

# Is uw bedrijf voldoende beveiligd ?



Het beschermen van (digitale) bedrijfsinformatie en de interne beveiliging tegen uiteenlopende bedreigingen vormt voor veel bedrijven of organisaties een probleem. Com-Connect heeft jarenlange politie ervaring met name op het gebied van digitale recherche. Van hieruit benaderen wij het beveiligingsvraagstuk op een andere wijze. Wij analyseren de zwakheden en sterktes van een bedrijf door de ogen van een potentiële dader.

Na een zorgvuldige scan van uw bedrijf of organisatie zullen wij u aanbevelingen doen over de fysieke beveiliging en over het afschermen van de gehele stroom van informatie binnen uw bedrijf of organisatie.

Maak vrijblijvend kennis met de **Security Scan** van Com-Connect.

**Com-Connect wil de klant een totaal pakket aanbieden op het gebied van Informatiebeveiliging, Security beleid en bestrijding van Internet criminaliteit.**

Com-Connect heeft zowel aandacht voor de fysieke beveiliging van uw systemen, netwerk(en) en organisatie maar ook voor de zwakste schakel van de beveiliging “de mens”.

### **Waarom een Security Scan?**

Het wordt voor u en uw organisatie van steeds groter belang veiligheidsrisico's te onderkennen en te beheersen. Daar waar mogelijk preventieve maatregelen te nemen, zowel strategisch als tactisch. Om de ongewenste risico's zoveel mogelijk te beperken, biedt de Security Scan van Com-Connect een aanzet tot een nieuwe kijk op het beveiligingsbeleid binnen uw organisatie.

### **Uniek ?**

Ja, want de Security scan wordt uit gevoerd door medewerkers van Com-Connect met jarenlange ervaring bij de politie en door vakkundige ICT medewerkers. Een unieke en vakkundige combinatie.

### **Wist u dat ...**

- een van de grootste risico's binnen het management van organisaties interne fraude blijkt te zijn.
- meer dan de helft van de organisaties en bedrijven niets doet om personeel bewust te maken van de gevaren van ict.
- veel bedrijven zijn slecht voorbereid op het verlies van digitale bedrijfsgegevens of it-aanvallen van buitenaf. Slechts één op de vier bedrijven maakt bijvoorbeeld geregeld een back-up
- identiteitsdiefstal in de VS het sterkst groeiende misdrijf is.
- cyberspionage fors toeneemt. Het was in 2007 al groter dan de voorafgaande jaren, en nu groeit het langzaam door naar economische spionage in de zakenwereld.
- nagenoeg één op de twee bedrijven de afgelopen twee jaar wel op de één of andere manier het slachtoffer is geworden van fraude en/of diefstal. De gemiddelde verliezen ten gevolge van hiervan zijn in twee jaar met 40 procent gestegen. Ongeveer de helft van de daders komt uit het bedrijf zelf; een vijfde daarvan zit in het hoogste management.
- dat de online criminaliteit nog iedere dag toeneemt in Nederland. Dat concludeerde de overheid naar aanleiding van eigen onderzoek. De omvang en omzet van cybercrime is te vergelijken met die van de drugshandel/



## De zwakste schakel

### Eigen personeel belangrijkste beveiligingsrisico

Persbericht 6 februari 2008  
(Bron. Webwereld)

Nederlandse ondernemingen zien het onbewust lekken van vertrouwelijke informatie door werknemers als grootste beveiligingsrisico voor de komende jaren, blijkt uit het 'Webwereld Security Onderzoek in samenwerking met NU-zakelijk.nl & Security.nl'.

Van de ondervraagde managers geeft 23% aan het eigen personeel als een van de grootste bedreigingen te zien. Bescherming van vertrouwelijke gegevens wordt door 19% gezien als de grootste bedreiging, gevolgd door gerichte aanvallen door hackers (14%); bewust doorspelen van vertrouwelijke informatie (9%) en spam (9%).

Het onderzoek schetst een beeld de stand van beveiliging in Nederland. 'Bedrijven blijken vooral aan symptoombestrijding te doen', zegt Tom Sanders, hoofdredacteur van Webwereld. 'Zij blokkeren concrete bedreigingen, maar het ontbreekt vaak aan structureel beleid dat toekomstige beveiligingsproblemen kan voorkomen.'

Zo verzuimt 30 procent van de bedrijven om accounts van vertrokken werknemers snel te verwijderen. Bij 2 procent bleek dit zelfs tot een half jaar te kunnen duren. Een derde van de bedrijven licht de beveiliging van het bedrijfsnetwerk niet regelmatig door en laat het ook niet certificeren.

### Ik heb toch een alarm !

Gelukkig heeft u dat goed geregeld.  
Maar de criminaliteit van nu heeft weinig of geen boodschap aan de gesloten deur of het alarm van uw organisatie of bedrijf. Binnenkomen was eigenlijk nog nooit zo gemakkelijk als nu ....

### Kent u deze begrippen ...

- Social Engineering
- Phishing
- Keyloggers
- Pharming
- Identity Theft
- Computer virus
- Interne fraude
- Adware
- Spyware
- Cookie
- Spam
- Zombie network
- Hacker
- Man in the middle attack
- Data heler
- Bedrijfs spionage
- Acquisitie fraude
- Calimiteiten plan
- Domeinnaam hacking
- Beroepsmatige surfers
- Beveiligde USB stick
- Internet protocol
- Firewall

Komen deze begrippen u bekend voor ?  
Of bent u als MKB'er de weg wat kwijt !

Wij gaan u helpen .....



## Inhoud Security Scan (basic)

- fysieke scan van uw bedrijf door twee van onze medewerkers
- scan van de beveiliging van uw bedrijfsnetwerk
- controle infrastructuur binnen uw bedrijf
- check toegangscontrole
- check informatiebeveiliging
- check bedrijfshulpverlening

Van deze basisscan ontvangt u een rapportage met hierin de bevindingen van de basisscan en de eventuele aanbevelingen en verbetertrajecten.

De kosten van deze scan bedragen € 650,00. Indien na de uitgebrachte rapportage een vervolg opdracht wordt geplaatst worden deze kosten voor de helft gecrediteerd.

## Referenties

Com-Connect is werkzaam voor o.a.:

- ING bank Nederland
- RABO bank Maashorst
- Politie Vormingscentrum
- CitaVerde Scholengemeenschap
- Body Cote Nederland
- Shared Parts Services

**INFORMATIEBEVEILIGING**

**SECURITY**

**BEDRIJFSTRAINING**

**VEILIGHEIDSTRAINING**

**SEMINARS**

**INTERNET AWARENESS**

## Meer informatie

WEBSITE [www.com-connect.nl](http://www.com-connect.nl)  
EMAIL [informatie@com-connect.nl](mailto:informatie@com-connect.nl)  
TELEFOON 077-3976060  
ADRES Energiestraat 2 5961 PT Horst  
POB 901

