

Zinloos alarm – is uw IT-oplossing zijn naam wel waard?

IT, automatisering, het klinkt voor de meeste organisaties als een ingewikkeld, abstract proces. Dat het onmisbaar is, twijfelen we niet aan, maar zolang we de uitvoering kunnen uitbesteden aan een 'mannetje' die om - voor velen onbegrijpelijke reden - graag met computers speelt, vinden we het wel best. Advisering? Maatwerk? Daar wordt niet altijd aandacht aan besteed. Het is als de visser die een vis voor je vangt, maar niet leert om met een hengel om te gaan.

Zinvolle of zinloze oplossing?

In de praktijk leidt dit nog wel eens tot overbodige en zinloze oplossingen. Waarom? Het volgende voorbeeld zal dat trachten te illustreren. Beveiliging is voor ieder bedrijfspannend noodzakelijk. Er moet een slot op de deur, er dient een werkend alarmsysteem te zijn geïnstalleerd, documenten gaan achter gesloten kasten, geld gaat in een kluis en de IT omgeving dient beveiligd te zijn door middel van een firewall.

Hartstikke goed toch, zult u denken? Dat een dergelijke beveiliging in staat is om een simpele constatering van een inbraak te doen, is een feit. Maar degene die vervolgens met slaperige ogen en zware benen zijn bed uit moet kruipen om polshoogte te nemen, loopt niet alleen potentieel gevaar voor eigen leven, maar is vaak ook nog eens te laat. De dieven zijn al spoorloos, de buit is eruit en de beveiliging slaat de plank volledig mis.

Wat dan wel?

Wat zou in ons voorbeeld dan wél een oplossing kunnen zijn? Een aantal simpele netwerkcamera's kan het werk al doen. Door het registreren van bewegingen en de overdracht van relevante informatie naar een Android telefoon, krijgt de juiste persoon een melding van de stroperij op het kantoorpand en ziet daarbij de beelden van de dader. Een gericht telefoontje naar de politie zorgt vervolgens dat niet een medewerker, maar een professional naar de locatie des onheils verkast.

De goedbedoelende medewerker

En wat dacht u van de niets vermoedende telefoniste die gebeld wordt door het IT bedrijf, met de vraag of ze haar wachtwoord even kan doorgeven? De behulpzame receptioniste die voor een klant een simpel printje maakt van een bestand op diens USB-stick, niet wetend dat deze een verborgen inbraakprogramma bevat? De voorbeelden van punten waarop goede IT beveiliging mis kan gaan zijn legio. De gevolgen helaas ook.

Maatwerk

Voor uw onderneming is het dus van uiterst belang dat u de juiste IT oplossingen heeft, en bovendien dat elke medewerker weet wat wel en niet mag. Een handleiding, een concreet overzicht van de do's en don'ts ten aanzien van het versturen van e-mails, de bijgaande disclaimers en het bezoeken van websites is een concrete oplossing. En om deze naleving goed te kunnen monitoren, is het een wijs besluit om eens per kwartaal een beveiligingsaudit uit te voeren.

Waarom? Omdat het niet de vraag is óf uw computers worden gehackt, maar wanneer, door wie en welke om informatie het gaat. Pessimistisch? Nee, realistisch mét het volste vertrouwen dat de gepaste oplossing voor iedere onderneming bestaat!