

Informatiebeveiliging en IT Oost Nederland

Informatie is vaak het meest waardevolle bezit van een organisatie. Om uw bedrijfsvoering veilig te stellen moet informatie goed worden beveiligd. Uw relaties verwachten van uw organisatie dat bijvoorbeeld privacygevoelige informatie zorgvuldig behandeld wordt.

Goede informatiebeveiliging is daarom voor veel organisaties heel belangrijk. Een informatiebeveiligingsplan (IBP) ligt dan voor de hand.

Bij de implementatie staat de mens centraal, zowel binnen als buiten de organisatie. Informatiebeveiliging is namelijk niet alleen een ICT aangelegenheid. Veel risico's hebben te maken met de menselijke factor. Goede informatiebeveiliging is vooral ook bewustwording van al uw medewerkers (zowel op de werkvloer als op managementniveau). Technische hulpmiddelen zijn immers niets waard als ze niet, of op een verkeerde wijze worden gebruikt.

Organisaties die informatiebeveiliging serieus nemen stemmen hun maatregelen af op hun beleidsuitgangspunten.

IT Oost Nederland maakt gebruik van haar consultancy ervaring die zij heeft opgedaan bij haar relaties. IT Oost Nederland helpt u informatiebeveiligingsprojecten te plannen, te evalueren en te implementeren en biedt u de training en kennisoverdracht die u een effectief IBP garanderen.

Workshop informatiebeveiliging

Het doel van de workshop is het opdoen van praktische kennis om zelfstandig een informatiebeveiligingsbeleid met een bijbehorend informatiebeveiligingsplan te kunnen opstellen. In overleg met u wordt het programma opgesteld.

Risicoanalyse

Bij een risicoanalyse worden, zoals de naam al aangeeft, risico's geïnventariseerd en geanalyseerd. Hierdoor wordt in kaart gebracht wat beveiligd moet worden. De risico's worden gekwantificeerd door het bepalen van de kans dat een bedreiging zich voordoet maal de gevolgen daarvan: $\text{risico} = \text{kans} \times \text{gevolg}$.

Een risicoanalyse vormt de basis voor het opstellen van een IBP. Het is immers noodzakelijk om goed te weten wat er in het bedrijf gaande is op het vlak van risico's en welke preventiemaatregelen kunnen helpen om deze risico's uit te schakelen, te verminderen of zich ertegen te beschermen.

Bij een risicoanalyse wordt binnen het bedrijf naar de volgende punten gekeken:

- of er gevaren zijn;
- of deze schade kunnen veroorzaken.

Dit wordt op het niveau van de organisatie, de werkplek en de werknemer gedaan. Zo ontstaat een volledig beeld als input voor het IBP.

Opstellen IBP

Het opstellen van uw IBP bestaat uit drie fasen.

In fase één worden de (werkelijke) bedrijfsrisico's voor de bedrijfsprocessen en informatiesystemen beoordeeld en worden de bedrijfsprocessen en informatiesystemen geclassificeerd.

In fase twee worden dreigingen, kwetsbaarheden en reeds getroffen beveiligingsmaatregelen geïnventariseerd en onderzocht.

In fase drie wordt op basis van de relevante bedreigingen uw IBP opgesteld.

Hoe kijkt IT Oost Nederland tegen informatiebeveiliging?

Naast mogelijke menselijke factoren heeft IT Oost Nederland de volgende factoren geïdentificeerd die u meer grip omtrent uw informatie en de beveiliging daarvan kan opleveren:

- Firewall;
- IPS (Intrusion Prevention Systems);
- Application Control;
- VPN (Virtual Private Network)/Remote Login;
- Tokens;
- DLP (Data Loss Prevention);
- Encryptie;
- Media/Port Control;
- Anti-Virus;
- Backup;
- Netwerk Segmentatie/NAP (Network Access Protection);
- Mobiele apparaten;
- UZI Kaart (Unieke Zorgverlener Identificatie);
- Wireless.

Semper Vigil

IT Oost Nederland is altijd waakzaam met betrekking tot alle relevante ontwikkelingen op het gebied van informatiebeveiliging. Dit heeft als resultaat dat in alle sectoren positief meegedacht kan worden naar informatiebeveiliging en de positie daarvan binnen uw organisatie.

Hora est

Laat IT Oost Nederland u begeleiden bij het optimaal inrichten van uw informatiebeveiligingsplan. Informatie waar u op moet kunnen vertrouwen en informatie die nodig is voor de continuïteit van uw organisatie en zeker niet zomaar voor anderen is bestemd. En voorkom zo, dat door onachtzaamheid of door kwade opzet uw strategische en gevoelige informatie op straat kan komen te liggen.

IT Oost Nederland kan het volgende bieden:

- Workshop informatiebeveiliging;
- Risicoanalyses;
- Opstellen IBP.

Wij horen graag van u of u tijdens een persoonlijk gesprek meer wenst te weten van onze nieuwe kijk op Informatiebeveiliging. Neemt u daarvoor contact op met ons via:

Frank Donk Marlin

Account Manager

IT Oost Nederland BV

F.DonkMarlin@itoostnederland.nl | www.itoostnederland.nl

Tel: 074 - 850 42 00 | Fax: 074 - 850 42 90

IT Oost Nederland 

Citrix® Solutions Network Platinum Solution Advisor

Microsoft® Gold Certified Partner

VMware® VIP Enterprise Partner

VMware® Authorized Consultant (VAC)

NetApp Gold Partner

DellEqualLogic Partner

RES® Software Gold Partner

CheckPoint® Authorized Silver Partner

TrendMicro® affinity ONE Partner

CommVault® Partner

HP Preferred Partner 2011