



Risico IT reductie een management-benadering

Hoe de risico's die IT met zich meebrengt
met minimale investering te verlagen

Auteur: drs. R.B. Gloudemans
Consultant
E-Mail: r.gloudemans@i-to-i.nl
Datum: 27 september 2004

Ideas to Interconnect BV
Radex gebouw,
Kluyverweg 2a,
2629HT Delft,
Nederland

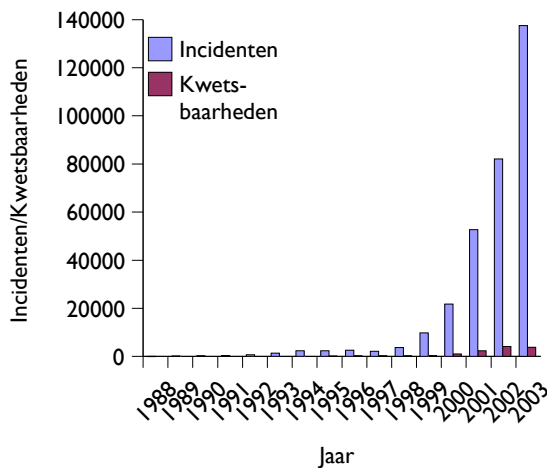
Tel: +31 (0)15 268 25 13
Fax: +31 (0)15 268 25 21
E-Mail: info@i-to-i.nl
Web: www.i-to-i.nl

De FBI schatte in 2001 dat over 2000 wereldwijd 1500 miljard dollar aan schade was veroorzaakt door beveiligingsincidenten. Grote organisaties die IT inzetten om hun zakelijke doel te bereiken verliezen gemiddeld 1 miljoen dollar per serieus beveiligingsincident; 99% van de bedrijven gebruikt anti-virus software, maar toch wordt 82% ieder jaar getroffen door virussen. De Meta groep schat dat in 2006 12% van het IT budget besteed wordt aan beveiliging.

Dit artikel zal een aanzet geven over de wijze waarop omgegaan dient te worden met beveiliging zonder dat daardoor:

- hoge of kosten, nu of op de langere termijn, gemaakt worden
- het bedrijfsrisico onacceptabel stijgt
- werknemers en klanten gehinderd worden in hun dagelijkse werkzaamheden

Het risico



Het aantal aangegeven incidenten bij het "Computer Emergency Response Team" laat een duidelijke trend zien. Het aantal gemelde incidenten per jaar stijgt bijna logaritmisch. Dit terwijl het aantal gemelde kwetsbaarheden in de gebruikte software, zeker in de laatste jaren, ongeveer constant blijft. De eerste gegevens uit 2004 bevestigen dit.

Eén van de belangrijke factoren die verantwoordelijk is voor de stijging in incidenten is de toename in het aantal gebruikers.

Figuur 1, Aantal incidenten gemeld bij CERT

Tegelijkertijd lijken software makers het probleem steeds meer onder controle te krijgen. Het aantal gemelde kwetsbaarheden is stabiel bij een groeiende markt met steeds complexere producten.

Men zou kunnen concluderen dat de dreiging (en dus het risico) niet stijgt. Immers de stijging in het aantal Internet-gebruikers zou de stijging in het aantal incidenten goed kunnen verklaren. Software wordt er niet slechter op, dus waarom verdere acties ondernemen?

Hiervoor zijn de volgende redenen te geven:

- Meer Internetgebruikers houdt impliciet in dat er meer kwaadwillenden zullen zijn. Virusmakers zijn hier een goed voorbeeld van. Niet alleen worden het er steeds meer; per maker worden ook steeds meer virussen uitgebracht;
- Nieuwe technologieën, zoals WiFi en Bluetooth, die nog niet volwassen zijn. Daardoor zijn ernstige problemen met beveiliging te verwachten. Het oplossen van deze problemen is, technisch gezien, niet het grootste probleem. Het probleem is met name dat consumenten en het bedrijfsleven zich niet bewust zijn van de risico's;
- Steeds verdergaande centralisatie van IT-diensten. Hierdoor kan een incident potentieel meer schade aanrichten;

- Business die steeds afhankelijker wordt van het Internet. Mail is tegenwoordig belangrijker dan telefoon. Beveiliging van netwerken en systemen zal dan ook steeds vaker botsen met "Business needs";
- Beschrijf­bare media als USB pennen en flashcards worden steeds meer gebruikt. Dit verhoogt niet alleen het risico op virusbesmettingen (vanwege de wisselende contacten van de gebruikte media), maar ook op het uitlekken van bedrijfsgegevens. Een floppy disk bevatte nooit meer dan een paar documenten. Een USB pen kan met gemak de hele administratie meenemen.

Hoe kan nu het bedrijfsrisico beperkt worden met zo weinig mogelijke negatieve bijwerkingen zoals:

- hoge groei in kosten?
- onacceptabele beperkingen?
- inflexibel worden van de infrastructuur?
- niet meer openstaan voor nieuwe ontwikkelingen?

De antwoorden hierop zijn grotendeels verbazingwekkend simpel. De volgende voorbeelden illustreren hoe dit doel bereikt kan worden.

De inkoper

Wanneer een nieuwe auto gekocht moet worden, wordt steeds vaker gekeken naar veiligheidsaspecten zoals de resultaten van de Euro NCAP botsproeven. Men wil immers zeker weten dat het gezin niet alleen in een mooie auto zit, maar ook in een veilige.

Gek genoeg gebeurt dit met de inkoop van software veel minder. Na de geleverde functionaliteit wordt er op dit moment het meest gekeken naar de "Total Cost of Ownership" (TCO) van een product. De TCO kan een vertekend beeld geven. Kosten voor de beveiliging en eventuele herstelwerkzaamheden aan de infrastructuur vallen vaak onder een andere post. Zo kan het zijn dat er een nieuw product wordt aangeschaft, waardoor de TCO van een deel van de infrastructuur daalt, terwijl de TCO van de totale infrastructuur stijgt.

Dus:

- Leveranciers moeten goed specificeren welke kosten er zijn meegerekend in de voorspelde TCO;
- Voor aanschaf moet een leverancier kunnen aantonen dat
 - zijn product zo min mogelijk additionele maatregelen behoeft binnen de huidige infrastructuur;
 - zijn product het bedrijfsrisico niet verhoogt.

De opleiding

Dit is misschien wel de meest effectieve methode. Onderzoek van de "Computer Technology Industry Association" (CompTIA) toont aan dat wanneer 25% van de medewerkers een goede opleiding heeft gehad, dit een daling van 20% in het aantal beveiliging-gerelateerde incidenten tot gevolg heeft. Het gemiddelde bedrag per incident van 1.000.000 dollar, genoemd in de eerste alinea van dit artikel, is goed voor meer dan 1000 dagen training. Als men daarbij ook nog de tijd meerekent die besteedt wordt aan het aantal niet serieuze incidenten, dan is training een investering die bijna gegarandeerd wordt terugverdiend.

Er kan nog een stap verder gegaan worden. In de bedrijfscultuur is het meestal zo dat de afdeling of persoon die zich bezig houdt met beveiliging niet populair is.

Hij verbiedt immers dingen. Er moet aandacht besteed worden aan hoe beveiliging een zaak van iedereen wordt. Negatieve motivatie moet plaats maken voor positieve motivatie.

Het beveiligingsdenken - Kantoornetwerk

Ook de opbouw van de infrastructuur kan meestal beter, zonder hierbij te hoeven investeren in nieuwe hardware of software. Als er een analogie getrokken moet worden met de meeste bedrijfsnetwerken, dan is die van een kasteel met slotgracht en hele passende. Het is moeilijk om binnen te komen, maar als er in het kasteel iets gebeurd, dan is dit meestal rampzalig. Denk bijvoorbeeld aan een kok die de vlam in de pan laat slaan of een persoon die de dienstpoort open laat staan.

Het bedrijfsnetwerk kan beter opgebouwd worden als een ommuurde stad met een centrale burcht. Alle kritische systemen dienen in de burcht te worden ondergebracht. De burcht sluit ook goed aan op de centralisatie trend. Alle bedreigingen voor de burcht dienen op minimaal twee verschillende manieren afgevangen te worden. Net zoals de inrichting van een echte burcht het mogelijk maakt de vijand te bestoken met kruisvuur.

Voor de stad dient een aantal belangrijke details in acht te worden genomen:

- Stedelingen worden niet vertrouwd en mogen niet zomaar de burcht binnen treden;
- Binnen de stad dienen natuurlijke barrières gevormd te worden zodat eventuele branden niet overslaan;
- Binnen de stad dient een aantal grote afgeschermden wegen te bestaan, zodat het leger snel kan manoeuvreren van de ene naar de andere positie.

Als we dit vertalen naar het bedrijfsnetwerk kan het volgende opgemerkt worden:

- Er dient te worden nagedacht over de manier waarop centrale diensten benaderd worden en hoe deze afgeschermd kunnen worden;
- Er is helemaal geen reden waarom clients op het netwerk elkaar moeten kunnen benaderen. Dit is simpel uit te schakelen in de centrale netwerk infrastructuur en voorkomt bijvoorbeeld dat virussen zich binnen het netwerk kunnen repliceren;
- De grote afgeschermden wegen zijn er voor de support afdeling, zodat ze gebruikers niet alleen met raad, maar ook met daad kunnen bijstaan.

De overgang naar het stad/burcht-model lijkt een behoorlijke ingreep, maar is meestal te realiseren door een herconfiguratie van de bestaande infrastructuur en het aanpassen van de lokale procedures. Support processen kunnen onveranderd blijven.

Het stad/burcht-model rekent ook af met de risico's die het gebruik van WiFi, Bluetooth en laptops met zich meebrengen. Ook de ingehuurde consultant kan zijn eigen laptop aan het bedrijfsnetwerk koppelen zonder dat dit grote risico's met zich meebrengt.

In het stad/burcht-model zal het vaker gebeuren dat een werkplek uitgeschakeld wordt door een beveiligingsincident. Echter: door de opzet van de hele infrastructuur zal dit incident altijd een beperkte impact hebben. Dit weegt op tegen de grotere vrijheid die de medewerkers gegeven kan worden. Als daarnaast de medewerkers ook goed opgeleid worden, dan zal het aantal

incidenten waarschijnlijk zelfs afnemen. Het stad/burcht model geeft dan de mogelijkheid de medewerkers te vertrouwen op het vlak van beveiliging, zodat ze hun opleiding in de praktijk kunnen brengen.

Het is van groot belang dat de burcht echt veilig is. Het opstellen en nalopen van dagelijkse/wekelijkse checklists is een manier om dit te waarborgen.

Het beveiligingsdenken – Internet diensten

Verbeteringen op dit vlak zijn vaak niet eenvoudig te bereiken. De simpele reden hiervoor is dat er meestal al goed over is nagedacht. De meeste winst valt hier meestal te behalen door processen en procedures goed vast te leggen en ervoor te zorgen dat de beheerders adequaat getraind zijn. Vooral dit laatste is, gek genoeg, vaak een probleem. De beheerinterfaces en gereedschappen maken de beheerwerkzaamheden steeds eenvoudiger. Hierdoor is er te weinig aandacht voor de onderliggende kennis.

Internet-diensten dienen aangeboden te worden vanuit een afgesloten compartiment van de burcht, waarbij de beheerder in de stad leeft.

Indien de dienst op maat gemaakt wordt door een leverancier, dan is het kopje "Inkoop" ook van toepassing. De belangrijkste bijdrage aan het reduceren van risico van een Internet dienst ligt in de programmeercode achter deze dienst. De leverancier dient dus te bewijzen dat hij kundige medewerkers in dienst heeft die meer kunnen dan een functionele en esthetisch aangename dienst opleveren.

Als het dan toch fout gaat; de "Rapid Reaction Force"

Een behoorlijk percentage van alle bedrijven heeft een calamiteiten-plan. Dit plan probeert de bedrijfsvoering veilig te stellen na het plaatsvinden van een calamiteit. Tussen beveiligingsincident en calamiteit ligt een heel breed gebied.

Nu is het zo dat beveiligingsincidenten te vaak uitmonden in een calamiteit, doordat niet snel genoeg gehandeld (kan) worden. Een virusbesmetting kan bijvoorbeeld vele tientallen werkplekken per minuut besmetten. Het is daarom van het uiterste belang dat er razendsnel gehandeld kan worden.

Hiervoor kan een "Rapid Reaction Force" (RRF) worden ingericht. De RRF dient te bestaan uit beheerders, management en gebruikers en moet in noodsituaties de autoriteit hebben om in te grijpen. Het spreekt voor zich dat de term "noodsituatie" dan wel goed gedefinieerd moet worden. Daarnaast is het van belang dat de RRF, net als de bedrijfsbrandweer, op regelmatige basis oefent.

Aandachtsgebieden voor de RRF:

- Beslissingen nemen voor het beperken van de impact
- Technische maatregelen voor het beperken van de impact
- Informeren van management
- Informeren van gebruikers
- Informeren van klanten
- Het nemen van maatregelen die leiden tot het herstel van de normale werkzaamheden. De daadwerkelijke herstelwerkzaamheden kunnen gedaan worden door de normaal verantwoordelijke personen
- Evaluatie van het incident

Daarnaast draagt de RRF, door zijn samenstelling, bij aan bewustwording en acceptatie van het beveiligingsdenken.

Eventueel kan de RRF multi-inzetbaar gemaakt worden door de leden EHBO trainingen te geven en ze te laten deelnemen aan de bedrijfsbrandweer. Op deze wijze ontstaat er een herkenbare eenheid binnen het bedrijf.

Conclusie

De conclusie van dit artikel luidt dat door goed, gestructureerd na te denken over beveiliging, de kosten en het "risico IT" onder controle gehouden kunnen worden.

Investerings in een goede set maatregelen nu leiden niet alleen tot een kostenbesparing in de toekomst, maar ook tot een lager bedrijfsrisico en een betere aansluiting van IT op de business.

Het belangrijkste doel is dat beveiliging een integraal onderdeel wordt van ieder bedrijfsproces. Deze integratie moet dusdanig ver gaan, dat het een vanzelfsprekendheid wordt. Daarnaast is het belangrijk om een deel van de verantwoordelijkheid neer te leggen op de plaatsen waar de meeste pijn vandaan komt: de gebruikers zelf. De meeste incidenten vinden niet plaats vanuit kwaadwillendheid, maar uit onwetendheid en naïviteit.

Een echte kwaadwillende kan meestal toch niet buiten de deur gehouden worden. Alle maatregelen die genomen worden vertragen hem alleen maar. En daardoor heeft een RRF de kans om tijdig in te grijpen.

Ideas to Interconnect BV (i-to-i) is een management en consultancy bedrijf dat haar klanten helpt bij het inzetten van informatie en communicatie technologie voor het verbeteren van hun bedrijfsprocessen. Het toepassen van technologie in een organisatie heeft vaak vele veranderingen tot gevolg. Samen met onze klanten realiseren we die veranderingen. Werken aan optimale oplossingen zonder daarbij het doel van de technologie uit het oog te verliezen. Onze gezamenlijke inspanningen dienen immers te leiden tot het verbeteren van de kwaliteit van de dienstverlening, het verhogen van de omzet en het verbeteren van de kosteneffectiviteit van de klantorganisatie. Kortom, werken aan veranderingen van groot strategisch belang. Daarom koppelen we bij implementatie onze branche kennis en technische expertise aan een nuchtere, praktische aanpak (in het gezamenlijke streven naar maximale acceptatie.).

We geloven in zaken doen op ethisch verantwoorde wijze waarin we continu werken aan vertrouwen en een stevige, lange termijn relatie met onze klanten. We geloven ook in het delen van risico's met onze klanten. Het succes van onze klanten is daarmee ons succes.

*Ideas to Interconnect BV
Radex gebouw, Kluyverweg 2a, 2629HT Delft, Nederland*

*Tel: +31 (0)15 268 25 13, Fax: +31 (0)15 268 25 21
E-Mail: info@i-to-i.nl, Web: www.i-to-i.nl*