat in het beleid staat vermeld dat externe koppelingen alleen mogelijk zijn wanneer deze versleuteld zijn en dat de externe partij een geheimhoudingsverklaring tekent. Ook staat in het beleid dat de externe koppeling alleen via een beveiligde ingang toegang krijgt tot het netwerk. Ronald geeft tevens aan wat de risico's zijn wanneer deze maatregelen niet worden getroffen.

Op basis hiervan vraag Martin aan Ronald om een bondig rapport te maken met daarin minimaal een aantal alternatieven, de kosten en de doorlooptijd. Ronald gaat met deze vraag aan de gang en voert een risicoanalyse uit.

Op basis van het rapport kiest Martin voor de optie waarbij er wel een beveiligde toegang wordt gerealiseerd, maar geen versleuteling van de verbinding. In deze optie wordt voorgesteld om alleen een uniek klantnummer met een verschuldigd bedrag via de koppeling te versturen naar het incassobureau. Het incassobureau heeft een database met persoonsgegevens, waarin het unieke klantnummer gerelateerd is aan persoonsgegevens. Het aftappen van de koppeling levert op deze manier geen gevoelige informatie op.

Ronald vraag Martin de gekozen optie per e-mail te bevestigen. Deze e-mail kan Ronald later gebruiken als onderbouwing bij een eventuele audit om uit te leggen waarom is afgeweken van het beveiligingsbeleid.

Ronald bouwt de koppeling samen met de beveiligingsmaatregelen. Na ingebruikname sluit Ronald het project met een tevreden gevoel af en kan hij met schone lei starten aan het volgende project. <<

Meer weten

- www.nen.nl, NEN-ISO/IEC 27001

Dat een goede beveiliging van ICT-systemen belangrijk is, kunt u bijna dagelijks in de krant lezen. De hoeveelheid gevoelige gegevens die bedrijven opslaan, wordt steeds groter en niets is vervelender dan dat die op straat komen te liggen of in verkeerde handen vallen. Wat er allemaal mis kan gaan en hoe u de ICT-systemen in uw bedrijf veiliger kunt maken komt uitgebreid aan bod in *ICT security in de praktijk*. Het boekje richt zich op systeembeheerders van kleinere bedrijven met praktische aanbevelingen, maar biedt ook interessante inzichten voor managers en directeuren, bijvoorbeeld over beveiligingsbeleid.

ICT security in de praktijk is geschreven door een brede groep deskundigen die elk hun persoonlijke ervaringen, kennis en aanbevelingen met u delen. Een voorbeeld op basis van een fictief bedrijf verlevendigt de bijdrage van elke auteur.

ICT security in de praktijk gaat in op drie hoofdonderwerpen:

- *Beleid en Leiderschap:* hoe ziet ICT-securitybeleid eruit, hoe geeft u het vorm en hoe draagt u het uit?
- *Medewerkers:* hoe maakt u medewerkers bewust van beveiligingsrisico's en hoe voorkomt u incidenten?
- *Processen en Technologie:* welke processen en technologie heeft u en waarmee moet u rekening mee houden vanuit ICT-security oogpunt?

Succes met het toepassen van de aanbevelingen uit *ICT security in de praktijk* en het veiliger maken van uw bedrijf.

ISBN 978-90-814070-2-1

OGD ict-diensten

ICT-kring Delft

TNO

LBVD INFORMATIEBEVEILIGERS