

Eindrapportage nulmeting

in het kader van het MKB-experiment van het Nationaal

Project Aanpak Cybercrime

uitgevoerd door Syntens

in opdracht van Digibewust

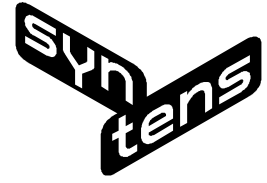
contactpersoon ir. Henk van Heerde
afdeling
telefoon
e-mail hvh@syntens.nl
datum 27 oktober 2006

Syntens
Postbus 1300
3430 BH Nieuwegein

Bezoekadres
Kelvinbaan 42
3439 MT Nieuwegein

T [088] 444 04 44
F [088] 444 04 99
info@syntens.nl
www.syntens.nl

KvK 27169058



Eindrapportage nulmeting



Inhoudsopgave

1	Inleiding	6
1.1	Opdracht en context	6
1.2	Doelgroep	7
1.3	Beoogde werkwijze	7
2	Beschrijving van de procesgang in het experiment	8
2.1	Vertaling opdracht naar uitvoeringsteam	8
2.2	Vertaling naar inzet adviseurs en externen	8
2.3	Werving en selectie van deelnemers	9
2.4	Vertaling naar voorlichtingsmomenten (workshops)	11
2.4.1	Digikring	11
2.4.2	Afvallers	11
2.4.3	Deelnemers na hun scan	12
2.4.4	Overigen in het ICT-werkveld	12
2.5	Opzet demonstrator, bouw en inzet bij workshops	13
3	Deelnemers en resultaten	16
3.1	Verdeling naar sectoren	16
3.2	Verdeling naar grootte	16
3.3	Technisch beheer	16
3.4	Fysieke beveiliging van de apparatuur	18
3.5	Back-up van gegevens	18
3.6	Koppeling met internet	19
3.7	Mobiele veiligheid	20
3.8	Website en beveiliging van de e-business	21
3.9	Personeel	22
3.10	Organisatie en beleid	23
3.11	Schade	23
4	Uitkomsten per sector in grote lijnen	24
5	Bijzondere cases	25
6	Relatie deelnemers – ICT-toeleveranciers en invloed op informatiebeveiliging	26
7	Beschouwing kwaliteit ICT-toeleveranciers en aanbevelingen daarbij	28
8	Evaluatie aanbod tot reparatie van veiligheidslekken	29

9	Gebruikte instrumenten	30
9.1	Vragenlijst	30
9.2	Rapportsjabloon	31
9.3	Externe technische hulp	32
9.4	Workshopsjabloon	32
9.5	Demonstrator	33
10	Bewustwordingsacties tot dusver	34
11	Conclusies	37
11.1	Hoge afhankelijkheid, géén maatregelen	37
11.2	Informatiebeveiliging is geen technologie	37
11.3	Mensen zijn de zwakste schakel	37
11.4	Ondernemers schuiven af	38
11.5	ICT-dienstverleners dienen kritisch te kijken naar hun eigen kwaliteit (zelfreflectie)	38
12	Aanbevelingen voor instrumentontwikkeling	39
12.1	Boekje over informatiebeveiliging	39
12.2	Voorbeelden	39
12.3	Workshops	40
12.4	Audits en keurmerk	40
13	Aanbevelingen voor landelijke voortzetting	42
13.1	Eerstelijns ondersteuning	42
13.2	Verbreding naar heel Nederland	42
13.3	Specifieke aanpak e-business	42
13.4	Inschakelen ICT-branche	42
	Bijlage 1: vragenlijst cybercrimescan	44
	Bijlage 2: rapportageformat scandeelnemer	54
	Bijlage 3: Syntens handleiding informatiebeveiliging	59

Samenvatting

Dit rapport doet verslag van een pilot in Flevoland over informatiebeveiliging in het MKB. Bij 50 bedrijven is door adviseurs van Syntens onderzocht aan de hand van een speciale vragenlijst en enkele technische metingen hoe het praktisch is gesteld met de beveiliging van de computernetwerken en de gegevens van ondernemers, welke schade

zij hebben opgelopen en aan welke risico's ze bewust of onbewust bloot staan. Het gaat dan niet alleen om het gevaar via internet maar ook om uitval van systemen door andere oorzaken. De mens blijft een cruciale factor, in de vorm van de ondernemer maar vooral ook door wat hij vraagt of toelaat van zijn werknemers – en dit laatste bleek 'veel' te zijn. Geconstateerd is dat beleid op het gebied van informatiebeveiliging meestal ontbreekt.

Onverwacht was het feit dat ondanks de grote mate van uitbesteding van ICT-beheer er veel vermijdbare 'lekken' werden aangetroffen.

Er zijn met diverse doelgroepen workshops gehouden om richting te geven aan de pilot en de tussenresultaten te borgen. De belangstelling hiervoor was heel verschillend en bij ondernemers in het algemeen teleurstellend. Het begrip informatiebeveiliging of 'cybercrime' leeft onvoldoende om spontaan 'in beweging' te komen.

Onderdeel van het experiment is het creëren van een proefopstelling waarmee gevolgen van 'lekken' in de beveiliging kunnen worden gedemonstreerd.

De conclusies van de onderzoekers:

1. ondernemers zijn sterk afhankelijk van informatiesystemen maar nemen geen adequate maatregelen om de beschikbaarheid te borgen,
2. informatiebeveiliging heeft meer met organisatie en cultuur dan met technologie te maken,
3. mensen zijn de zwakste schakel,
4. ondernemers schuiven de verantwoordelijkheid af naar hun ICT-toeleveranciers,
5. ICT-dienstverleners dienen kritisch te kijken naar hun eigen kwaliteit (zelfreflectie)

De volgende aanbevelingen worden gedaan ten aanzien van instrumentontwikkeling:

1. actualiseer een reeds bestaande uitgave over informatiebeveiliging,
2. werk direct bruikbare voorbeelden uit voor beheerovereenkomsten, procedures en beleid,
3. organiseer praktische en laagdrempelige workshops,
4. ontwikkel audits en een keurmerk op MKB-niveau.

Adviezen over de aanpak van het vervolg:

1. organiseer landelijk een eerstelijns ondersteuning op dit gebied,
2. verbreed het experiment naar heel Nederland en kijk nog eens nadrukkelijk naar de onderbelichte sectoren,
3. onderzoek specifiek en dieper de informatiebeveiliging van e-commerce websites,
4. schakel de ICT-branche in voor verbreding en kwaliteitsborging.

1 Inleiding

1.1 Opdracht en context

Het Nationaal Platform Criminaliteitsbeheersing (NPC) is een publiek-privaat samenwerkingsverband dat zich bezighoudt met het tegengaan van criminaliteit waarmee het bedrijfsleven in Nederland wordt geconfronteerd. Dit platform heeft in het kader van het Actieplan Veilig Ondernemen II (AVO II) de aanzet gegeven voor een programma tot het tegengaan van cybercrime; het NICC (Nationale Infrastructuur Cybercrime). Het NICC initieert, ontwikkelt en experimenteert maar heeft niet tot doel zelf de nieuwe nationale infrastructuur te worden. Het NICC brengt partijen zoals het bedrijfsleven, GOVCERT, het KLPD en het Meldpunt Cybercrime bij elkaar, zet ontwikkelde producten uit bij deze partijen of laat nieuwe producten door deze partijen ontwikkelen.

Digibewust is een publiekprivaat programma om de bewustwording van veilig gebruik van digitale middelen bij burgers en bedrijven te vergroten. De afgelopen jaren is door verschillende initiatieven gewerkt aan deze bewustwording. Daarmee is al veel bereikt, maar er moet nog veel meer gebeuren. In het Digibewust programma zijn bestaande activiteiten en nieuwe initiatieven ondergebracht. Naar aanleiding van de resultaten van de MKB nulmeting met betrekking tot cybercrime zullen in 2007 specifieke activiteiten voor het MKB opgezet worden. Digibewust (www.digibewust.nl) is een driejarig programma van het Ministerie van Economische Zaken en wordt uitgevoerd door ECP.NL.

De veiligheidsscan bij het MKB m.b.t. cybercrime is onderdeel van het Programma Nationale Infrastructuur Cybercrime en het Digibewust programma. Syntens was verantwoordelijk voor de uitvoering van de veiligheidsscan.

Doelstelling van de nulmeting is om het inzicht in de kwetsbaarheid van het MKB voor cybercrime-aanvallen te vergroten en zo die kwetsbaarheid te reduceren, zodat de schade die het MKB als gevolg van cybercrime lijdt zoveel mogelijk wordt verminderd.

De opdracht aan Syntens is op 17 mei 2006 verleend. Het project was voorzien voor de periode van 24 april tot 15 november. In deze periode is door vijf adviseurs van Syntens gewerkt aan het doorlichten van 50 MKB-bedrijven.

1.2 Doelgroep

50 MKB-bedrijven binnen Flevoland (5-150 werkzame personen) verdeeld over de sectoren industrie, bouw, logistiek en groothandel, creatieve industrie, human health en food & agri. De doelgroep is te klein en te divers om wetenschappelijk verantwoorde uitspraken te doen. In dat licht moeten ook de cijfers worden gezien zoals die in hoofdstuk 3 worden weergegeven. De uiteindelijke deelnemers zijn ook niet aselekt gekozen, zoals in paragraaf 2.3 wordt toegelicht.

1.3 Beoogde werkwijze

Uit de opdracht "Door Syntens wordt een adviestraject uitgevoerd waarbij met behulp van een cybercrimescan in kaart wordt gebracht welke issues bij dat specifieke bedrijf spelen. De uitkomsten hiervan worden aan het bedrijf teruggekoppeld. De mogelijkheid wordt geboden om vervolgens een beroep te doen voor 'reparatie' op de (huis) ICT-leverancier en/of de huisaccountant, waarbij een tegemoetkoming in de kosten daarvan wordt verleend. Het uitvoeren van de nulmeting bestaat uit de volgende stappen:

- Het uitvoeren van een cybercrimescan (onderzoek op locatie) bij 50 bedrijven. Hiervoor maakt Syntens gebruik van de beveiligingsscan die zij in het kader van Nederland gaat Digitaal heeft ontwikkeld.
- Het uitbrengen van een advies aan 50 MKB-bedrijven waarbij de uitkomsten van de scan het vertrekpunt zijn. Hiervoor ontwikkelt Syntens een cybercrime adviesformat.
- Het (mogelijk) inschakelen van de (huis) ICT-leveranciers, accountant of andere kennisleverancier.
- Reparatie op locatie. Geconstateerde gaten in de informatiebeveiliging van de deelnemende bedrijven worden kosteloos gerepareerd. Kosten voor de aanschaf van hard- en software moeten echter door de ondernemer zelf betaald worden.
- Proefopstelling voor het MKB in de E-room van Syntens te Lelystad.
- Om de eigen bevindingen te verifiëren en te toetsen organiseert Syntens tijdens de looptijd van het project een aantal workshops."

2 Beschrijving van de procesgang in het experiment

Coördinatie, contacten met de opdrachtgever en rapportage heeft binnen Syntens plaatsgevonden vanuit het programma Nederland gaat Digitaal door programmaleider Erik Peeters en Henk van Heerde van de NDBI expertgroep. De opdrachtgever liet zich bijstaan door een klankbordgroep, waarin o.a. NICC, MKB Nederland, Govcert en de regionale initiatiefnemers VNO-NCW en KvK vertegenwoordigd waren.

2.1 Vertaling opdracht naar uitvoeringsteam

De operationele activiteiten vonden plaats in het werkgebied van de Syntens business unit Noordoost. Deze staat onder leiding van businessunitdirecteur John Joosten. Het betrof het uitvoeren van de 50 scans en de bijbehorende technische zaken, organisatie van workshops en het verwerven van een proefopstelling (demonstrator). Er is een uitvoeringsteam samengesteld met adviseurs uit twee in Flevoland opererende adviesteams, die samen vier van de zes sectoren afdekken. Vanwege de korte periode en de geboden haast zijn de overige twee sectoren ook door deze vijf adviseurs bediend. Het uitvoeringsteam stond onder leiding van Rinze Douma, die ook operationele contacten onderhield met de opdrachtgever. De andere adviseurs waren Kelvin Klijsma, Saïd Akdim (tot 1-7-2006), Peter Elskamp en Henk van Heerde. Het betreft hier adviseurs met jarenlange ervaring in ICT-adviezen aan MKB-ondernemers, onder andere in projecten als Sp.OED en Nederland gaat Digitaal.

2.2 Vertaling naar inzet adviseurs en externen

Bij nadere beschouwing bleken eerder gebruikte technische instrumenten vanwege de voortschrijdende techniek en toegenomen beveiligingsmaatregelen niet toereikend. Het bleek ook niet efficiënt – en in feite qua tijd onmogelijk – alle betrokken adviseurs een stoomcursus informatiebeveiliging op het momenteel gevraagde gespecialiseerde niveau te geven. Aangezien dergelijke technische expertise, met bijbehorende instrumenten, in de regio beschikbaar was, is besloten de scan in twee stukken te knippen:

- a. Een onderzoek met een lijst met vragen, door de adviseur aan de ondernemer te stellen (eventueel aan degene bij wie automatisering in het takenpakket zit), aangevuld met een rondje door het bedrijf waarbij vooral aandacht aan de opstelling van de servers wordt geschonken.
- b. Een technisch onderzoek, o.a. met speciale software, uitgevoerd door een specialist, ter plaatse uit te voeren op het netwerk van het bedrijf.

Er zijn offertes gevraagd aan vier bedrijven voor het binnen een heel korte tijd (1-2 uur) bepalen van de technische status van de firewallbescherming, de virusbescherming (toestand virusscanner), de bescherming tegen spyware en de bescherming tegen spam. Uiteindelijk is daar aan toegevoegd de update status van de besturingssoftware, de

daadwerkelijke omgang met wachtwoorden en de bescherming van een eventueel aanwezig draadloos netwerk.

Met twee bedrijven kon snel worden gestart, een derde haakte wat later aan. Voor de rapportage is een uniform model gehanteerd. De technische rapportages konden op die manier, na ontvangst door de desbetreffende Syntens adviseur, gemakkelijk worden verwerkt in zijn adviesrapport aan het bedrijf – na het zoveel mogelijk ont-‘vaktermen’. Dit laatste bleek overigens toch nog een behoorlijke klus. Zelfs Syntens adviseurs ontkwamen er niet helemaal aan om – naarmate het project vorderde – met vaktermen ‘besmet’ te raken en die te gebruiken in hun communicatie met ondernemers. Het blijft opletten om ook het ‘zoveelste’ rapport binnen hetzelfde kader ook qua taalgebruik op MKB-niveau te houden – zeker als het gaat om ICT.

Afspraken voor de scans werden gemaakt door Marjolein Hoekstra, vanuit de backoffice van Syntens toegevoegd aan het operationele team. Zij zorgde er voor dat de adviseur een half uur eerder op bezoek werd ingepland dan de specialist om de inleiding goed te kunnen doen en om de reden van de specialistische meting uit te leggen aan de ondernemer. In de praktijk werd na de inleiding samen de serverruimte bekeken en splitsten zich daar de wegen tussen specialist die achterbleef en adviseur met ondernemer die de rest van de vragen gingen doornemen. Aan het einde voegde de specialist zich weer bij adviseur en ondernemer voor een kort overzicht van de bevindingen.

Conclusie: techniek van informatiebeveiliging is echt een vak apart.

2.3 Werving en selectie van deelnemers

Op het moment dat Syntens werd gevraagd de uitvoering te offreren was een initiatiefgroep in Flevoland al met de werving begonnen, middels enkele artikelen in de Kamerkrant (uitgave mei 2006) en een brief: *“VNO-NCW MKB Flevoland, de gezamenlijke bedrijfskringen en de Kamer van Koophandel Flevoland bieden u namens het ministerie van EZ de mogelijkheid van deze gratis veiligheidscheck aan. Wilt u meer informatie of u nu reeds aanmelden voor deelname aan dit project, dan kunt u contact opnemen met Mariëlle Wielandt (mwielandt@lelystad.kvk.nl) of 0320 - 286 286). Het honoreren van aanvragen gebeurt op volgorde van binnenkomst, dus wees er snel bij!”*

In dezelfde Kamerkrant een interview met Edwin Mac Gillavry van het NICC onder de titel ‘Cybercrime-check met open vizier’ en een interview met Henk-Jan Angerman, een jonge ondernemer op dit gebied met als titel ‘Security is specialisme’.

De actie leidde tot een lijst met 58 bedrijven die wel wat voor zo’n gratis check voelden. Bij nader inzien stonden op deze lijst veel bedrijven die niet tot de doelgroep

behoorden, zoals aangegeven in de opdracht: bedrijven in Flevoland met 5-150 werkzame personen, verdeeld over de sectoren industrie, bouw, logistiek, creatieve industrie & multimedia, human health en agro & food. Het ging daarbij om zelfstandigen zonder personeel, detailhandel en vooral veel zakelijke dienstverlening van diverse aard die niet onder één van de aangegeven sectoren geschaard konden worden. Na overleg met de regionale initiatiefnemers, die de werving voor hun rekening zouden nemen, is besloten enkele voor het ondernemersnetwerk in Flevoland belangrijke bedrijven toch mee te laten doen en de overigen af te laten vallen. De afvallers kregen door Syntens een alternatief aangeboden: deelname aan een workshop over het thema in de e-room van Syntens in het Ondernemingshuis in Lelystad.

Het hele planningsproces van de uitvoering van de scans (zie ook het vorige punt) vergde veel tijd door de lange tijd tussen aanvang werving en aanvang planning en de kwaliteit van de uit de werving aangeleverde gegevens (onduidelijke bedrijfsnamen en contactpersonen). Daarnaast was planning lastig doordat het project in en rond de vakantie viel. Bij het maken van operationele afspraken voor de scan (datum, tijd, met wie) bleken veel ondernemers zich niet meer te herinneren waarvoor ze zich hadden opgegeven – of vonden het bij nader inzien toch niet zo nodig. Uiteindelijk bleven er 29 bedrijven over.

Een tweede mailing, tijdens de vakantieperiode, leverde zo'n tien aanmeldingen op. Alle overige deelnemers zijn geworven door de betrokkenen binnen Syntens, deelnemers zelf die collega-bedrijven attendeerden en ICT-toeleveranciers die hun klanten er op attendeerden. Bij de werving van de laatste deelnemers is er zoveel mogelijk naar gestreefd een evenredige verdeling over de beoogde sectoren te krijgen. Dat is ten dele gelukt: binnen de sector bouw was de belangstelling minimaal en er bleef nog een klein aantal bedrijven die slechts onder 'diversen' zijn te scharen.

Conclusie: het begrip 'cybercrime' of –wat breder – informatiebeveiliging leeft niet echt onder MKB-ondernemers.

Aanbeveling: werving, selectie en opvolging (maken van afspraken) moet kort achter elkaar worden uitgevoerd en goed gecoördineerd verlopen.

2.4 Vertaling naar voorlichtingsmomenten (workshops)

In de opdracht staat: om de eigen bevindingen te verifiëren en te toetsen organiseert Syntens tijdens de looptijd van het project een aantal workshops.

2.4.1 *Digikring*

Dat eerste moment was kort na de aftrap, bij het inventariseren van de beschikbare instrumenten en het afbakenen van de bij de ondernemingen precies te 'scannen' onderwerpen. Gewenst was de inzichten te toetsen bij en te delen met Flevolandse ondernemers binnen het ICT-werkveld. Hiervoor is op 20 juni 2006 een workshop gehouden waarbij (alleen) leden van de Digikring werden uitgenodigd. De Digikring is een initiatief van Syntens, binnen het programma Nederland gaat Digitaal, voor het bijeenbrengen van (vaak jonge) ICT-ondernemers voor netwerken, onderlinge kennisdeling, bevordering van samenwerking met als neven doel gemakkelijk toegang te krijgen tot deze groep om ze te helpen bij de verdere professionalisering in deze dynamisch maar vaak technisch georiënteerde sector. Als aanknopingspunt voor een brainstorming 'hoe krijg ik het MKB bezig met informatiebeveiliging' is de inhoud gebruikt van de standaard workshop 'computers en veiligheid' (in het voorjaar van 2006 geupdate) uit het programma Nederland gaat digitaal. Van de 80 leden waren er 10 aanwezig. Men was enthousiast, de workshop voldeed aan de verwachtingen van deelnemers en organisatoren. Afsproken is aan het einde van het project de resultaten ook terug te koppelen naar deze deelnemers.

2.4.2 *Afvallers*

Voor de ondernemers, die zich in eerste instantie hadden aangemeld maar niet tot de doelgroep bleken te behoren, zijn twee workshops georganiseerd, op 30 mei en 1 juni. De afvallers zijn allemaal persoonlijk per telefoon benaderd en kregen de keuze uit deze twee data. Van de 29 ondernemers hebben er slechts 5 gebruik gemaakt van dit alternatieve aanbod, zodat de tweede workshop is geannuleerd. Het ging hier om de standaard workshop 'computers en veiligheid' (in het voorjaar van 2006 geüpdatet) uit het programma Nederland gaat Digitaal. Deze workshop was binnen dit programma ook al enkele malen eerder in Flevoland aangeboden maar vanwege gebrek aan belangstelling steeds geannuleerd. Als reden om niet van het alternatieve aanbod gebruik te maken werd, naast het feit dat men vaak al vergeten was zich te hebben aangemeld voor de scan, veelvuldig genoemd dat men het reizen naar Lelystad er niet voor over had: 'ze zouden toch hier op het bedrijf komen'.

Conclusie: het begrip 'gratis' lokt ook diegenen die niet serieus in het onderwerp zelf geïnteresseerd zijn.

2.4.3 Deelnemers na hun scan

Reeds snel na het uitvoeren van de eerste scans bleken de gescande ondernemers belangstelling te hebben voor de resultaten bij de andere bedrijven, in feite voor 'benchmarking'. Voor het terugkoppelen van de resultaten tot dan toe zijn vier workshops geprogrammeerd op een moment dat de meeste scans achter de rug zouden zijn, vanaf medio september. De werving voor deelnemers aan de workshops, die konden kiezen uit vier data, bleek echter een moeizame zaak – ondanks het feit dat reeds tijdens de scans de workshops werden aangekondigd en al veel toezeggingen voor deelname werden gedaan. Daarbij is ook de inzet van de proefopstelling meegenomen.

Uiteindelijk zijn er slechts twee van de vier doorgedaan, met respectievelijk vijf en zeven deelnemers. De nadruk is vooral komen te liggen op een aantal demonstraties met de proefopstelling. Daarnaast was de vraag hoever je nu als ondernemer moet gaan in informatiebeveiliging. De deelnemers waren tevreden. Een enkeling had meer verwacht ten aanzien van benchmarking. Mogelijk speelt ook hier de timing een rol: betere programmering, coördinatie van datum van scans, toezending van hun eigen rapportage en datum van workshop. Resultaten van het geheel zijn echter pas nu bekend, misschien kan er nu wel interesse worden opgewekt bij de deelnemers.

2.4.4 Overigen in het ICT-werkveld

In voorbereiding is een workshop voor die bedrijven, die voor de deelnemers aan de scan het ICT-beheer uitvoeren, en hun collega's. Doel is het confronteren met de bevindingen en het nadenken over een betere kwaliteit in dienstverlening, mogelijk ook het aanbieden van nieuwe diensten op het gebied van informatiebeveiliging.

Er worden twee verschillende doelgroepen onderkend:

- a. ICT-beheerders: bedrijven die, al dan niet als vervolg op verkoop en installatie, het beheer van computernetwerken uitvoeren, zowel op locatie als op afstand.
- b. Websitebouwers en webapplicatieontwikkelaars: bedrijven die maatwerk e-businessoplossingen realiseren en daarbij zelf voor hosting zorgen of dit uitbesteden.

2.5 Opzet demonstrator, bouw en inzet bij workshops

Onderdeel van de opdracht was het samenstellen van een proefopstelling in de e-room van de Syntens vestiging in Lelystad. Het begrip 'demonstrator' is ook wel gebruikt. Bij de aanvang van het project waren geen heldere functionele of technische specificaties beschikbaar, zelfs een heldere doelstelling wat er met de proefopstelling bereikt zou moeten worden ontbrak. Er lag een logische verbinding met workshops en een mogelijke relatie bij individuele adviestrajecten. Na contact met diverse spelers in het veld van informatiebeveiliging is de volgende offerteaanvraag naar enkele bedrijven uit de regio gezonden:

"De proefopstelling zal worden gebruikt bij workshops met ondernemers op het gebied van computers en veiligheid en bij individuele adviestrajecten in het kader van dit project. Een individueel adviestraject omvat een beveiligingsscan op locatie van de ondernemer (in Flevoland), advies over verbetering van de informatiebeveiliging (inclusief eventueel lokale demonstratie van algemeen gebruikte freeware oplossingen) en bemiddeling in en gedeeltelijke betaling van 'reparatie' door de 'vaste' ICT-toeleverancier van het bedrijf. De proefopstelling kan een rol spelen bij het advies, zowel op locatie (op afstand gebruikt) als bij workshops ter demonstratie van het effect van preventieve maatregelen in de e-room.

Het is denkbaar dat de proefopstelling wordt uitgebreid aan de hand van de ervaringen tijdens het project. Voor de instandhouding/exploitatie is voldoende budget beschikbaar.

Bij de proefopstelling wordt gedacht aan een computerconfiguratie, zoals die bij een 'gemiddeld' MKB-bedrijf voorkomt:

- een server;
- minstens twee werkplekken (PC's, mogelijk één laptop) aangesloten op internet via een ADSL-verbinding of via het eigen netwerk van Syntens;
- met uitwisselbare opslagmedia zoals herschrijfbaar DVD / CD maar ook USB-sticks;
- Microsoft besturingssystemen;
- Microsoft software: Internet Explorer, Outlook voor e-mail, MSN als instant messenger;
- uitbreiding met een draadloos netwerk, waarmee tenminste één laptop is verbonden;

- optie: uitbreiding met een handheld computer (PDA), draadloos.

Voor het demonstreren van (gebrek aan) beveiliging wordt gedacht aan:

- een computerconfiguratie waarmee 'aanvallen' worden gesimuleerd;
- optie: een reeds enige tijd 'besmet' systeem;
- aansluitbare firewall (hardware, eventueel ook software);
- encryptie-software".

Van twee bedrijven werd een offerte ontvangen. De uiteindelijke keuze is gevallen op het bedrijf Vest-IT uit Naarden. Met dit bedrijf, die als projectmanager aanstelde drs. Jim de Haas, beveiligingsexpert en via zijn ervaring bij Media Plaza bekend met demonstraties voor ondernemers, werden details uitgewerkt en een voortvarend begin gemaakt met de bouw. Na de vakantieperiode konden de eerste resultaten worden doorgesproken en werd de oplevering gesynchroniseerd met de geplande workshops.

In eerste instantie waren de volgende demonstraties voorzien:

a. PC demo's:

- besmetting met virus, spam, spyware;
- risico's van instant messaging;
- risico's van peer to peer software;
- kwetsbaarheden in Windows;
- versturen van informatie zonder encryptie..

b. Netwerk demo's:

- kwetsbaarheden in Windows server;
- kwetsbaarheden in webserver;
- kwetsbaarheden in mailserver;
- spamfilter;
- firewall;
- hacking, het overnemen van een PC.

Na het geven van een demonstratie kunnen de PC's gereset worden middels het uitrollen van een nieuwe hard-disk image.

De demonstraties bestaan uit handelingen van de adviseur of gespecialiseerde ondersteuner, geïllustreerd met powerpointpresentaties op de betreffende PC's (één 'ondernemerswerkstation', en een 'hacker' PC). Voor een groepsdemonstratie wordt de 'hacker PC' aangesloten op de presentatiemiddelen van de e-room.

Een eerste uitbreiding was een demonstratie van de kwetsbaarheden van een draadloos netwerk. Dit aspect zijn we veelvuldig tegengekomen bij de scans en er is veel belangstelling voor bij ondernemers (twijfel, onrust).

Bij de voorbereidingen van de eerste workshop bleek een aantal demonstraties alleen mogelijk met gespecialiseerde ondersteuning vanuit Vest-IT, de leverancier. Daarnaast bleek de synchronisatie van de (standaard) inhoud van de workshop 'computers en veiligheid' met de proefopstelling veel tijd te vergen. In samenwerking met de leverancier, door ombouwen van de originele presentaties en integreren van het nieuwe ondersteunende materiaal kon de tweede workshop zoals gepland verlopen. De deelnemers waren tevreden en er was veel interactie. Nota bene: het betrof hier deelnemers waarbij de scan inmiddels was uitgevoerd. Een aantal van de gevaren, waar ze door de scan en het daaropvolgende adviesrapport bewust van zijn geworden, werden tijdens de workshop door middel van een echte 'hackersaanval' als zeer dichtbij ervaren.

De proefopstelling is gedemonstreerd aan de klankbordgroep op 10 oktober 2006. Een belangrijke opmerking was dat het MKB-gehalte gewaarborgd moet worden: niet te veel tegelijk en in heldere taal. Conclusie is dat gestreefd moet worden naar demonstraties door een 'gewone' Syntensadviseur (een generalist).

Het voortschrijdende inzicht in wat nu wel en niet relevant is voor ondernemers heeft geleid tot een aantal aanpassingen van de demonstrator: zowel uitbreidingen (meer onderdelen) als de methodiek van demonstreren (toolset waaruit een adviseur gemakkelijk een op de doelgroep en beschikbare tijd afgestemd scenario kan samenstellen). De aanpassingen zijn nog niet geheel doorgevoerd. De definitieve oplevering van de demonstrator, met documentatie zoals gevraagd, wordt begin november verwacht.

Een onverwacht neveneffect van de proefopstelling is dat ondernemers eenvoudig kunnen zien hoe een modern netwerk er eigenlijk uitziet aan componenten, inclusief de aansluiting op internet. Met o.a. de systeemdokumentatie, zoals die eigenlijk bij elk bedrijfsnetwerk hoort om beheer mogelijk te maken, kan ook eenvoudig de relatie worden gelegd met het organiseren van het beheer in het eigen bedrijf – al dan niet uitbesteed.

3 Deelnemers en resultaten

3.1 Verdeling naar sectoren

sector	Aantal bedrijven
bouw	7
creatieve industrie	11
food & agri	7
human health	4
industrie	3
logistiek & groothandel	14
overigen (vooral financiële dienstverlening)	4

De verdeling van de 50 uiteindelijke deelnemers over de sectoren weerspiegelt in grote lijnen de verdeling van de bedrijvigheid in Flevoland (exclusief detailhandel en horeca), waar het zwaartepunt ligt op zakelijke dienstverlening en groothandel.

3.2 Verdeling naar grootte

Grootte in aantal werknemers	Aantal bedrijven
Meer dan 250	3
100 - 250	4
10 - 100	34
5 - 10	6
Minder dan 5	3

De meeste deelnemende bedrijven vallen binnen de oorspronkelijke doelgroep qua grootte. Het gaat steeds om bedrijven met een zodanige omvang dat ICT en dus informatiebeveiliging een belangrijke rol speelt bij de bedrijfsvoering.

3.3 Technisch beheer

Informatiebeveiliging gaat over continuïteit van informatiesystemen. Een systeem is een combinatie van middelen, mensen en procedures.

Het beheer van de middelen noemt men wel technisch beheer, systeembeheer, IT beheer of netwerkbeheer. Grote bedrijven hebben hiervoor doorgaans een aparte afdeling. Zo'n afdeling werkt al dan niet volgens bepaalde normen zoals ITIL.

In het MKB komen dergelijke afdelingen vrijwel niet meer voor. Het gaat hoogstens om één of twee specialisten bij een bedrijf dat meer dan 100 werkstations en meerdere servers heeft.

We zien grofweg de volgende situaties:

1. Het bedrijf heeft alles uitbesteed, soms aan het bedrijf waar ook de spullen worden gekocht, soms aan een gespecialiseerd bedrijf. Zelf doet men helemaal niets.
2. Het bedrijf heeft één of twee mensen die een meer dan gemiddelde affiniteit met en kennis van IT-hulpmiddelen hebben. Zij doen het beheer en vallen bij calamiteiten terug op één of meer ICT-leveranciers.

Er zijn daarbij enkele varianten: bij 1 is er wel degelijk een intern aanspreekpunt, dat het beheer in min of meerdere mate op de voet volgt, bij 2 kan het ook zo zijn dat de interne beheerder voldoende kennis van zaken heeft van beheer op basis van zijn andere dagelijkse werkzaamheden of eerdere baan.

Een bedenkelijke variant op situatie 1, die helaas ook voorkomt, is die waarbij het beheer is 'uitbesteed' (liever gezegd: overgelaten) aan een extern 'mannelijke', dus geen professioneel IT-bedrijf. Dat kan variëren van de buurman, een student tot een ZZP-er die 'iets' met computers doet (maar geen specialist in IT-beheer is). Bij deze ondernemers wordt het risico van gevaren via het internet ook laag ingeschat. Er is wel een virusscanner, maar die is niet (meer) voldoende. Uiteindelijk wordt er vaak een heel scala aan 'lekken' ontdekt.

Nota bene: er is in elk bedrijf wel iemand die verantwoordelijk is voor ICT, zoals de directeur als die het niet gedelegeerd heeft aan zijn hoofd administratie of iemand anders met affiniteit voor automatisering. Dat betekent niet vanzelf dat er ook actief aan (preventief) beheer wordt gedaan.

Uitkomsten van dit experiment:

Soort beheer	aantal	opmerkingen
Eigen ICT afdeling	5	3 grote bedrijven
Alles uitbesteed	26	niet alleen regionaal
Zelfdoen met of zonder achtervang	14	8 zonder opgave welke achtervang
Niet (goed) geregeld	5	2 volledig niets geregeld

3.4 Fysieke beveiliging van de apparatuur

De meeste bedrijven zijn in behoorlijke (32%) of hoge mate (64%) afhankelijk van hun ICT-systeem voor hun dagelijkse werkzaamheden. Over het algemeen wordt er door de bezochte MKB bedrijven veel en voortdurend geïnvesteerd in computers en randapparatuur. Alleen bij enkele kleinere bedrijven uit de onderzochte groep wordt nog gewerkt met (sterk) verouderde apparatuur.

60% van de bedrijven heeft een goede tot uitstekende bescherming middels een aparte en afsluitbare ruimte voor servers en netwerkapparatuur. Vrijwel altijd is bescherming tegen brand en inbraak aanwezig. Ook koeling komt in ruime mate voor. De ruimtes worden helaas in veel gevallen overdag niet daadwerkelijk afgesloten.

Bij 28% van de bedrijven was er vrijwel niets geregeld qua fysieke bescherming. Servers stonden soms in de hal of onder de trap, klaar voor het meenemen. Bescherming tegen gegevensverlies door plotselinge stroomuitval bleek in 70% voor te komen (UPS), echter niet altijd daadwerkelijk gewaarborgd. Veel ondernemers geven aan dat hun belangrijkste storingen (niet kunnen werken en defecte apparatuur, gemiddeld drie per jaar) juist aan stroomuitval lagen. De gemiddelde schade per bedrijf bedraagt snel enkele duizenden euro's.

Als rapportcijfer kreeg de onderzochte groep hiervoor een 7. Er zijn echter ook diverse negens en zelfs een 10 uitgedeeld.

3.5 Back-up van gegevens

Voor 90% van de bedrijven is het gevolg van verlies van gegevens groot, voor de overigen blijft de schade beperkt. Alle bedrijven maken regelmatig een back-up van (een deel van) het systeem, variërend van dagelijks tot slechts één keer per week of maand. De helft maakt niet van alle data steeds een back-up. Bij 25% van de bedrijven wordt de back-up niet overgebracht naar een externe locatie, bij brand zullen dan alsnog alle gegevens verloren gaan.

In slechts de helft van de gevallen wordt ook de uitkomst van de back-up in het logboek gecontroleerd en adequate actie ondernomen. Vaak ontbreekt hiervoor een sluitende procedure, waarin bijvoorbeeld ook de vervanging bij ziekte en verlof wordt geregeld. Slechts 58% heeft het terugzetten getest en er zijn maar enkele bedrijven die regelmatig het terugzetten van een volledige back-up testen of een calamiteiten- c.q. uitwijktest houden.

30% vervangt de opslagmedia niet op tijd en 62% controleert nooit de belangrijkste databases of die nog wel technisch in orde zijn (corruptie). Dit laatste kan betekenen dat gedurende weken of maanden ingevoerde gegevens in de bedrijfssoftware, wanneer daar geen ingebouwde voorziening in zit, op een bepaald moment als verloren kunnen worden beschouwd (of opnieuw vanaf papier moeten worden ingevoerd).

Als rapportcijfer kreeg de onderzochte groep hiervoor een 6,5.

3.6 Koppeling met internet

Alle bedrijven hadden de beschikking over een netwerk met één of meerdere servers en meerdere werkstations dat gekoppeld was aan internet. Het ging steeds om breedband, meestal via ADSL. Gekozen verbindingen, zoals via ISDN, troffen we niet meer aan. Omdat de verbinding steeds aanwezig is, kunnen kwaadwilligen vanaf internet schade aanbrengen – indien het informatiesysteem niet beveiligd is.

In ruim 80% van de gevallen is de beveiliging niet volledig. Zowel servers als netwerkkapparatuur (firewalls, routers, gateways) zijn niet up-to-date met de nieuwste en noodzakelijke 'pleisters' (patches en upgrades). De servers zijn op onderdelen niet goed geconfigureerd, allerlei diensten staan onnodig aan (openstaande poorten) en het ontbreekt aan een regelmatige controle op de status van het systeem. Een mogelijke oorzaak is gelegen in het feit dat hoewel het beheer is uitbesteed, er vaak een helder en eenduidig contract of SLA (Service Level Agreement) ontbreekt. In 32% van de gevallen was het beheer in procedures vastgelegd. Bij slechts enkele bedrijven wordt over de verrichte werkzaamheden helder gerapporteerd.

Bescherming tegen de meest bekende kwalen van buitenaf was bij vrijwel iedereen aanwezig. Vier bedrijven beschikten niet over een firewall. Slechts één bedrijf had geen virusscanner. De bescherming tegen andere malware, zoals spyware, is minder doorzichtig: 46% gaf aan geen spywarescanner te gebruiken. Vaak was niet duidelijk of de bescherming daartegen mogelijk onderdeel was van de antivirussoftware of door de firewall werd uitgevoerd. In ieder geval lag niemand er wakker van en was nergens schade opgelopen.

18% gaf toe geen nieuwe versies van de antivirussoftware te gebruiken. Bij de technische controles bleken veel bedrijven, ook zij die automatisch updaten van software en/of virusdefinities hadden ingesteld, niet over de nieuwste bescherming te beschikken. Opvallend was dat bij grote bedrijven updates van het besturingsysteem vaak bewust worden uitgesteld omdat ze de gevolgen voor hun – vaak complexe – software niet kunnen nagaan.

De helft van de bedrijven gebruikt een firewall in de vorm van een apart apparaat. Veel bedrijven geven aan te beschikken over zo'n apparaat, maar het blijkt dan te gaan om een functie in de internetaansluiting (ADSL-modem of router) die tegenwoordig de naam firewall eigenlijk niet meer mag dragen en in ieder geval onvoldoende bescherming biedt. Het onderhoud van de firewall is een ondergeschoven kind.

De controle en beveiliging van het e-mail verkeer is bij teveel bedrijven onder de maat. 22% van de onderzochte bedrijven controleert de binnenkomende e-mail niet op virussen, men gaat er dan van uit dat dit wordt gedaan bij de provider. Bij bedrijven die het e-mailverkeer afhandelen door middel van een eigen mailserver (70%) is de viruscontrole wel adequaat opgezet, maar heeft slechts 43% daarvan de mailserver goed ingesteld zodat externe kwaadwilligen de server niet kunnen misbruiken voor het doorsturen van e-mail (meestal spam). 34% van de bedrijven verstuurt regelmatig een elektronische nieuwsbrief, de helft via e-mail en de helft via een webapplicatie. Vier bedrijven gaven toe ook regelmatig ongevraagde e-mail te versturen, twee van hen hadden hier negatieve reacties op gekregen.

Als rapportcijfer kreeg de onderzochte groep hiervoor een 6. De cijfers voor de individuele bedrijven liggen hier tussen 4 en 10.

3.7 Mobiele veiligheid

Een onderwerp dat in toenemende mate belangrijk wordt is het overal kunnen werken dankzij ICT. Het wordt mogelijk gemaakt door draadloze netwerken (intern), mobiele apparaten zoals laptops en PDA's (al dan niet verbonden via mobiele datacommunicatie zoals met GPRS en UMTS) en verwisselbare gegevensdragers (CD-ROM's, DVD's en vooral USB-sticks). Een gevaar is verlies of diefstal van de spullen en daarmee het op straat liggen van gegevens, dus imagoschade of misbruik door concurrenten. Draadloze netwerken kunnen eenvoudig worden afgetapt wanneer de gegevens niet beschermd worden.

Enkele cijfers uit dit experiment:

- a. 40% van de bedrijven heeft minstens één draadloos netwerk:
 - hiervan is 50% beschermd, maar alleen met de laagste vorm van gegevensversleuteling (WEP);
 - 25% controleert de bescherming wel eens;
 - 20% heeft incidenten gehad met draadloze netwerken.

- b. 70% heeft telewerkers:
 - 50% hiervan is beschermd met een virtual private network (VPN)
- c. Laptops worden veel gebruikt:
 - slechts 16% heeft geen enkele laptop;
 - aantal varieert van laptop op twintig werknemers tot één op vier (grote bedrijven: van één op 80 tot één op vijf);
 - gemiddeld zijn er vier laptops per bedrijf;
 - nergens wordt encryptie toegepast (gegevensversleuteling);
 - doorgaans wordt geen BIOS-wachtwoord toegepast (basisbescherming)
- d. PDA's (handpalmcomputers):
 - 40% van de bedrijven gebruikt PDA's;
 - meestal is er maar één (16%);
 - overige bedrijven: variërend van één PDA op 30 werknemers tot soms één op één;
 - gemiddeld vier per bedrijf (evenveel als laptops);
 - bescherming?
- e. Verwisselbare media:
 - vrijwel iedereen gebruikt DVD's / CD's en/of USB-sticks met eigen bedrijfsinformatie;
 - doorgaans wordt niet bijgehouden wat er mee gebeurt;
 - slechts één bedrijf gebruikte USB-sticks met automatische Encryptie.

Men is zich wel enigszins bewust van de gevaren die het gebruik van onbeschermd laptops en PDA's qua gegevensverlies met zich meebrengt, maar ondernemers liggen hier naar eigen zeggen "niet echt wakker van".

3.8 Website en beveiliging van de e-business

Zeven bedrijven gaven aan producten online te verkopen. Wanneer e-business wat breder wordt getrokken, vallen er nog enkele bedrijven binnen deze groep. Dertien bedrijven verzamelen klantgegevens via hun site, slechts drie doen dat via een beveiligde verbinding.

Bijna de helft van de bedrijven onderhoudt de website online (via een CMS) maar men weet niet precies hoe de backup van die inhoud en het terugzetten daarvan is geregeld. Een heldere overeenkomst (SLA) met de toeleverancier, websitebouwer en/of websitehost, ontbreekt. 28% van de ondernemers zegt wel eens problemen met de eigen website te hebben gehad.

Een keurmerk voor websites (of websiteleveranciers) zagen vijf ondernemers wel zitten,

maar ze wilden er niet of nauwelijks voor betalen. Beveiliging van websites, backup van de inhoud of beveiliging van de koppeling met de interne automatisering is een onderwerp dat nog nauwelijks leeft. De scan zette veel ondernemers aan het denken, vooral zij die veel belang hebben bij de website.

Als rapportcijfer kreeg de onderzochte groep hiervoor een 7.

3.9 Personeel

De beveiliging van de computersystemen ten aanzien van het personeel is bijna in alle gevallen zwak. Personeelsleden hebben vaak veel meer rechten dan nodig is voor de uitvoering van de dagelijkse werkzaamheden. Veelal kunnen ze naar hartelust e-mailen, chatten, bestanden downloaden en programma's installeren. Een enkele keer is het downloaden en installeren op de netwerkserver afgeschermd, maar op de werkstations is doorgaans alles toegestaan.

Het ontbreekt in 70% van de bedrijven aan een gedegen wachtwoordenbeleid. Deze vorm van toegangbescherming is niet alleen nodig om niet alle eigen mensen overal bij te kunnen laten, maar ook om bezoekers en ongenode gasten van de gegevens te weren. Bij tweederde van de bedrijven voldoen de wachtwoorden niet aan een complexiteitseis, voor de periodieke –door het systeem afgedwongen- verplichte wijziging geldt hetzelfde. Overigens werden nog regelmatig de wachtwoorden aangetroffen op het bekende gele papiertjes aan de zijkant van het beeldscherm. Ruim de helft van de werknemers logt niet uit bij het verlaten van de werkplek en er blijft vaak belangrijke informatie op het bureau achter.

Ondernemers gaan zeer laconiek om met de beveiliging van het systeem richting personeel. Ook tegen het niet-zakelijk gebruik van internet en e-mail wordt nauwelijks opgetreden, ondanks het feit dat de ondernemers hiervan op de hoogte zijn. Dit wordt door hen zelden als een grote bedreiging gezien, dit geldt ook voor diefstal van informatie door eigen medewerkers.

Als rapportcijfer kreeg de onderzochte groep hiervoor een 6 min. De spreiding in de rapportcijfers per bedrijf is echter hoog, van een 3 (meerdere malen) tot een 9.

3.10 Organisatie en beleid

Slechts 14% van de bedrijven heeft procedures of reglementen op het gebied van informatiebeveiliging. Alleen de grote bedrijven doen hier aan, en die ondernemers die al eens schade hebben opgelopen. Informatiebeveiligingsbeleid is een witte raaf.

Bij het merendeel van de bedrijven is op dit terrein weinig tot niets geregeld. Een enkele keer is een notitie of reglement opgesteld met betrekking tot een bepaald onderwerp (bijvoorbeeld internet of e-mail gebruik), maar dit is eerder uitzondering dan regel. Bovendien waren de redenen om een dergelijke notitie op te stellen vaak afkomstig van wettelijke verplichtingen of een kwaliteitsnormering. (bijvoorbeeld ISO)

Gevraagd naar de reden voor het ontbreken van beleid en procedures op dit terrein kwamen veel ondernemers met het argument dat ze geen idee hadden hoe dit aan te pakken. Twaalf maal werd als reden genoemd het ontbreken van tijd, vier maal van geld en zestien maal van voorbeeldplannen of checklijsten.

Als rapportcijfer kreeg de onderzochte groep hiervoor een 5. Het gemiddelde is nog geflatteerd omdat een kleine groep bedrijven een 9 kreeg.

3.11 Schade

De meeste schade hebben de bedrijven ondervonden van stroomstoringen. Naast het niet door kunnen werken, betekende een grote stroomstoring in Flevoland voor een aantal bedrijven vervanging van apparatuur. De daaropvolgend meest genoemde oorzaak van schade is spam. Hierdoor gaat veel tijd verloren en bestaat de kans op het kwijtraken van wel belangrijke berichten. Een enkeling noemt schade door kabelbreuk, waardoor er geen verbinding was met internet.

Er incidentele schades met uiteenlopende oorzaken. Slechts één klein bedrijf meldde dat hackers de oorzaak waren van problemen met zijn server, van één bedrijf werd de website gegijzeld.

4 Uitkomsten per sector in grote lijnen

Het is erg moeilijk om verschillen aan te geven tussen de sectoren. Kijkend naar de cijfers zijn er marginale verschillen. De spreiding binnen een sector is groter dan de verschillen in de gemiddelden van de sectoren. De aantallen zijn op zich al veel te klein om goed onderbouwde uitspraken te doen. Tenslotte is de indeling van sommige bedrijven in een bepaalde sector arbitrair en is de invloed van één groot bedrijf op het gemiddelde cijfer in die groep groot. De verschillen tussen de uitkomsten op basis van bedrijfsgrootte zijn groter dan die tussen sectoren.

De onderzoekers hebben, gezamenlijk terugkijkend op alle scans, in ieder geval geen verschillen geconstateerd anders dan die paar die met de aard van het omgaan met ICT in die sector mag worden verwacht: bedrijven in de 'creatieve industrie', hier vooral ICT- en multimediabedrijven, hebben meer personeel dat terzake van het omgaan met computers ervaring heeft en zich dus meer bewust is van de risico's die daaraan kleven. Aan de andere kant wordt hier dan ook veel meer van het personeel geaccepteerd. In de sector logistiek&groothandel is de informatiebeveiliging via het personeel relatief het best geregeld.

Zaken rond de website zijn het best geregeld in de sector creatieve industrie, hetgeen ook mocht worden verwacht.

De internetkoppeling is het slechtst beveiligd bij de bedrijven in de food & agri sector.

De technische zaken waren over de hele linie bij de sectoren human health, bouw en food & agri iets minder goed geregeld dan bij de andere sectoren. De afhankelijkheid van ICT, internet en website is daar ook minder dan vooral in de sectoren creatieve industrie en logistiek & groothandel.

5 Bijzondere cases

De onderzoekers zijn soms op merkwaardige zaken gestuit bij hun bedrijfsbezoeken. Zo bleek het hebben van een ultrakleine server een geluk bij een ongeluk, toen die door dieven bij een inbraak over het hoofd was gezien en als enige onderdeel van het netwerk, inclusief de belangrijke bedrijfsgegevens (hoezo back-up?) achterbleef. Een ander bedrijf was diefstal van spullen zo zat, dat alle beeldschermen en computerkasten met staalkabels aan het meubilair waren bevestigd.

In vier gevallen werd geconstateerd dat er draadloze netwerken met een uiterst matige bescherming actief waren op plaatsen, waar veel publiek komt. Eén ondernemer was zich van het gevaar bewust en had juist hiervoor om een scan gevraagd. Een grote onderneming daarentegen rekende zich helemaal veilig vanwege de professionaliteit van de ICT-afdeling op de hoofdvestinging maar dat bleek een enorme vergissing. Een uitspraak van een ondernemer: "eh, waar heb ik ook al weer al mijn draadloze routers hangen?"

Een bedrijf uit de sector human health vroeg op zijn website bij zijn (aanstaande) klanten het hemd van het lijf qua medische gegevens maar was zich niet bewust dat die gegevens in andere handen zouden kunnen vallen. Achteraf bleek het eigenlijk ook helemaal niet zo nodig te zijn dit op de website te vragen, de oplossing was dus eenvoudig.

Eén ondernemer, werkzaam op het platteland, zag de gevaren niet zo: dat komt alleen voor in de stad, hier niet. Achteraf zag hij toch wel een verband tussen cybercrime en het voortdurend 'vastlopen' van de computers van de kinderen, aangesloten op zijn bedrijfsnetwerk. Het was in ieder geval een aanleiding om weer eens te beginnen met het maken van back-ups vaker dan eens per maand. Tsjja, en dan al die wachtwoorden...

Een andere ondernemer, die na een calamiteit alles had laten vervangen en voortaan het beheer volledig uitbesteedde bij een groot ICT-beheerbedrijf kwam er via de scan achter dat zijn firewall maar zeer matig was en bovendien verouderd met alle mogelijke gevolgen vandien. De ICT-beheerder, hierop door de onderzoeker aangesproken, reageerde zeer laks en het is nog steeds niet opgelost.

Bij sommige bedrijven troffen we uiterst professioneel ingerichte serverruimtes aan, waar kosten noch moeite waren gespaard: apparatuur in rekken, toegangsbeveiliging en –rapportage, noodstroomvoorziening, koeling, inbraak- en branddetectie, zelfs was soms nagedacht over de positionering binnen het pand. In een ander geval troffen we de servers letterlijk aan onder de trap in de hal.

6 Relatie deelnemers – ICT-toeleveranciers en invloed op informatiebeveiliging

In grote lijnen kunnen zich ten aanzien van het IT-beheer, belangrijk aanknopingspunt voor informatiebeveiliging, drie situaties voordoen:

- a. Het bedrijf heeft eigen beheerpersoneel
- b. Het bedrijf heeft zijn computers en netwerk ergens gekocht en schakelt de leverancier in bij problemen
- c. Het bedrijf heeft zijn ICT-beheer uitbesteed, hetzij aan de toeleverancier van de apparatuur, hetzij aan een gespecialiseerd bedrijf.

Bij het experiment zijn we vooral situatie c tegengekomen (zie hoofdstuk 3). Grotere bedrijven, vanaf 100 geautomatiseerde werkplekken, hebben eigen ICT-mensen. In de praktijk gaat het dan om zakelijke dienstverleners in het MKB (tot 250 werknemers) en grote bedrijven.

De meeste bedrijven blijken voor informatiebeveiliging te maken te hebben met twee verschillende, en soms drie of vier toeleveranciers:

- a. netwerkbeheer;
- b. websitebeheer / hosting;
- c. back-up van gegevens via internet;
- d. softwarebeheer (ERP en CRM toepassingen).

In een enkel geval is sprake van een combinatie, bijvoorbeeld wanneer (een deel van) het netwerk wordt geleased.

De toeleveranciers hebben hun eigen rol en invloed op informatiebeveiliging. De grootste rol is daarbij weggelegd voor de netwerkbeheerder, vaak ook de leverancier van het netwerk zelf met server, werkstations en de standaardsoftware. Een groot deel van de (on)veiligheid is al bepaald bij de installatie. Wanneer beheer zonder aandacht voor nodige aanpassingen in de informatiebeveiliging gedurende jaren doorgaat, stijgt het risico voor de ondernemer ongemerkt – terwijl hij er op vertrouwt dat zijn informatiesysteem in goede handen is. In veel gevallen is er ook geen zicht op wat nu precies onder dat beheer wordt verstaan. Er is geen heldere overeenkomst (service level agreement, SLA) en/of er wordt niet helder gerapporteerd over de verrichte werkzaamheden. Dat laatste verdwijnt bij beheer op afstand, via internet, ook snel uit de aandacht van de ondernemer – behalve weer even op het moment dat de rekening moet worden betaald.

Er zijn gelukkig ook beheerders, die proactief hun rapportages onder de aandacht van de ondernemer brengen. Het gaat dan vaak om rapportages die met een browser kunnen worden bekeken en via doorklikken in een e-mailbericht door de ondernemer worden bereikt. In het experiment zijn we meermalen tegengekomen dat dergelijke

ondernemers meer bewust zijn van het belang van goed ICT-beheer voor informatiebeveiliging, mogelijk omdat ze er vaker actief mee in aanraking komen.

Opmerkelijk was dat vrijwel geen ondernemer heldere afspraken kon laten zien die gemaakt waren met zijn websiteleverancier. Meestal zorgt de bouwer van de website voor het hosten en regelt ook dat de website 'in de lucht' blijft –althans daar rekenen de ondernemers op, ook zonder garanties op papier. Onderhouden van de inhoud doen de bedrijven zelf, voor back-up van de inhoud rekenen ze weer blindelings op hun toeleverancier.

We zijn hierover in het experiment overigens geen problemen tegen gekomen, op één 'gekaapte' website na wegens niet nagekomen verplichtingen van websitebouwer aan websitehoster. Het 'uit de lucht' zijn van websites wordt doorgaans 'vanzelf' opgelost binnen een halve dag nadat het wordt opgemerkt.

7 Beschouwing kwaliteit ICT-toeleveranciers en aanbevelingen daarbij

In het experiment hadden we vooral te maken met gebreken en risico's die te maken hadden met instellingen van de besturingssoftware van servers en van netwerkapparatuur zoals routers en firewalls. Dat zijn zaken waarvan de meeste MKB-ondernemers geen benul hebben en waarbij ze vertrouwen op de kwaliteit van het bedrijf waar de spullen gekocht zijn en/of die ze voor hen in conditie houdt. Dat vertrouwen blijkt in teveel gevallen misplaatst.

Gelukkig zijn er ook uitzonderingen, bedrijven die zich juist willen onderscheiden van de 'dozenschuivers' door toegevoegde waarde in de gebruiksfase van computers en netwerken. Missers van beheerders die we vaak tegenkwamen zijn:

- geen of standaard wachtwoorden voor beheerders op servers en netwerkapparatuur;
- niet aanbrengen van alle benodigde 'patches' in Windows besturingsystemen;
- verouderde firmware in netwerkapparatuur en verouderde 'firewalls';
- geen of niet goed functionerende automatische distributiefunctie van updates naar werkstations (zowel besturingssoftware als antimaware).

Daarnaast zijn er manco's waar weliswaar de ondernemer zelf verantwoordelijk voor is, maar waarbij de ICT-beheerder door meer aandacht de risico's kan beperken. Voorbeeld is pro-actief omgaan met backupverslagen, terugzetmogelijkheden (vooral vaardigheden!) van informatie, wachtwoordbeleid en rechten voor gebruikers.

Conclusie: aandacht voor informatiebeveiliging begint bij de ICT-toeleveranciers en zij kunnen die aandacht vasthouden door goede communicatie.

Aanbeveling: stimulering van professionalisering onder dit soort ICT-bedrijven. Aandacht voor het definiëren van een goede dienstverlening, gericht op continuïteit in de bedrijfsvoering van hun klanten en verzekering tegen schade. Kwaliteitsborging via toepassen van standaarden zoals ISO 17999 en ISO 20000. Toepassen van audits, zowel onder eigen personeel (kennisniveau, kwaliteit) als bij klanten. De scans van dit experiment kunnen daarbij als uitgangspunt dienen.

In het experiment hebben we niet kunnen kijken naar de daadwerkelijke situatie van de informatiebeveiliging van de websites. Aanbevolen wordt om hier als vervolg op dit experiment specifieke aandacht aan te besteden. Mogelijk leidt dit tot soortgelijke aanbevelingen als ten aanzien van netwerkbeheer. In ieder geval zal de communicatie op dit punt vanuit de websitebouwers naar hun klanten moeten worden verbeterd. Wij denken door het stellen van kritische vragen hierover tijdens de scans in ieder geval te hebben bereikt dat ondernemers het onderwerp aankaarten bij hun toeleveranciers.

8 Evaluatie aanbod tot reparatie van veiligheidslekken

Onderdeel van het experiment was het aanbod voor het laten repareren van gevonden 'lekken' door de eigen ICT (huis)leverancier, waarbij die kosten deels vergoed werden (alleen werk, geen spullen). Ondanks het feit dat het steeds ter sprake is gekomen bij de afsluitende evaluatie van de scan met de ondernemer aan het einde van het bezoek aan het bedrijf is er vrijwel geen gebruik gemaakt van die mogelijkheid. In een aantal gevallen is een onvolkomenheid direct tijdens de scan gerepareerd. Het gaat dan bijvoorbeeld om het aanbrengen van wachtwoorden of het veranderen van een te algemeen wachtwoord op de firewall of server.

Direct genoemde redenen om niet van het aanbod gebruik te maken zijn:

- a. ik ga mijn beheerder hierop wijzen, het hoort gewoon bij het beheercontract;
- b. ik ga mijn toeleverancier eerst eens vragen wat zijn reactie hier op is.

De kans is groot dat zonder actieve opvolging van het adviesrapport - dat per post is verstuurd - dus zonder nabellen of een herhalingsbezoek de actie van de ondernemer in veel gevallen uitblijft. De vervolgactie, confronteren van zijn toeleverancier met de gevonden gebreken, moet bij die toeleverancier leiden tot een al dan niet gratis actie. Wanneer het gaat om een operationele man (doorgaans is dat voor de ondernemer het eerste aanspreekpunt, bijvoorbeeld bij het eerstvolgende periodieke bezoek) bestaat de kans dat geadviseerde uitbreidingen zoals een betere firewall niet leiden tot een offerte. Tenslotte moet dit door de commerciële mensen van het betreffende ICT-bedrijf worden uitgebracht.

Conclusie: het nawerk na zo'n advies over veiligheid kost veel doorlooptijd en schakels en loopt de kans de aandacht te verliezen.

9 Gebruikte instrumenten

Direct na de start van het experiment bleken eerder ontwikkelde instrumenten, toegepast binnen het programma Nederland gaat Digitaal, te veel te zijn verouderd. In de afgelopen jaren zijn in korte tijd nieuwe besturingssystemen uitgebracht door Microsoft, de belangrijkste leverancier van software die we in dit experiment zijn tegengekomen. Veel ondernemers zijn die gaan gebruiken als logische onderdelen van de nieuwe apparatuur – het werd erbij meegeleverd bij vervanging of uitbreiding. Inmiddels heeft vrijwel elke onderneming een netwerk met één of meer servers en is voortdurend in verbinding met internet via ADSL.

9.1 Vragenlijst

Een groot deel van de scan bestaat uit het doornemen van een vragenlijst door een adviseur van Syntens met de ondernemer. De vragenlijst is gebaseerd op de Code voor Informatiebeveiliging, ISO 17999. Verder is er gebruik gemaakt van vragen en uitkomsten van het KWINT-onderzoek. De vragenlijst die bij de Code voor Informatiebeveiliging (2000) hoort, is zeer uitgebreid. In ruim 60 pagina's worden 10 categorieën bevraagd met 36 doelstellingen en 127 maatregelen. Veel onderdelen komen in sterk vereenvoudigde vorm terug in andere vragenlijsten.

Onderdelen die men niet in de andere vragenlijsten tegenkomt zijn configuratiemanagement (welke apparatuur, software, media en bestanden zijn er in het bedrijf en hoe kunnen die worden herkend), continuïteitsbeleid en uitvoering (onder andere stroomvoorziening, reserveapparatuur of uitwijk), operationeel beheer (systeembeheer, functioneel beheer, gegevensbeheer, incidentenbeheer en helpdesk) en informatiebeheer van de website. Het gaat hier weliswaar niet over cybercrime, maar wel over zaken die een MKB-bedrijf rechtstreeks en hard kunnen raken – en waarschijnlijk vaker zullen voorkomen dan een aanval door hackers. Het zijn wezenlijke onderdelen van informatiebeveiliging.

Voor de indeling in te onderzoeken categorieën is de indeling van de vernieuwde workshop 'computers en veiligheid' gebruikt:

1. apparatuur: fysieke beveiliging, single point of failure;
2. verbindingen: bescherming van de koppeling met internet, draadloze netwerken;
3. media: bescherming tegen verlies (met gegevens);
4. informatie: backup, corruptie van databases, diefstal van gegevens, externe gegevens (CMS, ASP);
5. mensen.

Toegevoegd is: 6. organisatie en beleid.

De vragenlijst is actueel gemaakt door expliciet te vragen naar bescherming tegen en schade door virussen, spyware en spam en de ervaring met draadloze netwerken. Spam is een fenomeen dat vooral sinds 2004 een grote rol speelt. E-mailrelayering is daarbij belangrijk, dat is onopgemerkt gebruik van de e-mailserver van een bedrijf door kwaadwilligen van buiten. Spyware kwam op in 2003 en lijkt inmiddels effectief onder controle.

Botnets hebben te maken met het overnemen van servers door slechte firewalls en onvoldoende 'gepatchte' besturingsystemen, dus met beheer en internetkoppelingen. Het gevolg is feitelijk diefstal van computercapaciteit. Er is niet specifiek naar gevraagd omdat de term niet erg bekend is onder MKB-ondernemers.

De overige onderwerpen spelen in feite al een rol sinds de introductie van automatisering maar MKB-ondernemers ondervinden deze nadelen pas sinds enkele jaren aan den lijve door het zeer snel toenemend belang en de afhankelijkheid van informatisering en e-business. Er is nog geen rekening gehouden met recent opkomende nieuwe vormen van cybercrime zoals het gijzelen van gegevens. Phishing is buiten beschouwing gelaten omdat het in een ander onderdeel van de cybercrime-aanpak wordt geïnventariseerd.

9.2 Rapportsjabloon

Doel was om het 'cybercrime adviesformat' precies de uiteindelijke vragenlijst ('cybercrimescan') te laten volgen. Vanwege de splitsing van de scan in een 'algemeen' en een technisch deel is uiteindelijk gekozen voor een hier op aangepaste vorm, waarbij de zes onderdelen in het algemene deel terugkomen en het technische deel op een aantal punten verbijzondering biedt. Dat deel is vooral bedoeld voor de communicatie tussen de ondernemer en de technisch beheerder.

Om benchmarking toe te kunnen passen is aan alle uitvoerders gevraagd om een beoordeling in cijfers te geven per onderdeel, rapportcijfers zoals op school. Voor het algemene deel wordt daarbij door de Syntens adviseur meegewogen het belang van informatiebeveiliging in de desbetreffende sector (een advocatenkantoor wordt dan zwaarder afgerekend als een bouwbedrijf). Elk rapport bevat uitleg over het project, de beoordeling in cijfers op een rijtje, de eindconclusie in woorden en dan per categorie de geconstateerde feiten en bijbehorende adviezen.

9.3 Externe technische hulp

Er is gebruik gemaakt van specialistische hulp van drie bedrijven. Die hebben steeds één specialist ingezet die rapporteerde in een format, dat kort na de start van het experiment in onderling overleg is vastgesteld. Er zijn door hen verschillende instrumenten gebruikt, maar de uitkomsten zijn goed vergelijkbaar. Wel zijn in de rapportages voorkeuren te herkennen voor bepaalde manco's en bepaalde oplossingen. Het was de taak van de Syntens adviseur om hierin enige censuur toe te passen, naast het 'ont-vaktermen'.

Omdat vooraf niet bekend is wat voor infrastructuur er wordt aangetroffen bij een bedrijf en wie het beheer uitvoert, is er een groot beroep gedaan op de flexibiliteit van de specialisten. Vanwege de beperkt beschikbare tijd moesten er soms prioriteiten worden gesteld. Er is steeds maar beperkt gekeken naar werkstations en laptops en daarvan maximaal één nader onderzocht. Elk bedrijf maakte al gebruik van virusscanners, dus waren systeemscans op virussen niet tijdefficiënt.

9.4 Workshopsjabloon

Uitgangspunt voor de workshops was een powerpointpresentatie, in het voorjaar van 2006 speciaal voor gebruik in de business unit Noordoost van Syntens opnieuw samengesteld door twee van de betrokken adviseurs op basis van actuele gegevens en de standaardworkshop uit het programma Nederland gaat Digitaal. Daarin wordt op basis van de vergelijking tussen de aandacht voor fysieke veiligheid (inbraak, brand) versus informatiebeveiliging in vijf categorieën bewustwording gecreëerd. Het gaat in deze workshop 'computers en veiligheid' om:

1. apparatuur: fysieke beveiliging, voorkomen van een single point of failure;
2. verbindingen: bescherming van de koppeling met internet, draadlozenetwerken;
3. media: bescherming tegen verlies (gegevensdragers met gevoelige gegevens);
4. informatie: backup, corruptie van databases, diefstal van gegevens, externe gegevens (CMS, ASP: software op afstand);
5. mensen.

Het sjabloon bleek goed toepasbaar voor de verschillende doelgroepen als bewustwordingsinstrument of 'aanknopingspunt' (herkenning, besprekingspunt). Per doelgroep werden onderdelen ingekort (tot alleen de samenvatting) of vervangen door demonstraties met de proefopstelling. Voor ondernemers die zelf te maken hebben gehad met één bepaald aspect van informatiebeveiliging is de huidige inhoud minder geschikt. Zij willen vooral oplossingen horen.

9.5 Demonstrator

De proefopstelling is tot nu toe alleen ingezet bij groepen (twee workshops voor ondernemers en uitleg aan de klankbordgroep). De plaatsing in de E-room op een vestiging van Syntens geeft hiervoor een goede mogelijkheid. Voor de beide groepen ondernemers waren de demonstraties verhelderend. Voor het aansluiten van de demonstrator op het internet is een aparte ADSL-aansluiting nodig. Binnen de huidige demonstraties is dit niet strikt noodzakelijk, maar wel voor het aantonen van echte aanvallen van buitenaf.

Er wordt momenteel gewerkt aan verbeteringen naar aanleiding van de eerste ervaringen. Een goede documentatie moet er voor gaan zorgen dat een Syntens adviseur in een één-op-één situatie met een ondernemer en/of zijn eigen ICT-mensen de demonstrator kan gebruiken voor eerstelijns advies. Onderzocht moet worden hoe de demonstrator ook een rol kan spelen in de communicatie tussen ICT-leverancier en MKB-ondernemer. Als onderdeel van het experiment is nog ruimte voor enkele aanpassingen en voor meer workshops met de demonstrator. De eerste uitbreiding zal het kraken van interactieve websites betreffen.

Of het gebruik van de demonstrator het beoogde effect heeft op alle ondernemers, valt te betwijfelen. Bij ondernemers leven na de scan veel eerder vragen als: hoe ver moet ik gaan met beveiligen, welk risico en welke schade loop ik nou daadwerkelijk (op)? Een aantal huidige demo's, zoals kraken van een draadloos netwerk en het overnemen van de server door een hacker zijn effectief, maar slechts gedeeltelijk live. Andere demo's hebben ook effect onafhankelijk van de fysieke aanwezigheid van apparatuur.

10 Bewustwordingsacties tot dusver

In de afgelopen jaren is informatiebeveiliging in de voorlichting naar het MKB onderdeel geweest van het programma Nederland gaat Digitaal, KWINT, Surfopsafe en nu dan Digibewust. Het ging steeds om onderdelen van informatiebeveiliging, vooral gericht op internet. Aspecten die te maken hebben met bedrijfsschade door uitval van informatiesystemen – steeds belangrijker voor bedrijven – en imagoschade door gekraakte websites en handelingen van werknemers zijn tot dusver niet of nauwelijks aan de orde geweest. Keurmerken voor websites hebben meer betrekking op de betrouwbaarheid van de eigenaar en het fulfillmentproces, dus de veiligheid van het geld van de klant. Er wordt nauwelijks ingespeeld op nieuwe onderwerpen, zoals telewerken door MKB-ondernemers.

Uit internationaal onderzoek (bron: ENISA) blijkt dat ondernemers in toenemende mate zowel op het werk als thuis online zijn: 36% tussen 5-14 uur thuis, 30% idem op het werk. Informatie wordt gezien als van levensbelang voor de onderneming maar slechts 33% van de ondernemingen in het VK hebben een informatiebeveiligingsbeleid en slechts 12% wijst hun medewerkers op hun verantwoordelijkheid qua informatiebeveiliging. Menselijke fouten zijn veel eerder dan technologie de oorsprong van veiligheidsproblemen. De uitdaging voor veel ondernemers is dus om een cultuur met veiligheidsbewustzijn te scheppen.

Ondanks allerlei acties wordt informatiebeveiligingsbeleid niet gezien als iets dat hoort bij het algemeen management, dat zorgt voor risicomangement en veiligheidszaken voor de onderneming, maar als een extra kostenpost en hinderlijk.

In dit experiment kunnen we die conclusies alleen gedeeltelijk onderschrijven. Telewerken komt heel veel voor, vooral door de ondernemer zelf en de commerciële buitendienst. Doorgaans zijn er technische maatregelen voor genomen – door toeleveranciers, en niet altijd afdoende. Het bewustzijn van een aantal gevaren is heel behoorlijk. Maar de schade vanwege virussen dateert al van enkele jaren geleden dus bijna vergeten – er zijn inmiddels virusscanners aangeschaft, die worden ‘voortdurend’ actueel gehouden, dus wat moet een ondernemer nog meer?

Spyware bleek nergens een onderwerp van belang, ‘omdat er door medewerkers alleen zakelijk gebruik wordt gemaakt van internet’. Spam is wel in toenemende mate irritant, maar slechts enkele ondernemers brengen het met bedrijfsschade in verband. Wel bleken door diverse publicaties ondernemers te willen weten hoe het nu precies zit met de veiligheid van draadloze netwerken. Die zijn in korte tijd razend populair geworden, ook bij MKB-ondernemers. En wordt er gegniffeld bij confrontatie met gebruik van USB-sticks, vanwege de schandalen in de pers rond kwijtraken door

ambtenaren. De link met het invoeren van procedures op basis van een informatiebeveiligingsbeleid wordt echter niet spontaan gelegd. De cijfers voor deze onderdelen, in de categorie 'organisatie' in de rapporten zijn dan ook erg laag. De vraag is nog maar of de ondernemers, die nu op dit punt getriggerd zijn, ook daadwerkelijk actie ondernemen.

Het ENISA rapport 'raising awareness in information security' (november 2005) vergelijkt de uitkomsten van bewustwordingscampagnes in de verschillende deelstaten, waaronder Nederland (o.a. KWINT) en doet negen aanbevelingen. Papier blijkt nog steeds een goede boodschapdrager naast websites. Bijeenkomsten met brancheorganisaties en ondernemersnetwerken zijn effectief in het bereiken van de ondernemers/eigenaren.

Belangrijk is dat ondernemers zelf in hun bedrijf worden gezien als voorbeeld op dit gebied en zelf het voortouw moeten nemen in de ogen van hun medewerkers. Bij alle campagnes moet voortdurend vinger aan de pols worden gehouden en worden bijgestuurd op basis van bevindingen en resultaten, zoals het daadwerkelijk opvragen door ondernemers van publicaties, checklijstjes etc.

Een gezamenlijke MKB aanpak van diverse overheidsinstellingen kan het vertrouwen bij ondernemers vergroten. Een aantal kernboodschappen kan worden verpakt in een campagne om ondernemingen zo ver te krijgen dat ze gaan voor een complete bemanning met mensen die niet alleen de veiligheidsrisico's zien maar daar ook professioneel mee om gaan zoals in hun vak en hun branche hoort. De boodschap moet altijd positief zijn en niet afschrikken. Campagnes en communicatiekanalen moeten zoveel mogelijk afgestemd zijn op het soort MKB-bedrijf en liever niet het MKB in het geheel. Ook afstemming op de grootte van het bedrijf is gewenst, waarbij de boodschap voor heel kleine bedrijven uiterst eenvoudig moet blijven. Voor hen is een lijstje met tien 'gouden regels' voldoende.

De ervaringen in dit experiment sluiten aan bij de bevindingen en aanbevelingen van dit rapport. Met dien verstande dat materialen uit bestaande campagnes, zoals flyers en websites, nauwelijks bekend zijn bij de deelnemers. Alleen de Waarschuwingsdienst is enkele malen spontaan genoemd en werd zeer gewaardeerd. Wel wordt regelmatig de behoefte genoemd aan checklijstjes en dergelijke instrumenten op papier. Omdat al snel bleek dat vooral het onderwerp 'informatiebeveiligingsbeleid' veel aandacht kan gebruiken is bij een laag rapportcijfer op dit gebied in combinatie met een wel bestaande interesse als bijlage bij het adviesrapport aan zo'n ondernemer een afdruk bijgevoegd van de checklists (beleid en plan) die op de website Digibewust.nl staan. Het is een goed voorbeeld van wat ondernemers willen, probleem is alleen om het hen op het juiste moment aan te reiken.

Aansluiten bij brancheverenigingen en regionale ondernemersnetwerken zijn twee verschillende zaken. Binnen Nederland gaat Digitaal zijn er positieve ervaringen in het bereiken van het MKB met workshops in nauwe samenwerking met brancheverenigingen. Dat gaat alleen op bij onderwerpen, die specifiek in die branche spelen op dat moment.

Samenwerken met ondernemersnetwerken in de regio, dus aanhaken in het sociale netwerk, zou in dit experiment mogen worden verwacht vanwege de initiatiefnemers om de pilot in Flevoland uit te voeren. In de praktijk is van die synergie niets terecht gekomen. Wel gewerkt heeft het triggeren van de Digikring (ICT/multimedia ondernemers), maar hier liggen de belangen direct dicht bij de eigen business.

Afstemming op de grootte van het bedrijf wordt door ons als zeer effectief gezien. Daarbij gaat het niet om de grootte in aantal werknemers maar aantal werkplekken met computers, en het aantal mensen dat zich grotendeels met ICT bezighoudt (functioneel en technisch beheer). In veel bedrijven van de middencategorie is er meestal wel één persoon, vaak hoofd van of belast met de administratie, die de verantwoordelijkheid heeft voor de automatisering en die gevoelig is voor onderwerpen binnen informatiebeveiliging. Door die personen bij elkaar te zetten, te informeren en onderling van elkaars ervaringen te laten leren kan 'interest' snel veranderen in 'desire' en 'action' (vergelijk: AIDA-model).

Bewustwording kan daarnaast plaatsvinden door die ICT-bedrijven, die professioneel beheer inclusief informatiebeveiliging als een factor zien waarmee ze zich van de concurrenten kunnen onderscheiden. Aan hen verstrekt informatiemateriaal kan dienen als wervingsmateriaal voor hun (extra) diensten. Eigenlijk zou de 'branche' dit zelf moeten oppakken, maar de bestaande brancheverenigingen lijken weinig leden te hebben onder deze doorgaans kleine bedrijven (één tot twintig mensen) en de beroepsverenigingen, zoals het Genootschap voor Informatie Beveiligers, kent vooral de specialisten als leden.

11 Conclusies

Informatiebeveiliging gaat over continuïteit van informatiesystemen. Een systeem is een combinatie van middelen, mensen en procedures.

Met de kwaliteit en beheersmatigheid van middelen gaat het steeds beter, ook in het MKB. De mensen vormen nu vaak de zwakste schakel. Procedures, die hierin zouden kunnen en moeten ondersteunen, ontbreken in het MKB vrijwel geheel.

11.1 Hoge afhankelijkheid, géén maatregelen

Bedrijven geven unaniem aan erg afhankelijk te zijn van ICT én van internet. Onderzoekers waren zelf ook onder de indruk van deze grote mate van afhankelijkheid. Maar de ondernemers blijven steken bij deze constatering en doen er nauwelijks iets mee.

Weinigen realiseren zich bijvoorbeeld dat het ADSL-aansluitkastje kapot kan gaan en niet direct vervangbaar is. Herstel is afhankelijk van type en leverancier en duurt enkele uren tot meerdere dagen. Slechts een enkeling heeft belangrijke apparatuur op reserve of een goede afspraak gemaakt met zijn leverancier.

11.2 Informatiebeveiliging is geen technologie

Cybercrime vinden velen iets hoogtechnologisch. Dat beveiliging juist veel met organisatie en met gezond verstand te maken heeft, was voor de meeste deelnemers nieuws.

Deelnemers hadden gerekend op louter diepgaand technisch onderzoek en waren verrast als de onderzoekers bij voorbeeld wezen op de gevaren van een slecht wachtwoordbeleid.

11.3 Mensen zijn de zwakste schakel

Bij het merendeel van de bedrijven hebben medewerkers onbeperkte rechten voor internetgebruik, zelfs voor het downloaden en installeren van software. Het gebruik van wachtwoorden vond men soms helemaal niet nodig en vaak werd er met wachtwoorden slordig omgesprongen.

Medewerkers blijken zich niet bewust van de –onzichtbare– gevaren die dergelijke praktijken met zich meebrengen. Ondernemers reageren laks; *wij kennen onze medewerkers en die doen niets onbehoorlijks.*

11.4 Ondernemers schuiven af

De deelnemende ondernemers hebben zich nauwelijks zélf verdiept in beveiliging. Oplossing die veelal gekozen wordt is om de beveiliging volledig af te schuiven aan óf een externe expert, óf aan een interne deskundige. Het woord delegeren is hier niet op z'n plaats, omdat hier nauwelijks sprake is van controle.

Wat hier waarschijnlijk een rol speelt is de overtuiging dat je veel verstand van ICT moet hebben om hier iets mee te kunnen doen.

11.5 ICT-dienstverleners dienen kritisch te kijken naar hun eigen kwaliteit (zelfreflectie)

De meeste ondernemers vertrouwen blind op hun externe beheerder. In het onderzoek blijkt dit vertrouwen in diverse gevallen onterecht.

In het meest schrijnende geval van wanbeheer in deze pilot werden wij door de ondernemster juist uitgenodigd voor een scan vanuit het idee dat zij een positief voorbeeld van informatiebeveiliging zou zijn.

12 Aanbevelingen voor instrumentontwikkeling

Instrumenten moeten niet alleen aangeven dat een ondernemer aan informatiebeveiliging moet doen of wat hij moet doen, maar vooral hoe hij het moet doen en controleren - en hem bij dit laatste praktisch ondersteunen.

12.1 Boekje over informatiebeveiliging

Eén van de bestaande instrumenten is het boekje 'met een veilig gevoel, informatiebeveiliging in de praktijk'. Het is drie jaar geleden uitgegeven door Syntens binnen het programma Nederland gaat Digitaal in samenwerking met het Genootschap van Informatie Beveiligers. Het is nog steeds bruikbaar, al is de aandacht enigszins verschoven naar nieuwere bedreigingen en zijn de vermelde webadressen niet allemaal meer up-to-date.

Aanbevolen wordt de inhoud te actualiseren en onder de vlag van Digibewust opnieuw uit te brengen. Verspreiding moet dan gecontroleerd (gemeten) plaatsvinden via de website, bij workshops (niet bij grootschalige bijeenkomsten, daar krijgt het geen aandacht) en vooral ter ondersteuning van eerstelijns adviezen door Syntens en anderen. Distributie via ICT-bedrijven kan ook worden overwogen, mits het ook hier 'gecontroleerd' kan gebeuren.

12.2 Voorbeelden

In het experiment werd regelmatig gevraagd naar voorbeelden (liefst sjablonen) voor afspraken met en regels voor werknemers over gebruik van internet en e-mail. Van één (groot) bedrijf kregen we een bestaand document mee en inmiddels hebben we ontdekt dat op de website van VNO-NCW een voorbeeld staat. Aanbevolen wordt op basis van de 'best practices' voor verschillende categorieën bedrijven reglementen te maken en die op alle mogelijke manieren te verspreiden. De brancheverenigingen kunnen hier een belangrijke rol bij spelen.

Andere aanbevolen sjablonen of checklijsten (de opsomming is niet uitputtend):

- Hoe ziet goede documentatie van het netwerk er uit, waar moet ik op letten in de documentatie en rapportage wanneer ik het beheer heb uitbesteed?
- Wat moet er in een overeenkomst staan bij uitbesteding van netwerkbeheer, wat is belangrijk en wat zou ik kunnen schrappen?
- Idem in het contract (SLA) met een websiteleverancier.
- Wat te doen en te regelen bij de komst van een nieuwe medewerker, en wanneer een medewerker weggaat?

- Hoe kan ik zien of mijn back-up is geslaagd, wanneer kan ik echt op mijn back-upgegevens vertrouwen?
- Welke virusscanners (antimalwarescanners) zijn goed voor gebruik in het MKB, waarop moet ik letten bij installatie en bij gebruik?
- Hoe weet ik of ik een goede firewall heb en of die nog goed werkt, wat zou ik anders moeten kopen?
- Hoe kan ik mijn e-mailomgeving zo inrichten dat ik zo weinig mogelijk spam heb?
- Hoe blokkeer ik toegang tot bepaalde (soorten) internetsites?
- Wat moet ik zelf onderhouden of controleren aan mijn draadloze netwerk, hoe weet ik of ik echt veilig draadloos werk?

12.3 Workshops

Workshops kunnen niet alleen bijdragen aan bewustwording maar ook aan de praktische inbedding van informatiebeveiliging in de bedrijven. Denk ook aan het onderling delen van kennis, tips en ervaringen door mensen die zich binnen MKB-ondernemingen voor een belangrijk deel van hun tijd bezig houden met automatisering. Hetzelfde geldt voor workshops als bijdrage aan professionalisering, vooral kwaliteitsbesef, van bedrijven die technisch beheer leveren aan MKB-ers. Belangrijk is dat informatiebeveiliging een doorlopend onderwerp wordt bij bedrijven, geen éénmalige actie. Workshops waarin 'best practices' en nieuwe ontwikkelingen worden gedeeld en waarin continue verbetering en aanpassing centraal staan kunnen dit bevorderen.

12.4 Audits en keurmerk

Vertrouwen is goed, controle is beter. Het experiment heeft aangetoond dat een MKB-er niet zonder meer op zijn ICT-leveranciers kan vertrouwen. Een hulpmiddel kan een jaarlijkse audit zijn, het liefst professioneel uitgevoerd. Vanwege de kosten die daarmee gepaard gaan is het de moeite waard een audittool te ontwerpen die de bij de MKB-onderneming voor informatiebeleid verantwoordelijke medewerker kan gebruiken om samen met de kwaliteitsman van zijn eigen ICT-beheerder een aantal met name te noemen zaken kan controleren. Vergelijk het met de in het experiment uitgevoerde scan, waarbij de ondernemer in plaats van de Syntens adviseur en een andere specialist dan de reguliere beheerder maar wel van de eigen toeleverancier de check uitvoeren. Een gedurfde variant op dit thema is dat het desbetreffende ICT-bedrijf een werknemer van zijn collega / concurrent de audit laat uitvoeren.

Aanbevolen wordt om tot een kwaliteitskeurmerk van informatiebeveiliging te komen voor ICT-bedrijven op dit gebied, afgestemd op toepassing binnen MKB-bedrijven. Zonder meer toepassen van de ISO-standaarden op dit gebied wordt voor MKB-bedrijven veel te duur waardoor het gevolg zal zijn dat ze 'niets' doen. Het kwaliteitskeurmerk moet een MKB-ondernemer het vertrouwen geven dat het desbetreffende bedrijf alle maatregelen zal nemen en blijven bewaken die noodzakelijk en voldoende zijn voor zijn eigen bedrijf binnen de actuele risico's rond computers en internet die voor hem relevant zijn. Vergelijk het met bedrijven die een APK-keuring mogen uitvoeren. Het vertrouwen moet gerechtvaardigd zijn en blijven via professionele audits door onafhankelijke instanties.

13 Aanbevelingen voor landelijke voortzetting

13.1 Eerstelijns ondersteuning

De ervaringen van de adviseurs in dit experiment leren dat ondernemers die met de neus op de feiten worden gedrukt bereid zijn tijd en geld te investeren in informatiebeveiliging. Aanbevolen wordt ondernemers te stimuleren informatiebeveiligingsbeleid en uitvoering daarvan daadwerkelijk aan te pakken, met behulp van een reeks praktische instrumenten voor henzelf en met behulp van hun eigen ICT-beheerder (intern of extern). Bij de keuze van een nieuwe toeleverancier of in geval van twijfel over de huidige toeleverancier kan een onafhankelijk adviseur via één of twee gesprekken in het bedrijf ondersteuning bieden. De Syntens adviseur die al contact heeft met het bedrijf is hiervoor de aangewezen persoon.

Voor ondernemers die al verder zijn wordt aanbevolen jaarlijkse workshops bij te wonen volgens het 'leren van elkaar' model zoals Syntens al jaren met succes toepast.

13.2 Verbreding naar heel Nederland

De doelgroep binnen dit experiment waren uitsluitend Flevolandse ondernemers. Het aantal bedrijven in de maakindustrie, voedingsmiddelenindustrie en uitvoerende bouw was mede hierdoor relatief laag. Herhaling van dit experiment met deelnemers over heel Nederland kan beter inzicht geven over verschillen per sector.

13.3 Specifieke aanpak e-business

Een aspect dat in het experiment naar voren kwam, maar onvoldoende scherp kon worden beoordeeld is de externe veiligheid bij e-business, in handen van bouwers van websites en webapplicaties en webhosts. Hoe wordt het hele proces van kopen tot uitleveren gewaarborgd en wat is daarbij de rol van techniek en van mensen? Wie is verantwoordelijk en hoe kan men op die verantwoordelijkheid worden aangesproken? Aanbevolen wordt een aantal (minimaal 50) specifieke e-business bedrijven te onderzoeken inclusief hun toeleveranciers. Een goede verdeling in business-to-consumer webwinkels en business-to-business is daarbij gewenst. Vanwege de grotere rol van wetgeving hierbij (Wet Kopen op Afstand c.q. Europese richtlijn, Handelsregisterwet en Wet Bescherming Persoonsgegevens) is samenwerking met het Ministerie van Justitie aanbevolen.

13.4 Inschakelen ICT-branche

De instrumenten zoals gebruikt in het experiment bleken geschikt maar kunnen met weinig moeite op basis van de ervaringen worden verbeterd. Het gebruik van specialisten zoals in dit experiment gebruikt is duur, maar de kosten kunnen worden verlegd naar de (beoogde) toeleverancier van ICT-beheer. Er zijn al bedrijven die zo'n 'security scan' als acquisitie-instrument gebruiken. Anderen kunnen worden geholpen zich met professioneel ICT-beheer inclusief informatiebeveiliging te onderscheiden van hun concurrenten. De adviseurs van Syntens zijn hiervoor bij uitstek geschikt, de activiteiten passen in de werkwijze van het maken van innovatieactieplannen voor MKB-bedrijven.

Aanbevolen wordt om samen met de ICT-branche te komen tot een vorm van kwaliteitszorg en certificering.

Bijlage 1: vragenlijst cybercrimescan

Syntens quickscan informatiebeveiliging

0. Algemeen

Bedrijf:

Plaats:

Website:

Gesproken met:

Datum:

Adviseur:

Hoeveel medewerkers telt uw bedrijf:
en hoeveel daarvan werken met informatiesystemen:

In welke sector is uw bedrijf actief (graag een bredere specificatie van antwoorden):

Hoeveel heeft uw bedrijf het afgelopen jaar in totaal uitgegeven aan ICT:
(computers, software, opleiding, systeembeheer)

Hoeveel daarvan was voor beveiliging (software, hardware, opleidingen,
beveiligingsplan):

Hoe afhankelijk is uw bedrijf van ICT voor de interne bedrijfsvoering?
(nauwelijks – matig – behoorlijk – heel erg)

Hoe afhankelijk is uw bedrijf van ICT voor het maken van uw product of dienst?
(nauwelijks – matig – behoorlijk – heel erg)

Hoe afhankelijk is uw bedrijf van de verbinding met het internet?
(nauwelijks – matig – behoorlijk – heel erg)

Hoe afhankelijk is uw bedrijf van het functioneren van de website?
(nauwelijks – matig – behoorlijk – heel erg)

1. Apparatuur, fysieke beveiliging en beheer

Heeft uw organisatie een netwerk waarmee computers aan elkaar zijn verbonden?

Hoeveel computers worden er binnen uw bedrijf gebruikt?

(uitsplitsen naar servers en werkstations, laptops, PDA's en speciale computers)

(totaal werkstations plus laptops categoriseren: minder dan 10 - 10-25 - 25-50 - 50 en meer)

Waarvoor worden deze computers gebruikt:

Marketing – verkoop – inkoop – voorraadbeheer - werkvoorbereiding – productie /

dienstverlening – boekhouding / administratie - management

(bedrijfsprocessen noemen met aantallen)

Heeft uw bedrijf het afgelopen jaar een ernstige storing in het netwerk meegemaakt?

Zo ja, hoe vaak?

Wat was de langste periode van storing?

Wat was de oorzaak van deze storing?

Wat was de geschatte schade veroorzaakt door de storing?

Hoe heeft u dat probleem opgelost ?

Welke fysieke beveiligingsmaatregelen heeft u genomen ter bescherming van apparatuur

(bv afsluitbare serverruimte, toegangsverificatie, brandpreventie, inbraakpreventie)?

Hoe wordt het netwerk beheerd en door wie?

Waar zijn de werkzaamheden beschreven?

Hoe wordt er over gerapporteerd?

Welke maatregelen zijn er genomen tegen stroomstoring (bijv. UPS voor de server)?

Welke maatregelen heeft u genomen tegen uitval van een / de harde schijf?

Wat gebeurt er wanneer een bijzonder apparaat, zoals de verbinding met internet of een ander netwerkapparaat defect raakt?

2. Verbindingen / internetkoppeling

Heeft u een aansluiting op internet?

Hoe zou uw koppeling met het internet het best kunnen worden omschreven?

- één enkele computer heeft een internet verbinding;
- alle computers hebben een internet verbinding.

De internetverbinding is:

- vast, via huurlijn of ADSL;
- gekozen, dwz via een modem wordt steeds verbinding gemaakt.

Hoe goed bent u bekend met de gevaren die een internetkoppeling met zich mee brengt?

Zijn de computers / het netwerk beveiligd met een firewall?

Wat voor soort firewall is dat? (hardware, software, combinatie, complex)

Hoe wordt die onderhouden?

Wat zijn de ervaringen?

Zijn de computers beveiligd met anti-virus-software?

- elke werkplek afzonderlijk;
- alleen op de server;
- bij de provider;

Welke software is het precies?

Worden er steeds nieuwe versies gebruikt?

Hoe wordt het bestand met virusdefinities ververst?

Wordt in uw bedrijf alle inkomende e-mail gecontroleerd op virussen?

Wat zijn de ervaringen?

Zijn de computers beveiligd met anti-spyware software?

- met specifieke software (welke?);
- als onderdeel van antivirussoftware;

Worden nieuwe versies gebruikt?

Hoe vaak wordt er gescand?

Wat zijn de ervaringen?

Welke medewerkers mogen software downloaden en installeren?

Om wat voor software gaat het dan?

Koopt uw bedrijf online producten in?

Zo ja: hoe worden die dan betaald?

Inrichten van de e-mailcommunicatie:

Hoe wordt e-mail bij de provider opgehaald en weggebracht:

- rechtstreeks vanuit een PC,
- of via een server met speciale server (mailserver)?

In dat laatste geval: met welke software?

Op een aparte server?

Welk besturingssysteem heeft die?

Is die server beschermd tegen ongewenst doorsturen van post 'van buiten'?

Verstuurt u elektronische nieuwsbrieven?

Zo ja:

- per e-mail of;
- via de website / een webapplicatie?

Hoe is het inschrijven en uitschrijven van geadresseerden geregeld?

Welke informatie verzamelt u over abonnees, en wat doet u er verder mee?

Verstuurt u ongevraagde e-mail naar (potentiële) klanten?

Zo ja:

- bij welke gelegenheden;
- hoe vaak komt dat voor;
- hoe komt u aan de adressen;
- krijgt u wel eens negatieve reacties daarop?

Telewerken:

- hoe veel medewerkers;
- hoe intensief;
- welke functionarissen / wat voor bedrijfsprocessen;
- hoe is de verbinding beschermd;
- hoe veilig is de thuissituatie;
 - o eigen PC of;
 - o laptop van de zaak;
 - o als eigen PC: welke bescherming (virussen, spyware).

Draadloze netwerken:

- waarvoor gebruikt;
- hoe beschermd;
- ooit gecontroleerd;
- wel eens een incident gehad?

Software op afstand:

Wordt voor de website een CMS gebruikt?

Als u gebruik maakt van ASP:

- voor welke bedrijfsprocessen,
- bij welke provider

Als er sprake is van beheer op afstand: wie doet dat (netwerkbeheer, softwareleverancier)

3. Website

Verkoopt uw bedrijf producten online?

Kunnen uw klanten online aan u betalen?

Zo ja, op welke wijze:

- creditcard;
- iDeal;
- anders.

Verloopt de betaling via een beveiligde verbinding (SSL of anders)?

Verzamelt u gegevens van uw klanten via de website?

Zo ja:

- waar komen die dan terecht;
- hoe komen ze in uw bedrijf binnen?

Verloopt de verstrekking van deze gegevens via een beveiligde verbinding?

Hoe is geregeld dat anderen dan de klant zelf of uw medewerkers klantgegevens kunnen inzien?

Wie kunnen de prijzen van door u aangeboden producten en diensten veranderen?

Hoe dekt u dat af?

Hoe zorgt u ervoor dat de website altijd en correct 'in de lucht' is?

Zijn er wel eens problemen mee geweest?

Zo ja:

- welke?
- hoe zijn die opgelost?

Alleen wanneer het belang van e-business hoog is:
(bijvoorbeeld bij grotere groothandels en detaillisten)
Zou u een certificaat willen hebben als bewijs van een veilige website?
Hoeveel zou u over hebben voor het verkrijgen van zo'n certificaat?

4. Media en informatie

Backups

Gegevens op computers kunnen verloren gaan door bijvoorbeeld defecten, brand of door diefstal van computers. Hoe groot zijn de gevolgen voor uw bedrijfsvoering wanneer gegevens verloren zouden gaan:

- groot;
- gemiddeld;
- beperkt.

Maakt uw bedrijf back-ups van de belangrijkste informatie in de computersystemen?

- ja, van alle systemen;
- ja, maar gedeeltelijk;
- eigenlijk niet.

Indien uw bedrijf back-ups maakt, wordt er dan voor gezorgd dat deze veilig worden opgeborgen?

- ja, in een afgesloten kast;
- ja, in een brandveilige kluis;
- ja, op een externe locatie;
- eigenlijk niet.

Hoe vaak worden er back-ups gemaakt?

Op welk medium?

Wordt het logboek gecontroleerd?

Wordt de herstelprocedure wel eens uitgevoerd?

Worden de media wel eens vervangen?

Worden databases wel eens gecontroleerd op consistentie / corruptie?

Informatiebeheer

Als u een website heeft:

- wie beheert de informatie;
- wie brengt wijzigingen aan,

- hoe wordt de informatie bewaard? (backup)

Als er gebruik wordt gemaakt van software op afstand:

- wie beheert de informatie;
- wie brengt wijzigingen aan;
- hoe wordt de informatie bewaard (backup)?

Wordt er in uw bedrijf gewerkt met verwisselbare media voor opslag van gegevens, zoals:

- beschrijfbare CD's;
- USB-sticks.

Wordt er encryptie toegepast?

Zo ja, waarvoor:

- e-mail;
- harde schijf op laptop;
- USB-sticks;
- anders.

Welke informatie wordt via internet of CD's op verzoek aan derden verstrekt en hoe wordt dat vastgelegd en gecontroleerd? Wie zorgt ervoor dat iedereen dit weet en zich er aan houdt?

5. Mens / personeel

Wat mogen medewerkers doen op internet qua surfen, e-mailen, downloaden en chatten? Hoe dwingt u dat af? Wat staat er van op papier? (checken / meenemen)

In hoeverre is informatiebeveiliging een onderwerp bij werving en functioneren?

Hoe heeft u geregeld dat niet iedere medewerker alles kan binnen uw informatiesysteem?

Blijft er wel eens belangrijke informatie op een verlaten bureau liggen?

Wordt er uitgelogd bij het verlaten van de werkplek?

Hoe gaat men in het bedrijf om met wachtwoorden?
(zoals regelmatig veranderen en niet onderling delen)

6. Organisatie / beveiligingsbeleid

Is er beleid op het gebied van informatiebeveiliging?

Waar ligt dat vast?

Hoe is het bekendgemaakt / verspreid?

(check, kopie meenemen, datum en geldigheid vaststellen)

Wie is er verantwoordelijk voor de uitvoering van dat beleid?

Hoe wordt dat uitgevoerd?

Wanneer is er voor het laatst naar gekeken of iets aan gewijzigd?

Welke medewerkers 'doen' iets op het gebied van informatiebeveiliging?

Aan wie worden verdachte situaties gemeld, zoals mogelijke virussen of vermissing van bestanden?

Heeft u procedures opgesteld om (onderdelen van) informatiebeveiliging te structureren?

Zo nee: wat weerhoudt u hiervan (meerdere antwoorden mogelijk):

- niet nodig;
- geen tijd voor beschikbaar;
- geen geld voor beschikbaar;
- geen kennis over hoe dit aan te pakken;
- geen hulpmiddelen beschikbaar (checklists, actielijstjes, voorbeeldplannen e.d.);
- niet bewust van de noodzaak;
- niet van toepassing: wij hebben alles goed geregeld;
- anders, namelijk ...

Indien u procedures in gebruik heeft voor informatiebeveiliging, welke zijn dit:

- Werkinstructies voor betrokkenen.
- Procedurebeschrijvingen bevatten:
 - o onderdelen voor informatiebeveiliging;
 - o actieplan om informatiebeveiliging te verbeteren;
 - o beschrijving van verantwoordelijkheden;
 - o documenten over technische configuraties van IT componenten;
 - o Anders, namelijk ...

Hoe passen die procedures in uw kwaliteitssysteem?

Welke beweegredenen heeft uw bedrijf gehad om deze procedures in te voeren:

- om geen gegevens te verliezen;
- naar aanleiding van een incident (bijv. gegevensverlies door het stuk gaan van een computer);

- onderdeel van ISO9000;
- onderdeel van beveiligingscertificaat, zoals VCA en Borg;
- informatiebeveiliging is voor ons opgelegd door externen (bijv. klanten of overheid);
- om reputatiebeschadiging te voorkomen;
- anders, namelijk ...

7. Bedreigingen en subjectieve veiligheid

Hoe groot vindt u de volgende bedreigingen voor uw organisatie. Probeer deze vraag zoveel mogelijk te beantwoorden zonder rekening te houden met de maatregelen die uw organisatie al heeft getroffen voor veilig internet gebruik. Geef voor elk van de onderstaande situaties aan hoe bedreigend deze voor u is: Hoog, Midden of Laag.

Laag Midden Hoog

1. Diefstal van gegevens door hackers
2. Diefstal van computers
3. Niet zakelijk gebruik van internet door medewerkers
4. Virussen
5. Uitval van het internet
6. Veranderen van gegevens op de website
7. Uitval van stroom
8. Brand of waterschade

Kunt u nog andere ICT gerelateerde bedreigingen noemen voor uw organisatie ?

Welke maatregelen heeft uw bedrijf getroffen om deze risico's te beperken?

8. Conclusie en vervolg

Stellingen:

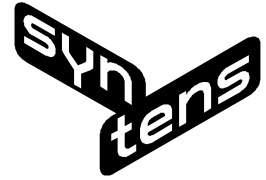
Mijn bedrijf heeft haar computers goed beveiligd

Mijn bedrijf heeft haar website goed beveiligd

Aan welke informatie / producten hebt u behoefte op het gebied van informatiebeveiliging (noem onderwerpen en/of voorwaarden waaraan de communicatie moet voldoen)?

Heeft u andere opmerkingen naar aanleiding van de vragenlijst?

Mag er contact worden opgenomen met uw externe ICT-leveranciers over deze onderwerpen?



Naam / contactpersoon / telefoonnummer ICT-leverancier:

Zijn er prioriteiten ten aanzien van door u of ons geconstateerde gebreken of 'lekken'?
Zo ja: welke?

Naam bedrijf / persoon technische ondersteuning bij deze quick scan:

Toegezegde datum van oplevering rapport aan Syntensadviseur:

Bijlage 2: rapportageformat scandeelnemer

Geachte (naam ondernemer),

Op (datum) heb ik met u gekeken naar de beveiliging van uw informatiesystemen, daarbij ondersteund voor het technische deel door (naam technisch specialist) van (naam ondersteunend bedrijf). Deze rapportage biedt u inzage in uw situatie ten tijde van de scan informatiebeveiliging.

Heeft u nog vragen naar aanleiding van deze rapportage dan kunt u contact opnemen met ondergetekende.

Met vriendelijke groet,

(naam adviseur)

Adviseur

Bijlage: rapportage scan informatiebeveiliging (MKB experiment Cybercrime)

Rapportage scan informatiebeveiliging (MKB experiment Cybercrime)

Inhoudsopgave

Inleiding

Digitale veiligheid versus fysieke veiligheid

Scores: status en risico

Conclusie

Behaalde scores zijn vermeld tussen haakjes achter ieder onderdeel.

1. Beleid en procedures

- 1.1 Apparatuur, fysieke beveiliging en beheer ()
- 1.2 Verbindingen / internetkoppeling ()
- 1.3 Website ()
- 1.4 Media en informatie ()
- 1.5 Informatiebeheer ()
- 1.6 Mens / personeel ()
- 1.7 Organisatie / beveiligingsbeleid ()
- 1.8 Bedreigingen en subjectieve veiligheid (-)

2. Techniek

- 2.1 Internet en gateway ()
- 2.2 Up-to-date: software, antimalware / anti-spam ()
- 2.3 Netwerk ()
- 2.4 Servers ()
- 2.5 Werkstations ()
- 2.6 Back-up en dataomgeving ()

Inleiding

ECP.NL voert in opdracht van het ministerie van Economische Zaken het Programma Digibewust uit. Een onderdeel van dit Programma is het MKB experiment Cybercrime. De doelstelling van het experiment is het inzicht in de kwetsbaarheid van het MKB voor cybercrime aanvallen te vergroten, en zo nodig die kwetsbaarheid te reduceren zodat de schade die het MKB als gevolg van cybercrime lijdt zoveel mogelijk wordt verminderd. Het onderdeel MKB experiment Cybercrime wordt uitgevoerd door Syntens.

Digitale veiligheid versus fysieke veiligheid

De digitale veiligheid en informatiebeveiliging in uw bedrijf zou net zo vanzelfsprekend moeten zijn als de fysieke veiligheid, denk aan brandalarm, inbraakbeveiliging en het op slot doen van deuren en ramen zodra u het pand verlaat. De keten van digitale veiligheid bestaat uit vijf belangrijke schakels: apparatuur, verbindingen, informatiedragers, informatie en de mens. Juist deze laatste geldt vaak als zwakste schakel in de keten. Het is belangrijk dat de maatregelen voor de fysieke veiligheid in uw bedrijf in balans zijn met de maatregelen voor de digitale veiligheid. De uitgevoerde scan informatiebeveiliging verschaft ook informatie over de mate van uw bewustzijn over het nut en de noodzaak van dit evenwicht. De stand van zaken in uw bedrijf met betrekking tot elke schakel in de keten van digitale veiligheid is in dit rapport uitgewerkt.

Scores: status en risico

Dit rapport biedt u inzage in uw situatie ten tijde van de scan informatiebeveiliging. Bent u wel zo veilig als u dacht? Nee? Hoe lost u dat dan op? En welk risico loopt u? Deze en andere vragen proberen wij in dit rapport zo concreet mogelijk te beantwoorden.

Per onderdeel in de scan is een cijfer toegekend tussen 1 en 10 waarbij het cijfer 10 het hoogst haalbare resultaat geeft.

Cijfer	Status	Risico
1 – 3	Slecht	Zeer Hoog
4 – 5	Matig	Hoog
6 – 7	Redelijk	Aanwezig
8 – 9	Goed	Klein
10	Zeer goed	Nihil

Conclusie

1. Beleid en procedures

1.1 Apparatuur, fysieke beveiliging en beheer ()

1.2 Verbindingen / internetkoppeling ()

1.3 Website ()

1.4 Media en informatie ()

1.5 Informatiebeheer ()

1.6 Mens / personeel ()

1.7 Organisatie / beveiligingsbeleid ()

1.8 Bedreigingen en subjectieve veiligheid (-)

2. Techniek

2.1 Internet en gateway ()

2.2 Up-to-date: software, antimalware / anti-spam ()

2.3 Netwerk ()

2.4 Servers ()

2.5 Werkstations ()

2.6 Back-up en dataomgeving ()

Bijlage 3: Syntens handleiding informatiebeveiliging

Onderstaande aandachtspunten zijn van belang bij het bewerkstelligen van voldoende en continue informatiebeveiliging bij ondernemers in het midden- en kleinbedrijf. Ze vormen een handleiding voor een ieder die werkzaam is in het werkveld, zowel non-profit (intermediairs met als aandachtsveld criminaliteitsbestrijding, innovatie of bedrijfsstimulering) en profit (ICT-dienstverleners op het gebied van ICT-beheer, beveiliging of organisatieadvies).

Nadat de mate van afhankelijkheid van ICT is vastgesteld kunnen bij de verschillende aandachtsgebieden sommige onderwerpen in meer of mindere mate prioriteit krijgen. De lijst is opgesteld voor de ondernemer zelf, maar bedoeld om samen met een adviseur gehanteerd te worden.

0. Afhankelijkheid van ICT

1. Bepaal hoe afhankelijk uw bedrijf van ICT is voor de interne bedrijfsvoering:
nauwelijks – matig – behoorlijk – heel erg
2. Bepaal hoe afhankelijk uw bedrijf van ICT is voor het maken van uw product of dienst:
nauwelijks – matig – behoorlijk – heel erg
3. Bepaal hoe afhankelijk uw bedrijf is van de verbinding met het internet:
nauwelijks – matig – behoorlijk – heel erg
4. Bepaal hoe afhankelijk uw bedrijf is van het functioneren van de website:
nauwelijks – matig – behoorlijk – heel erg

1. Apparatuur, fysieke beveiliging en beheer

1. Inventariseer de mate en status van de fysieke beveiligingsmaatregelen ter bescherming van apparatuur. Denk aan: afsluitbare serverruimte, toegangsverificatie, brandpreventie, inbraakpreventie.
2. Omschrijf de maatregelen die zijn genomen tegen stroomstoring, bijvoorbeeld een UPS voor de server, en tegen uitval van een / de harde schijf.
3. Ga na wat er gebeurt wanneer een bijzonder apparaat, zoals de verbinding met internet of een ander netwerkapparaat defect raakt (router, firewall, switch).
4. Omschrijf hoe het netwerk wordt beheerd en door wie, waar de werkzaamheden zijn beschreven en hoe er wordt over gerapporteerd. Zorg er bij uitbesteding voor dat dit door uw leverancier in een overeenkomst helder wordt beschreven, inclusief garanties voor herstel.

2. Verbindingen / Internetkoppeling

1. Omschrijf de firewall en ga na hoe die wordt beheerd en wat hiervan de status is.
2. Omschrijf de antivirusbescherming en antispywarebescherming en ga de werking na: is die op elke computer up-to-date en werkend.
3. Meld u aan bij de [Waarschuwingsdienst](http://www.waarschuwingsdienst.nl) (www.waarschuwingsdienst.nl) om op de hoogte te blijven van actuele dreigingen.
4. Inventariseer de rechten voor medewerkers voor het downloaden en installeren van software en pas deze eventueel aan.
5. Ga na hoe e-mail van buiten wordt opgehaald, hoe de viruscontrole plaatsvindt, of er adequaat spamfiltering plaatsvindt en of er gevaar is voor ongewenst of ongecontroleerd doorsturen van post. .
6. Wanneer u elektronische nieuwsbrieven verstuurd: ga na of het inschrijven en uitschrijven van geadresseerden goed geregeld is zodanig dat geen sprake is van ongewenste post (spam). Hetzelfde geldt voor andere e-mailingen naar adressenbestanden.
7. Controleer welke informatie u verzamelt over abonnees en wat er verder mee wordt gedaan (denk aan wetgeving ter bescherming van de privacy).
8. Wanneer er sprake is van toegang tot uw netwerk van andere locaties, bijvoorbeeld thuis:
 - hoe is de verbinding beschermd (virtual private network, encryptie, inloggen)
 - hoe veilig is de thuissituatie (t.a.v. virussen, spyware)
9. Wanneer u een draadloos netwerken gebruikt: ga de bescherming na (niet uitzenden netwerknaam, beheerderstoegang, encryptie) en de controle daarop.
10. Wanneer u software op afstand gebruikt, bijvoorbeeld voor het onderhoud van de website (CMS): ga na hoe verzekerd is dat er alleen toegang is voor de juiste personen en hoe de gegevens zijn beveiligd (opslag: backup en terugzetten; over internet: encryptie, bijvoorbeeld met SSL).
11. Hetzelfde geldt als er sprake is van beheer op afstand: wie doet dat (netwerkbeheer, softwareleverancier).

3. Website

1. Ga na hoe geregeld is dat de website altijd correct 'in de lucht' is, hoe de backup van gegevens is geregeld en hoe eventueel verdwenen gegevens worden teruggezet of beschadigde gegevens worden gerepareerd: zowel de inhoud van webpagina's als inhoud van eventuele databases. Zorg voor een goede overeenkomst waarin dit helder is vastgelegd en op basis waarvan u de uitvoering kunt nagaan en afdwingen.

2. Wanneer gegevens van uw klanten via de website worden verzameld: ga na waar die terecht komen, hoe ze in uw bedrijf komen en hoe wordt geregeld dat er alleen de juiste dingen mee worden gedaan (denk aan wetgeving: WBP) door de juiste personen.
3. Ga na of de verstrekking van deze gegevens via een beveiligde verbinding verloopt (SSL).
4. Wanneer u prijzen vermeld van door u aangeboden producten en diensten: ga na wie dit mag aanpassen en hoe dat geregeld is.

4. Media en informatie

Backups

Gegevens op computers kunnen verloren gaan door bijvoorbeeld defecten, brand of door diefstal van computers. Maak daarom dagelijks back-ups van tenminste de belangrijkste informatie in alle computers.

1. Ga na of dit daadwerkelijk gebeurt en of dit het gewenste effect heeft: controleer de afloop van elke back-up, kan de back-up ook daadwerkelijk worden teruggezet en hoe moet dit dan precies.
2. Ga na of de media, waarop de back-upgegevens worden opgeslagen, niet versleten zijn.
3. Ga na of de back-upgegevens veilig worden opgeborgen op een externe locatie.
4. Ga na of databases, bijvoorbeeld behorend tot uw bedrijfssoftware (ERP, CRM) wel eens worden gecontroleerd op consistentie of corruptie.

Informatiebeheer

1. Als u een website heeft, ga dan na en leg vast:
 - a. wie beheert de informatie,
 - b. wie brengt wijzigingen aan,
 - c. hoe wordt de informatie bewaard (backup)
2. Als er gebruik wordt gemaakt van software op afstand, ga dan na en leg vast:
 - a. wie beheert de informatie,
 - b. wie brengt wijzigingen aan,
 - c. hoe wordt de informatie bewaard (backup)
3. Indien er in uw bedrijf gewerkt wordt met laptops of verwisselbare media voor opslag van gegevens, zoals beschrijfbaar CD's of USB-sticks: pas dan encryptie toe.
4. Leg vast welke informatie er door uw medewerkers via internet of CD's op verzoek aan derden mag worden verstrekt en hoe dit moet worden vastgelegd.

5. Mens / personeel

1. Bepaal wat medewerkers mogen doen op uw eigen netwerk en op internet qua surfen, e-mailen, downloaden en chatten. Leg dit vast en zorg ervoor dat iedereen het weet. Dwingt af dat men zich hieraan houdt, door technische maatregelen, controles en bij gesprekken bij werving en functioneren.
2. Zorg er voor dat er geen belangrijke informatie op een verlaten bureau blijft liggen en dat er wordt uitgelogd bij het verlaten van de werkplek (ook bij pauzes, eventueel technisch afgedwongen).
3. Bepaal hoe er in het bedrijf met wachtwoorden moet worden omgegaan: regelmatig veranderen, niet onderling delen, geen eenvoudige wachtwoorden.

6. Organisatie / beveiligingsbeleid

1. Stel beleid vast op het gebied van informatiebeveiliging (zie de checklijst) in relatie tot het algemene / strategische beleid van uw onderneming, dus rekening houdend met uw missie, markt en producten / diensten.
2. Maak het bekend aan alle medewerkers, denk ook aan nieuwe medewerkers, en zorg dat ze dit ten allen tijde kunnen hanteren.
3. Maak iemand verantwoordelijk voor de uitvoering van dat beleid. Kijk er ook regelmatig naar, bijvoorbeeld eens per jaar, en ga na wat er aan gewijzigd moet worden – en voor die wijziging ook daadwerkelijk door.
4. Stel vast welke medewerkers betrokken kunnen worden bij de uitvoering van informatiebeveiliging, bijvoorbeeld aan wie worden verdachte situaties moeten worden gemeld (mogelijke virussen of vermissing van bestanden).
5. Stel procedures op om informatiebeveiliging te structureren, zoals werkinstructies voor betrokkenen, beschrijving van verantwoordelijkheden en documenten over technische configuraties van netwerkkapparaten en computers.
6. Zorg er voor dat die procedures passen in cq aansluiten bij uw kwaliteitszorgsysteem.

7. Aanpak

1. Bepaal de prioriteiten voor aanpassingen.
2. Ga na bij welke onderdelen u hulp nodig hebt van toeleveranciers (zoals uw huisleverancier voor ICT, uw websitebouwer, uw kwaliteitszorgadviseur en uw P&O-adviseur).
3. Stel een tijdsschema op voor de implementatie.
4. Communiceer met de werknemers en train ze waar nodig.
5. Herzien en update het plan zes tot twaalf maanden na implementatie of na grote veranderingen in het bedrijf.