



RESEARCH INTERNATIONAL

BEDRIJFSBE- VEILIGING





BEDRIJFSBE- VEILIGING



IN DE NIEUWSMEDIA en zakelijke pers verschijnen helaas steeds meer berichten over incidenten die te maken hebben met de veiligheid van informatie- en communicatietechnologie. Verloren en gestolen notebooks, ontbrekende USB-sticks en cd's, het komt allemaal in het nieuws. Hacking, phishing en virussen in e-mails kunnen het ICT-netwerk van een organisatie danig verwoesten.

De berichten in de pers worden bevestigd door recent onderzoek. In de Information Security Breaches Survey, die in 2008 werd uitgevoerd ten bate van het Britse Department of Business, Enterprise & Regulatory Reform (BERR)¹, werd geconstateerd dat 45% (dus bijna de helft) van de onderzochte kleine bedrijven (maximaal 50 werknemers) in het afgelopen jaar een incident met betrekking tot de beveiliging had meegemaakt. Het gemiddelde was zes² incidenten per jaar, waarbij de kosten voor het ernstigste incident meestal opliepen tot € 11.000 - 22.500.

ICT-professionals bij grote bedrijven maken zich terecht zorgen over de veiligheid. In een peiling³ die in 2008 door de Computing Technology Industry Association werd gehouden, gaf bijna één derde van de respondenten aan dat de beveiliging van netwerken en gegevens hun belangrijkste probleem was. Bij andere

recente onderzoeken zijn daarnaast het voorkomen van gegevenslekage en het bewerkstelligen van externe, mobiele en samenwerkingsmogelijkheden als belangrijke thema's naar voren gekomen.

De resultaten van Cisco's eigen enquête onder kleine en middelgrote ondernemingen in het Verenigd Koninkrijk, Frankrijk, Nederland en Spanje (in 2008⁴ uitgevoerd door Research International) laten echter een tegenstrijdige houding zien ten opzichte van bedrijfsbeveiliging.

Op de vraag wat de belangrijkste voordelen van technologie voor hun organisatie waren, zeiden ICT-besluitnemers een betere beveiliging en verbeterde vertrouwelijkheid van informatie als de minst belangrijke aspecten aan vergeleken met andere voordelen zoals verbeteringen in de efficiëntie, productiviteit en communicatie, en tijd- en kostenbesparingen. Bezorgdheid over beveiliging, of het gebrek daaraan, is wijdverspreid, maar toch worden betere beveiliging en vertrouwelijkheid niet als essentiële voordelen van ICT gezien. Waarom niet?

Veel besluitnemers houden zich in de eerste plaats bezig met de financiële uitkomst: productiviteit, omzet en winst. Misschien wordt beveiliging vooral beschouwd als een vaste kostenpost, een 'lastpost' zogezegd. De belangrijkste motieven om in ICT-oplossingen

te investeren hebben te maken met een verbeterde bedrijfsvoering, maar "bedrijfsbeveiliging" wordt veeleer gezien als een gezondheidskwestie, een lastig probleem dat telkens weer de kop opsteekt.

De gegevens van Research International ondersteunen deze hypothese. Ofschoon veiligheid als minst belangrijke voordeel wordt aangewezen, gebruikt 83% van de ondervraagde bedrijven momenteel beveiligingsoplossingen en vindt 95% van de besluitnemers veiligheid een belangrijke factor bij investeringen in geavanceerde communicatietechnologie. Beveiliging is met andere woorden zeker belangrijk voor bedrijven, maar we hebben met zijn allen niet het gevoel dat we er veel van profiteren.

Zo lijkt ICT-beveiliging vergelijkbaar met andere bedrijfskosten zoals verzekeringen: het kost geld, maar levert weinig op. Een noodzakelijk kwaad dus, een verdedigingslinie die weliswaar verliezen voorkomt maar verder weinig voordelen biedt. Net als met verzekeringen worden de kosten van ICT-beveiliging afgewogen tegen de risico's die ontoereikende beveiliging met zich meebrengt. Hiermee zet u letterlijk uw hele bedrijf op het spel.

Er zijn een aantal belangrijke redenen waarom bedrijfsbeveiliging in een positiever licht zou moeten worden gezien.

Zonder goede beveiliging gaan de voordelen van technologie verloren.

Elk beveiligingslek noopt tot een reactie waarbij middelen worden gebruikt die eigenlijk voor iets anders waren bestemd. Een ernstig lek kan bovendien schade toebrengen aan de constante dialoog tussen het bedrijf en zijn klanten en andere belanghebbenden. 'Praatjes' onder consumenten en op blogs kunnen ongewenste aandacht in de media veroorzaken, waardoor uiteindelijk mogelijk een beroep moet worden gedaan op programma's voor crisisbeheersing. Een beveiligingslek is kortom een garantie voor lagere productiviteit, communicatieproblemen, verspilde tijd en extra kosten. Bij zes incidenten per jaar wordt beveiliging opeens een belangrijke investering in de 'echte' voordelen van technologie.

Bescherm uw reputatie met beveiliging.

Bedrijven zijn zo sterk als hun reputatie; in het digitale tijdperk kunnen reputaties bliksemsnel worden opgebouwd én vernietigd dankzij geruchten en praatjes op internet. Wat is de schade van een onverwacht ICT-beveiligingsincident voor uw bedrijf en uw reputatie? Potentiële klanten kunnen bij het leggen van zakelijke relaties evenveel belang gaan hechten aan een adequate beveiliging van privégegevens en goede beveiligingsmaatregelen als aan het sociale en ecologische beleid van een bedrijf.

Een goede beveiliging kan een verkoopargument zijn.

Bedrijven moeten aandacht schenken aan beveiliging om zich tegen elektronische en menselijke bedreigingen te verdedigen, maar ook om hun klanten het vertrouwen en de zekerheid te kunnen geven dat hun gegevens, geld of intellectuele eigendommen zowel binnen als buiten uw bedrijfsnetwerk in goede handen zijn. Het onderzoek van Research International wees uit dat 100% van Cisco's netwerkbeveiligingsklanten tevreden was (waarvan 70% 'zeer' of 'uiterst tevreden') met Cisco's technologieën.

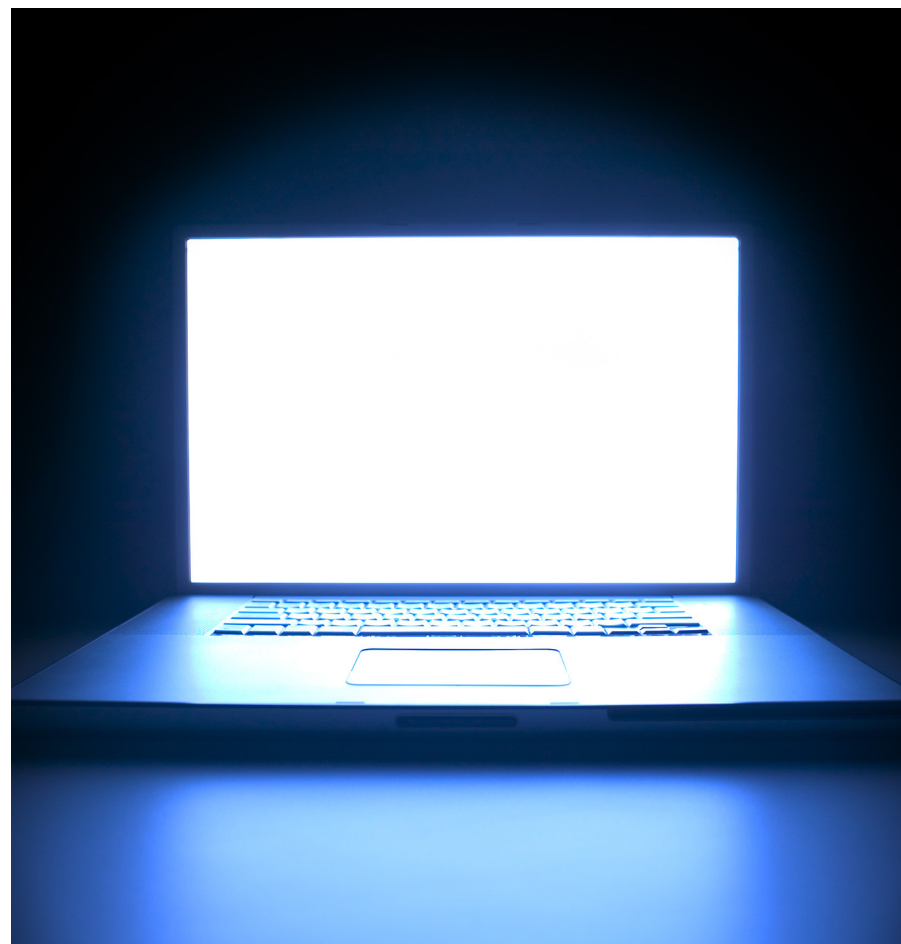
Samenvatting.

Is een goede beveiligingsinfrastructuur de moeite waard? Kunnen bedrijven wel zonder? Een veilig en sterk netwerk is niet alleen een verdedigingsbolwerk of een kostenpost, maar een goede economische investering in uw bedrijf. Het is tijd voor een nieuw perspectief. Progressieve organisaties beschouwen hun medewerkers als een waardevolle investering, niet als een kostenpost. Waarom zou een veilig, betrouwbaar ICT-systeem niet dezelfde eer ten deel vallen? Beschouw veiligheid niet alleen als een combinatie van de juiste software en hardware, maar tevens als een positieve houding die al uw medewerkers bijgebracht moet worden.

Proactieve beveiliging is een voorwaarde om de andere vruchten van technologie te plukken.

Hoe kunt u de communicatie over beveiliging én uw bedrijf vooruit helpen? Maak eerst de balans op van uw bestaande netwerk en apparatuur. In hoeverre zijn uw elektronische bedrijfsmiddelen bestand tegen elektronische of menselijke bedreigingen, zowel van binnenuit als van buitenaf? Het formuleren van een ICT-rampenherstelplan zal de alertheid ten opzichte van verschillende rampscenario's verbeteren en, indien een dergelijk scenario werkelijkheid wordt, de respons verbeteren.

Hoe kunt u te werk gaan als bij een of meerdere van deze processen tekortkomingen worden blootgelegd? Of het nu om een netwerkprobleem, een technisch probleem of om de naleving van regelgeving gaat, het is cruciaal dat u proactieve stappen onderneemt om uw ICT en bedrijf te beschermen. Onderzoek alle beschikbare opties en neem ze grondig door met de desbetreffende leveranciers en consultants, zodat ze zich volledig bewust zijn van de problemen waarmee u zich geconfronteerd ziet. Alleen dan kunnen ze u optimaal adviseren. Met de juiste beveiligingstechnologie kunt u zich op uw bedrijf concentreren in plaats van op uw angsten.



¹ 2008 Information Breaches Security Survey, Department of Business Enterprise and Regulatory Reform, oorspronkelijk in april 2008 gepubliceerd. Onderzoek uitgevoerd door PriceWaterhouseCoopers van oktober 2007 t/m januari 2008, 1007 respondenten.

² Mediaaancijfer.

³ Onderzoek van de Computing Industry Association uitgevoerd van juni t/m augustus 2008, 934 respondenten.

⁴ Onderzoek van Research International uitgevoerd in 2007-2008 onder Cisco-klanten uit het midden- en kleinbedrijf, en externe respondenten in het Verenigd Koninkrijk, Frankrijk, Nederland en Spanje. 607 respondenten.

Onafhankelijk onderzoek in opdracht van:

