BELGISCHE GIDS VOOR CYBER-VEILIGHEID

BESCHERM UW INFORMATIE

ICC BELGIUM INTERNATIONAL CHAMBER OF COMMERCE

VBO Verbond van Belgische Ondernemingen

b·ccentre BELGIAN CYBERCRIME CENTRE OF EXCELLENCE FOR TRAINING, RESEARCH & EDUCATION

ISACA Trust in, and value from, information systems Belgium Chapter

EY Building a better working world

Microsoft

Deze gids en de begeleidende documenten werden gezamelijk opgesteld door ICC Belgium, VBO, EY, Microsoft, L-SEC, B-CCENTRE en ISACA Belgium.

ICC Belgium, VBO, EY, Microsoft, L-SEC, B-CCENTRE en ISACA Belgium wijzen elke aansprakelijkheid voor de inhoud van deze gids af.

Deze gids heeft niet de bedoeling om een volledig overzicht te bieden van potentiële cyberbedreigingen of controlemaatregelen.

De vermelde informatie:

- is louter algemeen van aard en is niet gericht op de specifieke situatie van een individu of een rechtspersoon;
- is niet noodzakelijk volledig, accuraat of bijgewerkt;
- is geen professioneel of juridisch advies;
- vervangt het advies van een expert niet,
- geeft geen garanties voor een veilige bescherming.

VOORWOORD

CYBERVEILIGHEID...
EEN CRUCIALE OPDRACHT VOOR ELKE ONDERNEMING

Beste lezer,

Deze gids heeft tot doel u beter vertrouwd te maken met een heel belangrijk en brandend actueel onderwerp: informatieveiligheid.

Elke dag duiken overal ter wereld verschillende vormen van cybercriminaliteit of cyberwangedrag op. Velen negeren dit fenomeen gewoon of houden het verborgen, voor anderen is het een bron van grote bezorgdheid. Recentelijk waren er in ons eigen land een aantal ernstige incidenten rond cyberveiligheid. Het wordt steeds duidelijker dat diverse buitenlandse regeringen bereid zijn om zwaar te investeren in het verzamelen van waardevolle informatie. Onwetendheid, nalatigheid of paniek zijn slechte raadgevers om het fenomeen van cybercriminaliteit aan te pakken.

In het zakenleven moeten we kansen grijpen en risico's verstandig beheren. Elke ondernemer of manager weet welke kennis, technologieën of processen zijn bedrijf sterk of zelfs uniek maken, maar tegelijkertijd ook kwetsbaar. Het zijn net deze waardevolle troeven die we moeten beschermen door middel van goed beheer van de informatieveiligheid. Bovendien zal zo'n goed beheer het bedrijf helpen beschermen tegen zware schade veroorzaakt door allerlei slechte gewoontes en nalatigheid die voortkomen uit de huidige trend van het gebruik van sociale media, gepersonaliseerde apparaten en apps.

Zorg dat uw drang naar meer bescherming leidt tot een nieuwe dimensie in uw bedrijfscultuur en tot nieuwe competenties voor uw bedrijf: een reflex voor informatieveiligheid in de voortdurend evoluerende digitale omgeving.

Deze gids informeert u over de belangrijkste elementen van dit onderwerp. U vindt hierin een aantal controlelijsten die u op het goede spoor helpen en waarmee u de verstrekte adviezen gemakkelijker kunt implementeren.

We hopen dat deze brochure nuttig zal zijn voor allen die verantwoordelijkheden dragen in de bedrijven in ons land.

Rudi Thomaes
Secretaris-generaal van ICC Belgium

Philippe Lambrecht
Secretaris-generaal van VBO

INHOUDSTAFEL

WAAROM EEN GIDS OVER CYBERVEILIGHEID?

DIT HOOFDSTUK IS NIET BEDOELD OM U ANGST IN TE BOEZEMEN, HOEWEL HET DAT MISSCHIEN WEL DOET!

Toenemende veiligheidsrisico's

Elke dag worden we zowel op persoonlijk als op bedrijfsniveau blootgesteld aan dreigingen in cyberspace. In de meeste gevallen zijn we ons niet eens bewust van deze dreigingen en als dat wel het geval is, reageren we er soms op weinig gepaste wijze op. De media communiceren dagelijks over incidenten rond informatieveiligheid en over de impact die deze hebben op individuen en bedrijven. Deze incidenten zijn maar het topje van de ijsberg; we zijn er allemaal veel meer aan blootgesteld dan we denken. Bovendien nemen de risico's op het internet spijtig genoeg nog steeds toe. Het risico bij informatieveiligheid bestaat uit een combinatie van drie factoren: activa, kwetsbaarheden en dreigingen (activa staan bloot aan kwetsbaarheden die blootgesteld kunnen zijn aan dreigingen).

Spijtig genoeg kende elk van deze drie factoren de voorbije jaren een aanzienlijke toename:

1. Informatie[1] en informatiesystemen zijn activa. Nooit eerder beschikten we over meer elektronische informatie. We zijn afhankelijk van de correcte – en dus veilige – werking van de systemen waarop deze informatie wordt opgeslagen en verwerkt.
2. We beschikken over cloud- en sociale mediadiensten, mobiele apparatuur en andere nieuwe tools en technologieën. Deze technologische evolutie zal zich voortzetten en zal ons steeds meer afhankelijk maken van de correcte werking van deze technologieën. Deze evolutie brengt echter ook nieuwe kwetsbaarheden met zich mee waarvoor bedrijven vaak nog geen oplossing hebben.
3. Ten slotte is ook het aantal cyberdreigingen toegenomen. Ook de complexiteit en de efficiëntie van deze dreigingen kennen een zorgwekkende groei.

Is er dan alleen maar slecht nieuws? Niet echt, maar toch...

Het goede nieuws is dat er de voorbije jaren een grotere bewustwording rond de problematiek merkbaar is wat tot een aantal gepaste tegenmaatregelen heeft geleid. Bij de overheid en op institutioneel niveau werden al een aantal goede initiatieven gelanceerd, die misschien echter nog niet voldoende werden overgenomen door het bedrijfsleven.

In dat bedrijfsleven bestaat er nog veel onzekerheid over het "wat" en het "hoe" om risico's afkomstig van cyberdreigingen te beperken. Typisch is dat vooral grotere, internationale bedrijven meer initiatieven nemen, hoewel middelgrote firma's en familiebedrijven net zo vatbaar zijn voor dezelfde dreigingen en kwetsbaarheden. Zelfs in grotere bedrijven worden initiatieven over informatieveiligheid vaak onvoldoende ondersteund door de top van het bedrijf. Toch zijn wij van mening dat informatieveiligheid op de agenda moet staan van elk bedrijf, ongeacht de omvang, de complexiteit en de aard van de activiteiten, maar ook van elk individu binnen het bedrijf.

Heel wat bedrijven beschermen hun materiële activa (fabrieken, machines, personeel) zeer goed. Meestal is het een kwestie van gezond verstand en zelfs een gewoonte om instructies over fysieke beveiliging, veiligheid en gezondheid deel te laten uitmaken van de gewone gang van zaken. Informatie is echter ook waardevol en diefstal, verlies, foutief gebruik of ongeoorloofde wijziging en bekendmaking ervan kunnen een grote impact met ernstige gevolgen teweegbrengen. De kennis en de data van een bedrijf zijn vaak de belangrijkste activa. Ondernemingen moeten de vertrouwelijkheid, de integriteit en de beschikbaarheid van hun data waarborgen. Deze

drie veiligheidsdoelstellingen hangen samen met drie belangrijke vragen: “Wie krijgt de data onder ogen?”, “Zijn de data veranderd zonder toestemming?” en “Heb ik toegang tot de data wanneer ik ze nodig heb?”

Het is ook uw verantwoordelijkheid

Van bedrijfsleiders wordt niet verwacht dat ze experten zijn op het vlak van cyberveiligheid. Niettemin is het hun plicht om de bedrijfsactiva te beschermen. Zij zullen de verantwoordelijkheid bijgevolg delegeren aan hun managementteams en aan externe experten. Dit garandeert dat cyberveiligheid een vast onderwerp blijft op directieraden en dat alle nodige acties worden ondernomen om de informatie te beschermen.

Elektronische verwerking van persoonsgegevens houdt aanzienlijke verplichtingen in voor het bedrijf. Het bedrijf is immers verantwoordelijk voor de gegevens die het beheert en moet daarom een gepast beveiligingsniveau garanderen. Aldus moet het bedrijf relevante maatregelen treffen om de data te beschermen tegen toevallige of onwettige vernietiging en om ongeoorloofd gebruik of wijziging van gegevens te voorkomen.

Bovenop andere sancties die het bedrijf kan oplopen, voorziet de wetgeving ook een aantal strafrechtelijke maatregelen. De ontwerptekst van de EU-verordening Gegevensbescherming lijkt deze maatregelen nog te verstrengen en het bedrijf zal verplicht kunnen worden tot het betalen van aanzienlijke schadevergoedingen aan de getroffen personen.

Volgens de ontwerptekst van de EU-verordening Gegevensbescherming moet een bedrijf in geval van misbruik door derden van persoonsgegevens die het bewaart, verlies van deze gegevens of andere inbreuken hierop, onmiddellijk de Privacycommissie en de persoon in kwestie verwittigen zodra blijkt dat de inbreuk op de gegevens waarschijnlijk een nadelige invloed zullen hebben op de privacy.

Tijd voor actie

Ten prooi vallen aan een incident rond informatieveiligheid kan heel wat gevolgen hebben, die overigens niet beperkt blijven tot het verlies van data of informatie. De effecten op de reputatie van uw bedrijf kunnen langdurig van aard zijn en ernstige financiële gevolgen hebben.

Het volstaat niet om te bevestigen dat het beschermen van de bedrijfsinformatie de verantwoordelijkheid is van iedereen binnen het bedrijf. U moet dit concreet toepassen op alle niveaus in uw bedrijf en zorgen voor de verankering van goede veiligheidsprincipes in de dagdagelijkse werkomgeving. Deze principes moeten pragmatisch zijn en blijk geven van gezond verstand, zodat ze een duurzame impact hebben en zowel in grote als in kleine bedrijven toegepast kunnen worden. Een “one size fits all”-benadering dient aldus vermeden te worden.

Een professioneel beheer van de informatieveiligheid is een kwestie van:

(A) een bedrijfsvisie en bedrijfsprincipes over het onderwerp creëren, die vertaald worden in een concreet beleid rond informatieveiligheid,
(B) dit beleid implementeren in de organisatie en de processen door gepaste functies en verantwoordelijkheden te definiëren,
(C) de juiste cultuur, het juiste gedrag en het juiste denkkader creëren door goede principes voor informatieveiligheid te implementeren.

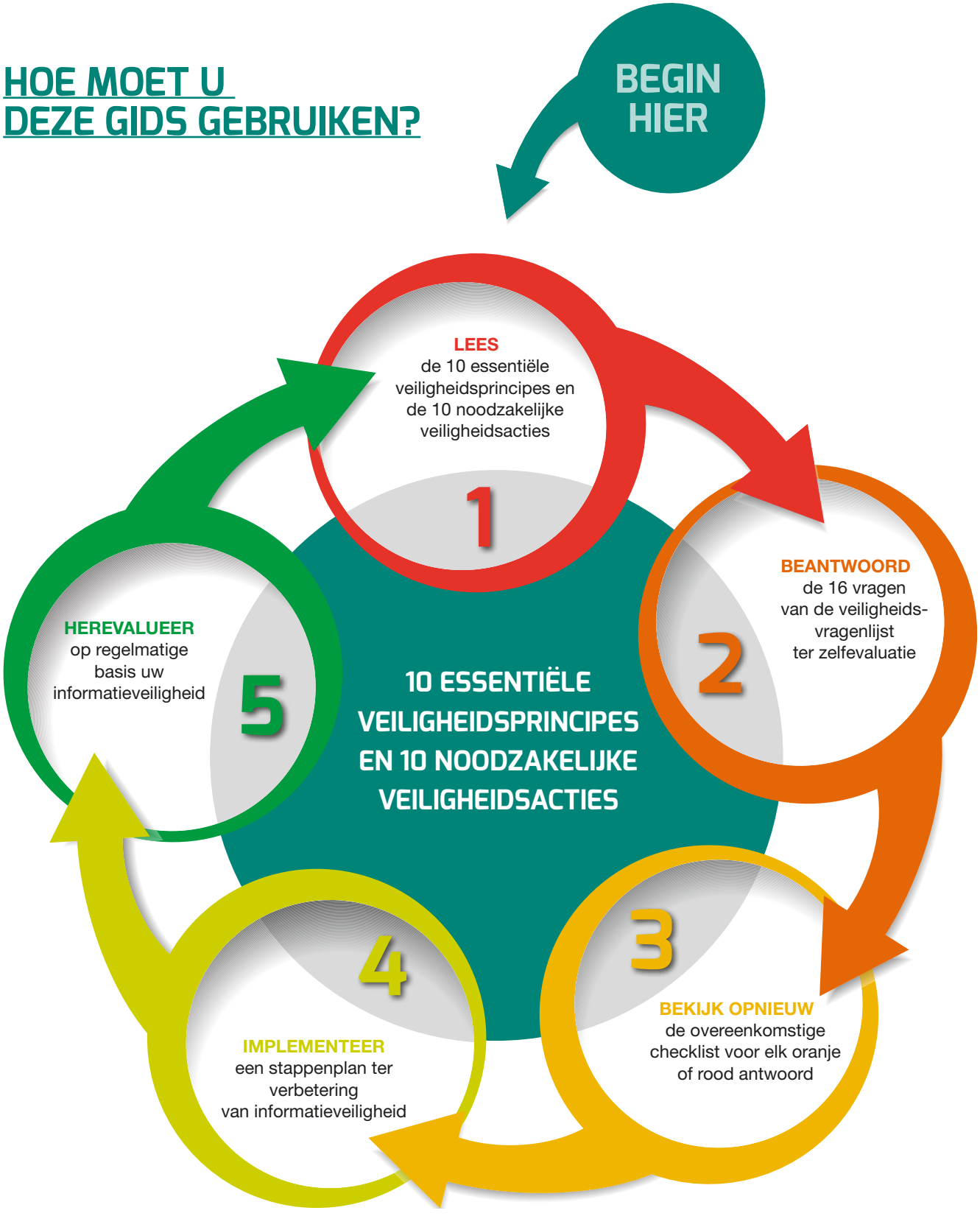
Deze mix zou uw bedrijf moeten toelaten om duurzame resultaten te boeken op het vlak van informatieveiligheid. Individuele verantwoordelijkheid en basisdiscipline, eerder dan gesofisticeerde beveiligingstechnologieën, zijn de eerste en meest eenvoudige acties om uw informatieveiligheid aanzienlijk te verbeteren.

We zullen nooit voor 100 % beveiligd zijn, maar dat mag ons niet tegenhouden om alsnog een zo hoog mogelijk niveau trachten na te streven. Deze gids, geschreven onder meer door mensen uit de bedrijfswereld, moet bedrijven helpen die aan het begin staan van de weg naar een betere en duurzamere informatieveiligheid.

[1] De gevoelige informatie van een bedrijf omvat: financiële data, HR data, data over klanten en leveranciers, prijslijsten, notulen van de Raad van Bestuur, ...

HOE MOET U DEZE GIDS GEBRUIKEN?

HOE MOET U DEZE GIDS GEBRUIKEN?



A. VISIE

B. ORGANISATIE & PROCESSEN

C. DENKKADER

10 ESSENTIËLE VEILIGHEIDSPRINCIPES

Er zijn een aantal kernprincipes die men moet beschouwen als de basis voor een gedegen cultuur van informatieveiligheid. De benadering van informatieveiligheid kan echter verschillen van bedrijf tot bedrijf, afhankelijk van de aard van de activiteiten, het risiconiveau, de omgevingsfactoren, de reglementaire vereisten en de grootte van het bedrijf. Daarom zijn deze principes van toepassing op alle bedrijven, ongeacht hun grootte of sector.

Deze gids definieert **10 kernprincipes** in drie domeinen van informatieveiligheidsbeheer:

(A) visie,

(B) organisatie & processen en

(C) denkkader,

aangevuld met een reeks absoluut noodzakelijke **veiligheidsacties**.

De voorgestelde principes en acties in deze gids zullen de weerbaarheid van een bedrijf tegen cyberaanvallen aanzienlijk verhogen en zullen de impact van incidenten beperken.

1.

— KIJK VERDER DAN DE TECHNOLOGIE —

Bekijk informatieveiligheid in de breedste zin, niet louter in termen van informatietechnologie.

Uit ervaring[2] blijkt dat 35% van de veiligheidsincidenten het gevolg zijn van menselijke fouten en niet van doelbewuste aanvallen. Meer dan de helft van de resterende 65% van de veiligheidsincidenten die het resultaat waren van een doelbewuste aanval, hadden vermeden kunnen worden indien mensen op een veiligere manier met de informatie waren omgegaan.

Dit geeft duidelijk aan dat informatieveiligheid moet worden beschouwd als een combinatie van mensen, processen en technologie. Het is belangrijk te beseffen dat informatieveiligheid een bekommernis is voor het hele bedrijf en niet louter voor de IT-afdeling. De invoering van beschermingsmaatregelen mag niet worden beperkt tot de IT-afdeling, maar moet doordringen tot alle geledingen van het bedrijf. Het bereik van en de visie op informatieveiligheid hebben daarom betrekking op mensen, producten, installaties, processen, beleidslijnen, procedures, systemen, technologieën, netwerken en informatie.

In een volwassen bedrijf wordt informatieveiligheid beschouwd als een vereiste die rechtstreeks verbonden is met strategische objectieven, bedrijfsdoelstellingen, beleidslijnen, risicobeheer, nalevingsvereisten en performantiemetingen. Managers doorheen het hele bedrijf moeten begrijpen hoe informatieveiligheid de bedrijfsactiviteiten faciliteert.

De voordelen van verder kijken dan de technologie en nadruk leggen op informatieveiligheid als een faciliterende factor, zijn onder meer:

- **strategisch:** beter beslissingsproces in het bedrijf door een verhoogde zichtbaarheid van de blootstelling aan risico's;
- **financieel:** lagere kosten, wat leidt tot financiële voordelen;
- **operationeel:** aangepaste noodplannen voor het bedrijf.

[2] EY – 2012 Global Information Security Survey - Fighting to close the gap

2.

— NALEVING VAN REGELS VOLSTAAT NIET —

Bedrijven zijn onderworpen aan heel wat wetten en reglementeringen, waarvoor vaak gepaste veiligheidscontroles moeten worden geïmplementeerd. Wetten en reglementeringen hebben betrekking op de persoonlijke levenssfeer, de controle op het financiële rapporteringsproces, de bescherming van de klant en de bescherming van specifieke gegevens. Zij worden vaak aangevuld met sectorgebonden regelgeving of met veiligheidsnormen en -modellen.

De naleving van deze wetten, verordeningen en normen heeft geleid tot een verbeterde informatieveiligheid. Toch blijft de naleving maar al te vaak het enige doel. Aangezien de naleving altijd gericht is op specifieke onderwerpen, ontbreekt dikwijls de op risico gebaseerde globale aanpak. Zo ligt bij inspanningen op het vlak van de persoonlijke levenssfeer de focus vaak alleen op de bescherming van persoonsgegevens en kijkt men bij de controle op de financiële rapportering vooral naar de integriteit van financiële data.

Daarom moeten we twee belangrijke aspecten begrijpen:

- **Eerst en vooral** betekent “naleven” niet noodzakelijk “veilig werken”. Veiligheidsdoelstellingen geformuleerd in wetten, reglementeringen en normen zijn steeds een deelverzameling van de algemene veiligheidsdoelstellingen voor bedrijven. Met dat in het achterhoofd, mag men aannemen dat het implementeren van goede veiligheidspraktijken voor bedrijven de naleving bijna zeker zal vereenvoudigen of garanderen, terwijl dit tegelijkertijd tegemoetkomt aan de behoeften van het bedrijf.

- **Ten tweede**, moeten veiligheidsinspanningen worden afgestemd op en – waar mogelijk – geïntegreerd in de werkzaamheden voor naleving en risicobeperking om te vermijden dat er te veel verschillende overlappende initiatieven en verantwoordelijkheden zouden ontstaan.

3.

— VERTAAL UW VEILIGHEIDSDOELSTELLINGEN NAAR EEN INFORMATIEVEILIGHEIDSBELEID —

Informatieveiligheid is een probleem voor het hele bedrijf, niet louter een technologisch probleem. Bedrijven moeten informatie en informatiesystemen willen beschermen omwille van gegronde bedrijfsdoeleinden. Een gepaste omkadering van het veiligheidsbeleid zorgt ervoor dat de bedrijfsvisie op het vlak van informatieveiligheid naar de praktijk wordt vertaald. Dit gebeurt typisch door het uitwerken van een beleid op topniveau met de bijbehorende ondersteunende richtlijnen en normen, die uiteindelijk worden ingebouwd in operationele procedures.

Bedrijfsbeleidslijnen rond informatieveiligheid bieden diverse voordelen:

- zij demonstreren het engagement van een bedrijf om de vitale informatieactiva te beschermen,
- zij voorzien een basisnorm voor informatieveiligheid doorheen het hele bedrijf voor alle afdelingen en medewerkers, en
- zij verhogen het bewustzijn rond informatieveiligheid.

De omkadering van het veiligheidsbeleid vormt de basis waarop de aanpak van en de activiteiten rond informatieveiligheid worden uitgebouwd.

4.

— VERZEKER HET ENGAGEMENT VAN DE DIRECTIE —

De verantwoordelijke voor informatieveiligheid moet voldoende engagement in het bedrijf hebben om binnen de ganse organisatie een adequaat antwoord te kunnen bieden op de huidige en toekomstige dreigingen op het vlak van informatieveiligheid. Daarom moet de directie zich zichtbaar engageren voor het beheer van het cyberveiligheidsbeleid van het bedrijf evenals het toezicht op de naleving ervan. Zij moeten zorgen dat er voldoende middelen, zowel financiële budgetten als mensen, worden toegewezen voor de bescherming van het bedrijf. Een formele goedkeuring van het veiligheidsbeleid van het bedrijf wijst op een actieve ondersteuning.

Het directieteam moet het belang begrijpen van de beheersing van cyberrisico's als cruciaal element voor succes en voor de bescherming van de intellectuele eigendom, en dit dan ook als dusdanig ondersteunen. Het beschermen van uw kennis is elementair om op een competitieve wijze producten en diensten te kunnen leveren aan uw klanten.

Er moet formeel gerapporteerd worden over de geschiktheid en de doeltreffendheid van de toepassing van de maatregelen rond informatieveiligheid:

- op regelmatige basis aan de hoogste veiligheids-verantwoordelijke in uw bedrijf
- en ten minste eenmaal per jaar aan de directie en aan de raad van bestuur.

Deze rapportering moet gebaseerd zijn op een aantal indicatoren en meetsystemen rond informatieveiligheid en moet inzicht geven in de mate waarin uw bedrijf zijn activa beschermt. Het evalueren van de vooruitgang en de doeltreffendheid van de maatregelen is van cruciaal belang voor het nemen van geïnformeerde beslissingen over het beleid rond informatieveiligheid en de bijbehorende investeringen.

5.

— CREËER EEN ZICHTBARE VEILIGHEIDSFUNCTIE IN UW BEDRIJF EN VERANKER INDIVIDUELE VERANTWOORDELIJKHEDEN —

Om de informatieveiligheid doeltreffend en efficiënt te beheren, moet een deugdelijk informatieveiligheidsbeleid gedefinieerd en geïmplementeerd worden. De geschikte personen moeten aansprakelijk zijn voor de informatie en de bescherming ervan en zij moeten aldus beschikken over de juiste bevoegdheden, middelen en opleiding om deze taak tot een goed einde te brengen. Er moet een functie bestaan die de initiatieven rond informatieveiligheid leidt en faciliteert, terwijl de informatieveiligheid op zich een gedeelde verantwoordelijkheid blijft doorheen het hele bedrijf.

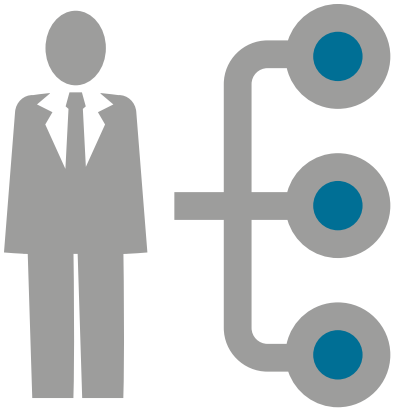
Zelfs kleine bedrijven moeten beschikken over een interne of externe persoon die regelmatig nagaat of het informatieveiligheidsnivau toereikend is en die er formeel voor instaat. Hoewel dit in kleine bedrijven misschien geen voltijdse baan is, is het toch een belangrijke functie die cruciaal kan blijken voor het overleven van het bedrijf.

In grote bedrijven moet de toewijzing van functies, taken en verantwoordelijkheden een bewuste mix zijn van individuen en (virtuele) werkgroepen en comités. Elk teamlid moet een duidelijk inzicht hebben in zijn verantwoordelijkheden en aansprakelijkheden. Gepaste documentatie en communicatie zijn hierbij essentieel.

Inspanningen om medewerkers op te leiden en hen te informeren over hun verantwoordelijkheden en over de dreigingen waarmee zij geconfronteerd kunnen worden, zijn noodzakelijk. Een belangrijke dreiging die slechts succesvol kan worden aangepakt met een gedegen opleiding voor de medewerkers, is “*social engineering*”. Social engineering is de techniek om mensen zodanig te manipuleren dat ze acties uitvoeren waardoor gevoelige of vertrouwelijke informatie vrijgegeven wordt.

Geef aan geselecteerde medewerkers de toelating om de juiste informatie te delen met collega’s en andere relevante partijen binnen de sector, zowel om hen te helpen om toonaangevende praktijken uit te bouwen als om hen te waarschuwen tegen mogelijke toekomstige aanvallen.

Hoewel ze vaak de *zwakste schakel* worden genoemd op het vlak van informatieveiligheid, kunt u uw medewerkers transformeren tot de *grootste troeven voor een goede informatieveiligheid* door hen een bewustzijn over informatieveiligheid bij te brengen dat leidt tot efficiënte vaardigheden.



6.

— BLIJF VEILIG WANNEER U UITBESTEEDT —

Dankzij steeds beter wordende verbindingen en communicatiemiddelen, worden de waardeketens steeds meer geïntegreerd en bieden zij bedrijven heel wat extra voordelen. Uitbesteding, offshoring en nieuwe samenwerkingsmodellen met derde partijen zijn een standaard norm van zakendoen geworden.

Toch kunnen derden die informatie of informatiesystemen onvoldoende beschermen een ernstige bedreiging vormen voor de activiteiten, de reputatie en de merkbekendheid van een bedrijf.

Het is een goede praktijk om leveranciers, vooral IT-dienstverleners, aan te moedigen om op zijn minst de principes rond informatie en informatieveiligheid over te nemen die worden toegepast binnen het eigen bedrijf. Men kan hen tevens uitdagen om te bewijzen dat deze principes veilig zijn. Dit kan gebeuren door audits uit te voeren of dienstverleners te vragen om een formeel onafhankelijk audit rapport over hun praktijken op het vlak van informatieveiligheid voor te leggen. Speciale aandacht moet worden besteed aan het evalueren en begrijpen van service level agreements, vooral op het vlak van systeembeschikbaarheid en herstellingstijden.

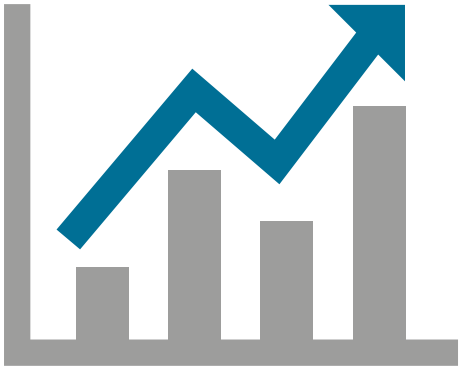
In de huidige wereld van clouddiensten is dit principe belangrijker dan ooit. Clouddiensten zijn oplossingen waarbij u gebruik maakt van een externe dienstverlener om uw data op te slaan, te verwerken of te beheren via een netwerk zoals het internet, met een hoge mate van flexibiliteit en directe monitoring.

IT-dienstverleners kunnen ook oplossingen voor informatieveiligheid aanbieden. U kunt inlichtingen inwinnen over bijkomende diensten die een externe dienstverlener en met name de cloud service providers leveren rond informatieveiligheid. Sommige van deze diensten omvatten ook back-up- en herstelfuncties en encryptie, wat interessant kan zijn voor kleine bedrijven.

Zorg ervoor dat u toegang hebt tot activiteitenlogs van de uitbestede diensten. Die zijn cruciaal voor een correcte analyse en evaluatie van de dreigingen.

7.

— VERZEKER DAT VEILIGHEID EEN MOTOR IS VOOR INNOVATIE —



Een adequate veiligheidsaanpak beschermt het bedrijf niet alleen, het kan ook een omschakeling naar nieuwe technologieën mogelijk maken. Risicomijdend gedrag mag de invoering van nieuwe technologieën niet verhinderen. De dreigingen van nieuwe technologieën moeten door middel van een adequate evaluatie worden afgewogen tegen de mogelijke voordelen.

Wanneer nieuwe innovatieve oplossingen en toestellen in gebruik genomen worden, dienen gepaste veiligheidsmaatregelen zo vroeg mogelijk in de overgangsperiode te volgen. Idealiter gebeurt dit bij de identificatie van de bedrijfsvereisten. Het “security-by-design”-principe moet worden toegepast om te garanderen dat van bij het begin van de ontwikkeling en bij de aankoop van nieuwe tools en toepassingen een adequate veiligheid ingebouwd wordt.

Mensen die innovaties doorvoeren in een bedrijf moeten ofwel beschikken over voldoende kennis over informatieveiligheid, ofwel één of meerdere veiligheidsexperten inhuren om informatieveiligheid in te bouwen in het ontwerp van elke nieuwe oplossing, om te zorgen dat deze optimaal geschikt is.

8.

— BLIJF UZELF UITDAGEN —

Veiligheidsdreigingen evolueren constant waardoor er geen pasklare oplossing voor bestaat. Beleidslijnen en procedures kunnen verouderd raken of in de praktijk ondoeltreffend blijken.

Door een periodieke evaluatie van de weerbaarheid van een bedrijf tegen cyberdreigingen en kwetsbaarheden kan de vooruitgang en de doeltreffendheid van de veiligheidsactiviteiten gemeten worden. Dit kan gebeuren door interne en/of onafhankelijke evaluaties en audits, zoals bijvoorbeeld penetratietesten en detectiesystemen. Deze kunnen ook helpen om de bedrijfscultuur te verbeteren. Bedrijven moeten mensen toelaten om fouten te maken en moeten een open communicatie over veiligheidsincidenten stimuleren, zodat mensen niet bang zijn om veiligheidsincidenten te melden wanneer deze zich voordoen.

Naast deze evaluaties kan ook een actief engagement met collega's in de sector, de bredere bedrijfsomgeving en de politie helpen om op de hoogte te blijven van de huidige en toekomstige dreigingen.

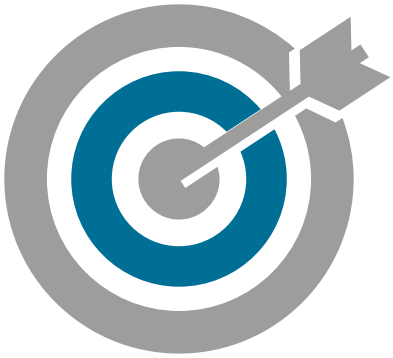
9.

— BEHOUD FOCUS —

In de huidige kenniseconomie is informatie uiterst waardevol geworden. Deze activa identificeren en vervolgens proberen om de bijbehorende kwetsbaarheden en dreigingen aan te pakken, kan een enorme taak zijn.

U moet uw veiligheidsinspanningen concentreren op de bescherming van de meest waardevolle informatie waarvan het verlies van haar vertrouwelijkheid, integriteit of beschikbaarheid het bedrijf enorme schade kan berokkenen.

Dit betekent niet dat u de veiligheid van andere informatie kan negeren. Dit betekent dat een op risico's gebaseerde aanpak met de nadruk op de "kroonjuwelen" van het bedrijf, de meest efficiënte en doeltreffende benadering is om informatieveiligheid in de praktijk om te zetten. Tegelijk onderschrijft deze aanpak de idee dat het niet mogelijk noch nodig is om risico's voor 100% te elimineren.



10.

— WEES VOORBEREID OM VEILIGHEIDSINCIDENTEN AAN TE PAKKEN —

Veiligheidsincidenten zijn niet noodzakelijk een probleem; het is de aanpak ervan die telt. In de huidige omgeving vol dreigingen en kwetsbaarheden moet u zich niet afvragen “of”, maar “wanneer” u het slachtoffer zal worden van een veiligheidsincident en hoe goed u hierop bent voorbereid. Uw bedrijf moet zowel organisatorisch als technisch voorbereid zijn om dergelijke informatieveiligheidsincidenten aan te pakken om de impact op het bedrijf tot een minimum te beperken. Idealiter werden gespecialiseerde derde partijen die u kunnen helpen om de veiligheidsincidenten in te dammen en op te lossen reeds geïdentificeerd vooraleer het incident plaatsvindt.

Een goede reactie op incidenten, inclusief een gepaste communicatiestrategie, kan het verschil maken tussen een onderbreking van de bedrijfsactiviteiten van minder dan één dag en een onderbreking van meerdere dagen, tussen een “fait divers” van 10 lijntjes op pagina 7 en een kop op de voorpagina van de kranten.

Het is cruciaal om veiligheidsincidenten intern, en eventueel ook extern, op een gepaste manier te communiceren. Bovendien moet u onthouden dat rapportering aan de bevoegde overheden de manier bij uitstek is om het algemene informatieveiligheidslandschap te verbeteren. Het is bovendien in een aantal gevallen zelfs verplicht.

VOORKOMEN IS ALTIJD BETER DAN GENEZEN

10 ABSOLUUT NOODZAKELIJKE VEILIGHEIDSACTIES

Deze lijst met acties focust vooral op de bescherming van een bedrijf tegen veiligheidsincidenten. Natuurlijk zijn ook het ontdekken, beheersen en beteugelen van incidenten evenals het herstel achteraf van belang. Voor praktische begeleiding hierbij verwijzen we naar het overzicht en de lijst met contactgegevens in deze gids.

1.

— ORGANISEER GEBRUIKERSOPLEIDINGEN & BEWUSTMAKINGSINITIATIEVEN —

Informatieveiligheid is een opdracht voor het hele bedrijf. De mensen die de informatie van een bedrijf creëren en behandelen spelen eveneens een belangrijke rol bij de beveiliging ervan. Als zij de informatie niet correct behandelen, worden ze niet alleen een bron van veiligheidsincidenten, maar vergemakkelijken zij ook het werk van de tegenstanders.

Mensen bewustmaken van de belangrijkste cyber-dreigingen en veiligheidsproblemen is overal en op ieder moment in het bedrijf van cruciaal belang.

Hier volgen enkele voorbeelden van onderwerpen voor de bewustmaking over informatieveiligheid:

- Veilig en verantwoord communiceren
- Sociale media verstandig gebruiken
- Digitale bestanden veilig versturen
- Wachtwoorden correct gebruiken
- Verlies van belangrijke informatie vermijden
- Garanderen dat alleen de juiste mensen uw informatie kunnen lezen
- Beschermd blijven tegen virussen en andere malware
- Weten wie u moet verwittigen bij een potentieel veiligheidsincident
- Weten hoe u zich niet in de val laat lokken om informatie vrij te geven.

Dergelijke bewustmaking zorgt ervoor dat alle medewerkers die toegang hebben tot informatie en informatiesystemen hun dagdagelijkse verantwoordelijkheden bij het omgaan met, het beschermen en het ondersteunen van de informatieveiligheidsacties van het bedrijf begrijpen. Zo kunnen veiligheidsbewuste omgang, motivatie en naleving de aanvaarde en verwachte norm worden in de bedrijfscultuur. Regelmatige herhaling van de mededelingen aan de medewerkers over informatieveiligheid is de beste manier om de gewenste vaardigheden en eigenschappen rond informatieveiligheid te ontwikkelen.

Aangezien de meeste medewerkers het internet ook gebruiken voor privédoeleinden mag hun opleiding niet beperkt blijven tot het gebruik van bedrijfsinformatie. Het is belangrijk dat zij begrijpen hoe zij hun persoonlijke levenssfeer kunnen beschermen wanneer ze het internet gebruiken voor privédoeleinden.

Algemene informatie over cyberveiligheid en bewustmaking van eindgebruikers vindt u op www.safeonweb.be, een initiatief van CERT.be (het federale cyber emergency team) en op http://www.enisa.europa.eu/media/multimedia/material, een initiatief van ENISA. U mag al deze informatie, video's, infografieken, … gebruiken voor opleidingsdoeleinden binnen uw bedrijf.

2.

— HOU SYSTEMEN UP-TO-DATE —

Heel wat van de geslaagde hackpogingen en virusaanvallen maken misbruik van de kwetsbaarheden van systemen waarvoor oplossingen en correcties reeds beschikbaar waren, vaak zelfs meer dan een jaar vóór het incident.

Systemen en software, inclusief netwerkapparatuur, moeten worden bijgewerkt wanneer patches en firmware upgrades beschikbaar zijn. Deze upgrades en veiligheidspatches maken komaf met de kwetsbaarheden van het systeem waarvan de aanvallers misbruik kunnen maken.

Maak gebruik van geautomatiseerde updates waar mogelijk wanneer deze tegen billijke voorwaarden beschikbaar zijn, vooral voor veiligheidssystemen zoals anti-malware toepassingen, web filtering tools en inbraakdetectiesystemen.

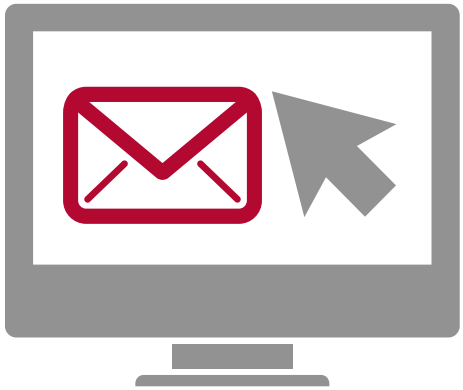
Om te garanderen dat alle relevante systemen optimaal beschermd zijn, is het een goed idee om een overzicht op te stellen van alle systemen met de definitie van de minimale veiligheidsnorm die hiervoor moet worden toegepast.

Gebruikers mogen alleen geldige updates van beveiligingssoftware aanvaarden die rechtstreeks werden verstuurd door de originele verkoper. Zij mogen dus nooit ingaan op voorstellen voor software-updates opgenomen in een extern e-mailbericht.

3.

— BESCHERM INFORMATIE —

Meer dan ooit moet bij de strategie rond informatieveiligheid de nadruk liggen op de gegevens in plaats van op de technologie. Bescherming van netwerkperimeters en traditionele toegangscontrole volstaan niet meer, vooral wanneer informatie werd opgeslagen in minder betrouwbare omgevingen, zoals het internet of draagbare media.



Er bestaan verschillende encryptietechnieken die hun doeltreffendheid reeds hebben bewezen in specifieke omstandigheden (zoals dataopslag, datatransmissie of datatransport), bijvoorbeeld:

- E-mailberichten die via het internet worden verstuurd naar zakenpartners, klanten en anderen zijn steevast onversleuteld (clear text). Daarom moeten bedrijven de middelen ter beschikking stellen om e-mails te voorzien van encryptie wanneer gevoelige informatie wordt verstuurd.

- Draagbare toestellen zoals laptops, USB-sticks en smartphones kunnen uiterst gemakkelijke doelwitten voor diefstal zijn of kunnen verloren raken. Daarom moeten bedrijven er voor zorgen dat deze toestellen ofwel standaard versleuteld zijn (laptops en smartphones) ofwel dat de gebruikers beschikken over de middelen om de gegevens die erop zijn opgeslagen te versleutelen (USB-sticks).

4.

— BEVEILIG MOBIELE APPARATEN —

Het gebruik van mobiele apparaten brengt een grote uitdaging met zich mee op het vlak van veiligheid en beheer, vooral wanneer ze vertrouwelijke en gevoelige informatie bevatten of toegang hebben tot het bedrijfsnetwerk:

- gegevensverlies
- aanvallen met behulp van social engineering
- malware
- bedreigingen op het vlak van data-integriteit
- misbruik van middelen
- aanvallen via netwerken en het internet
- …

Het BYOD ("Bring Your Own Device") concept spreekt heel wat organisaties en medewerkers sterk aan, maar het heeft als inherent nadeel dat het het risico op ongewenste vrijgave van gevoelige bedrijfsinformatie groter maakt.

Daarom moet u een duidelijk standpunt innemen over welke apparaten toegang mogen hebben tot het bedrijfsnetwerk en/of de bedrijfsinformatie en moet u het veiligheidsbeleid en bijbehorende procedures daarop afstemmen.

De gebruikers moeten hun mobiele toestellen steeds beschermen met een sterk wachtwoord. Bedrijven moeten gebruikers de mogelijkheid bieden en/of verplichten om de gepaste veiligheidsinstellingen voor mobiele apparaten te configureren om te vermijden dat cybercriminelen informatie stelen via het mobiele toestel. De software op deze toestellen, en vooral de veiligheidssoftware, moet steeds worden bijgewerkt om ervoor te zorgen dat ze beschermd zijn en blijven tegen de meest recente versies van malware en virussen.

Bovendien moeten er procedures bestaan voor aangifte van gestolen of verloren apparatuur en moeten indien mogelijk functies voor wissen vanop afstand voorzien zijn om alle bedrijfsinformatie op gestolen of verloren toestellen te wissen. **Gebruikers moeten zich er ook van bewust zijn dat zij de reflex moeten aankweken om hun omgeving te controleren voor en tijdens het gebruik van hun mobiele toestellen, en om een aantal veiligheidsstrategieën toe te passen:**

- gepaste beveiligingsoplossingen voor e-mail installeren,
- niet openen van onverwachte tekstberichten van onbekende afzenders,
- onbekende links niet openen,
- niet chatten met onbekenden.

5.

— GEEF ENKEL TOEGANG TOT INFORMATIE OP BASIS VAN 'NEED-TO-KNOW' —

Toegang mag alleen worden verleend aan wie deze echt nodig heeft om de vertrouwelijkheid, integriteit en beschikbaarheid te waarborgen. Niemand in een organisatie mag toegang hebben tot alle datasystemen. Medewerkers mogen alleen toegang krijgen tot de specifieke data en informatiesystemen die zij nodig hebben voor hun functie. Administratieve privileges (supergebruikersrechten) mogen alleen worden toegekend aan een paar vertrouwde IT-medewerkers. Tegenwoordig bestaan er opties die systeembeheerders toelaten hun werk te doen zonder dat ze toegang hebben tot de data.

Bovendien moeten alle verantwoordelijke managers (ten minste eenmaal per jaar) een overzicht krijgen van alle (interne en externe) gebruikers die toegang hebben tot de toepassingen en gegevens van hun dienst en moeten zij dit overzicht nakijken en valideren.

Bovendien mogen medewerkers niet de rechten hebben om zonder voorafgaande toestemming software te installeren op de bedrijfslaptops en -desktops. Ze mogen voorgeïnstalleerde veiligheidsinstellingen en veiligheidssoftware ook niet kunnen aanpassen. Dergelijke toegang gaat gepaard met een heel hoog risico op incidenten en moet daarom worden beschouwd als een voorrecht dat alleen mag worden toegekend wanneer het echt nodig is.

6.

— STEL REGELS OP VOOR VEILIG INTERNETGEBRUIK EN PAS ZE TOE —

Het interne netwerk van het bedrijf mag alleen toegang bieden tot die diensten en middelen op het internet die noodzakelijk zijn voor de activiteiten en behoeften van uw medewerkers. Hoewel internetgebruik voor privédoeleinden niet noodzakelijk moet worden geblokkeerd, moet het toch worden beperkt tot diensten en websites die geen veiligheidsrisico inhouden. Diensten en websites die een verhoogd risico op malware inhouden voor de PC of het bedrijfsnetwerk (bijvoorbeeld peer-to-peer file sharing en pornografische websites) moeten worden geblokkeerd. Er bestaan gebruiksvriendelijke monitoring tools voor websites die gebruikmaken van een automatische indeling in categorieën en die verschillende toegangsmodi mogelijk maken (nooit, altijd, tijdens bepaalde uren, tot een bepaald volume enz.). Het is essentieel dat deze regels voor het surfen op het internet transparant zijn voor alle gebruikers in de organisatie en dat er een mechanisme bestaat om bedrijfswebsites waartoe de toegang werd geweigerd, te deblokkeren.

De risico's die gepaard gaan met het surfen naar malafide websites zijn niet beperkt tot virussen en spyware. Het maakt het bedrijf ook kwetsbaarder voor phishing[3] wat een groter risico impliceert op diefstal van persoonsgegevens van medewerkers. Een ander risico is de blootstelling aan inbreuken op het auteursrecht door het illegaal kopiëren of downloaden van auteursrechtelijk beschermde software, video's, muziek, foto's of documenten.

Sommige browsers kunnen frauduleuze websites standaard identificeren. **Op elk toestel waarmee men online gaat, moet de meest recente versie geïnstalleerd zijn van de geprefereerde browser en personen moeten een opleiding krijgen met basistips om verdachte websites te identificeren, bv.:**

- Controleer op contactgegevens (adres, telefoonnummer en/of e-mail adres) die geverifieerd kunnen worden, evenals de aanwezigheid van een privacybeleid.
- Controleer de bestemming van hyperlinks door met de muis over de link te gaan en naar de linkerbenedenhoek van uw browser te kijken waar het echte adres van de website (meestal) wordt weergegeven.
- Controleer op 'https://' aan het begin van het webadres voor u persoonlijke informatie invoert.

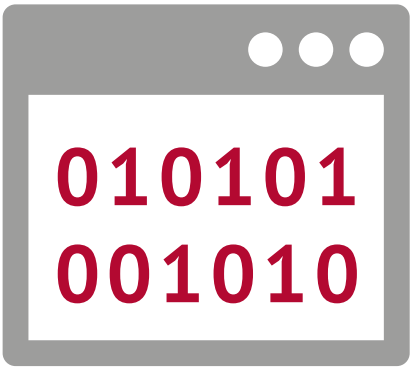
[3] http://nl.wikipedia.org/wiki/Phishing : Het oplichten van mensen door ze te lokken naar een valse (bank)website, die een kopie is van de echte website en ze daar — nietsvermoedend — te laten inloggen met hun inlognaam en wachtwoord of hun creditcard-nummer. Hierdoor krijgt de fraudeur de beschikking over deze gegevens

7.

— GEBRUIK STERKE WACHTWOORDEN EN BEWAAR ZE VEILIG —

Wachtwoorden zijn de belangrijkste manier om onze informatie te beschermen. Daarom is het van cruciaal belang dat u sterke wachtwoorden gebruikt. Om te garanderen dat wachtwoorden sterk zijn, moet u een aantal principes toepassen en opleggen:

- Gebruikers moeten beschikken over een eigen uniek user-ID en eigen wachtwoorden en mogen deze niet delen.
- Men moet een lengte en/of complexiteit voor wachtwoorden opleggen zodat anderen ze moeilijk kunnen raden, maar zodat de gebruiker ze toch gemakkelijk kan onthouden.
- Gebruikers moeten verplicht worden om hun wachtwoord periodiek te vervangen (om de 3 maanden is een goede praktijk).
- Gebruikers moeten verschillende wachtwoorden gebruiken voor verschillende toepassingen.
- Gebruikers mogen persoonlijke en professionele wachtwoorden niet door elkaar gebruiken.



Overweeg ook om meerdere authenticatiemethodes te gebruiken waarbij naast een wachtwoord ook bijkomende informatie nodig is om toegang te krijgen, vooral wanneer dergelijke toegang gepaard gaat met een verhoogd risico (bijvoorbeeld toegang vanop afstand).

Bij meervoudige authenticatie beslissen bedrijven om een combinatie van elementen te gebruiken, bv. *dingen die ik weet (zoals een wachtwoord of een pincode), dingen die ik bezit (zoals een smartcard of sms) en dingen die ik ben (zoals vingerafdruk of irisscan).* Bij de beslissing over welke combinaties ze zullen gebruiken, moeten bedrijven rekening houden met beperkingen opgelegd in de regelgeving en met de aanvaardbaarheid voor de medewerkers.

8.

— MAAK EN CONTROLEER BACK-UPKOPIEËN VAN BEDRIJFSGEGEVENS EN -INFORMATIE —

Net zo belangrijk als het beschermen van de vertrouwelijkheid en de integriteit van de gegevens, is het maken van back-ups ervan. Indien informatie wordt gestolen, gewijzigd, gewist of verloren gaat, is de beschikbaarheid van een back-up van cruciaal belang.

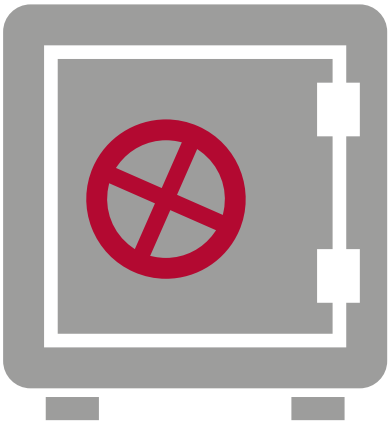
Een beleid moet worden geïmplementeerd waarin men bepaalt:

- van welke gegevens een back-up wordt gemaakt en hoe;
- hoe vaak een back-up wordt gemaakt van gegevens;
- wie verantwoordelijk is voor het maken van back-ups;
- waar en hoe de back-ups worden opgeslagen;
- wie toegang heeft tot deze back-ups.

Bij het nemen van deze beslissingen moet u zorgen dat de juridische en wettelijke voorschriften voor het bewaren van informatie begrepen zijn en nageleefd worden.

Tegelijkertijd moet u onthouden dat fysieke media zoals een schijf, tape of drive die worden gebruikt om back-ups van gegevens op te slaan, ook kwetsbaar zijn. Back-ups moeten dus hetzelfde niveau van bescherming krijgen als de brongegevens, vooral op het vlak van fysieke beveiliging, aangezien men deze items gemakkelijk kan verplaatsen.

Een van de belangrijkste problemen bij het beheer van back-ups is het valideren van de inhoud van de bedrijfsdata en de informatie in de back-upbestanden. Daarom moet u de discipline aankweken om de back-ups regelmatig terug te zetten om de doeltreffendheid, de volledigheid en de snelheid bij het terugzetten van de data te controleren. Indien derden worden ingezet voor het opslaan van informatie (zoals bij clouddiensten), moeten zij ervoor zorgen dat back-ups worden gemaakt van die informatie.



9.

— BESTRIJD VIRUSSEN EN ANDERE MALWARE VANUIT VERSCHILLENDE INVALSHOEKEN —

Omwille van de vele verschillende soorten toestellen en gebruikers met verschillende behoeften, vereist een doeltreffende bescherming tegen virussen, spyware en andere kwaadaardige software een gelaagde benadering om het bedrijf te beveiligen. Antivirussoftware is een must, maar dit mag niet de enige verdediging van het bedrijf zijn. Een combinatie van meerdere technieken om te beschermen tegen virussen is noodzakelijk om een doeltreffende beveiliging te garanderen.

Door het gebruik van webfiltering, antivirusbeveiliging, proactieve beveiliging tegen malware, firewalls, sterke wachtwoorden en opleiding van gebruikers te combineren, kan het risico op infecties sterk verminderd worden. Overweeg om verschillende merken van technologieën te gebruiken voor gelijkaardige functies (zoals verschillende leveranciers voor software die beschermt tegen malware). De veiligheidssoftware, het besturingssysteem en de toepassingen bijgewerkt houden, verhoogt de effectieve veiligheid van informatiesystemen.

10.

— VOORKOM, DETECTEER EN ONDERNEEM ACTIE —

Bedrijven zijn zich vaak niet bewust dat een incident rond informatieveiligheid heeft plaatsgevonden. Bedrijfssystemen worden aangevallen en geïnfecteerd maanden of jaren voor iemand dergelijk incident[4], ontdekt, als dit trouwens al gebeurt.

Bedrijven moeten investeren in een combinatie van informatiesystemen voor detectie en preventie. De kracht van de tools is recht evenredig met de kwaliteit van de implementatie en de opleiding van de gebruikers. Vraag ervaren partners om advies en ondersteuning wanneer uw bedrijf niet beschikt over deze kennis.

Professionals met een specifieke belangstelling voor cyberveiligheid hebben niet alleen baat bij technologie, maar mogelijk ook bij partnerschappen op verschillende niveaus, met sectoren, met de overheid of, op globaal niveau, met initiatieven zoals het World Economic Forum for Cyber Resilience.

Bedrijven moeten altijd ernstig overwegen om incidenten rond informatieveiligheid te melden aan het federale cyber emergency response team (CERT.be) via cert@cert.be.

Rapporteren aan CERT is van cruciaal belang om na te gaan of het al dan niet gaat om een geïsoleerd incident. Een aanval kan een horizontaal karakter (gericht op bedrijven uit dezelfde sector) of een verticaal karakter (gericht op onderaannemers) hebben of het kan gaan om een veiligheidsrisico voor een specifieke software of hardware. CERT kan informatie en advies over het incident verstrekken die het bedrijf als slachtoffer kan helpen om efficiënte tegenmaatregelen te treffen.

Organisaties die het slachtoffer zijn van (cyber)misdrijven moeten tevens een klacht indienen bij de politie. De lokale politie is hierin niet gespecialiseerd en fungeert eerder als contactpersoon voor traditionele misdrijven. Bij cybercrime (hacking, sabotage, spionage) is het beter om rechtstreeks contact op te nemen met de Federal Computer Crime Unit (FCCU), vooral indien het gaat om een aanval op kritieke IT-infrastructuur. Los daarvan kunt u ook contact opnemen met het openbaar ministerie. Bovendien helpt dit de ordehandhaving om een beter beeld te krijgen van de cyberdreigingen bij Belgische bedrijven.

Bij het afhandelen van veiligheidsincidenten, en vooral in geval van cybercriminaliteit, moeten de (IT-) verantwoordelijken van bij de aanvang het bewijsmateriaal vrijwaren. Richtlijnen voor het verzamelen van data bij veiligheidsincidenten[5] voor onderzoek door ICT-medewerkers of bij infecties met malware[6], zijn online beschikbaar op de website van CERT-EU.

[4] http://www.verizonenterprise.com/DBIR/2013/ -Verizon 2013 Data Breach Investigations Report
[5] http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_12_004_v1_3.pdf
[6] http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_11_003_v2.pdf

KORT EN KRACHTIG

VRAGENLIJST ZELFEVALUATIE INFORMATIEVEILIGHEID

Dit hoofdstuk bevat een eenvoudige controlelijst die de directie kan ondersteunen bij de interne evaluatie van de vaardigheden van het bedrijf op het vlak van cyberbescherming en haar kan helpen om de juiste vragen te stellen aan de teams die betrokken zijn bij deze initiatieven. De vragen die worden gesteld kunnen bijdragen tot de identificatie van sterke en zwakke punten en mogelijke verbeteringen binnen het eigen bedrijf.

Tegelijkertijd kunnen bedrijven die nog maar net starten met initiatieven voor informatieveiligheid deze vragenlijst voor zelfevaluatie gebruiken als een controlelijst en als basis voor het plannen van hun digitale weerbaarheid.

Voor elk van de onderstaande vragen moeten de bedrijven uit de weergegeven opties diegene kiezen die de huidige praktijken van het bedrijf het best weerspiegelt. Elke optie heeft een gekleurde stip met de volgende betekenis:

- ✘ Dit is het minst gunstige antwoord; u moet duidelijk verbeteringen overwegen.
- ● Bijkomende verbeteringen zijn mogelijk om het bedrijf beter te beveiligen.
- ✔ Dit antwoord weerspiegelt de beste bescherming tegen cyberdreigingen.

Onder elke vraag vindt u bovendien een specifieke controlelijst die u kan helpen om te identificeren en te documenteren wat de status van uw bedrijf is met betrekking tot de basisvaardigheden rond informatieveiligheid.

Bedrijven kunnen de principes en acties uit de twee vorige hoofdstukken gebruiken als leidraad om hun bescherming te verbeteren voor het onderwerp van elk van de vermelde vragen.

1. EVALUEERT U HOE GEVOELIG DE INFORMATIE IN UW BEDRIJF IS?

✘ Nee, maar we hebben een firewall om ons te beschermen tegen diefstal van informatie.

○ Ja, we beseffen hoe belangrijk onze informatie is en we nemen algemene veiligheidsmaatregelen.

✔ Ja en we beschikken ook over een classificatiemodel voor informatie en weten waar onze gevoelige informatie wordt opgeslagen en verwerkt. We nemen veiligheidsmaatregelen op basis van de gevoeligheid van de informatie.

De volgende 5 vragen zijn bedoeld als mogelijke basiscontroles op het informatieveiligheidsniveau van uw bedrijf.

	JA	NEE
Zijn uw gevoelige gegevens geïdentificeerd en geclassificeerd?		
Bent u zich bewust van uw verantwoordelijkheid met betrekking tot de geïdentificeerde gevoelige gegevens?		
Zijn de meest gevoelige gegevens extra beveiligd of versleuteld?		
Is het beheer van persoonlijke privégegevens onderhevig aan specifieke procedures?		
Zijn alle medewerkers in staat om gevoelige en niet-gevoelige data te identificeren en correct te beveiligen?		

PRINCIPE(S) VAN TOEPASSING

MOGELIJKE ACTIES OM UW AANPAK TE VERBETEREN

2. VOERT U RISICO-EVALUATIES UIT VOOR INFORMATIEVEILIGHEID?

✘ We voeren geen risico-evaluaties uit.

O We voeren risico-evaluaties uit, maar niet specifiek met het oog op informatieveiligheid.

✔ We voeren specifieke risico-evaluaties voor informatieveiligheid uit.

De volgende 5 vragen zijn bedoeld als mogelijke basiscontroles op het informatieveiligheidsniveau van uw bedrijf.

	Yes	No
Pakt u de resultaten over de kwetsbaarheid aan, te beginnen bij de hoge risico's, en vervolgens de lagere?		
Zijn gebeurtenissen die de bedrijfsprocessen kunnen onderbreken geïdentificeerd en werd de impact van de potentiële bijbehorende onderbrekingen ingeschat?		
Beschikt u over een recent plan voor bedrijfscontinuïteit dat werd getest en regelmatig wordt bijgewerkt?		
Voert u regelmatig een risico-evaluatie uit om het vereiste niveau van bescherming voor de data en de informatie aan te passen?		
Identificeert u de mogelijke risico's in uw bedrijfsprocessen om verstoringen bij de gegevensverwerking of opzettelijk misbruik te voorkomen?		

PRINCIPE(S) VAN TOEPASSING

MOGELIJKE ACTIES OM UW AANPAK TE VERBETEREN

3. OP WELK NIVEAU WORDT HET BEHEER VAN INFORMATIEVEILIGHEID TOEGEPAST?

✘ Er is geen beleid voor informatieveiligheid.

O Het beheer van de informatieveiligheid wordt toegepast binnen de ICT-afdeling aangezien de informatie daar moet worden beveiligd.

✔ Het beheer van informatieveiligheid wordt toegepast op bedrijfsniveau om een impact op het hele bedrijf te garanderen.

De volgende 5 vragen zijn bedoeld als mogelijke basiscontroles op het informatieveiligheidsniveau van uw bedrijf.

	JA	NEEN
Voorziet de raad van bestuur een budget voor informatieveiligheid?		
Maakt informatieveiligheid deel uit van het bestaande risicobeheerspraktijken van de bestuurders?		
Keurt de directie het beleid van het bedrijf rond informatieveiligheid goed en communiceert het dit op gepaste wijze aan de medewerkers?		
Worden de raad van bestuur en de directie regelmatig geïnformeerd over de laatste ontwikkelingen op het vlak van beleid, normen, procedures en richtlijnen rond informatieveiligheid?		
Maakt ten minste één kaderlid deel uit van de managementstructuur die verantwoordelijk is voor de beveiliging van gegevens en van de bescherming van persoonlijke informatie?		

PRINCIPE(S) VAN TOEPASSING

MOGELIJKE ACTIES OM UW AANPAK TE VERBETEREN

4. BESCHIKT UW BEDRIJF OVER EEN INFORMATIEVEILIGHEIDSTEAM OF EEN SPECIFIEKE INFORMATIEVEILIGHEIDSFUNCTIE?

✘ We hebben geen informatieveiligheidsteam of specifieke taken & verantwoordelijkheden met betrekking tot informatieveiligheid.

○ We hebben geen informatieveiligheidsteam, maar er werden wel specifieke taken en verantwoordelijkheden voor informatieveiligheid gedefinieerd binnen het bedrijf.

✔ We hebben een informatieveiligheidsteam of een specifieke informatieveiligheidsfunctie.

De volgende 5 vragen zijn bedoeld als mogelijke basiscontroles op het informatieveiligheidsniveau van uw bedrijf.

	JA	NEE
Is er een erkende informatieveiligheidsspecialist of een bevoegd team dat de kennis in het bedrijf coördineert en de directie assisteert bij het beslissingsproces?		
Is de aangeduide informatieveiligheidsspecialist of het bevoegde team verantwoordelijk voor het evalueren en systematisch bijwerken van het beleid rond informatieveiligheid gebaseerd op belangrijke veranderingen of incidenten?		
Heeft de aangeduide informatieveiligheidsspecialist of het bevoegde team voldoende zichtbaarheid en ondersteuning om te interveniëren bij elk initiatief rond informatie(veiligheid) binnen het bedrijf?		
Zijn verschillende managers verantwoordelijk voor verschillende soorten data?		
Worden de haalbaarheid en de doeltreffendheid van het beleid rond informatieveiligheid en de efficiëntie van het informatieveiligheidsteam regelmatig geëvalueerd door een onafhankelijk orgaan?		

PRINCIPE(S) VAN TOEPASSING

MOGELIJKE ACTIES OM UW AANPAK TE VERBETEREN

5. HOE BEHANDELT UW BEDRIJF DE RISICO'S VOOR INFORMATIEVEILIGHEID DIE GEPAARD GAAN MET LEVERANCIERS DIE TOEGANG HEBBEN TOT UW GEVOELIGE INFORMATIE?

✘ We hebben een relatie gebaseerd op wederzijds vertrouwen met onze leveranciers.

○ In sommige contracten nemen wij clausules over informatieveiligheid op.

✔ We beschikken over processen om de toegang voor leveranciers te valideren en de specifieke veiligheidsrichtlijnen worden gecommuniceerd aan en ondertekend door onze leveranciers.

De volgende 5 vragen zijn bedoeld als mogelijke basiscontroles op het informatieveiligheidsniveau van uw bedrijf.

	JA	NEE
Worden aannemers en leveranciers geïdentificeerd met een ID-badge met een recente foto?		
Beschikt u over beleidslijnen voor achtergrondcontroles voor aannemers en leveranciers?		
Wordt de toegang tot de gebouwen en informatiesystemen automatisch ingetrokken wanneer de opdracht van een aannemer of leverancier afloopt		
Weten leveranciers hoe en aan wie ze verlies of diefstal van informatie onmiddellijk moeten melden binnen uw bedrijf?		
Zorgt uw bedrijf ervoor dat leveranciers hun software en toepassingen bijwerken met beveiligingspatches?		

PRINCIPE(S) VAN TOEPASSING

MOGELIJKE ACTIES OM UW AANPAK TE VERBETEREN

6. EVALUEERT UW BEDRIJF REGELMATIG DE COMPUTER- EN NETWERKBEVEILIGING?

✘ We voeren geen audits of penetratietests uit om onze computer- en netwerkbeveiliging te evalueren.

o We voeren niet systematisch veiligheidsaudits en/of penetratietests uit, maar soms wel op ad hoc basis.

✔ Regelmatige veiligheidsaudits en/of penetratietests maken systematisch deel uit van onze evaluatie van onze computer- en netwerkbeveiliging.

De volgende 5 vragen zijn bedoeld als mogelijke basiscontroles op het informatieveiligheidsniveau van uw bedrijf.

	JA	NEE
Test u regelmatig en registreert u de geïdentificeerde dreigingen?		
Beschikt u over procedures om menselijke dreigingen voor uw informatiesystemen (bv. oneerlijkheid, social engineering en misbruik van vertrouwen) te evalueren?		
Vraagt uw bedrijf rapporten van veiligheidsaudits aan zijn aanbieders van informatiediensten?		
Wordt het nut van elk type opgeslagen gegevens ook geëvalueerd tijdens de veiligheidsaudits?		
Voert u een audit van uw informatieprocessen en -procedures uit met het oog op de naleving van de andere bestaande beleidslijnen en normen binnen het bedrijf?		

PRINCIPE(S) VAN TOEPASSING

MOGELIJKE ACTIES OM UW AANPAK TE VERBETEREN

7. EVALUEERT UW BEDRIJF POTENTIËLE INFORMATIEVEILIGHEIDSRISICO'S BIJ HET INTRODUCEREN VAN NIEUWE TECHNOLOGIEËN?

✘ Informatieveiligheid maakt geen deel uit van het proces voor het implementeren van nieuwe technologieën.

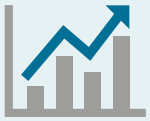
○ Informatieveiligheid wordt alleen ad hoc geïmplementeerd in het proces voor nieuwe technologieën.

✔ Informatieveiligheid maakt deel uit van het proces voor het implementeren van nieuwe technologieën.

De volgende 5 vragen zijn bedoeld als mogelijke basiscontroles op het informatieveiligheidsniveau van uw bedrijf.

	JA	NEE
Wanneer u overweegt om nieuwe technologieën te implementeren, evalueert u dan hun potentiële impact op het bestaande beleid voor informatieveiligheid?		
Neemt u beschermende maatregelen om het risico bij de implementatie van nieuwe technologieën te beperken?		
Zijn de processen voor het implementeren van nieuwe technologieën gedocumenteerd?		
Kan uw bedrijf bij de implementatie van nieuwe technologieën beroep doen op partnerschappen voor gezamenlijke inspanningen en voor het delen van kritieke beveiligingsinformatie?		
Wordt het informatieveiligheidsbeleid van uw bedrijf vaak gezien als een belemmering voor technologische opportuniteiten?		

PRINCIPE(S) VAN TOEPASSING



MOGELIJKE ACTIES OM UW AANPAK TE VERBETEREN

8. IS INFORMATIEVEILIGHEID AANWEZIG IN UW BEDRIJF?

✘ We vertrouwen onze medewerkers en zien geen toegevoegde waarde in begeleiding bij informatieveiligheid.

○ Alleen onze ICT-medewerkers krijgen een specifieke opleiding om onze ICT-omgeving te beveiligen.

✔ Er worden regelmatig bewustmakingssessies over informatieveiligheid georganiseerd voor alle medewerkers.

De volgende 5 vragen zijn bedoeld als mogelijke basiscontroles op het informatieveiligheidsniveau van uw bedrijf.

	JA	NEE
Zijn sommige bewustmakingssessies over informatieveiligheid aangepast aan de activiteiten van de medewerkers?		
Worden de medewerkers opgeleid om alert te zijn voor hiaten in de informatieveiligheid?		
Beschikt uw bedrijf over richtlijnen voor gebruikers om zwakke punten of bedreigingen bij de beveiliging van systemen of diensten te rapporteren?		
Weten medewerkers hoe ze gegevens van kredietkaarten en persoonsgegevens correct moeten beheren?		
Krijgen externe gebruikers (indien relevant) ook een gepaste opleiding over informatieveiligheid en regelmatige updates van de beleidslijnen en procedures binnen de organisatie?		

PRINCIPE(S) VAN TOEPASSING

MOGELIJKE ACTIES OM UW AANPAK TE VERBETEREN

9. HOE GEBRUIKT U WACHTWOORDEN BINNEN UW BEDRIJF?

✘ We delen wachtwoorden met andere collega's en/of er bestaat geen beleid met betrekking tot het veilige gebruik van wachtwoorden of het regelmatig aanpassen van wachtwoorden.

o Alle medewerkers en het management beschikken over unieke wachtwoorden, maar er worden geen regels opgelegd voor de complexiteit ervan. Het wijzigen van wachtwoorden gebeurt optioneel, maar is niet verplicht.

✔ Alle medewerkers, inclusief de directie, beschikken over een persoonlijk wachtwoord dat moet voldoen aan de gedefinieerde vereisten voor wachtwoorden en dat regelmatig moet worden gewijzigd.

De volgende 5 vragen zijn bedoeld als mogelijke basiscontroles op het informatieveiligheidsniveau van uw bedrijf.

	JA	NEE
Implementeerde uw bedrijf een algemeen aanvaard beleid rond wachtwoorden dat ook wordt afgedwongen?		
Kunt u garanderen dat alle wachtwoorden binnen uw bedrijf niet worden opgeslagen in gemakkelijk toegankelijke bestanden, slecht, blanco of standaard zijn of zelden worden gewijzigd, zelfs op mobiele apparaten?		
Voelt u zich goed beschermd tegen ongeoorloofde fysieke toegang tot systemen?		
Zijn gebruikers en aannemers zich bewust van hun verantwoordelijkheid om ook apparatuur die onbeheerd wordt achtergelaten te beveiligen (uitloggen)?		
Werden medewerkers opgeleid om social engineering te herkennen en te reageren op deze bedreiging?		

PRINCIPE(S) VAN TOEPASSING

MOGELIJKE ACTIES OM UW AANPAK TE VERBETEREN

10. BESTAAT ER EEN BEDRIJFSBELEID VOOR HET CORRECTE GEBRUIK VAN INTERNET EN SOCIALE MEDIA?

✘ Neen, we hebben geen beleid voor het correcte gebruik van het internet.

O Ja, we hebben een beleid dat op een centrale locatie toegankelijk is voor alle medewerkers, maar het werd niet ondertekend door de medewerkers.

✔ Ja, een beleid voor correct internetgebruik maakt deel uit van het contract / alle medewerkers hebben het beleid ondertekend.

De volgende 5 vragen zijn bedoeld als mogelijke basiscontroles op het informatieveiligheidsniveau van uw bedrijf.

	JA	NEE
Bestaan er binnen het bedrijf algemene communicatierichtlijnen en -processen voor medewerkers, ook over de relaties met de pers en de sociale media?		
Bestaat er een tuchtprocedure voor medewerkers die de communicatierichtlijnen van het bedrijf overtreden?		
Screent een specifieke communicatieverantwoordelijke of team het internet om de risico's en de status van de e-reputatie na te trekken?		
Heeft uw bedrijf zijn aansprakelijkheid geëvalueerd voor handelingen van medewerkers of andere interne gebruikers of aanvallers die het systeem gebruiken om misdrijven te plegen?		
Heeft uw bedrijf maatregelen genomen om te voorkomen dat een medewerker of andere interne gebruiker andere sites aanvalt?		

PRINCIPE(S) VAN TOEPASSING

MOGELIJKE ACTIES OM UW AANPAK TE VERBETEREN

11. MEET EN RAPPORTEERT UW BEDRIJF ASPECTEN VAN INFORMATIEVEILIGHEID EN VOLGT HET DEZE OP?

✘ We controleren en rapporteren de efficiëntie en de geschiktheid van onze geïmplementeerde veiligheidsmaatregelen niet en volgen deze niet op.

○ Ons bedrijf heeft instrumenten en methodes geïmplementeerd om de efficiëntie en de geschiktheid van een selectie van onze geïmplementeerde veiligheidsmaatregelen te controleren, te rapporteren en op te volgen.

✔ Ons bedrijf heeft instrumenten en methodes geïmplementeerd om de efficiëntie en de geschiktheid van al onze geïmplementeerde veiligheidsmaatregelen te controleren, te rapporteren en op te volgen.

De volgende 5 vragen zijn bedoeld als mogelijke basiscontroles op het informatieveiligheidsniveau van uw bedrijf.

	JA	NEE
Worden audittrajecten en logs over de incidenten bewaard en worden proactieve acties ondernomen zodat het incident zich niet opnieuw voordoet?		
Controleert uw bedrijf de naleving van wettelijke en reglementaire vereisten (bv. geheimhouding van data)?		
Heeft uw bedrijf eigen instrumenten ontwikkeld om het management bij te staan bij het evalueren van de beveiligingsstatus en om het bedrijf in staat te stellen potentiële risico's sneller te verkleinen?		
Beschikt uw bedrijf over een stappenplan voor informatieveiligheid inclusief doelstellingen, evaluatie van de vooruitgang en potentiële samenwerkingsmogelijkheden?		
Worden controlerapporten en incidenten gerapporteerd aan de autoriteiten en aan andere belangengroepen, zoals een sectorfederatie?		

PRINCIPE(S) VAN TOEPASSING

MOGELIJKE ACTIES OM UW AANPAK TE VERBETEREN

12. HOE WORDEN SYSTEMEN IN UW BEDRIJF BIJGEWERKT?

✘ We vertrouwen voor de meeste van onze oplossingen op het automatische patchbeheer dat wordt aangeboden door de verkoper.

○ Veiligheidspatches worden systematisch toegepast op maandelijkse basis.

✔ We beschikken over een procedure om de kwetsbaarheid te beheren en gaan voortdurend op zoek naar informatie over mogelijke kwetsbaarheden (bv. door een abonnement op een dienst die automatisch waarschuwingen verstuurt voor nieuwe kwetsbaarheden) en passen patches toe op basis van de risico's die zij verkleinen.

De volgende 5 vragen zijn bedoeld als mogelijke basiscontroles op het informatieveiligheidsniveau van uw bedrijf.

	JA	NEE
Is een kwetsbaarheidsscan een regelmatig geplande onderhoudstaak binnen het bedrijf?		
Worden toepassingen beoordeeld en getest na aanpassingen aan het besturingssysteem?		
Kunnen gebruikers zelf controleren op het bestaan van toepassingen waarvoor geen patches werden uitgevoerd?		
Zijn de gebruikers zich ervan bewust dat zij het besturingssysteem en de toepassingen, inclusief de beveiligingssoftware, van hun mobiele apparaten ook moeten bijwerken?		
Zijn de gebruikers opgeleid om een legitiem waarschuwingsmelding (waarbij toestemming wordt gevraagd voor een update) of een valse antivirusmelding te herkennen en om het veiligheidsteam correct te waarschuwen indien iets verkeerds of verdachts gebeurd is?		

PRINCIPE(S) VAN TOEPASSING

MOGELIJKE ACTIES OM UW AANPAK TE VERBETEREN

13. WORDEN DE TOEGANGSRECHTEN VAN GEBRUIKERS TOT TOEPASSINGEN EN SYSTEMEN REGELMATIG HERZIEN EN BEHEERD?

✗ De toegangsrechten tot toepassingen en systemen worden niet consequent ingetrokken of herzien.

○ De toegangsrechten tot toepassingen en systemen worden alleen ingetrokken wanneer een medewerker het bedrijf verlaat.

✓ Er werd een beleid voor toegangscontrole geïmplementeerd met regelmatige herzieningen van de toegekende toegangsrechten voor alle relevante bedrijfstoepassingen en ondersteunende systemen.

De volgende 5 vragen zijn bedoeld als mogelijke basiscontroles op het informatieveiligheidsniveau van uw bedrijf.

	JA	NEE
Wordt de toegang tot elektronische informatiesystemen en gebouwen beperkt door beleidslijnen en procedures?		
Past uw bedrijf een privacy beleid toe met vermelding van de informatie die het verzamelt (bv. over uw klanten: fysieke adressen, e-mailadressen, browserhistorieken enz.) en verwerkt?		
Vermelden de beleidslijnen en procedures de methodes die worden gebruikt voor de fysieke toegangscontrole tot beveiligde ruimtes (bv. deursloten, systemen voor toegangscontrole of videobewaking)?		
Wordt de toegang tot gebouwen en informatiesystemen automatisch ingetrokken wanneer medewerkers niet meer in dienst zijn?		
Worden gevoelige data geclassificeerd (uiterst vertrouwelijk, gevoelig, uitsluitend voor intern gebruik, …) en wordt een inventaris van de toegestane gebruikers opgesteld?		

PRINCIPE(S) VAN TOEPASSING

MOGELIJKE ACTIES OM UW AANPAK TE VERBETEREN

14. MOGEN DE MEDEWERKERS VAN UW BEDRIJF HUN EIGEN PERSOONLIJKE TOESTELLEN, ZOALS MOBIELE TELEFOONS EN TABLETS, GEBRUIKEN OM BEDRIJFSINFORMATIE OP TE SLAAN OF OVER TE DRAGEN?

✘ Ja, we mogen bedrijfsinformatie opslaan op of overdragen naar persoonlijke toestellen zonder extra veiligheidsmaatregelen te implementeren.

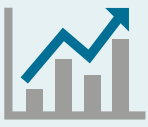
○ Er bestaat een beleid dat het gebruik van persoonlijke toestellen om bedrijfsinformatie op te slaan of over te dragen verbiedt, maar technisch gezien is het mogelijk om dit toch te doen zonder extra veiligheidsmaatregelen te implementeren.

✔ Bedrijfsinformatie mag alleen worden opgeslagen op of overgedragen naar persoonlijke toestellen nadat veiligheidsmaatregelen werden geïmplementeerd op het toestel en/of nadat een professionele oplossing werd voorzien.

De volgende 5 vragen zijn bedoeld als mogelijke basiscontroles op het informatieveiligheidsniveau van uw bedrijf.

	JA	NEE
Past uw bedrijf een algemeen aanvaard “Bring Your Own Device” (BYOD) beleid toe?		
Zijn mobiele toestellen beveiligd tegen ongerechtigde gebruikers?		
Worden alle toestellen en verbindingen permanent geïdentificeerd op het netwerk?		
Is encryptie geïnstalleerd op alle mobiele toestellen om de vertrouwelijkheid en de integriteit van de data te beschermen?		
Is men er zich in het hele bedrijf van bewust dat ook als de individuele gebruiker aansprakelijk is voor een toestel, het bedrijf nog altijd aansprakelijk is voor de data?		

PRINCIPE(S) VAN TOEPASSING



MOGELIJKE ACTIES OM UW AANPAK TE VERBETEREN

15. HEEFT UW BEDRIJF MAATREGELEN GENOMEN OM VERLIES VAN OPGESLAGEN INFORMATIE TE VOORKOMEN?

✘ We hebben geen back-up / beschikbaarheidsprocedure geïmplementeerd.

○ We hebben een back-up / beschikbaarheidsprocedure geïmplementeerd, maar er werden geen hersteltests uitgevoerd.

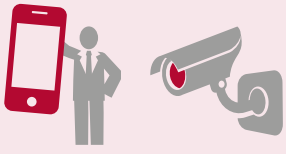
✔ We hebben een back-up / beschikbaarheidsprocedure geïmplementeerd die herstel / weerbaarheidstests omvat. We hebben back-upkopieën opgeslagen op een andere beveiligde locatie of gebruiken andere oplossingen met hoge beschikbaarheid.

De volgende 5 vragen zijn bedoeld als mogelijke basiscontroles op het informatieveiligheidsniveau van uw bedrijf.

	JA	NEE
Zijn voldoende personeelsleden in staat om een opvraagbare back-up- en archiefkopieën te creëren?		
Is de apparatuur beveiligd tegen stroompannes door een permanente stroomvoorziening, zoals multiple feeds, noodstroomvoeding (ups), noodgenerator enz.?		
Worden de back-upmedia regelmatig getest om te garanderen dat zij kunnen worden hersteld binnen de tijdsspanne vermeld in de herstelprocedure?		
Past uw bedrijf rapporteringsprocedures voor verloren of gestolen mobiele apparatuur toe?		
Krijgen medewerkers een opleiding over wat ze moeten doen wanneer informatie per ongeluk wordt gewist en hoe ze informatie kunnen herstellen bij rampen?		

PRINCIPE(S) VAN TOEPASSING

MOGELIJKE ACTIES OM UW AANPAK TE VERBETEREN



16. IS UW BEDRIJF VOORBEREID OM INFORMATIE-VEILIGHEIDSINCIDENTEN TE BEHANDELEN?

✘ We zullen dergelijke incidenten niet meemaken. Indien dit toch gebeurt, zijn onze medewerkers voldoende competent om ze te behandelen.

O We beschikken over procedures voor incidentbeheer, maar die zijn niet aangepast om informatieveiligheidsincidenten te behandelen.

✔ We beschikken over een specifieke procedure om informatieveiligheidsincidenten te behandelen. Deze procedure is voorzien van de nodige escalatie- en communicatiemechanismen. We streven ernaar om incidenten zo efficiënt en doeltreffend mogelijk af te handelen zodat we leren hoe we ons in de toekomst beter kunnen beveiligen.

De volgende 5 vragen zijn bedoeld als mogelijke basiscontroles op het informatieveiligheidsniveau van uw bedrijf.

	JA	NEE
Behandelt uw procedure verschillende soorten incidenten, gaande van DDoS (Distributed Denial of Service) tot inbreuken op de vertrouwelijkheid, enz., evenals manieren om deze af te handelen?		
Beschikt uw bedrijf over een plan aangaande de communicatie over incidentbeheer?		
Weet u welke autoriteiten u moet verwittigen in geval van incidenten alsook de wijze waarop dit dient te gebeuren?		
Heeft uw bedrijf contactinformatie uitgesplitst en geïdentificeerd voor elk soort incident?		
Doet u beroep op een interne communicatieverantwoordelijke voor contacten met medewerkers en hun families?		

PRINCIPE(S) VAN TOEPASSING

MOGELIJKE ACTIES OM UW AANPAK TE VERBETEREN

CASUSSEN

CASUSSEN OVER INFORMATIEVEILIGHEID

Voor elke casus wordt beschreven hoe een bedrijf een aantal van de eerder vermelde principes en acties al dan niet toepast. Hieruit blijkt dat de principes en acties onafhankelijk zijn van de grootte en de complexiteit van een organisatie.

1.

— GROOT NATIONAAL BEDRIJF (INDUSTRIE) DAT INTERNATIONAAL OPEREERT —

Het bedrijf is gespecialiseerd in de vormgeving en het slijpen van componenten voor machines. Het is in grote mate afhankelijk van gespecialiseerde computers in de productieomgeving. In de productiehal staan slechts een paar desktop computers, die rechtstreeks zijn aangesloten op het intranet van het bedrijf, dat voornamelijk wordt gebruikt voor administratieve doeleinden. Het onderhoudsteam van het bedrijf begon desktops te gebruiken als een efficiëntere manier om programma-updates over te dragen naar de productieomgeving. Tijdens de pauzes gebruiken de onderhoudsmedewerkers diezelfde desktops echter ook om op het internet te surfen, spelletjes te spelen en hun sociale netwerken bij te werken. Zoals te verwachten was, werd één van deze toestellen besmet met kwaadaardige spyware. De spyware verstuurde vanaf de desktop gegevens over de activiteiten van de desktop computer naar de vijandige host. De spyware downloadde ook bijkomende malware, waaronder een tijdsgevoelig mechanisme dat het opstarten van de besmette toestellen blokkeerde, behalve indien een code werd ingevoerd.

Het onderhoudsteam ging door met zijn dagelijkse activiteiten en werkte de productiemachines bij, waardoor de malware zich verspreidde naar de hele operationele omgeving van de organisatie. Na een week startten drie gespecialiseerde computers in de productieafdeling niet meer op, net als alle geïnfecteerde desktops in de productiehal.

Een gespecialiseerde veiligheidsexpert werd ingehuurd om de desktop computers te onderzoeken. Hij ontdekte een hele reeks malware en ransomware toepassingen die “achter de schermen” actief waren. In de spyware was een keylogger ingebouwd die alle toetsaanslagen van de gebruiker van de computer registreerde en bewaarde. Op deze manier waren cybercriminelen erin geslaagd om toegang te krijgen tot het systeem om de elektronische tijdbom te installeren. Op de computer werd een internet security package met antivirus en antispyware correct geïnstalleerd. Men ontdekte echter dat de automatische updates niet geactiveerd waren en dat scans niet stelselmatig werden uitgevoerd om de doeltreffendheid van de beveiliging te controleren. Als gevolg hiervan kon de infectie zich niet verder verspreiden dan de productiehal en de besmette toestellen.

Op de geïnfecteerde desktops verscheen een boodschap waarin het bedrijf werd gevraagd om een bedrag over te schrijven naar een specifieke bankrekening om een speciale digitale code te verkrijgen om het mechanisme te deblokkeren. Omwille van het feit dat de productiecapaciteit aanzienlijk verminderd was, dat het geëiste losgeld slechts beperkt was en veel lager lag dan de kost om reservesystemen te installeren, besloot de directie om de gevraagde bedragen over te schrijven. Onmiddellijk na dit miniproject werden de computers volledig gereinigd door de veiligheidsexpert en werden ze opnieuw geïnstalleerd voor operationeel gebruik.

Het bedrijf besliste om geen verdere juridische acties te ondernemen en om de zaak niet te melden aan de politie. De directie besliste echter wel om de interne beleidslijnen over informatieveiligheid ook uit te leggen aan de mensen in de productieafdeling. Het bedrijf meldde dit specifieke incident aan zijn partners, leveranciers en concurrenten en legde de basis voor een vertrouwensrelatie met deze partners om regelmatig informatie uit te wisselen over gelijkaardige incidenten.

2.

— MIDDELGROTE RETAILER DIE ONLINE ACTIEF IS —

Dit bedrijf is een grote internationale retailer met vestigingen in België en daarbuiten. Het bedrijf heeft meer dan 6 miljoen klanten in Europa en de klanten hebben hun eigen profiel met persoonlijke gegevens aangemaakt. De retailer slaat ook data op over voorkeuren van gebruikers, historische gegevens en interesses. Om de gevoelige data te beschermen tegen hackers en malware, besliste het bedrijf om al zijn websites te beschermen. Het bedrijf werkt dagelijks om zijn producten in stand te houden en op de markt te brengen, zijn klanten te bedienen en manieren te zoeken om de functionaliteiten voortdurend te verbeteren en extra diensten aan te bieden.

De operationele website verwerkt dagelijks duizenden transacties en gebruikt verschillende merken van technologie om al deze transacties correct te beheren. Het bedrijf maakt gebruik van fraude detectie mechanismen om (potentiële) frauduleuze transacties op te sporen en voert tests op de onderliggende technologieën uit op basis van gekende kwetsbaarheden. Wanneer risico's worden gedetecteerd, worden deze automatisch en onmiddellijk gemeld. Een gespecialiseerd team van ontwikkelaars, veiligheidsexperts en vertegenwoordigers van het bedrijf vergadert regelmatig om potentiële risico's te bespreken en om te controleren of kwetsbaarheden effectief werden weggewerkt door de gepaste maatregelen te treffen.

Omwille van de aard van zijn activiteiten en de risico's die het loopt op zijn websites, besliste het bedrijf om onderdelen van zijn procedure voor veiligheidsbeheer te automatiseren. Het bedrijf besliste ook om bijkomende programmatie voortdurend te herbekijken door de code te laten beoordelen door derden en om voldoende tests te garanderen, zelfs nadat de functionaliteiten werden gepubliceerd. De infrastructuur wordt regelmatig aangepast in overeenstemming met de voortdurend veranderende vereisten en noden en om flexibel te blijven binnen de eigen markt. Op de systemen moet bijna dagelijks een patch worden uitgevoerd. Het bedrijf laat ook een externe scan van zijn infrastructuur uitvoeren, waarbij wordt gerapporteerd over bestaande en potentiële kwetsbaarheden.

Het bedrijf wordt constant geconfronteerd met meerdere pogingen van hackers en legitieme gebruikers die proberen om toegang te verkrijgen tot persoonlijke gegevens of andere gevoelige informatie. Het bedrijf beseft dat het, omwille van de aard van zijn activiteiten, op een dag het slachtoffer zal worden van hackers en heeft zijn directie en zijn procedures voorbereid om de risico's en mededelingen dienovereenkomstig aan te passen.

3.

— KMO ACTIEF IN BOEKHOUDINGSDIENSTEN —

Dit is een klein familiebedrijf actief in boekhoudingsdiensten met als klanten een lijst van reeds lang bestaande KMO's en heel grote bedrijven. In 2012 werd het bedrijf het slachtoffer van een reeks aanvallen met malware, combinaties van virussen en Trojaanse paarden, die zich verspreidden via gratis downloadbare software. Het virus besmette bestanden waardoor deze onbruikbaar werden. Het virus richtte zich vooral op Microsoft Word documenten en Excel spreadsheets. Voor een bedrijf dat vertrouwt op het Microsoft Office pakket is het virus uiterst schadelijk. Het virus schakelt de beveiligingsfuncties van de geïnstalleerde antivirussoftware uit, waardoor de weg vrij is voor infecties door andere virussen.

Men ontdekte dat het virus zich verspreidde via een gratis downloadbare software, Defense Center, die eigenlijk was bedoeld om de gebruiker te beschermen tegen kwaadaardige bedreigingen.

De software was afkomstig van een internetwebsite en begon de lokale apparatuur te besmetten zodra deze werd geïnstalleerd door de medewerker. De kwaadaardige software installeerde een bepaalde code (een zogenaamd "Trojaans paard") die de auteurs van de malware toelaat om de apparatuur rechtstreeks te hacken zodra de kwaadaardige software een kennisgeving met alle relevante gegevens over hoe de verbinding moet worden gelegd heeft verstuurd naar alle moedersystemen. Telkens een gebruiker een MS Officedocument opende, besmette de malware de documenten en verspreidde het virus zich verder via de e-mailcontacten van het bedrijf.

De ontvangers hadden de normale reflex om bijlagen afkomstig van een persoon die zij vertrouwen te openen. Alleen de partners die beschikten over recent bijgewerkte mechanismen tegen malware konden de malware in de bijlagen opsporen. Gelukkig contacteerde het bedrijf de ontvangers om verdere schade te voorkomen.

De malware verspreidde zich zo snel via het netwerk naar ander computers in het bedrijf dat alle computers, zonder enige uitzondering, werden besmet. De kwaadaardige software vernietigde alle .xls (spreadsheet) en .doc (word document) bestanden die waren opgeslagen op de harde schijven en verving ze door de tekst "DATAError".

Het verlies van klantgegevens kon mogelijk leiden tot een volledige storing van het bedrijf en zelfs tot een faillissement. Gelukkig beschikte het bedrijf over een doeltreffend back-upsysteem. Op het einde van elke week werden alle data van alle computers van medewerkers via het netwerk verzameld en werden ze gekopieerd op een nieuwe dvd, vervolgens correct gedateerd en veilig bewaard buiten de vestiging. Hoewel alle gegevens van elke computer verloren waren gegaan, konden ze toch worden hersteld dankzij de back-up dvd's. Het bedrijf slaagde erin de meeste bestanden te herstellen met de back-ups, maar verloor toch drie volledige dagen werk na de meest recente back-up.

De besmette e-mailberichten omzeilden de netwerk-beveiliging aangezien ze werden gedownload door een vertrouwde gebruiker, achter de firewall. De gevolgen vestigden de aandacht op de nood aan een goede opleiding voor medewerkers over hoe om te gaan met internetbronnen en aan een evaluatie van de beschermingsprocedure om regelmatig en met een hogere frequentie audits uit te voeren om te garanderen dat de bestanden konden worden hersteld.

4.

— BELGISCHE START-UP —

Dit jonge bedrijf is een volledig geautomatiseerde demand response aggregator die netbeheerders flexibele hoeveelheden stroom aanbiedt, die een oplossing kunnen bieden wanneer een extreem hoge vraag naar stroom de stabiliteit van het elektriciteitsnet in gevaar brengt. Het bedrijf neemt deze stroom af van industriële stroomverbruikers die hun industriële processen kort kunnen verminderen zonder negatieve impact op hun output. Het eigen technologieplatform van de start-up maakt een volledig geautomatiseerde dienstverlening mogelijk.

De nood aan informatieveiligheid

De nood aan informatieveiligheid bij de start-up steunt op twee cruciale elementen:

1. **Technologische koppeling aan missiekritische systemen.** Het technologieplatform is verbonden met controlecentra van netbeheerders en met automatiseringssystemen van nutsbedrijven en industriële bedrijven, die beide bekend staan als enkele van de meest missiekritische en gevoelige doelen van cyberaanvallen. Veiligheidsinbreuken zouden de reputatie en de bedrijfsvooruitzichten van de start-up ernstig schaden.
2. **Gevoelige geheime informatie.** Als start-up actief in de technologiesector onderscheidt het bedrijf zich vooral door zijn eigendomstechnologie. Daarom moet het deze informatie zorgvuldig beschermen tegen concurrenten en andere externe partijen.

Bewustmaking van de directie en de medewerkers

- De raad van bestuur heeft meermaals gewezen op de noodzaak om de nadruk te leggen op beveiliging, om de directie aan te moedigen om duidelijke beleidslijnen te definiëren en om handelsgeheimen en intellectuele eigendommen te beschermen.
- Behandeling van vertrouwelijke informatie: principes en procedures worden gedefinieerd en meegedeeld.
- Het R&D team van het bedrijf leeft gepaste richtlijnen na over sterke authenticatie, wachtwoordencryptie en focus op beveiliging in elke fase van het ontwikkelingsproces.

Hoofdpunten van het actieprogramma van de start-up om informatieveiligheid te implementeren

Huidige benadering:

1. Technische maatregelen:
   a. Het technologieplatform wordt beheert in datacentra waarin geavanceerde beveiligingsmaatregelen werden geïmplementeerd.
   b. De kritische klanten zijn verbonden via een eigen netwerk, andere klanten via IPsec tunnels, waarbij strenge regels voor firewalls worden toegepast.
   c. De toegangscontrole tot het technologieplatform gebeurt via een combinatie van hardware sleutels en strikt beheerde sterke wachtwoorden.
2. Organisatorische maatregelen: alle documenten worden gemarkeerd volgens een vertrouwelijkheidniveau dat wordt geïmplementeerd op basis van ‘need to know’ .
3. Procedurele maatregelen: er worden verschillende goedkeuringsniveaus voor het technologieplatform gedefinieerd per gebruikersgroep. De specifieke uitdaging voor een klein bedrijf zoals deze start-up is dat het zich geen eigen specifieke veiligheidsmedewerkers kan veroorloven. Daarom werd in 2013 een externe audit gevraagd om een structurele beoordeling en risicoevaluatie van het beveiligingsniveau van de start-up uit te voeren.

Middellange focus:

1. Een specialist in energieveiligheid zal een volledige gap- en risicoanalyse op het vlak van informatieveiligheid uitvoeren;
2. De start-up zal een heel jaar lang tijd en inspanningen investeren om zich voor te bereiden op deze certificatie, met de nadruk op de implementatie van procedures, de bewustmaking en het ontwikkelen van een duurzaam model om de informatieveiligheid te evalueren;
3. ISO 2700X: de start-up streeft ernaar om het ISO 27001 certificaat te behalen in 2014, als een proactieve stap om uit te groeien tot een meer cyberbeveiligde onderneming.

CONTACTGEGEVENS EN OVERZICHT VAN DE MEEST GEBRUIKELIJKE RAAMWERKEN VOOR CYBER- EN INFORMATIEVEILIGHEID

INFORMATIEVEILIGHEID IN BELGIË – CONTACTGEGEVENS

Alle contactgegevens zijn bijgewerkt te vinden op **www.b-ccentre.be.**
The contact list is split between the public bodies and organisations on one side, and some private not-for-profit organisations on the other. The description of the information security role of each selected organisation, in both categories, has been most the time provided by the organisation itself. When you need more information on the information security services provided by a commercial firm, we invite you to consult the firm's website, as for example **www.ey.com/BE/** or **www.microsoft.com/belux/**.

NAAM	CONTACTGEGEVENS	FUNCTIE IN DE INFORMATIEVEILIGHEID
OVERHEIDSINSTELLINGEN EN ORGANISATIES		
B-CCENTRE	**www.b-ccentre.be** **Belgian Cybercrime Centre of Excellence for Training, Research and Education** Sint-Michielsstraat 6, bus 3443 3000 Leuven België +32 16 32 07 82 contact@b-ccentre.be	Het Belgian Cybercrime Centre of Excellence for Training, Research and Education (B-CCENTRE) is een grootschalige overkoepelende joint-venture tegen cybercriminaliteit in België gecoördineerd door het Interdisciplinair Centrum voor Recht en Informatica van de KU Leuven. B-CCENTRE is het belangrijkste platform voor samenwerking en coördinatie op het vlak van problemen met cybercriminaliteit in België. Het combineert expertise van academische onderzoeksgroepen, industriële spelers en overheidsorganen tot een groot kennisnetwerk. Tot de belangrijkste activiteiten behoren interdisciplinair fundamenteel onderzoek, het organiseren van opleidingen en bewustmaking door vorming.
BIPT	**www.bipt.be** **Belgisch Instituut voor Postdiensten en Telecommunicatie** Ellipse Building - Gebouw C Koning Albert II laan 35 1030 Brussel België netsec@bipt.be	Het Belgisch Instituut voor Postdiensten en Telecommunicatie (BIPT) superviseert zowel de postdiensten als de telecommunicatiesector, nu de "elektronische communicatie" genoemd. Het BIPT staat in voor de economische regulering, de technische organisatie en de naleving van het regelgevend kader. BIPT is betrokken bij de veiligheid van openbare netwerken en van publiek toegankelijke elektronische communicatiediensten.

NAAM	CONTACTGEGEVENS	FUNCTIE IN DE INFORMATIEVEILIGHEID
OVERHEIDSINSTELLINGEN EN ORGANISATIES		
CERT.be	**www.cert.be** **Federal Cyber Emergency Team** Louizalaan 231 1050 Brussel België +32 2 790 33 33 cert@cert.be	CERT.be is het belangrijkste Belgische contactpunt voor het aanpakken van cyberdreigingen en kwetsbaarheden die de Belgische belangen schaden. ICT professionals kunnen gratis en volledig vertrouwelijk terecht op CERT.be om cyberincidenten (gehackte data en netwerkinfrastructuren, phishing, cyberaanvallen enz.) te melden. CERT.be geeft burgers en bedrijven ook advies over het veilige gebruik van het internet. Meer informatie vindt u op www.cert.be (voor bedrijven) en www.safeonweb.be (voor particulieren).
CRID	**www.unamur.be/droit/crid** **Centre de Recherche Informatique et Droit** Rue de Bruxelles 61 5000 Namur België +32 81 72 40 00	Het CRID werd in 1979 opgericht om verbeteringen uit te werken op het vlak van informatica en recht. Het CRID was betrokken bij heel wat onderzoeksprojecten over cyberveiligheid en publiceerde diverse witboeken over dit onderwerp.
ENISA	**www.enisa.europa.eu** **http://cybersecuritymonth.eu/** **Europees Agentschap voor Netwerk- en Informatieveiligheid (European Network & Information Security Agency)** Science and Technology Park of Crete Vassilika Vouton, 700 13 Heraklion Griekenland +30 28 14 40 9710 info@enisa.europa.eu	Het Europees Agentschap voor Netwerk- en Informatieveiligheid (ENISA) is het antwoord van de EU op de problemen van de Europese Unie op het vlak van cyberveiligheid. Als dusdanig is het de gangmaker voor de informatieveiligheid in Europa en een expertisecentrum. Het doel is de ENISA website te laten uitgroeien tot de Europese 'hub' voor de uitwisseling van informatie, beste praktijken en kennis op het vlak van informatieveiligheid.
FCCU	**www.polfed-fedpol.be/crim/crim_fccu_nl.php** **Federal Computer Crime Unit** Notelaarstraat 211 1000 Brussel België +32 2 743 74 74	De Belgian Federal Computer Crime Unit (FCCU) is verantwoordelijk voor het bestrijden van ICT- en cybercriminaliteit, met als doel alle burgers in de cyberwereld te beschermen tegen alle vormen van "traditionele" en "nieuwe" misdrijven. Deze opdracht omvat ook: het bestrijden van andere criminele fenomenen in de IT-omgeving met gespecialiseerde onderzoeksondersteuning. Ook telecommunicatiefraude en fraude met betaalkaarten behoren tot de bevoegdheden.

NAAM	CONTACTGEGEVENS	FUNCTIE IN DE INFORMATIEVEILIGHEID
OVERHEIDSINSTELLINGEN EN ORGANISATIES		
FEDICT	**www.fedict.belgium.be** **Federale Overheidsdienst voor Informatie en Communicatietechnologie** Maria-Theresiastraat 1 1000 Brussel België +32 2 212 96 00 info@fedict.belgium.be	Fedict heeft diverse bewustmakingscampagnes over internetbeveiliging gelanceerd en adviseert heel wat Belgische overheidsdiensten over informatieveiligheid.
ICRI	**www.law.kuleuven.be/icri** **Interdisciplinair Centrum voor Recht en Informatica** Sint-Michielsstraat 6, bus 3443 3000 Leuven België +32 16 32 07 90 adminicri@law.kuleuven.be	Het Interdisciplinair Centrum voor Recht en Informatica (ICRI) is een onderzoekscentrum aan de Faculteit Rechtsgeleerdheid van de KU Leuven. Het werkte mee aan heel wat onderzoeksprojecten over informatieveiligheid en publiceerde diverse witboeken over dit onderwerp. Het ICRI coördineert de activiteiten van B-CCENTRE.
NATIONALE BANK VAN BELGIË	**www.nbb.be** **Nationale Bank van België** de Berlaimontlaan 14 1000 Brussel België +32 2 221 21 11 info@nbb.be Specifieke operationele functies op het vlak van prudentieel toezicht tf@nbb.be	De Nationale Bank van België publiceerde gedetailleerde richtlijnen over informatieveiligheid voor alle financiële instellingen.
PRIVACY-COMMISSIE	**www.privacycommission.be** **Commissie voor de Bescherming van de Persoonlijke Levenssfeer** Drukpersstraat 35 1000 Brussel België +32 2 274 48 78 commission@privacycommission.be	De kerntaak van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer is garanderen dat de privacy wordt gerespecteerd bij de verwerking van persoonsgegevens. Het is een Belgische federale instantie, die sinds december 2009 nauw samenwerkt met de Vlaamse Toezichtcommissie voor het Elektronische Bestuurlijke Gegevensverkeer. De Commissie voor de Bescherming van de Persoonlijke Levenssfeer publiceerde duidelijke richtlijnen over de correcte aanpak van privacy incidenten in de cyberwereld.
STAATS-VEILIGHEID	**justitie.belgium.be/nl/overheidsdienst_justitie/organisatie/onafhankelijke_diensten_en_commissies/veiligheid_van_de_staat/** +32 2 205 62 11 info@vsse.be	Eén van de taken van de Staatsveiligheid, officieel de 'Veiligheid van de Staat', de burgerlijke geheime dienst van België, is het beschermen van de fundamentele waarden en belangen van de Staat. De Staatsveiligheid staat Belgische bedrijven bij om zich te beschermen tegen cyberaanvallen.

NAAM	CONTACTGEGEVENS	FUNCTIE IN DE INFORMATIEVEILIGHEID
PRIVÉORGANISATIES		
AGORIA	**www.agoria.be** **Agoria** Diamant Building A. Reyerslaan 80 1030 Brussel België +32 2 706 78 00 Ferdinand.CASIER@agoria.be	Agoria, de Belgische federatie voor de technologische industrie, ondersteunt de 1.700 bedrijven die lid zijn in de strijd tegen cybercriminaliteit met regelmatige evenementen en workshops. De verstrekte informatie is meestal gericht op de CEO's die aspecten van cyberveiligheid willen integreren in hun bedrijfsstrategie.
BELTUG	**www.beltug.be** **Belgian Telecom User Group** Knaptandstraat 123 9100 Sint Niklaas België +32 3 778 17 83 Info@beltug.be	BELTUG omvat een speciale belangengroep voor beveiliging, waar de leden samenkomen om alle onderwerpen te bespreken die te maken hebben met IT-beveiliging. BELTUG organiseerde heel wat rondetafelgesprekken en publiceerde diverse witboeken over informatieveiligheid.
FEBELFIN	**www.febelfin.be** **FEBELFIN** Aarlenstraat 82 1040 Brussel België +32 (0)2 507 68 11 info@febelfin.be	Febelfin, de overkoepelende federatie voor de Belgische financiële sector, ondersteunt haar 268 leden in de strijd tegen cybercriminaliteit door informatie te delen en samen te werken met alle belanghebbenden. Febelfin onderhoudt een speciale website www.safeinternetbanking.be en lanceerde diverse bewustmakingscampagnes over veilig internetbankieren met een aantal provocerende video's.
ICC BELGIUM	**www.iccbelgium.be** **Belgian Committee of the International Chamber of Commerce** Stuiversstraat 8 1000 Brussel België +32 (0)2 515 08 44 info@iccwbo.be	De International Chamber of Commerce (ICC) is de grootste handelsorganisatie ter wereld. De wereldwijde ICC Commission on Digital Economy organiseert discussies over cybercriminaliteit en over de mogelijke ontwikkeling van ICC-richtlijnen voor juridische problemen van bedrijven wereldwijd. Daarnaast bestrijdt ICC via zijn eigen misdaadbestrijdingsafdeling (Commercial Crime Services) gevestigd in het Verenigd Koninkrijk, beleidsorganen en andere initiatieven, alle vormen van criminaliteit waarmee bedrijven te maken hebben, inclusief cybercriminaliteit.

NAAM	CONTACTGEGEVENS	FUNCTIE IN DE INFORMATIEVEILIGHEID
PRIVÉORGANISATIES		
ISACA	**www.isaca.be** **ISACA Belgium** Koningsstraat 109-111 b.5 1000 Brussel België +32 2 219 24 82 president@isaca.be	ISACA is een internationale kennisorganisatie zonder winstoogmerk met meer dan 110.000 individuele leden in 160 landen, die onderzoek doet naar waarden en vertrouwen op het vlak van informatie en technologie, inclusief informatie en informatieveiligheid. ISACA faciliteert en valideert vaardigheden en kennis via de Certified Information Security Manager (CISM) en Certified in Risk and Information Systems Control (CRISC) certificeringen. ISACA creëerde COBIT for Information Security, een omkadering die bedrijven in alle sectoren en geografische gebieden helpt om hun informatieveiligheid te beheren en bij te sturen. ISACA beschikt over een grote verzameling witboeken, enquêtes en auditprogramma's over informatieveiligheid.
ISPA	**www.ispa.be** Montoyerstraat 39 b 3 1000 Brussel België +32 2 503 22 65 info@ispa.be	ISPA Belgium is de vereniging van Internet Service Providers die actief zijn in België. Door niet alleen access en service providers, maar ook hosting en transit providers samen te brengen, zorgt ISPA ervoor dat het potentieel van het internet voor de consumenten en bedrijven in België ten volle kan worden benut. ISPA organiseert workshops en evenementen over cyberveiligheid en is actief in heel wat projecten die bijdragen tot een veiliger gebruik van het internet in België.

NAME	CONTACT DETAILS	INFORMATION SECURITY ROLE
PRIVÉORGANISATIES		
L-SEC	**www.lsec.be** **Leaders in Security** Kasteelpark 10 3001 Heverlee België +32 16 32 85 41 Info@lsec.be	LSEC is een Europese vereniging zonder winstoogmerk, gevestigd in België en al meer dan 10 jaar actief in bewustmaking en opleiding over informatieveiligheid. De vereniging brengt experten uit de ICT-beveiliging, onderzoekers over ICT-beveiliging en eindgebruikers samen om actief samen te werken in projecten om de algemene cyberveiligheid in Europa te verbeteren. Via de leiderschapsactiviteiten die LSEC maandelijks organiseert, informeert de organisatie bedrijfsleiders, beveiligingsmanagers en beveiligingsexperten over de aanhoudende uitdagingen, de beste praktijken en vernieuwende benaderingen op het vlak van cyberveiligheid en informatieveiligheid. LSEC is een actieve partner van EC FP7, Horizon 2020 en ondersteunt de Digitale Agenda. LSEC staat de regeringen van de Lidstaten bij met actieve bijdragen over beleidsvorming en kennisdeling. LSEC heeft vestigingen in België, Nederland en het Verenigd Koninkrijk en werkt samen met partners in andere Europese lidstaten. LSEC publiceert botvrij.be en biedt een platform voor ISACs van bedrijven. www.lsec.be is de portaalsite voor experten en expertise rond informatieveiligheid in België.
VBO	**www.vbo-feb.be** **Verbond van Belgische Ondernemingen** Ravensteinstraat 4 1000 Brussel België +32 2 515 08 11 info@vbo-feb.be	Het Verbond van Belgische Ondernemingen (VBO) vertegenwoordigt meer dan 50.000 bedrijven, samen goed voor 80% van de tewerkstelling in de privésector. Het VBO is een bevoorrechte partner van diverse overheidsinstanties in een aantal actieprogramma's om de nationale economie te beschermen. Samen met ICC Belgium nam het VBO het initiatief om een gids over cyberveiligheid op te stellen voor alle Belgische bedrijven.

RAAMWERKEN VOOR CYBER- EN INFORMATIEVEILIGHEID

Als u wilt starten met informatieveiligheid, raden wij u aan om één of meer van de volgende, algemeen erkende goede praktijken, normen en omkaderingen te raadplegen:

NAAM	ORGANISATIE	WEBSITE
ISO 22301:2012	**ISO**	http://www.iso.org/iso/home.html
ISO 27XXX series	**ISO**	http://www.iso.org/iso/home.html
COBIT5 for information security	**ISACA**	www.isaca.org/cobit
SP800 gamma	**NIST**	http://csrc.nist.gov/publications/PubsSPs.html
Standard of Good Practice for Information Security	**ISF**	https://www.securityforum.org/tools/sogp/
CIIP and NCSS	**ENISA**	http://www.enisa.europa.eu/activities/Resilience-and-CIIP
Opleidingstechnieken Informatieveiligheid	**SANS**	http://www.sans.org/reading-room/
BSIMM	**BSIMM**	http://www.bsimm.com
GAISP	**GAISP**	http://all.net/books/standards/GAISP-v30.pdf
Richtlijnen voor goede praktijken	**BCI**	http://www.thebci.org/index.php/resources/the-good-practice-guidelines
ISAE 3402 en SSAE 16	**AICPA**	http://isae3402.com/
DMBOK	**DAMA**	http://www.dama.org
SABSA TOGAF	**Open Group**	http://www.opengroup.org/togaf/
OCTAVE	**CERT**	http://www.cert.org/octave/
EBIOS	**ANSSI**	http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/
PAS 555:2013	**British Standards Institute**	http://www.itgovernance.co.uk/shop/p-1356-pas-555-2013-cyber-security-risk-governance-and-management.aspx
Handleiding Evaluatiecriteria voor IT-beveiliging	**Bundesamt für Sicherheit in der Informationstechnik**	https://www.bsi.bund.de/EN/Topics/topics_node.html

BIBLIOGRAFIE

Allen & Overy. (2012). *EU and U.S. propose new cybersecurity strategies.* London, Verenigd Koninkrijk.
Gedownload van
http://www.allenovery.com/publications/en-gb/Pages/EU-and-U-S--propose-new-cybersecurity-strategies.aspx

Bergsma, K. (2011). *Information Security Governance.*
Gedownload van
https://wiki.internet2.edu/confluence/display/itsg2/Information+Security+Governance

Bescherm je bedrijf.
Gedownload van
http://www.beschermjebedrijf.nl

CERT-EU. (2012). Incident Response – Data Acquisition Guidelines for Investigation Purposes version 1.3.
Gedownload van
http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_12_004_v1_3.pdf

CERT-EU. (2011). Security White Paper 2011-003 - Guidelines for handling common malware infections on Windows based workstations.
Gedownload van
http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_11_003_v2.pdf

CESG. (2012). *10 Steps to Information security.* London, Verenigd Koninkrijk.
Gedownload van
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf

Cyber Security Strategy.be.(2012). België.
Gedownload van
http://www.b-ccentre.be

Deloitte. (2010). *Cyber crime: a clear and present danger*. New York, NY.
Gedownload van
http://www.deloitte.com/assets/dcom-unitedstates/local assets/documents/aers/us_aers_deloitte cyber crime pov jan252010.pdf

Department for Business, Innovation & Skills. (2012). Cyber Risk Management: A Board Level Responsibility. London, Verenigd Koninkrijk.
Gedownload van
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/34593/12-1119-cyber-risk-management-board-responsibility.pdf

EYGM Limited. (2012). *Fighting to close the gap: Ernst & Young's 2012 Global Information Security Survey.*
Gedownload van
http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf

Federal Communications Commission, Information security Planning Guide, 2012

Federal Communications Commission. (2012). *Information security Planning Guide*. Washington, DC:
Gedownload van
http://www.fcc.gov/cyber/cyberplanner.pdf

Information Security Governance.
Gedownload van http://searchsecurity.techtarget.com/tutorial/Information-Security-Governance-Guide

ISACA (2013). *Transforming Cybersecurity: Using COBIT® 5*. USA.
Gedownload van
http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Transforming-Cybersecurity-Using-COBIT-5.aspx

KPMG. (2012). *The Data Loss Barometer: A global insight into lost and stolen information*. Verenigd Koninkrijk.
Gedownload van
http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/Documents/PDF/Advisory/data-loss-barometer-2012.pdf

KPMG. (2013). *Vijf denkfouten over cybersecurity: Een bestuurdersperspectief op cybersecurity*. Amstelveen, Nederland.
Gedownload van http://www.kpmg.com/NL/nl/IssuesAndInsights/ArticlesPublications/Documents/PDF/Risk-Consulting/Vijf-denkfouten-over-cybersecurity.pdf

Ministerie van Veiligheid en Justitie. (2011). *De Nationale Cyber Security Strategie (NCSS)*. Den Haag, Nederland.
Gedowmload van
http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/02/22/nationale-cyber-security-strategie-slagkracht-door-samenwerking/de-nationale-cyber-security-strategie-definitief.pdf

Nationaal Cyber Security Centrum. (2013). *Cybersecuritybeeld Nederland*. Den Haag, Nederland
Gedownload van
https://www.ncsc.nl/binaries/nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten/cybersecuritybeeld-nederland-3/1/NCSC+CSBN+3+3+juli+2013.pdf

Open Web Application Security Project (OWASP).
Gedownload van
https://www.owasp.org

Safe on Web.
Gedownload van
http://www.safeonweb.be.

SANS, Information Security Management, ISO 17799 Audit Check List 1.1, augustus 2003

World Economic Forum. (2012). *Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World - Principles and Guidelines*. Genève, Zwitserland.
Gedownload van
http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf

MET DANK AAN

ONTWERPCOMITÉ:

B-CCENTRE
Belgian Cybercrime Centre of Excellence for Training, Research and Education,
ICRI KU Leuven - iMinds
Mennens, A.
Roex R.
Smeulders, C.

EY Belgium Advisory
Deprez, A.
Dewulf, K.
Wulgaert, T.

FEB/VBO - Verbond van Belgische Ondernemingen
Dammekens, A.
Darville, C.

ICC Belgium - Belgian committee of the International Chamber of Commerce
Bodard, K.
Deré, J.
Maes, M.
Thomaes, R.

ISACA Belgium
Vael, M.

L-SEC
Seldeslachts, U.

Microsoft Belgium
Dekyvere, K.
Schroder, B.

STUURGROEP:

BIPT-IBPT
CERT.BE
ELECTRABEL
ENISA
FCCU
FEBELFIN
FPS Economy
Guldentops, E.
IBJ-IJE
ISPA
UMICORE
VSSE

NOTITIES

NOTITIES

graphic design & production:
www.in-depth.be

publisher:
ICC Belgium
Stuiversstraat 8
1000 Brussel
België
+32 (0)2 515 08 44
info@iccwbo.be
www.iccbelgium.be

BELGISCHE GIDS VOOR CYBERVEILIGHEID
BESCHERM UW INFORMATIE

Deze gids en de begeleidende documenten
werden gezamelijk opgesteld door

ICC Belgium, VBO, EY, Microsoft,
B-CCENTRE en ISACA Belgium.

With the financial support from the Prevention of and Fight against Crime Programme of the European Union
European Commission — Directorate-General Home Affairs