

# De mens blijft zwakste schakel

**De groei van de informatietechnologie en het internet leiden vanzelfsprekend tot meer beveiligingsincidenten. Er wordt dan ook veel geïnvesteerd in beveiligingstoepassingen. Toch zal ook moeten worden gelet op de zwakste schakel in de hele beveiligingsketen, de mens. Voorlichtingscampagnes voor een beter veiligheidsbewustzijn zijn daarom essentieel.**

Door Ronald van der Let

**A**l jarenlang stijgen de uitgaven op het gebied van de informatietechnologie. Er komen steeds meer gebruikers, op steeds meer plaatsen en IT kent een niet aflatende toename van het aantal toepassingen. De behoefte aan informatiebeveiliging houdt hiermee gelijke tred en wordt dan ook steeds belangrijker. De uitgaven op het gebied van informatiebeveiliging groeien minstens even hard, zo niet harder, dan reguliere IT-uitgaven.

De toenemende uitgaven zijn onder meer het gevolg van een inhaalslag, omdat informatiebeveiliging lange tijd zou zijn verwaarloosd. Volgens het Amerikaanse onderzoeksbureau Gartner groeit de omzet van de markt voor beveiligingssoftware dit jaar met 11 procent. Daar komt nog bij dat informatiebeveiliging, of vooral de beveiligingsincidenten, tegenwoordig veel media-aandacht krijgen. Geruchtmakende incidenten halen gemakkelijk de voorpagina's van de dagbladen. Informatiebeveiliging is dus hot, mede doordat IT-toepassingen een breed maatschappelijk karakter hebben en iedereen inmiddels bekend is met negatieve uitwassen als spam, virussen en phishing.

## Trends

De trends op het gebied van informatiebeveiliging laten zien dat, zoals gewoonlijk binnen de IT, de techniek hoogtij viert. Er is opvallend weinig aandacht voor de menselijke factor, ondanks dat

Ronald van der Let ([rlet@nivo.nl](mailto:rlet@nivo.nl)) is zelfstandig ondernemer en als franchisenemer aangesloten bij NiVo network architects.

beveiligingsincidenten eigenlijk door mensen worden veroorzaakt en dat het uiteindelijk ook mensen zijn die er last van hebben. De enige aandacht is er eigenlijk voor de personen die misbruik willen maken.

Wanneer de trends een abstractieniveau hoger worden getild, wordt duidelijk dat veel valt te herleiden op het, al genoemde, alomtegenwoordige aspect van IT. Meer internet, meer toepassingen en meer gebruikers leiden domweg tot meer incidenten. Dit wordt versterkt door een toenemende verspreiding van de IT-toepassingen over steeds meer de-

## Toenemende beveiligingsuitgaven zijn een inhaalslag

vices. Inmiddels zijn virussen en aanvallen op mobiele telefoons sterk in opkomst en algemeen bekend. Het wachten is nu op *hacks* van koffieautomaten of wasautomaten, aangezien dit soort apparatuur inmiddels ook via het internet wordt ontsloten. Verder is er een toenemende variatie en verschijningsvormen van aanvallen en technieken om zich hier weer tegen te weren. De *buzzwords* van dit moment zijn onder meer *Data Leakage Prevention* (DLP), technieken die moeten voorkomen dat informatie ongemerkt verloren gaat, *Network Access Control* (NAC) voor het weren van niet-geautoriseerde apparaten op het eigen netwerk en *botnets*, waarbij individuele gehackte computers van ar-

geloze gebruikers, de bots, gezamenlijk als een netwerk worden gebruikt voor grootschalige aanvallen op systemen van onder andere banken of overheden. Zo werd zeer recent, naar aanleiding van de berichtgeving over Tibet, met botnets vanuit China een aanval gelanceerd op de website van nieuwszender CNN. Een andere zorgwekkende ontwikkeling is de professionalisering van cybercrime. De georganiseerde misdaad heeft cybercrime ontdekt en professionele *attack kits* zijn vrijelijk verkrijgbaar. De aanval op de CNN werd grotendeels uitgevoerd met behulp van online verkrijgbare tools voor *Distributed Denial Of Service* (DDOS)-aanvallen.

## Beveiliging

Op tal van fronten wordt geprobeerd zich tegen deze toename van bedreigingen te wapenen. Ook overheden zien in dat er regulering nodig is om het gebruik van alle informatietechnologie in goede banen te leiden, opdat iedereen



IT veilig kan gebruiken. Tevens wordt informatiebeveiliging inmiddels als integraal onderdeel van IT gezien, wat leidt tot een toenemende integratie van beveiligingstoepassingen binnen IT-toepassingen en -middelen.

Ook binnen de organisaties van bedrijven en instellingen vindt steeds vaker integratie van informatiebeveiliging plaats. Beveiligingsprocessen en procedures worden in organisaties verankerd, onder andere door het implementeren van onder meer de *Code voor Informatiebeveiliging*.

Daarnaast wordt onderkend dat een integrale beveiliging een samenspel is van beleid, procedures, technische middelen en menselijk gedrag. Mensen kunnen echter binnen dit samenspel van maatregelen een onvoorspelbare factor zijn. Beveiliging zou lastig zijn en niets opleveren, zo was lange tijd de opinie die nog regelmatig opgeld doet. Deze houding kan worden veroorzaakt omdat gebruikers zich onvoldoende bewust zijn van de risico's. Handhaving van het beveiligingsbeleid is daarom essentieel, maar er zijn meer factoren.

#### Human factor

Tegenwoordig zien eenvoudige computergebruikers zich met vele beveiligingsmaatregelen, zoals virusscanners, spamfilters en firewalls, geconfronteerd. Een omgeving met zoveel bedreigingen en even zovele maatregelen daartegen, kan

**Gebruikers moeten een beter veiligheidsbewustzijn hebben.**



## Binnen IT-sector krijgt de human factor beperkte aandacht

verschillende effecten hebben op de gemiddelde gebruiker. Zo kunnen gebruikers zich met al die maatregelen juist veilig wanen en daardoor geneigd zijn meer risico's te nemen. Zo is in het verkeer al vele keren aangetoond dat passieve beveiligingsmaatregelen, zoals ABS en airbags, als neveneffect hebben dat bestuurders zich veiliger wanen en harder rijden of minder afstand houden. Dit wordt als een maatschappelijk probleem gezien en bewustwordingscampagnes en handhaving zijn er dan ook op gericht het gedrag van weggebruikers te veranderen.

Veiligheidsbewustzijn is echter vaak niet aangeboren en duidelijkheid, herhaling en strikte naleving zijn daarom noodzakelijk om gebruikers er zodanig van te doordringen, dat het een tweede natuur wordt. Pas als gebruikers zich echt van de risico's bewust zijn, zal naleving van beleid goed kunnen worden bewerkstelligd. In de petrochemische industrie is al geruime tijd geleden op deze manier een cultuur ontstaan waarin veiligheidsbesef met succes wordt aangeleerd.

Wie echter de IT- en informatiebeveiligingssector kent, zal moeten constateren dat de *human factor* verhoudingsgewijs beperkt aandacht krijgt. Binnen de IT bestaat de neiging om bij het menselijke probleem naar twee oplossingen te grijpen: tools en techniek. Het vertrouwen in tools, het gereedschap, is vaak dusdanig groot, dat alleen de introductie ervan al als een verbetering wordt ervaren. Iedere goede bouwvakker weet dat goed gereedschap een randvoorwaarde is voor een goed resultaat, maar goed gereedschap maakt van mensen nog geen goede bouwvakkers. In IT is het werken volgens Prince- en ITIL-methodieken volgens veel organisaties al voldoende om te stellen

dat zij hun project- en servicemanagement adequaat hebben ingericht.

Teveel organisaties ervaren echter dat het toepassen van goed IT-gereedschap, niet automatisch tot verbetering leidt. Inmiddels zijn er veel bedrijven die beweren dat zij veiliger werken, nu zij de Code voor Informatiebeveiliging hebben geïmplementeerd. Let wel, de Code kan wel degelijk helpen om de beveiliging te verbeteren, maar aandacht voor de mensen die er mee om gaan en de handhaving ervan is eveneens een randvoorwaarde.

Hetzelfde geldt voor het rotsvaste vertrouwen in techniek. Hoewel hiermee op zich een aanzienlijk betere beveiliging kan worden gerealiseerd en dat gereedschap mensen kan helpen het werk beter, efficiënter en in dit kader vooral veiliger uit te voeren, zijn er toch risico's. Zo rust het ministerie van Defensie zijn medewerkers sinds kort uit met versleutelde USB-sticks. Op zich is dit een logische en verstandige oplossing, maar deze kan ook als symptomatisch worden gezien. Militairen verliezen USB-sticks en dus is de oplossing USB-sticks met en-

ADVERTENTIE

## Waar begint succes?

### Bij bereikbaarheid.

Bij een scherpe, onafhankelijke blik op de dagelijkse praktijk. Bij het vermogen know-how en ervaring helder om te zetten in resultaat. Bij verstand van ICT en een kloppend telefonie hart.

### Bij BenN.

Bij ardy.bullee@BenN.nl.



On the move  
with BenN

Telecom Consulting & Management  
[www.BenN.nl](http://www.BenN.nl)



## Beveiliging is samenspel van verschillende factoren

cryptie. De vraag is of dit nu betekent dat defensiemedewerkers ongestoord USB-sticks mogen verliezen. Dat defensiemedewerkers zich continu bewust zijn van de gevaren rondom informatietechnologie, lijkt minstens zo belangrijk. Aangezien ervan uit kan worden gegaan dat dit wel degelijk gebeurt, zijn er echter nog andere krachten aan het werk, zoals de eerder genoemde media-aandacht.



**Technische oplossingen, zoals zwaar beveiligde USB-sticks, zijn niet altijd zaligmakend.**

### Normvervaging en imagoschade

Binnen de media-aandacht rondom informatiebeveiliging komen er twee duidelijke zaken naar voren. Ten eerste is er nu sprake van een soort normvervaging van wat nu als gevoelige informatie moet worden beschouwd. Lange tijd trok iets pas de aandacht, als iemand strikt vertrouwelijke informatie had weten te

**Binnen de petrochemische industrie is al lang geleden een veiligheidscultuur ontstaan (Bron foto: Shell).**



verkrijgen. Tegenwoordig is echter puur het *kunnen* verwerven van informatie al voldoende om veel ophef te creëren. Dit wordt mede veroorzaakt door een tweede fenomeen, namelijk dat het tegenwoordig maatschappelijk onverantwoord is dat bedrijven of instellingen slordig met informatie omgaan. Heel Nederland staat klaar om er schande van te spreken als ambtenaren digitale informatie laten slingeren, ongeacht de soort informatie die het betreft.

Verder is de interesse vaak selectief, want zelfs al is de overheid minstens even intensief bezig met campagnes om het beveiligingsbewustzijn van haar personeel te verbeteren, dan nog heeft dit een lagere nieuwwaarde dan versleutelde USB-sticks. Al deze aandacht zorgt ervoor dat het begrip imagoschade hoog op de agenda's prijkt van informatiebeveiligers van overheden en bedrijven. Zij zijn uiterst beducht voor negatieve publiciteit door beveiligingsincidenten, hoe onbelangrijk en risiceloos deze feitelijk ook mogen zijn.

**Veiligheidsbewustzijn**  
Het is echter vreemd te moeten consta-

teren dat één aspect door alle techniek, organisatie en regulering wordt ondergesneeuwd, namelijk de menselijke factor. Ogenschijnlijk is er maar weinig aandacht voor de cruciale rol die mensen spelen als deze gebruikmaken van IT en informatiebeveiliging nodig hebben om zich tegen de gevaren van IT te kunnen beschermen.

De beveiligingswereld, maar ook de overheid, zouden er dan ook verstandig aan doen te beseffen dat beveiliging ook belangrijk kan worden verbeterd door een beter veiligheidsbewustzijn bij gebruikers te bewerkstelligen. De informatiebeveiligingsindustrie ziet dit wellicht niet als sexy, maar diegenen die voor de beveiliging verantwoordelijk zijn, kunnen er wel degelijk de vruchten van plukken.

Bedrijfs- en overheids campagnes zijn intensief en kosten tijd, maar wie bereid is over de schutting te kijken, ziet dat deze veiligheids campagnes wel degelijk effect kunnen hebben. De BOB-campagnes tegen alcohol in het verkeer laten dit bijvoorbeeld zien. Voorlichting, handhaving en herhaling zijn uiterst belangrijk om te voorkomen dat de doelgroepen weer in het oude gedrag terugvallen, wat wordt geïllustreerd door de niet af latende campagnes sinds *Glaasje op? Laat je rijden!*

Dit geldt ook voor de wereld van informatiebeveiliging. Het creëren van een veiligheidsbewustzijn moet in ieder geval voor beveiligingsverantwoordelijken een tweede natuur zijn. Pas dan kan worden verwacht dat een beter veiligheidsbewustzijn ook aan gebruikers kan worden aangeleerd. ■

### Conclusie

Het is goed dat informatiebeveiliging de laatste jaren uitermate serieus wordt genomen, maar wanneer bedrijven, overheid en maatschappij zich niet meer gaan en blijven concentreren op de menselijke factor binnen de IT, is het mogelijk dat we onszelf uiteindelijk lelijk in de vingers snijden. Mensen maken of kraken nu eenmaal beveiliging, zowel bewust als onbewust. Campagnes van beleidsmakers, of die nu vanuit de bedrijven zelf of vanuit de overheid komen, kunnen daarbij uitkomst bieden. Wellicht dat BOB, naast zijn werk als Bewust Onbeschonden Bestuurder, kan gaan bijklussen als Bewust Oplettende Beveiligiger.