Cyberveiligheid

Is uw onderneming er klaar voor?

economie
FOD Economie, K.M.O., Middenstand en Energie

.be

economie
FOD Economie, K.M.O., Middenstand en Energie

Federale Overheidsdienst Economie, K.M.O., Middenstand en Energie
Vooruitgangstraat 50
1210 Brussel
Ondernemingsnr.: 0314.595.348
https://economie.fgov.be

tel. 0800 120 33 (gratis)

facebook.com/FODEconomie

@FODEconomie

youtube.com/user/FODEconomie

linkedin.com/company/fod-economie

Verantwoordelijke uitgever: Jean-Marc Delporte
Voorzitter van het Directiecomité
Vooruitgangstraat 50
1210 Brussel

Internetversie

209-18

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Inhoudstafel

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

1. Inleiding

Uw onderneming een goed imago geven op het internet is van kapitaal belang.

Aanwezig zijn op het internet, of dit nu is om uw onderneming eenvoudigweg te leren kennen of om uw diensten of goederen aan te bieden, vertegenwoordigt een belangrijke bron van vernieuwing en vertrouwen.

Het beheer van uw imago op het web zal voor een groot deel ook uw relaties met uw professionele partners bepalen, alsook met uw eindklanten.

Wat uw toekomstige **professionele partners** betreft, zij zoeken eerst informatie over uw onderneming op voor zij een contract met u sluiten. Het is dus van groot belang om een professionele website te maken en uw imago te beheersen. Door uw site en gegevens op een efficiënte manier te beveiligen, voelen uw professionele partners zich meer gerustgesteld en sluiten zij makkelijker met u een contract. Hun veiligheid kan immers afhangen van de uwe.

Zich verzekeren dat men over betrouwbare partners beschikt, die hun IT-omgeving zorgvuldig beheren, wordt steeds belangrijker voor elke onderneming.

Wat uw toekomstige **eindklanten** betreft, weet dat steeds meer consumenten eerst online op zoek gaan naar informatie alvorens een aankoop te doen in de winkel of via internet. Uw onlinereputatie is dus van essentieel belang.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Er zijn verschillende redenen waarom consumenten hun aankopen online verrichten:

- het is handig (bestellen kan op elk uur van de dag, snelle leveringstermijnen, ...);
- de prijzen (die kunnen makkelijker online worden vergeleken);
- de keuze;
- de kwaliteit van de verschafte informatie (productbeschrijving, mening van andere consumenten, informatie over een eventuele terugbetaling, over de leveringstermijnen, de garantie, ...).

Maar een van de factoren die door de consumenten worden gezien als een rem bij het online aankopen, is vooral de twijfel bij de veiligheid van de informatie die online wordt doorgegeven. In 2016 besloot één Belgische internetgebruiker op vijf om uit veiligheidsoverwegingen geen onlineaankopen van goederen of diensten voor privégebruik te doen. Consumenten vrezen voornamelijk dat misbruik wordt gemaakt van hun persoonlijke gegevens en dat hun bankgegevens worden gestolen.

Daarom kunnen geschikte maatregelen voor de veiligheid van informatie en het meedelen van deze maatregelen aan uw klanten, de consumenten geruststellen en ervoor zorgen dat het transactievolume toeneemt.

Aanwezig zijn op het web biedt opportuniteiten voor ondernemingen, maar vereist eveneens het ontwikkelen van een digitale strategie waarin de nodige beschermingsmaatregelen inbegrepen zijn.

Cyberaanvallen veroorzaken immers heel wat problemen, ongeacht de grootte van uw onderneming:

- uw imago kan bezoedeld raken en de buitenwereld verliest het vertrouwen in uw onderneming;
- waardevolle commerciële informatie wordt vernietigd en/of gestolen;
- de officiële website is niet meer bereikbaar of het werkinstrument raakt beschadigd door bepaalde cyberaanvallen;
- er kunnen mogelijke sancties volgen, bijvoorbeeld wanneer persoonlijke gegevens worden gelekt.

Bij elk incident kunnen de financiële gevolgen en de imagoschade aanzienlijk zijn en wanneer geen gepaste maatregelen werden voorzien, kan de continuïteit van de activiteit in het gedrang komen. Het is daarom belangrijk dat u op de hoogte bent van de risico's die uw onderneming kan lopen en van de middelen waarmee u deze risico's afwendt en uw klantenbestand veiligstelt.

Sinds 25 mei 2018 is ook de Europese Algemene Verordening Gegevensbescherming ("AVG" of "GDPR"[1] in het Engels) van kracht. Deze verordening legt verschillende verplichtingen op m.b.t. gegevensbescherming aan alle bedrijven die zijn gevestigd in de Europese ruimte [2].

Een van die nieuwe verplichtingen is met name om passende technische en organisatorische maatregelen te nemen om de bescherming van de persoonsgegevens te garanderen, die uw onderneming verwerkt. Het huidige document zal u helpen om deze technische en organisatorische maatregelen beter te begrijpen en hoe deze geïntegreerd kunnen worden in uw onderneming.

Het niet-naleven van de bepalingen van de GDPR gaat gepaard met zware boetes, die variëren naargelang het type inbreuk. Ze kunnen oplopen tot 20 miljoen euro of tot 4 % van de jaarlijkse totale globale omzet van het voorgaande boekjaar, waarbij telkens het hoogste bedrag in aanmerking wordt genomen!

Voor meer informatie, raadpleeg de website van de Gegevensbeschermingsautoriteit en het punt 4.2.4. van het huidige document: "Principe 4. Neem maatregelen met betrekking tot de bescherming van de persoonlijke levenssfeer".

De risico's beperken voor uw onderneming, conform zijn met de GDPR, uw professionele partners geruststellen en beschikken over een goede onlinereputatie t.o.v. consumenten vereist de ontwikkeling van een digitale strategie voor uw onderneming, welke ook voorziet in de nodige veiligheidsmaatregelen.

Slechts een klein percentage van de kmo's is zich echter bewust van de verplichtingen die zij hebben, wanneer zij een website beheren en/of persoonsgegevens verwerken.

De FOD Economie is zich meer en meer bewust van het belang van cybersecurity voor kmo's. Het is in dat opzicht dat de FOD Economie lid is van de Cyber Security Coalition, alsook meewerkt aan de werkzaamheden van de European Cyber Security Organisation (ECSO). Binnen dat kader wenste de FOD Economie een handleiding cybersecurity te publiceren, specifiek ontworpen om te beantwoorden aan de noden van de kmo's. Achtereenvolgens wordt behandeld:

- de verplichte informatie die zichtbaar moet zijn op uw website alsook het maturiteitsniveau van uw onderneming (1.0 of 2.0);
- de Onderneming 1.0, die staat voor een beginners- of semibeginnersniveau (5 principes, 6 acties);

1 Zie woordenlijst.

2 Art. 3 GDPR. De GDPR is eveneens van toepassing op bedrijven die zijn gevestigd buiten de Europese ruimte wanneer de betrokkenen Europeanen zijn (aanbod van goederen, diensten of nog profilering) en/of wanneer het recht van een lidstaat van toepassing is via de regels van het internationaal publiekrecht.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

- de Onderneming 2.0, die staat voor een gevorderd of expertniveau (10 principes, 12 acties);
- de top 10 incidenten in Europa;
- in geval van incident: wat moet u doen?;
- de belangrijkste normen.

Om u te helpen bij het bepalen van de maturiteit van uw onderneming op het vlak van cybersecurity, kunt u de vragenlijst voor zelfevaluatie invullen die beschikbaar is op de website van de FOD Economie.

U kunt ook andere vragenlijsten raadplegen om uw maturiteitsniveau te bepalen:

- de ICC Cyber Security Guide for Business;
- tools om de digitale matuurheid van kmo's te berekenen, ontworpen door Digital Wallonia;
- een Luxemburgse tool ontwikkeld door CASES, die kmo's in staat stelt om een auto-evaluatie uit te voeren en u voorstelt, naargelang uw profiel, een aangepaste strategie te volgen van "start" tot "top".

Begrijpt u bepaalde gebruikte termen niet? Neem dan zeker ook een kijkje in onze woordenlijst.

2. Websites: domeinnaam en verplichte vermeldingen

2.1. Domeinnaam

Indien u een website wilt maken, moet u eerst en vooral beschikken over een domeinnaam.

Hoe kiest u deze?

- Kies een domeinnaam die een verband heeft met uw onderneming, makkelijk te schrijven en te onthouden is.
- Geef de voorkeur aan een gekende extensie (.eu of .be bijvoorbeeld).
- Denk eraan om ook varianten van de gekozen domeinnaam te reserveren (op die manier beschermt u zichzelf tegen webpagina's van concurrenten met een gelijkaardige naam als de uwe) alsook andere extensies voor dezelfde naam (.eu of .brussels, indien u bv. voor .be gekozen heeft) om zo omleidingen van het handelsverkeer te vermijden.
- Uw naam op het web moet niet ieder jaar van eigenaar veranderen: indien mogelijk, reserveer de naam voor de maximaal geautoriseerde duurtermijn en vergeet niet om de hernieuwing van uw domeinnaam aan te vragen, indien deze zou verlopen. Zo voorkomt u akelige verrassingen.

- Vergeet niet om melding te maken en het regelmatig updaten van informatie met betrekking tot:
  - ➢ De identiteit van de houder van de domeinnaam,
  - ➢ Het administratief contactpunt van de WHOIS-databank van het register.
- Indien u overweegt om het beheer van uw website uit te besteden aan een derde, vergeet dan niet om een contract op te stellen waarin voorzien wordt dat aan het einde van het contract, de domeinnaam aan u teruggegeven wordt. Vergeet ook niet om te voorzien in een toegangsrecht tot uw gegevens gedurende de hele uitvoering van het contract met de onderaannemer (identiteitsgegevens, wachtwoorden, ...).
- Controleer regelmatig uw website en reageer snel indien u merkt dat er sprake is van een onrechtmatige reservatie van een domeinnaam met een gelijkaardige naam als de uwe, door gebruik te maken van de bestaande arbitrage en gerechtelijke procedures.

Voor meer informatie over de keuze van een domeinnaam alsook voor wat betreft de registratie van deze naam, kunt u terecht op de website van de FOD Economie.

Om meer te weten over het onderwerp, raadpleeg ook:

- De website van de FOD Economie,
- De gids opgesteld door ANSSI over de goede praktijken voor het verwerven en uitbaten van domeinnamen.

2.2. Verplichte vermeldingen

Wanneer u beschikt over een domeinnaam, mag u niet vergeten om nog een aantal verplichte vermeldingen op te nemen op uw website!

Indien u een vennootschap heeft opgericht, bepalen de artikelen 78 en 80 van het Wetboek van vennootschappen dat, naast uw persoonlijke aansprakelijkheid, de volgende informatie moet voorkomen op al uw stukken, met inbegrip van uw website:

1) De naam van de vennootschap;

2) De rechtsvorm, voluit of afgekort (besloten vennootschap (bv), naamloze vennootschap (nv), coöperatieve vennootschap (cv),...)

- in voorkomend geval, de woorden "burgerlijke vennootschap met handelsvorm" leesbaar gereproduceerd en onmiddellijk voor of achter de naam van de vennootschap geplaatst;
- in het geval van een coöperatieve vennootschap, of de aansprakelijkheid beperkt dan wel onbeperkt is;

- in het geval van ondernemingen met een sociaal oogmerk moet deze vermelding of initialen worden gevolgd door de woorden "met een sociaal oogmerk";

3) Een nauwkeurige aanduiding van de zetel van de vennootschap;

4) Het ondernemingsnummer (KBO)

5) De term "rechtspersonenregister" of de afkorting "RPR", gevolgd door de vermelding van de zetel van de rechtbank van het rechtsgebied waarbinnen de vennootschap haar zetel heeft

6) In voorkomend geval, het feit dat de vennootschap in vereffening is.

Als u een gereglementeerd beroep uitoefent (bijvoorbeeld een vrij beroep):

- de beroepsvereniging of -organisatie waarbij u bent aangesloten,
- uw beroepstitel en het land waar deze is toegekend,
- een verwijzing naar de toepasselijke beroepsregels en de middelen om deze te verkrijgen.

Andere wettelijke bepalingen kunnen ook op u van toepassing zijn.

- Btw: Vergeet niet om uw btw-nummer te vermelden.
- Contact: Uw contactgegevens, inclusief uw e-mailadres, zodat men snel contact met u kan opnemen en direct en efficiënt met u kan communiceren.
- Persoonsgegevens: Vergeet niet om de contactgegevens van uw functionaris voor gegevensbescherming (DPO) en uw "privacybeleid" te vermelden (zie punt 3.2.4 Principe 4. "Neem maatregelen met betrekking tot de bescherming van de persoonlijke levenssfeer", zie ook de website van de Gegevensbeschermingsautoriteit).
- Cookies: In artikel 5, lid 3, van Richtlijn 2002/58/EG heeft de Europese wetgever het beginsel vastgesteld van voorafgaande toestemming van de gebruiker voorafgaand aan de opslag van informatie op de apparatuur van een gebruiker of de toegang tot al opgeslagen informatie, tenzij dergelijke acties strikt noodzakelijk zijn voor de levering van een dienst van de informatiemaatschappij waar de abonnee of gebruiker uitdrukkelijk om heeft verzocht. Opgelet: Richtlijn 2002/58 wordt binnenkort vervangen door een nieuwe Europese Verordening (ePrivacy Regulation) om te voldoen aan de nieuwe Algemene Verordening Gegevensbeschermings (GDPR).
- Auteursrecht: U wenst gebruik te maken van auteursrechtelijk beschermde werken op uw site, zoals muziek, audiovisuele werken, persartikelen, literaire fragmenten, ...? Weet u hoe u inbreuken op het auteursrecht kunt voorkomen? De FOD Economie beantwoordt de meestgestelde vragen over dit onderwerp.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

- Gedragscodes: een verwijzing naar eventuele gedragscodes die op u van toepassing zijn en informatie over de wijze waarop deze codes elektronisch kunnen worden geraadpleegd.

Opgelet: indien u via uw site rechtstreeks met een consument een contract kunt afsluiten, zijn bepaalde bijzondere bepalingen op u van toepassing (met name boek VI van het Wetboek economisch recht voor de vennootschappen en boek XIV voor de vrije beroepen). Voor meer informatie kunt u terecht op de website van de FOD Economie.

3. Onderneming 1.0

In het ideale geval kan een onderneming 1.0 online-informatie verschaffen over de goederen of diensten die ze te koop aanbiedt. Maar in dit stadium mag ze geen onlinebetalingen voorstellen aan de klanten; mocht ze dat wel doen, dan doet ze daarbij beter een beroep op de diensten van een vertrouwde externe partij om de veiligheid van de transacties te kunnen waarborgen.

De meeste bedrijven beschikken over belangrijke gegevens (productiegeheimen, klantengegevens, facturatiegegevens, boekhouding, ...) en werkinstrumenten die onmisbaar zijn. Voor een onderneming komt het er dus op aan om deze gegevens en werkinstrumenten op een gepaste wijze te beschermen.

Om de veiligheid van de informatie op een degelijke manier te kunnen aanpakken, moet op lange termijn worden gedacht waarbij ook een aantal acties op korte en middellange termijn moeten worden gepland.

Om de eerste resultaten op korte termijn te boeken, kunt u verschillende acties ondernemen.

Voer een aantal eenvoudige en snelle maatregelen door waarmee u uw werknemers sensibiliseert voor de beveiliging van de werkinstrumenten en de bescherming van de gege-

vens van uw onderneming. Deze maatregelen hangen uiteraard af van de mate waarin uw onderneming bezig is met veiligheidscultuur. Maar u kunt alvast beginnen met:

- het bijwerken van het besturingssysteem (OS) en de applicaties (software),
- met het beveiligen van de wifitoegang van de onderneming (via een toegangscode),
- met de toepassing van een echt beleid over het wachtwoordbeheer van uw werknemers,
- de uitwerking van een back-upbeheer van de digitale gegevens van uw onderneming, ...

Om u te helpen bij uw eerste stappen in cybersecurity, geven we u hieronder vijf essentiële veiligheidsprincipes en zes noodzakelijke veiligheidsacties die u makkelijk kunt invoeren in uw onderneming.

Voor meer informatie over deze acties en principes, bezoek de website van de Internationale Kamer van Koophandel (ICC) en de ICC cyber security guide for business.

3.1. Vijf essentiële veiligheidsprincipes

3.1.1. Principe 1. Leg de focus op informatie, niet op de technologie

Er zijn slechts 24 uur in een dag en cyberveiligheid is niet uw corebusiness? Concentreer u dus op het belangrijkste door te focussen op de bescherming van uw essentiële informatie en werk stap voor stap aan uw onderneming van morgen.

Het is niet allemaal een kwestie van technologie, ook uw werknemers zijn een belangrijke component in cyberveiligheid. Heel wat incidenten zijn het gevolg van organisatorische en menselijke fouten. Heel wat aanvallen hadden afgeslagen kunnen worden indien de onderneming zijn werknemers had geleerd hoe ze op een veilige manier moeten omgaan met gevoelige informatie of risico's te herkennen, zoals phishing (social engineering, zie ook punt 5 "Top 10 van incidenten").

Sensibiliseer de medewerkers rond cybersecurity. De Cyber Security Coalition en het Centrum voor Cybersecurity Belgium (CCB) hebben een "Cyber Security KIT" gecreëerd, dat een tool kan zijn bij de sensibiliseringsacties.

Ontwerpt uw onderneming een nieuw programma? Stelt u een lijst op van de informatie waarover u beschikt? Denk er dan aan om dit op een globale manier aan te pakken. Indien u van in het begin oog heeft voor de veiligheid en de bescherming van de persoonsgegevens, dan wint u kostbare tijd in de realisatie van uw project! Doet u dat niet, dan riskeert u om helemaal te moeten herbeginnen.

Wanneer u innoveert, denk dan ook meteen aan het aspect "veiligheid" en "privéleven".

3.1.2. Principe 2. Ontwikkel een weerbare mentaliteit: leer om makkelijk terug op te veren

Er is heel wat wetgeving van toepassing op de bedrijven maar "in orde zijn" met deze verplichtingen betekent niet automatisch dat uw onderneming ook op een correcte manier is beschermd. Kijk daarom verder dan uw strikt wettelijke verplichting en voorzie een verdedigingsmechanisme dat aangepast is aan uw behoeften.

Indien u de regels kent die op u van toepassing zijn en u denkt na over het verminderen van uw risico's, dan zult u het makkelijk vinden om terug op te veren na een incident.

3.1.3. Principe 3. Wees voorbereid om veiligheidsincidenten aan te pakken

Op het web is het niet de vraag "of" u op een dag wordt geraakt, maar "WANNEER" u wordt geraakt. Bereid u dus voor om hierop gepast te kunnen reageren!

Overweeg in het bijzonder na te gaan of:

- u weet met wie u contact moet opnemen om technische problemen op te lossen;
- u weet waar uw back-up zich bevindt en hoe u er snel bij kunt;
- u weet welke bevoegde autoriteiten moeten worden gewaarschuwd en op welke manier;
- u weet of u al dan niet gedekt bent door een verzekering en zo ja, welke schade gedekt wordt door uw eventuele cyberverzekering;
- u heeft nagedacht over een communicatiestrategie naar uw leveranciers, uw klanten, ... ;
- u heeft de tijd genomen om deel uit te maken van een community van uw peers (zoals de Cyber Security Coalition) om op de hoogte te zijn van de huidige trends op het gebied van cyberdreigingen voor uw sector, uw bedrijfstype, ...

3.1.4. Principe 4. Laat zien dat u uw verantwoordelijkheid neemt

U vindt uw onderneming te "klein" en dus "niet van toepassing"? Niets is minder waar! Kmo's zijn het geliefkoosde slachtoffer van hackers omdat zij het grootste deel uitmaken van het nationale economische weefsel. Ze beschikken ook over een grote hoeveelheid informatie (gegevens van de klanten, knowhow, zakelijke geheimen, ...) en ze kunnen ook makkelijk gebruikt worden als springplank naar grotere doelwitten waarmee die kmo's een vertrouwensrelatie hebben (leveranciers, ...).

"Ik heb nog nooit een diefstal gehad, zoiets overkomt mij toch nooit"? Maar is uw onderneming wel in staat om een inbraak te detecteren? Waarom zou een hacker u trouwens laten weten dat hij kan inbreken in uw systeem en in dat van uw klanten?

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Weet ook dat de nieuwe Europese Algemene Verordening Gegevensbescherming (AVG of GDPR) sancties kan opleggen in geval van inbreuken. Deze kunnen oplopen tot 20 miljoen euro[3] of, wanneer het gaat om bedrijven, tot 4 % van de jaarlijkse globale omzet van het voorgaande boekjaar, waarbij steeds het hoogste bedrag in aanmerking wordt genomen.

Als het management zich bezorgd voelt en zich betrokken toont door het goede voorbeeld te geven, zullen medewerkers begrijpen dat het ook voor hen belangrijk is om betrokken te raken.

Hoe kunt u laten zien dat u uw verantwoordelijkheid opneemt?

- Duid een contactpunt aan in geval van een incident

Het "contactpunt" kan intern of extern zijn. Afhankelijk van de grootte en de behoeften van uw onderneming, kan deze functie zelfs worden uitgevoerd op een parttime basis (maar wees voorzichtig om potentiële belangenconflicten te vermijden) of door een gespecialiseerde onderneming.

Opgelet! Het "contactpunt" wordt niet voor alles verantwoordelijk! Zijn functie is om informatie naar het juiste niveau binnen uw onderneming te sturen, zodat die snel en effectief kan reageren in het geval van een incident. Elke werknemer blijft daarnaast verantwoordelijk voor zijn eigen daden en de onderneming moet ervoor zorgen dat haar personeel wordt gesensibiliseerd en zich bewust is van zijn verantwoordelijkheden.

- Voorzie een manier om de naleving van uw veiligheidsbeleid te controleren

Voorzie testen en audits op het gebied van informatiebeveiliging en vergeet niet om regelmatig rapporten te vragen (bij elk incident, elke maand, minstens een keer per jaar, ...) :

  - over de doeltreffendheid en relevantie van de technische en organisatorische maatregelen die binnen uw onderneming worden geïmplementeerd;
  - op gebieden die voor verbetering vatbaar zijn.

In de beginfase kan de audit nog eenvoudig zijn en slechts betrekking hebben op een deel van uw informatiesysteem. Het doel is dan vooral om verbeterpunten te identificeren (quick-wins) die uw onderneming kan implementeren. In dit stadium is het belangrijker om meer te investeren in bescherming van uw informatiesystemen dan te betalen voor sterk geavanceerde audits, die niet onmiddellijk nut hebben voor een onderneming 1.0.

- Durf uzelf in vraag te stellen

Bedreigingen kunnen niet voor eens en altijd worden weggenomen. Kwetsbaarheden evenmin. Denk in plaats daarvan aan het voortdurend verbeteren van uw risicomanage-

3 Zie voor meer informatie het punt "Onderneming 2.0, Principe 4. Neem maatregelen met betrekking tot de bescherming van de persoonlijke levenssfeer".

ment en durf uw beveiligingsbeleid regelmatig (jaarlijks) te herzien. Niet alles zal hoeven te veranderen, maar er zijn bepaalde dingen die zeker voor verbetering vatbaar zijn.

3.1.5. Principe 5. Implementeer uw visie

- Stel een informatieveiligheidsbeleid op

Een informatieveiligheidsbeleid toont aan dat u uw belangrijkste bedrijfsmiddelen (informatie, reputatie, enz.) wilt beschermen en stelt u in staat om aan al uw medewerkers een referentiekader te bieden om uit te leggen wat zij wel en niet kunnen op het gebied van informatieveiligheid.

- Denk na over uw externe relaties

a) Met uw digitale leveranciers

Vraag eens raad aan uw leveranciers van digitale diensten; meestal kunnen zij u de gepaste veiligheidsoplossingen voorstellen. Deze veiligheidsoplossingen kunnen o.a. omvatten:

- het beheer van de back-ups (opslag van gegevens),
- het beheer van herstelpunten (recovery)[4],
- versleuteling[5],
- audits van uw informatieveiligheidssysteem,
- terbeschikkingstelling van een private cloud, ...

Vergeet ook niet te vragen om toegang te krijgen tot de logboeken (activiteitensporen) voor de diensten die u hebt uitbesteed. Bij een incident zijn deze sporen essentieel om te achterhalen wat er precies is gebeurd en om te vermijden dat een gelijkaardig incident zich opnieuw voordoet.

b) Met uw andere leveranciers

Verzeker uzelf dat uw leveranciers ook over een effectief informatieveiligheidsbeleid beschikken. Hun cyberincidenten kunnen ook een invloed hebben op uw commerciële handel en/of reputatie. Aarzel niet om te vragen of ze een certificaat hebben (zie punt 8. Belangrijkste normen), om kopieën van veiligheidsaudits te ontvangen (minstens een keer per jaar), ...

4 Zie woordenlijst.

5 Zie woordenlijst.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

c) Met uw professionele partners

Denk eraan om met uw professionele partners te praten over de informatiebeveiliging langs de hele keten. U heeft er alles aan gedaan langs uw kant om de veiligheid te verzekeren, maar ook zij hebben er alle baat bij om zich te beschermen! Zo niet, zouden uw professionele partners kunnen dienen als toegangspoort tot uw systemen om deze te infecteren en zouden zij eveneens bv. niet meer in staat kunnen zijn om te voldoen aan uw noden, aangezien een cyberaanval hun productieketen verlamd heeft.

U hoeft niet meteen al alles aan te pakken: stel een lijst op met actiepunten die u eerst moet realiseren, waarbij u rekening houdt met uw echte behoeften en met de financiële en menselijke middelen waarover u beschikt.

Begrijpt u bepaalde gebruikte termen niet? Raadpleeg dan zeker onze woordenlijst.

3.2. Zes acties

3.2.1. Actie 1. Bewaar uw informatie en controleer het herstelproces

Wat zou er gebeuren als al uw computers in tien minuten geïnfecteerd worden? Hebt u een kopie van uw vitale informatie? Is deze kopie gekoppeld aan het netwerk van geïnfecteerde computers? Weet u zeker dat uw kopieën bruikbaar zijn en dat ook zij niet geïnfecteerd zullen worden? Hebt u gekozen voor een clouddienst en zo ja, welke garanties worden geboden op het gebied van vertrouwelijkheid, integriteit en authenticiteit?

Vergeet niet om op voorhand de juiste vragen te stellen... om zo veel problemen te vermijden in geval van een incident.

Uw informatie efficiënt opslaan betekent m.n.:

a) dat u de informatie die u moet bewaren, kunt identificeren (Classificeer uw informatie),

b) dat u back-upprocedures instelt,

c) dat u regelmatig tests uitvoert om de kwaliteit van uw beveiligingen en herstelprocessen te controleren.

a) Classificeer uw informatie

Een algemene infomail naar een van uw klanten wordt niet op dezelfde manier beveiligd als een uitvinding van uw onderneming. Vergeet niet om informatie die van essentieel belang is voor uw onderneming te identificeren en die ook beter te beveiligen.

Hieronder kunt u een voorbeeld van een eenvoudig classificatiemodel vinden:

- "Publiek": iedereen kan toegang krijgen tot deze informatie, zowel binnen als buiten uw onderneming. Deze informatie vereist geen speciale bescherming, markering of behandeling. Het nieuws of algemeen contactnummer dat u op de website van uw onderneming plaatst, is een goed voorbeeld van informatie die als "publiek" kan worden bestempeld;
- "Beperkt": alleen specifieke personen mogen toegang hebben tot deze informatie. De personen die er toegang toe kunnen hebben, zijn over het algemeen beperkt tot een geselecteerde groep personen, waaronder bepaalde werknemers, klanten, leveranciers, enz. Deze informatie moet met verschillende waarborgen worden gecontroleerd en van het opschrift "beperkt" worden voorzien. Het arbeidsreglement van uw onderneming of de zakelijke contactnummers van al uw medewerkers zijn een goed voorbeeld van beperkte informatie;
- "Vertrouwelijk": De toegang tot deze informatie is beperkt tot een beperkt aantal aangewezen personen binnen uw organisatie. Het verlies of de diefstal van deze informatie kan uw onderneming ernstig schaden. "Vertrouwelijke" documenten of informatie moeten met zorg worden gelabeld en behandeld en mogen uw onderneming idealiter niet verlaten. Voorbeelden van vertrouwelijke informatie zijn bedrijfsgeheimen en persoonlijke data over uw klanten.

Vergeet niet om de regels die van toepassing zijn op de etikettering, verwerking of overdracht van informatie en documenten op papier te zetten en uw werknemers op te leiden om te voldoen aan deze regels.

b) Stel back-upprocedures op

Niet alles hoeft bewaard te worden. Identificeer de informatie die u nodig hebt en stel u voor dat u deze morgen kwijtraakt. Wat heeft u nodig om snel terug te kunnen opveren? In welk formaat kan vitale informatie sneller worden gerecupereerd ?

Denk er ook aan om:

- indien mogelijk, gegevens op te slaan op een andere plaats dan uw hoofdgebouw (brand, overstroming,...),
- indien nodig, uit te besteden (cloud): denk in dit geval na over het vereisen van een goed beveiligingsniveau, de mogelijkheid om externe audits te organiseren, recovery tests, en, waarom niet, het versleutelen van uw opgeslagen gegevens,
- uw omgevingen van elkaar te scheiden: als uw pc geïnfecteerd is met ransomware, zouden uw back-ups dan ook worden beïnvloed?

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

c) Organiseer regelmatig testen

Vergeet niet om testen te organiseren om de kwaliteit van uw back-ups te controleren (hebt u alle opgeslagen informatie kunnen recupereren?) evenals de kwaliteit van uw back-upprocessen (was het gemakkelijk om deze gegevens te herstellen?). Hebt u softwareconflicten gedetecteerd? ...).

3.2.2. Actie 2. Houd uw IT-systemen steeds up-to-date

Er worden regelmatig nieuwe zwakke punten ontdekt. Eens die kwetsbaarheden geïdentificeerd zijn, stellen de officiële programma's alles in het werk om de veiligheidslekken te dichten door de verspreiding van "patches". Maar dan moet u wel regelmatig uw besturingssysteem (OS) en uw software updaten om steeds de nieuwste patches op het systeem te hebben! Denk er dus aan om regelmatig al uw programma's te updaten! Automatische updates van anti-malwareprogramma's, webfiltertools, inbraakpreventiesystemen (IPS[6]) en inbraakdetectiesystemen (IDS[7]) zijn aan te raden.

3.2.3. Actie 3. Investeer in opleidingen

Veiligheid is een zaak voor iedereen! Vergeet niet om daar regelmatig over te spreken met uw werknemers, hen op te leiden en te informeren over de goede gebruikspraktijken binnen uw onderneming. Waarom vraagt u ook eens niet de mening van uw werknemers over de kwetsbaarheden van uw onderneming en/of over de juiste middelen om die te verminderen?

De opleidingen kunnen intern en/of extern zijn, wat belangrijk is, is dat er een veiligheidscultuur ontwikkeld wordt binnen uw onderneming.

3.2.4. Actie 4. Houd uw IT-omgeving in de gaten

- Toegang en uitrusting

Bepaal wie toegang kan krijgen tot uw computers en uw netwerk! Heeft een leverancier toegang? Hebt u uw omgeving (gebouwen, servers,..) beschermd? Indien u hiervoor niet over de nodige capaciteiten beschikt, kunt u altijd uitbesteden (cloud)[8].

Bepaal daarnaast welke apparaten (mobiele apparaten,...) toegang kunnen krijgen tot uw bedrijfsnetwerk/informatie en vergeet ook niet om uw apparaten te beveiligen (wachtwoorden, versleuteling, blokkering vanop afstand, ...).

6 Zie woordenlijst.

7 Zie woordenlijst.

8 In dit geval, zie ook Onderneming 2.0, "Principe 10. Werk aan uw relatie met derden"

Een laptop, tablet, gsm of USB-stick? Deze dingen raken al eens zoek... of worden makkelijk gestolen! In geval van verlies of diefstal, zouden derden toegang kunnen krijgen tot kostbare informatie indien u er niet aan gedacht hebt om deze gegevens te encrypteren (versleutelen) of indien u het niet fysiek onmogelijk heeft gemaakt om bepaalde informatiedragers te gebruiken (u kunt bv. de USB-poorten blokkeren op bedrijfscomputers).

Overweeg ook om uw personeelsleden te vertellen hoe ze u snel op de hoogte kunnen stellen in geval van een incident (bijvoorbeeld als een mobiel apparaat met de gegevens van uw onderneming is gestolen of verloren).

- Wachtwoord

Een wachtwoord is als een tandenborstel: maak uw werknemers duidelijk dat ze een wachtwoord nooit mogen uitlenen en dat het wachtwoord van de onderneming nooit voor andere doeleinden gebruikt mag worden (Facebook, persoonlijke boodschappendiensten, datingsites, ...).

Verplicht elke werknemer om een voldoende lang wachtwoord te kiezen (minimum 8 lettertekens) met minstens een hoofdletter, kleine letters, cijfers, een speciaal letterteken (!, %,@, ...).

Let er op dat ze ook regelmatig hun wachtwoorden veranderen (in het ideale geval minstens 1 keer per seizoen) en dat hetzelfde wachtwoord niet tot in het oneindige kan worden hergebruikt.

Benadruk dat wachtwoorden niet mogen worden genoteerd op goed zichtbare plaatsen (post-it, borden, ...) en voorkom beginnersfouten door de meest courante wachtwoorden te weigeren: 1234567 (17 % van de gebruikers!), 123456789, wachtwoord, password, google, azertyuiop, qwerty, qwertyuiop, mynoob, 123qwe, 123azer, ...

Deze "wachtwoorden" zijn veel te gemakkelijk om in te voeren. Het is alsof u uw sleutels gewoon op de voordeur van uw onderneming laat zitten!

Voor toegang vanop afstand (telewerk, externe vergaderingen, ...) gebruikt u het beste niet enkel een wachtwoord, maar met minstens twee systemen (bijvoorbeeld: wachtwoord + gebruik van de identiteitskaart via CSAM). Verstuur ook nooit gevoelige informatie via een openbare verbinding (openbare wifi), maar gebruik steeds een beveiligde verbinding (met. een VPN).

Wilt u meer weten over wachtwoorden? Ga dan zeker ook de aanbevelingen na van ANSSI en CNIL (Frankrijk).

Wilt u weten of uw wachtwoord sterk genoeg is? U kunt het hier testen.

Klagen uw medewerkers over het moeten gebruiken van meerdere wachtwoorden en/of dat ze deze regelmatig vergeten? Gebruik bijvoorbeeld een wachtwoordmanager zoals Keepass of Zenyway.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

- Regels van gezond verstand

Denk eraan om uw medewerkers te herinneren aan de regels van voorzichtigheid:

  - niet chatten met vreemden op het bedrijfsnetwerk;
  - geen bankgegevens per e-mail of telefoon verstrekken zonder de identiteit van deze persoon op verschillende manieren te hebben geverifieerd;
  - kijk in de linkerbovenhoek van uw scherm en controleer of het vermelde webadres begint met https:// (met het icoon van gesloten hangslot);
  - controleer of de site waarnaar u wordt gestuurd geen spelfouten bevat in de naam en een "contact"-sectie en een "privacy"-sectie bevat. Controleer ook of de andere verplichte informatie (zie punt 2 "Websites: domeinnamen en verplichte informatie") op de website van uw correspondent verschijnt.

- Beperk de beheerdersaccounts[9]

Kunnen uw werknemers om het even welk programma zomaar op hun computer installeren? Hoe weet u of uw onderneming de algemene voorwaarden respecteert van de licenties (programma's) die het heeft aangekocht als iedereen om het even wat op zijn pc kan installeren? Vergewis u ervan dat maar een handvol IT-beheerders beschikt over toegangsrechten tot uw computers. Stel ook niet al uw vertrouwen in een enkele persoon en denk eraan om de beheerdersaccounts regelmatig te controleren omdat die een geliefkoosd doelwit zijn van hackers.

3.2.5. Actie 5. Vermenigvuldig de verdediging om risico's te verminderen

Er bestaan veel malwares[10] en er komen elke dag nieuwe schadelijke programma's bij.

Denk eraan om minimaal te beschikken over:

- antivirussoftware,
- een firewall[11],
- programma's voor inbraakpreventie en inbraakdetectie (IPS[12]/IDS[13])

en vergeet niet om deze regelmatig (/automatisch) bij te werken!

9 Zie woordenlijst.

10 Zie woordenlijst.

11 Zie woordenlijst.

12 Zie woordenlijst.

13 Zie woordenlijst.

Vergeet ook niet om te voorzien in:

- een goed informatieveiligheidsbeleid,
- een goede opleiding van uw medewerkers.

Aarzel tot slot niet om, indien nodig, een cyberverzekering af te sluiten.

3.2.6. Actie 6. Bereid u voor op incidenten

Hebt u alles voorzien in geval van een incident?

Weet u:

- hoe u een incident kan detecteren?
- met wie u contact moet opnemen om beslissingen te nemen?
- welke autoriteiten u moet contacteren?
- wie u technisch kan helpen (back-ups, ...)
- welke sporen (bewijzen) moeten worden bewaard[14]?
- hoe u communiceert met uw klanten?

Bereid u nu alvast voor om heel wat schade te vermijden tijdens en na een incident.

14 Richtlijnen m.b.t. het bewaren van gegevens zijn beschikbaar op de website van CERT.eu
Een gids m.b.t. forensische technieken is eveneens beschikbaar op de website van NIST.

4. Onderneming 2.0

Als u wilt dat uw onderneming verder gaat, vindt u hier informatie over 10 principes en 12 acties die nuttig zijn om binnen uw onderneming op te zetten.

4.1. Stap 1. Analyse van de risico's of "Ken uzelf"!

De eerste stap bestaat erin om een risicoanalyse uit te voeren. Zo achterhaalt u snel wat uw kritieke activa zijn om die beter te kunnen beschermen.

a) De risicoanalyse kan rudimentair zijn, op basis van eenvoudige vragen:

- Beschikt uw onderneming over een informatieveiligheidsbeleid? (Ja/Neen)
- Hebt u plannen om de komende 12 maanden een informatieveiligheidsbeleid en/of een beleid voor de bescherming van persoonsgegevens te ontwikkelen en/of te updaten? (Ja/Neen)
- Indien het antwoord op een van de twee eerste vragen neen was, wat is daar dan de belangrijkste reden voor (gebrek aan expertise, te duur, onvoldoende personeel, ...)?

- Hebt u normen[15] over veiligheid en/of de bescherming van persoonsgegevens ontwikkeld of wilt u die implementeren? (Ja/Neen)
- Houdt uw beveiligingsbeleid rekening met de volgende elementen:
  - Relatie met interne medewerkers (arbeidsreglement, vertrouwelijkheidsbepalingen, ...)
  - Risicobeheer (met inbegrip van een regelmatige audit, rapport, ...)
  - Beleid over de bescherming van persoonsgegevens (adequaat register, informatie te bezorgen aan de autoriteiten, aan de betrokken personen, ...)
  - Business Continuity Plan (BCP)[16] ("bedrijfscontinuïteitplan")
  - Disaster Recovery Plan (DRP)[17] ("rampherstelplan")
  - Crisis Management Plan (CMP)
  - Governance, Risk management and Compliance (GRC) (beheer van de processen, risico's en uw wettelijke en contractuele verplichtingen)
  - Incident Management Plan (IMP)
  - Incidentenlogboek
  - Relaties met derden (dienstencontracten, leveringscontracten, clausules die voorzien moeten worden met betrekking tot veiligheid en vertrouwelijkheid, consultants die zich regelmatig bij u op kantoor bevinden, ...)
  - Een bijzonder punt voor elk van de meest voorkomende incidenten[18]
- Na hoeveel tijd zonder internettoegang zou u problemen beginnen te ondervinden om uw onderneming te beheren (enkele minuten, enkele uren, enkele dagen)? Waar zou u het eerst problemen mee hebben?
- Wat zou er gebeuren wanneer een van uw concurrenten informatie in zijn bezit krijgt waarover u beschikt (klantenlijst, productiegeheimen, specifieke leveranciers, ...)?

De website van de FOD Economie biedt u ook een evaluatievragenlijst aan om u hierbij te helpen.

15 Zie punt 8 "Belangrijkste normen".

16 Zie woordenlijst.

17 Zie woordenlijst.

18 Zie punt 5 "Top 10 van de incidenten".

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

U kunt ook andere vragenlijsten raadplegen om uw maturiteitsniveau te bepalen:

- De ICC Cyber Security Guide for Business
- Tools om de digitale matuurheid van kmo's te berekenen, ontworpen door Digital Wallonia
- De Luxemburgse site CASES, die kmo's in staat stelt om een auto-evaluatie uit te voeren en u voorstelt, in functie van uw profiel, een aangepaste strategie te volgen van "start" tot "top".

b) De risicoanalyse kan ook complexer gebeuren, waarbij meer specifieke methodes en instrumenten gebruikt worden:

- MEHARI
- EBIOS
- MONARC
- OCTAVE
- IRAM2
- ...

Voor meer informatie over de verschillende methodologieën voor het uitvoeren van een risicoanalyse, kunt u de website van het European Network and Information Security Agency (ENISA) raadplegen.

Een risicoanalyse, of die nu rudimentair of complex is, vertrekt steeds van het principe dat het risico het resultaat is van de waarschijnlijkheid dat een bedreiging (intern of extern) een kwetsbaarheid in uw onderneming uitbuit en u een zekere schade toebrengt (impact).

Wanneer de schade (impact) als verwaarloosbaar wordt beschouwd, kan de directie het risico beschouwen als "aanvaardbaar". Zij moet echter duidelijk identificeren wat zij als "acceptabel" beschouwt en wat niet.

Om het risico te berekenen, vermenigvuldigt men de waarschijnlijkheid van een bedreiging met de kwetsbaarheid en de impact, wat samengevat neerkomt op de volgende formule:

Risico = (Waarschijnlijkheid . Bedreiging) . Kwetsbaarheid . Impact

Het is zeer moeilijk om in te grijpen op de bedreigingen omdat die voortdurend evolueren.

Toch kunnen de risico's worden ingeperkt door de andere punten in de formule aan te pakken.

Zo is het mogelijk om het risico dat een bedreiging uw kwetsbaarheden uitbuit, te verminderen, door gewoonweg uw kwetsbaarheden in het algemeen te verminderen. Bijvoorbeeld wanneer u geen antivirus hebt, is de waarschijnlijkheid dat een virus toeslaat in uw onderneming en zware schade toebrengt, uiteraard veel groter dan wanneer u een beveiliging hebt geïnstalleerd op verschillende niveaus, waaronder een antivirusprogramma dat regelmatig wordt geüpdatet.

Het is eveneens mogelijk om uw schade (impact) te verminderen door de risico's te verminderen tot op een aanvaardbaar niveau en/of door de risico's[19] te verzachten, d.w.z. door een deel of het geheel van risico's te beperken en/of te verplaatsen. Bijvoorbeeld wanneer een van de computers van uw onderneming wordt getroffen door ransomware[20], en u kunt terugvallen op een goed beheer van uw back-ups en iedereen weet hoe te reageren dankzij de sensibiliseringsmaatregelen van uw onderneming, kan het incident vrij snel worden opgelost en kan uw onderneming na enkele minuten opnieuw normaal functioneren.

Sinds 25 mei 2018 is ook de nieuwe Algemene Verordening Gegevensbescherming (AVG/GDPR[21]) van kracht. Deze nieuwe vordering legt een aantal verplichtingen over de bescherming van de persoonsgegevens op, zoals het nemen van passende technische en organisatorische maatregelen om de bescherming van de door uw onderneming verwerkte persoonsgegevens te garanderen[22] alsook, in bepaalde gevallen, de verplichting om een impactanalyse uit te voeren m.b.t. de bescherming van de gegevens ("Data Protection Impact Assessment" of "DPIA"[23]).

De sancties die voorzien worden in de GDPR[24] kunnen, op basis van het type inbreuk, gaan:

- tot 10.000.000 euro of, wanneer het gaat om een onderneming, tot 2 % van de jaarlijkse globale omzet van het voorgaande boekjaar, waarbij steeds het hoogste bedrag in aanmerking wordt genomen,
- tot 20.000.000 euro of, wanneer het gaat om een onderneming, tot 4 % van de jaarlijkse globale omzet van het voorgaande boekjaar, waarbij steeds het hoogste bedrag in aanmerking wordt genomen.

Maar het risico dat u een dergelijke boete krijgt, daalt aanzienlijk wanneer u de nodige informatie hebt bezorgd aan de betrokken personen en wanneer u de gepaste technische en organisatorische maatregelen hebt genomen. Maar u kunt maar beter van in het begin het aspect van de bescherming van de persoonsgegevens in uw risicoanalyses en uw informatieveiligheidsbeleid opnemen!

Ook al is het voornaamste doel van de GDPR (of AVG) niet om cyberaanvallen te voorkomen, toch beperkt u door het naleven van deze nieuwe verordening en de hierin opgelegde technische en organisatorische maatregelen, sterk de nefaste gevolgen van het merendeel van de cyberaanvallen! U respecteert niet enkel de wettelijke verplichtingen opgelegd

19 Zie woordenlijst.

20 Zie woordenlijst.

21 Zie woordenlijst.

22 Art. 32 GDPR.

23 Zie art. 35 en volgende van de GDPR.

24 Art. 83 van de GDPR.

aan uw onderneming, maar u kunt eveneens genieten van deze gelegenheid om aan uw klanten (natuurlijke personen) te tonen hoezeer u hun privacy respecteert!

Wilt u hierover meer informatie, bezoek dan de website van de Gegevensbeschermingsautoriteit en laat u op de hoogte houden van de richtlijnen die worden verspreid door het Europees Comité voor gegevensbescherming (ex -"werkgroep artikel 29").

Voor meer informatie over de maatregelen die u kunt toepassen om de impact en/of de kwetsbaarheden te beperken, lees het punt 5 "Top 10 van de incidenten".

Raadpleeg ook het punt 4.2.4: Principe 4. Neem maatregelen met betrekking tot de bescherming van de persoonlijke levenssfeer. U hoeft niet meteen alles aan te pakken: stel een lijst op met de grootste risico's waarbij u rekening houdt met uw echte behoeften en met de financiële en menselijke middelen waarover u beschikt. Risico's die zeer waarschijnlijk zijn en die een aanzienlijke impact kunnen veroorzaken, moeten eerst worden aangepakt.

Voor meer informatie, raadpleeg de Gids "Data Protection" gepubliceerd door het VBO (Verbond van Belgische Ondernemingen) alsook de website van de Cybersecurity Coalition.

4.2. Stap 2. 10 principes

4.2.1. Principe 1. Organiseer een "meerlagige" verdediging

In een gereedschapskist heeft elk gereedschap zijn eigen functie. Dat geldt ook voor cyberaspecten: voorzie in een verdediging die niet is gebaseerd op een enkele tool! Denk ook aan de volgende instrumenten:

- antivirus,
- firewall[25],
- antispam[26]-, antiphishing[27]-, anti-exploit-, antiransomware[28]-, antimalwaresoftware,[29] ...

25 Zie woordenlijst.

26 Zie woordenlijst.

27 Zie woordenlijst.

28 Zie woordenlijst.

29 Zie woordenlijst.

Vergeet ook niet om te zorgen voor tools waarmee u incidenten kunt detecteren (IDS[30]/ IPS[31]). Maar baseer uw verdediging niet alleen daarop. Zorg er ook voor dat de kwaliteit van de detectie- en correlatieregels, de dekking van de incidenttypes en de responsprocessen bij detectie ook op een doeltreffende manier worden geïmplementeerd.

Uw aandacht moet eveneens minstens uitgaan naar volgende controle-elementen:

1) updatebeheer van uw tools en applicaties! (Java, Flash,...).
2) lijst van de geautoriseerde/niet-geautoriseerde hardware en software;
3) doeltreffende configuratie (en updates) van de hardware- en software-elementen voor servers, laptops, gsm's;
4) doeltreffende configuratie van routers[32], firewalls[33], switches[34];
5) naleving van de licenties van aangekochte programma's;
6) regelmatige analyses van de zwakheden en de mogelijke oplossingen;
7) doeltreffende antimalware;
8) specifiek beleid voor mobiele toestellen;
9) specifiek beleid voor wifitoegang en toegang vanop afstand;
10) scans van alle binnenkomende e-mails[35];
11) een beperkt aantal (bevoorrechte) beheerders en met noodzakelijke toegang (+ specifieke controle);
12) regelmatige tests van de back-ups;
13) aangepaste plannen: Business Continuity Plan, Disaster Recovery Plan, Incident Management Plan, Crisis Management Plan, ...

Voor meer informatie, aarzel niet om het witboek van CERT.eu: "Mitigating Risks Related to Network Devices (2017)" te raadplegen.

30 Zie woordenlijst.

31 Zie woordenlijst.

32 Zie woordenlijst

33 Zie woordenlijst

34 Zie woordenlijst

35 Zie ook het CERT.eu Security Whitepaper "Defating E-mail Abuse" (2017) -

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

4.2.2. Principe 2. Maak uw personeel bewust van informatieveiligheid

De gegevens die in uw bezit zijn (zakelijke geheimen, productiegeheimen, persoonsgegevens, ...) moeten op een correcte manier beschermd worden.[36]

Daarom moet u uw werknemers laten weten wat ze wel en niet mogen doen met de gegevens van de onderneming door een doeltreffend veiligheidsbeleid uit te werken dat eventueel gepaard gaat met een gedragscode. Deze documenten moeten, bij voorkeur, worden opgesteld als bijlage bij het arbeidsreglement van uw onderneming.

Om uw projecten in overeenstemming met uw veiligheidsbeleid op te stellen, baseert u zich idealiter op beproefde methodes in referentie-instrumenten zoals:

- ITIL: een volledige reeks goede praktijken om een doeltreffend beheer te garanderen van het informatiesysteem;
- COBIT:een framework dat goede praktijken over informaticabeheer voorstelt in een logica van risicocontrole en beheer.
- Prince2: een methode voor projectmanagement die is gericht op projectbeheer.

U kunt zich eveneens baseren op de internationale normen zoals de reeks ISO/IEC 27000, ISO/IEC 9000, NIST (SP800, SP1800, ...). Voor meer informatie zie het punt 8 "Belangrijkste normen". Zodra het veiligheidsbeleid en de gedragscode werden opgesteld, moet u die gaan verspreiden! Zorg voor een degelijke opleiding van uw werknemers, zodat deze gepast kunnen reageren door de regels toe te passen die u hebt bepaald.

Om uw personeel te sensibiliseren, kunt u verschillende informatiekanalen gebruiken: informatiesessies voor nieuwe werknemers, regelmatige herinneringen in uw interne boodschappen (nieuwsbrief, ...), sensibilisering van de hiërarchische meerderen zodat die de naleving van het beleid en van de te volgen regels opnemen in de evaluatie van de werknemers, steun aan sensibiliseringscampagnes (Safer Internet Day, Take Back the Internet, ...).

Hier volgen alvast enkele ideeën om u op weg te helpen:

- Kit voor de kmo's: social engineering, wachtwoorden en phishing
- Phishing
- CEO-fraude

36 Zie hiervoor punt 4.2.4. Neem maatregelen met betrekking tot de bescherming van de persoonlijke levenssfeer.

Houd er ook rekening mee dat uw werknemers de gewoonten van thuis ook vaak meenemen naar de werkplek!

Geef hen dus de nodige informatie om ervoor te zorgen dat hun internetgedrag veilig is ... waar ze ook zijn: cybersimpel, risico-info, safeonweb, CCB, GBA ...(zie punt 7. "Meer weten? Actoren en nuttige links")

Waar u ten slotte ook aan moet denken, is aan de permanente opleiding van de werknemers en/of teams die belast zijn met informatiebeveiliging en/of die werden aangeduid als IT-aanspreekpunt. De bedreigingen veranderen immers voortdurend en u bent maar beter op de hoogte van de goede praktijken die gelden in uw sector.

4.2.3. Principe 3. Identificeer de informatie waarover uw onderneming beschikt en classificeer ze!

Geef uw personeel een opleiding over de interne classificatie van de documenten! Iedereen moet immers weten welke regels precies van toepassing zijn op welk type documenten.

Vooraleer u kunt "classificeren", moet u eerst de informatie die in aanmerking komt voor beschermingsmaatregelen identificeren en oplijsten.

Zo kunt u de volgende informatie identificeren:

- technische informatie: originele ideeën, kennis van de zwakke punten van een bepaald product, specifieke knowhow, architectuur van uw onderneming, originele ontwerpen, meerwaarde van een product of een dienst, ontwerpmethodes, prototypes, ...
- commerciële informatie: klantenbestanden, leveranciersbestanden, marketingplannen, klantenvoorkeuren op basis van verschillende profielen, ...
- financiële informatie: details van de verschillende boekhoudkundige posten, inhoud en voorwaarden van contracten en commerciële offertes, aankoopprijzen en verkoopprijzen, verzekeringen, ...
- strategische informatie: rekruteringsprojecten (HR), juridische en technologische marktmonitoring aangepast aan uw onderneming, overname-/fusieplannen, ...

Vergeet daarbij niet om de verschillende diensten van uw onderneming te betrekken: juridische dienst, HR, commerciële dienst, informatica-afdeling, boekhouding, ...

Hebt u die informatie uiteindelijk geïdentificeerd, dan kunt u ze classificeren! Hierbij kunt u vooral een classificatie van het type "Traffic Light Protocol" (of TLP)[37] gebruiken.

37 Zie het TLP-document op de website van de FOD Economie.

Opgelet, niet alles hoeft "vertrouwelijk" te zijn: ga oordeelkundig te werk als u de geloofwaardigheid van uw werkwijze niet in het gedrang wilt brengen. Als u al uw informatie als TLP Rood classificeert, krijgen heel wat werknemers, klanten, leveranciers, ... nooit toegang tot de informatie die u hen nochtans graag wilt meedelen. Zorg er daarom voor dat de codes echt worden toegekend op basis van de behoeften van uw onderneming en dat de verschillende hiërarchische niveaus steeds aan de noodzakelijke informatie kunnen.

Voor meer informatie over de classificatie van de informatie, verwijzen we u naar:

- het Traffic Light Protocol TLP
- Classificatie

Denk ook na over het veilig delen van informatie (m.b.t. bedreigingen en incidenten) in een cirkel van vertrouwen, idealiter met collega's uit uw activiteitensector. Hierdoor bent u niet alleen snel op de hoogte van de belangrijkste dreigingen die op u afkomen, maar kunt u ook de oplossingen identificeren die voor deze dreigingen/incidenten kunnen worden gebruikt. Voorbeelden van vertrouwenscirkels zijn bv. de CyberSecurity Coalition en de European Cyber Security Organisation (ECSO).

Het delen van informatie in een cirkel van vertrouwen impliceert m.n. dat u geïdentificeerd hebt:

- wie de informatie kan delen?
- welke informatie gedeeld kan worden (en welke niet)?

4.2.4. Principe 4. Neem maatregelen met betrekking tot de bescherming van de persoonlijke levenssfeer

NB: Dit punt heeft niet tot doel om de GDPR-verordening uitvoerig voor te stellen maar om enkele aandachtspunten naar voren te schuiven. Voor meer informatie raadpleeg regelmatig de website van de Gegevensbeschermingsautoriteit (GBA).

De Algemene Verordening Gegevensbescherming (AVG/GDPR)[38] legt verschillende verplichtingen op aan de verwerkingsverantwoordelijke (en aan zijn eventuele vertegenwoordiger) alsook aan de verwerker[39].

38 Zie woordenlijst.

39 Zie met name hoofdstuk IV van de GDPR, artikels 24 en volgende.

Hieronder volgen enkele bijzondere aandachtspunten waarmee u kunt voldoen aan uw verplichtingen:

Identificeer de taakverdeling

Om discussies op het allerlaatste moment te vermijden, identificeer duidelijk een aantal punten in uw contracten:

- Als u de verwerkingsverantwoordelijke bent:
  - de grenzen die u wilt bepalen voor uw verwerker, de bijzondere overeenkomsten (vertrouwelijkheidsovereenkomst, mogelijke audit, verwachte dienstniveaus, ...).
- Als u een verwerker bent:
  - de grenzen die u worden opgelegd door de verwerkingsverantwoordelijke. Deze grenzen mag u niet overschrijden.
  - Breng ook steeds de verwerkingsverantwoordelijke op de hoogte van elke handeling of richtlijn waarvan u denkt dat ze indruist tegen de verplichtingen die voorzien zijn in de GDPR.

Opgelet: De verwerkingsverantwoordelijke en de verwerker kunnen hoofdelijk worden veroordeeld (art. 82 en 83 GDPR).

Bedrijven moeten dus de regels bepalen die ze toegepast willen zien in hun contracten.

Houd een register van verwerkingsactiviteiten bij.

Volgens de nieuwe Europese Algemene Verordening Gegevensbescherming (GDPR/AVG),

- moet elke verwerkingsverantwoordelijke (en, in voorkomend geval, zijn vertegenwoordiger) een register bijhouden met de verwerkingsactiviteiten. Dit register moet de informatie bevatten die bepaald is in artikel 30 van de GDPR.
- Moet elke verwerker en, in voorkomend geval, de vertegenwoordiger van de verwerker, een register bijhouden van alle categorieën van verwerkingsactiviteiten die werden gerealiseerd voor rekening van de verwerkingsverantwoordelijke. Dit register moet de informatie bevatten vereist volgens artikel 30 van de GDPR.

Bekijk het registervoorbeeld op de website van de FOD Economie.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Duid een functionaris voor gegevensbescherming aan[40] (Data Protection Officer of "DPO") en omlijn zijn functies en opdrachten heel precies[41].

De DPO moet worden aangeduid op basis van zijn professionele kwaliteiten en in het bijzonder van zijn gespecialiseerde kennis van het recht en van de praktijken voor gegevensbescherming, van zijn goede kennis van uw onderneming en van zijn vermogen om de opdrachten te volbrengen die u hem toebedeelt. Vergeet ook niet om de boodschap over te brengen aan uw verschillende diensten: de DPO moet op passende wijze en op het juiste moment worden betrokken bij alle kwesties over de bescherming van persoonsgegevens.

Werkt u met een interne DPO, dan moet u hem of haar rechtstreeks laten afhangen van het hoogste machtsniveau in uw onderneming (directeur, beheerder, ...) en moet u elk mogelijk belangenconflict tussen zijn eventuele andere opdrachten en de opdrachten die hij moet volbrengen als DPO vermijden.

Is er sprake van een externe DPO, dan moet u eventuele belangenconflicten vermijden en moet u rekening houden met het risico dat een externe persoon uw onderneming minder goed kent en/of meer moeilijkheden kan ondervinden in zijn relaties met uw verschillende diensten.

Ongeacht of de DPO nu intern of extern is, u moet wel in zijn contract duidelijk stellen dat hij het beroepsgeheim moet respecteren en dat hij een vertrouwensverplichting heeft met betrekking tot de uitvoering van zijn opdrachten[42].

Vergeet ook niet om de gegevens van de DPO mee te delen aan de Gegevensbeschermingsautoriteit (GBA) en deze te publiceren op uw website alsook aan te brengen op uw officiële documenten die bestemd zijn voor uw klanten (natuurlijke personen), zodat de betrokken personen hem gemakkelijk kunnen contacteren[43].

Zorg er ten slotte ook voor dat uw DPO goed is opgeleid (initiële opleiding en voortgezette opleiding)!

Raadpleeg regelmatig de website van de Gegevensbeschermingsautoriteit. Die publiceert talloze templates en richtlijnen om u te helpen.

40 In heel wat gevallen is deze aanstelling verplicht: zie met name artikel 37 en volgende van de GDPR. Een dergelijke aanduiding is weliswaar niet verplicht voor uw onderneming, maar wordt ten stelligste aangeraden.

41 Zie met name artikel 39 van de GDPR.

42 Art.38 GDPR.

43 Art. 37 GDPR.

Werk een procedure uit voor de melding van incidenten

a) Melding aan een toezichthoudende autoriteit (artikel 33 GDPR)

In principe moet de verwerkingsverantwoordelijke bij een inbreuk op de persoonsgegevens dit zo snel mogelijk melden aan de Gegevensbeschermingsautoriteit (GBA) en, indien mogelijk, ten laatste 72 uur nadat hij er kennis van heeft genomen. Wanneer de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.

Het is beter om niet af te wachten en de Gegevensbeschermingautoriteit onmiddellijk te verwittigen, ook al beschikt u niet over alle informatie over het incident. Details bezorgt u naarmate u meer informatie ontvangt.

U moet ook in uw contracten voorzien dat de verwerker de verwerkingsverantwoordelijke zo snel mogelijk moet verwittigen nadat hij zelf op de hoogte werd gebracht van een inbreuk op persoonsgegevens.

b) Mededeling aan de betrokken personen (artikel 34 GDPR)

Wanneer de inbreuk op persoonsgegevens mogelijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke aan de betrokkene de inbreuk op persoonsgegevens onmiddellijk mee.

Deze mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:

- de verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk op persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling[44];
- de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer voordoet;
- de mededeling aan de betrokkene vergt onevenredige inspanningen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

44 Zie woordenlijst.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Indien u het risico aanzienlijk wilt terugdringen, moet u een aantal technische maatregelen overwegen zoals versleuteling[45]: de mededeling aan de betrokken personen moet enkel gebeuren wanneer er een groot risico bestaat dat hun rechten en vrijheden worden aangetast. Als u kunt terugvallen op goede versleutelingssystemen, dan is dit hoge risico weinig waarschijnlijk.

Raadpleeg regelmatig de website van de Gegevensbeschermingsautoriteit (GBA).

Consulteer eveneens:

- ENISA: Guidelines for SMEs
- Cyber Security Coalition: GDPR Check up (2017)
- CNIL (FR): (register, DPIA,...)
- BPI France en CNIL: Guide pratique de sensibilisation au règlement général de protection des données (2018)
- ICO (UK)

4.2.5. Principe 5. Organiseer regelmatig tests en controles

Voer regelmatig een audit uit van uw veiligheidsmaatregelen. Die audit kan intern of extern zijn. Vermijd indien mogelijk situaties waarbij uw digitale aanspreekpunt (adviseur informatiebeveiliging, Data Protection Officer, contactpersoon van uw personeel bij IT-incidenten, ...) zichzelf controleert. U neemt beter iets meer afstand door bijvoorbeeld minstens 1 keer per jaar een beroep te doen op een externe auditeur, om te bekijken of uw veiligheidsmaatregelen voldoende zijn en/of er punten zijn die vatbaar zijn voor verbetering. Let er evenwel op dat u in het contract met een extern auditeur niet alleen het exacte toepassingsgebied preciseert van de tests en de controles, maar ook de regels over veiligheid en vertrouwelijkheid om uw onderneming te kunnen beschermen tijdens de controle...en erna.

Vergeet niet om uw technisch team daar voldoende op voorhand van op de hoogte te brengen om in geval van problemen te kunnen terugvallen op een doeltreffend "herstelpunt"[46].

Vermijd indien mogelijk om testen uit te voeren op productie-omgevingen.

Opgelet: bijzondere maatregelen kunnen ook worden getroffen als uw onderneming wordt aangeduid als kritieke infrastructuur of als aanbieder van essentiële diensten. Aarzel niet

45 Zie woordenlijst.

46 Zie woordenlijst.

om daarover advies in te winnen bij de nationale autoriteit die verantwoordelijk is voor uw sector.

Begrijpt u bepaalde gebruikte termen niet? Raadpleeg dan onze woordenlijst.

4.2.6. Principe 6. Beperk uw risico's en haal indien nodig een goede verzekering in huis!

Op basis van de behoeften van uw onderneming, kunt u uw risico's verzachten, m.a.w. beperken en/of deels verplaatsen: denk bv. aan het verzekeren van uw onderneming tegen cyberrisico's.

Verschillende verzekeraars bieden tegenwoordig en voor een relatief billijke prijs specifieke producten aan. De naam en het toepassingsgebied van deze producten kunnen wel verschillen van de ene verzekeraar tot de andere: verzekering tegen Cyber Risks, Cyberverzekering, ...

Zorg ervoor dat u een duidelijk beeld krijgt van de voorgestelde dekking om te kunnen bepalen welke het beste past bij uw behoeften. Ga ook na of de aansprakelijkheid van de beheerders en bedrijfsleiders wordt gedekt en of u een diefstal- en brandverzekering hebt die uw werkinstrumenten dekt (computers, ...).

Voor meer informatie, lees Cyber Insurance: Recent Advances, Good Practices and Challenges.

4.2.7. Principe 7. Werk een realistisch "Incident Management Plan" uit

Voor cyberincidenten is alles louter een kwestie van tijd. Bent u tot nu toe steeds gespaard gebleven van cyberaanvallen? Dan is de kans groot dat u het volgende slachtoffer bent! U bereidt zich maar beter nu al voor!

Raadpleeg de Incident Management Guide van de Cyber Security Coalition.

4.2.8. Principe 8. Beveilig uw mobiele toestellen

De Smartphone Secure Development Guidelines van het European Network and Information Security Agency (ENISA, 2017) helpen u op weg.

4.2.9. Principe 9. Virtualiseer veilig

Voor meer informatie, raadpleeg Security aspects of virtualization van het ENISA(2017), alsook de Cloud Security Guide for SMEs (ENISA).

Zie ook punt 4.2..10 "Principe 10. Werk aan uw relaties met derden".

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

4.2.10. Principe 10. Werk aan uw relaties met derden

Vergeet niet om gelijkaardige veiligheidsniveaus te plannen in de volledige productieketen. De veiligheid van uw onderneming hangt ook af van de veiligheid van uw leveranciers.

Voorzie verwachte serviceniveaus met uw dienstenleveranciers (Service Level Agreement of SLA) alsook sancties, wanneer ze deze dienstenniveaus niet naleven.

Hieronder kunt u een niet-exhaustieve lijst vinden van clausules die u kunt opnemen in uw contracten:

1. Het vaststellen van een eventuele proeffase: is uw professionele partner klaar voor u?;
2. Herinner uw onderaannemer eraan dat ook hij de GDPR moet respecteren: uw onderaannemer heeft nl. de verplichting om u bij te staan in het kader van het respecteren van de verplichtingen m.b.t. de bescherming van persoonsgegevens (hij moet u bv. onmiddellijk verwittigen wanneer hij een mogelijke inbreuk vaststelt of een mogelijk verlies van gegevens, u de nodige informatie verschaffen voor uw impactanalyse, waken over het respecteren van de veiligheidsregels volgens de "regels van de kunst",...)
3. De identificatie van de locatie van de servers (zijn die gevestigd in Europa?). Indien de servers zich buiten Europa bevinden, vergeet niet om alle specifieke voorzorgsmaatregelen te nemen indien u persoonsgegevens verwerkt;
4. De mogelijkheid om tenminste eenmaal per jaar de door uw professionele partners voorgestelde prijslijst te kunnen raadplegen voor dezelfde type producten/diensten en voor een volume producten/diensten gelijkaardig aan het uwe (beste prijs);
5. Definieer de dienstverleningsniveaus (SLA's): beschikbaarheidsgraad van het systeem (in uren op werkdagen/niet-werkdagen) duur en maximale onbeschikbaarheid van een onderdeel of het systeem op maand-, kwartaal- of jaarbasis; gemiddelde responstijd van een toepassing of bepaalde verzoeken en maximale duur van bepaalde processen, ...;
6. Eisen dat gedurende de looptijd van het contract, aan u het hoogste niveau van dienstverlening geboden wordt, gelijkaardig aan een andere klant van de leverancier en dit voor dezelfde prijs (upgrade);
7. Beschikken over het tijdschema voor eventueel onderhoud (tijdig opdat uw diensten zich kunnen organiseren);
8. Veiligheidsaudits organiseren met de leverancier (definieer de omvang, frequentie, kostendekking, de door de partijen gemachtigde onafhankelijke auditor, ...);

9. Houd ook de onderaanneming van uw leverancier in het oog:
   - ofwel verbiedt u de onderaanneming van uw leverancier, zonder voorafgaande toestemming van uw onderneming met betrekking tot de identiteit van de beoogde onderaannemer en aan de reikwijdte van het beoogde contract (indien deze een verband heeft met de uitvoering van uw contract);
   - ofwel vraagt u om naar behoren te worden geïnformeerd over elke onderaanneming die gevolgen kan hebben voor de aan u aangeboden diensten en eist u dat de verplichtingen en voorzorgsmaatregelen in het contract met uw leverancier eveneens voorzien worden in de contracten met mogelijke onderaannemers (dezelfde regels moeten gelden voor de onderaannemer als voor de leverancier).

10. Voorbereiding op een incident:
    - incidentlogboeken aanvragen en toegang tot het bijhouden van gegevens (logs);
    - indicatoren hebben over de geschiedenis van de gehoste dienst, zoals de frequentie en de opvolging van de uitgevoerde updates (essentieel), de duur van de maximale onbeschikbaarheid en de opvolging van deze onbeschikbaarheid, ...;
    - zorgen voor de opvolging in geval van een incident: wie is de contactpersoon en hoe kan deze gecontacteerd worden (7/7, 24/24) zowel langs uw kant als bij uw leverancier; deze onmiddellijk waarschuwen in geval van aanvallen; escalatiematrices[47] definiëren alsook een definitie van wat juist verstaan moet worden onder "incident";
    - bepaalde handelingen na een incident verbieden of niet uitvoeren zonder uw voorafgaande toestemming (stop, start, herstel via back-up, fysieke isolatie van de rest van het netwerk, verwijderen van de logbestanden van incidenten, ...).

11. Voorzie in het einde van uw relatie (overdraagbaarheidsclausule):
    - deze clausule moet u toelaten het beheer van de uitbestede functie over te nemen, hetzij om deze rechtstreeks te beheren, hetzij om de werking ervan toe te vertrouwen aan een (nieuwe) derde van uw keuze;
    - de leverancier moet zich ertoe verbinden tijdens de migratieperiode de nodige bijstand te verlenen om de overdracht van hardware- en softwarebeveiligingsmiddelen en de overname van de exploitatie ervan door uw onderneming of door een andere door uw onderneming aangewezen dienstverlener te vergemakkelijken;
    - Aan het einde van de uitvoering van het contract zou de leverancier bijvoorbeeld kunnen worden verplicht:
      - ➢ om u informatie te verstrekken over de functionele en technische context van de applicaties, alsook over de vervolgaspecten van het project;
      - ➢ om een computerondersteuning voor te bereiden die in samenwerking met uw diensten wordt gedefinieerd en die alle elementen (documentatie, program-

47 Zie woordenlijst.

ma's, compilatieketens...) bevat die door de huidige leverancier worden beheerd en die aan het einde van deze dienst onder uw verantwoordelijkheid of die van uw toekomstige leverancier zullen worden geplaatst;

- tijdens de overdracht de veiligheid van de haar toevertrouwde gegevens en toepassingen te waarborgen overeenkomstig zijn verplichtingen;
- de kwaliteit en de voorwaarden van de diensten die tot dan toe geleverd werden aan uw onderneming niet te wijzigen zodra de overdraagbaarheidsfase is begonnen;
- als de door uw onderneming aan de leverancier toevertrouwde diensten worden stopgezet, moet alle aan de leverancier toevertrouwde hardware, software en documentatie worden vernietigd of terugbezorgd (vergeet niet een laatste audit te plannen om na te gaan of uw vorige leverancier goed heeft gepresteerd);
- het verzorgen van een diepgaande functionele opleiding (identificatie van het minimale/maximale aantal uren) aan uw personeel of aan dat van de toekomstige leverancier, met praktische training op het werkstation, in aanwezigheid van vertegenwoordigers van uw onderneming. Deze opleiding moet gebaseerd zijn op de gebruikers- en technische documentatie geschreven door uw leverancier.

Als u persoonsgegevens verwerkt, zie ook punt 4.2.4 "Principe 4. Neem maatregelen met betrekking tot de bescherming van de persoonlijke levenssfeer." Begrijpt u bepaalde gebruikte termen niet? Consulteer onze woordenlijst.

4.3. Stap 3. 12 acties

Raadpleeg ook de Gids voor de kmo van de Cyber Security Coalition in samenwerking met het Centrum voor Cybersecurity van België (CCB), die nuttige informatie bevat over de volgende 12 actiepunten:

4.3.1. Actie 1. Betrek het topmanagement erbij

Geef het goede voorbeeld aan uw medewerkers! Laat zien dat u de risico's begrijpt en dat u uw informatieveiligheidsstrategie plant op hetzelfde moment als uw organisatiestrategie.

Om consistent te zijn, vergeet niet om:

- uw activa te identificeren;
- uw prioriteiten (doelstellingen) vast te stellen;
- prestatiemaatstaven te bepalen voor de acties die u binnen uw onderneming hebt ondersteund (KPI);

- een of meerdere personen aan te duiden om verschillende pertinente functies in te vullen binnen uw onderneming die gelinkt zijn aan de veiligheid van informatie.

4.3.2. Actie 2. Publiceer een eigen veiligheidsbeleid en gedragscode.

a) Veiligheidsbeleid

De ideale manier om uw veiligheidsbeleid op te stellen is beproefde methodologieën te gebruiken. Voor meer informatie, zie "punt 8. Belangrijkste normen", het punt "8.1 Informatieveiligheid" en punt "4.2.2. Principe 2. Maak uw personeel bewust van informatieveiligheid".

Vergeet niet om uw gebruikers aan te sluiten bij uw veiligheidsbeleid zodra deze is vastgesteld!

b) Gedragscode

Als u een gedragscode wilt opstellen die uw veiligheidsbeleid respecteert, houd dan rekening met de volgende elementen:

Toegang tot uw resources:

- Wie heeft toegang tot uw internetnetwerk? Tot uw intranet? Tot uw opslagruimte?
- Wie kan toegang krijgen tot uw documenten/gegevens?

Ongewenst gebruik van uw netwerk of opslagruimte:

- raadpleging van pornografische sites, pedofiele sites of sites waarvan de inhoud de waardigheid van anderen kan aantasten;
- het versturen van e-mails voor winstgevende/commerciële doeleinden die geen verband houden met uw onderneming;
- het verzenden van e-mails met de bedoeling de afzender of de auteur van de oorspronkelijke e-mail schade toe te brengen;
- het verzenden van e-mails die de belangen van uw onderneming kunnen schaden;
- de opslag van persoonlijke bestanden op materiaal dat ter beschikking is gesteld aan de gebruikers, met name het gebruik van de professionele opslagruimte voor persoonlijke doeleinden;
- verzenden van bestanden met grote bijlagen (geef de maximaal toegestane bestandsgrootte op).

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

De "grondregels" van de ethiek. Bijvoorbeeld:

- voldoen aan de richtlijnen van de werkgever en het informatieveiligheidsbeleid;
- in het kader van de hun toegekende toegangsrechten en uitsluitend wanneer zij nodig zijn voor de uitoefening van hun functies, gebruikmaken van de hun ter beschikking gestelde informatiemiddelen (bv. gegevens), waarbij zij zich beperken tot de doeleinden waarvoor zij zijn bestemd;
- de beveiligingsmaatregelen op hun werkplek en op de apparatuur die de te beschermen gegevens bevat, in acht nemen en daarnaast de configuratie van de beveiligingsmaatregelen niet wijzigen of buiten werking stellen;
- voldoen aan de wettelijke voorschriften met betrekking tot het gebruik van producten waarvoor intellectuele eigendomsrechten kunnen bestaan, hetgeen met name inhoudt dat de gebruiksvoorwaarden van de licenties worden nageleefd en dat geen software wordt geïnstalleerd op de hardware die door de werkgever zonder diens voorafgaande toestemming wordt geleverd;
- zij stellen hun directe chef of het aangewezen contactpunt onmiddellijk in kennis van elke handeling waarvan zij kennis hebben en die een feitelijke of vermoedelijke inbreuk op de beveiligingsregels zou kunnen vormen, alsook van elke onregelmatigheid die afbreuk zou kunnen doen aan de bescherming van de informatiemiddelen van de vennootschap;
- bij het verlaten van de onderneming, de verschillende toegangskaarten (badges, enz.), de informatiemiddelen en alle computer- en telefoonapparatuur die hun in de uitoefening van hun functie ter beschikking zijn gesteld, overhandigen;
- het personeelslid moet gebruikmaken van zijn persoonlijke authentificatiemiddelen. Deze kunnen niet aan derden worden meegedeeld of toevertrouwd, behalve in het kader van een bijzondere procedure om de continuïteit van de dienst te waarborgen (plotseling vertrek, langdurige ziekte, ...);
- het personeelslid kan de automatische updates van de hem/haar ter beschikking gestelde antivirusprogramma's en bedrijfssoftware niet blokkeren of vertragen;
- het personeelslid oefent zijn taken loyaal, gewetensvol en integer uit, onder het gezag van zijn hiërarchische en functionele meerderen. Hierbij moet hij de geldende wettelijke en bestuursrechtelijke bepalingen alsmede de richtlijnen van de autoriteit waartoe hij behoort, naleven.
- het personeelslid is ook gebonden aan een algemene loyaliteitsplicht jegens zijn werkgever;
- het personeelslid vermijdt elk gedrag of elke handeling die de doeltreffendheid van zijn werk zou kunnen schaden;

- het personeelslid vermijdt buiten zijn werkzaamheden gedragingen of uitlatingen die het vertrouwen van het publiek in de onderneming zouden kunnen schaden. Het gaat onder meer om gedragingen en verklaringen die niet in overeenstemming zijn met de democratische beginselen, in het bijzonder het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, de wet van 30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden, de wet van 23 maart 1995 tot bestraffing van het ontkennen, minimaliseren, rechtvaardigen of goedkeuren van de genocide die tijdens de tweede wereldoorlog door het Duitse nationaalsocialistische regime is gepleegd en het Verdrag inzake de Rechten van het Kind (IVRK), aangenomen te New York op 20 november 1989;
- het is het personeelslid in geen geval toegestaan uit hoofde van zijn functie, rechtstreeks of via tussenpersoon, giften of voordelen van welke aard dan ook te vragen, te eisen of te ontvangen, zelfs niet buiten zijn functie (maar wel om redenen daaraan gelinkt);
- het personeelslid mag geen dossiers behandelen waarin hij direct of indirect een functioneel of persoonlijk belang heeft;

- het personeelslid schept, in de mate van het mogelijke, een vertrouwensrelatie met de klant. Bij de vervulling van zijn taken is hij beschikbaar en zorgvuldig. Het personeelslid gebruikt in zijn contacten met de klant, in welke vorm dan ook, een taal die voor het publiek verstaanbaar is. Het personeelslid behandelt de klant beleefd, respectvol, begripvol en zonder enige vorm van discriminatie, met inachtneming van de democratische beginselen die met name zijn vastgelegd in het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden.

  Verwerking van persoonsgegevens (zie ook punt 4.2.4 Principe 4. Neem maatregelen met betrekking tot de bescherming van de persoonlijke levenssfeer. Bijvoorbeeld:

- Het personeelslid verwerkt de persoonsgegevens met inachtneming van de bepalingen van de regels over de bescherming van de persoonlijke levenssfeer ten aanzien van de verwerking van persoonsgegevens en in het bijzonder met inachtneming van de Algemene Verordening inzake Gegevensbescherming (Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG).
- Personeelsleden mogen de persoonsgegevens waartoe zij toegang hebben, niet gebruiken om zichzelf of anderen direct of indirect voordeel te verschaffen.
- Behoudens de uitzonderingen voorzien in de Algemene Verordening Gegevensbescherming, kan het personeelslid geen bezwaar maken tegen het verzoek van een klant (natuurlijke persoon) om de hem betreffende persoonsgegevens te raadplegen. Het personeelslid wordt verzocht de daartoe vastgestelde procedure te volgen.

4.3.3. Actie 3. Maak uw werknemers bewust van de cyberrisico's.

- Herinner gebruikers regelmatig aan het belang van gezond en veilig gedrag m.b.t. informatieveiligheid.
- Herinner gebruikers er regelmatig aan dat informatie als gevoelig moet worden beschouwd en moet worden behandeld met respect voor de privacyregels.
- Informeer medewerkers van de boekhoudafdeling over het fenomeen "CEO-fraude" en plan procedures voor de controle van de uitvoering van betalingen.
- Informeer gebruikers over hoe ze phishing (e-mailfraude) kunnen herkennen en hoe ze moeten reageren.
- Evalueer regelmatig het bewustzijn en het reactievermogen van gebruikers en integreer zelfs de begrippen kennis en respect voor uw informatieveiligheidsbeleid in de evaluatie van het personeel.

Zie voor meer informatie punt 8.2 Risicobeheer en in het bijzonder ISO/IEC 27005:2011 Risicomanagement Informatiebeveiliging.

U kunt ook de website van Febelfin raadplegen m.b.t. bancaire risico's.

4.3.4. Actie 4. Beheer uw belangrijke ICT-onderdelen.

- Houd een gedetailleerde en bijgewerkte kaart bij van al uw netwerken en interconnecties.
- Stel een inventaris op van alle ICT-apparatuur en softwarelicenties.
- Zorg ervoor dat u de serviceniveaus die u verwacht, correct definieert en voorzie effectieve sancties in geval van beschadiging/verstoring van de diensten (SLA Service Level Agreement). Stel indien nodig een service level manager aan.
- Voer regelmatig een audit uit van alle configuraties (inclusief servers, firewalls en netwerkcomponenten).
- Identificeer de kerncompetenties en de mensen die binnen uw onderneming hierover beschikken.
- Implementeer een proces voor wijzigingsbeheer (change/releasemanager).

4.3.5. Actie 5. Update alle programma's.

- Voer automatische beveiligingsupdates uit van alle software en introduceer een interne patchcultuur[48] (werkstations, mobiele apparaten, servers, netwerkcomponenten, ...).
- Voer vóór de update een volledige serverback-up uit en maak na de update noodreparatieschijven.

4.3.6. Actie 6. Installeer een antivirusbescherming.

- Installeer antivirussoftware op alle servers, werkstations en mobiele apparaten.
- Werk automatisch uw antivirussoftware bij.
- Zorg voor een deskundige (intern en/of extern) die incidenten en waarschuwingen kan analyseren.
- Controleer de effectiviteit van uw antivirus via: http://www.eicar.org.

4.3.7. Actie 7. Maak een back-up van alle informatie.

- Maak dagelijks een back-up van uw belangrijke gegevens.
- Maak offline back-ups en op een aparte locatie (indien mogelijk op afstand van de bron).

48 Zie woordenlijst.

- Host uw back-upoplossingen op uw eigen servers of in de cloud, maar denk na over het beveiligen ervan en indien mogelijk het versleutelen van uw gegevens.
- Voer regelmatig hersteltests uit om de kwaliteit van uw back-ups en processen te beoordelen.

4.3.8. Actie 8. Beheer de toegang tot uw computers en netwerken.

- Onderhoud een beperkte en actuele lijst van accounts van systeemadministratoren en volg de activiteiten op deze accounts nauwlettender op(voornaamste doelwitten).
- Zorg ervoor dat gebruikers enkel toegang krijgen tot de informatie die ze nodig hebben om hun taken uit te voeren (een IAM[49] instellen).
- Voer regelmatig een audit uit op de centrale directory (Active Directory of LDAP[50] directory).
- Voorkom directe internettoegang. Dwing de doorgang via een proxy[51] en IDS[52].
- Spoor onregelmatige toegang tot informatie en systemen op (vertragingen, toepassingen, gegevens, ...).
- Gebruik bij voorkeur een authenticatie op basis van meerdere factoren (bv. wachtwoorden, codes verzonden via sms, ...).
- Stel een effectief wachtwoordbeleid op.
- Denk eraan om alle originele wachtwoorden op de u geleverde hard- en software te wijzigen (routers, firewall, ...).
- Pas de parameters van uw firewall aan in functie van de benodigdheden van uw onderneming.
- Limiteer de geautoriseerde pogingen om zich aan te melden op uw netwerk (3 pogingen).
- Deactiveer ongebruikte accounts onmiddellijk.
- Organiseer het schoonmaken van kantoren tijdens de werkuren of onder permanent toezicht.

49 Zie woordenlijst.

50 Zie woordenlijst

51 Zie woordenlijst.

52 Zie woordenlijst.

4.3.9. Actie 9. Beveilig werkposten en mobiele apparaten.

- Schakel de "Autorun"-functie van externe media uit.
- Verbied de verbinding van persoonlijke apparaten (BYOD[53]) met het informatiesysteem van de organisatie.
- Voorkom technisch dat niet-geregistreerde draagbare media kan worden aangesloten OF Installeer een automatisch antivirusprogramma voor alle externe mediaspelers (USB, ...).
- Houd een "witte lijst" bij van toegestane programma's en een "zwarte lijst" van verboden programma's.
- Herinner het personeel er regelmatig aan dat het belangrijk is om de apparatuur (gsm, pc, tablet, enz.) nooit onbeheerd achter te laten.
- Installeer de automatische vergrendeling na enkele minuten wanneer geen gebruik wordt gemaakt van de werkstations en mobiele apparaten.
- Versleutel informatie op uw servers, clouds en harde schijven van uw laptop.
- Gevoelige of vertrouwelijke gegevens en persoonsgegevens worden idealiter versleuteld verzonden.
- Bewaar en zorg ervoor dat u een kopie hebt van alle bedrijfsgegevens die u nodig hebt.
- Als u een cloudprovider gebruikt, zorg er dan voor dat de garanties van uw provider overeenkomen met het niveau van krikitaliteit van de opgeslagen informatie.
- Vernietig oude harde schijven, media en printers met gegevens OF controleer dat deze op de juiste wijze, volledig en meerdere keren werden schoongemaakt voordat u ze aan een goed doel doneert.
- Vermijd bij voorkeur dat programma's van het type "exe" zonder uw voorafgaande toestemming, worden uitgevoerd.

4.3.10. Actie 10. Beveilig servers en netwerkcomponenten.

- Gebruik veilige toepassingen en protocollen.
- Leg een VPN[54] op voor externe verbindingen.
- Wijzig alle standaardwachtwoorden en deactiveer ongebruikte accounts.

53 Zie woordenlijst.

54 Zie woordenlijst.

- Sluit ongebruikte poorten en diensten.
- Beperk de fysieke toegang tot servers en netwerkcomponenten tot een minimum.
- Registreer alle fysieke toegang tot servers en netwerkcomponenten.
- Gebruik een netwerk dat logistiek gescheiden is van het netwerk van de gebruiker voor serverbeheer.
- Zorg voor een IDS[55]/IPS (inbraakdetectie-/preventiesysteem).
- Bewaar beveiligingslogs op servers en firewalls bij voorkeur 6 maanden.
- Zorg ervoor dat u een SIEM[56] hebt om kwaadaardig gedrag te detecteren.
- Evalueer alle gebeurtenissen en waarschuwingen met betrekking tot server-, firewall- en netwerkcomponenten.
- Voer inbraaktests en kwetsbaarheidsscans uit.
- Versterk alle systemen volgens de aanbevelingen van de leverancier.
- Bescherm de wifi van uw onderneming met de nieuwste en regelmatig bijgewerkte technologieën (WPA2 Enterprise) en registreer uw apparaten.
- Maak een openbaar wifinetwerk los van het netwerk van uw onderneming.
- Bescherm uw domeinnaam tegen "spoofing[57]".

4.3.11. Actie 11. Beveilig de toegang op afstand.

- Beperk de toegang op afstand tot het strikt noodzakelijke.
- De toegang op afstand moet automatisch worden gesloten in geval van inactiviteit gedurende een bepaalde periode.
- Vereis een sterke authenticatie wanneer u verbinding maakt met externe openbare netwerken.
- Sta alleen VPN[58]-verbindingen (Virtual Private Network) toe vanaf eindpunten.
- Beveilig en versleutel alle verbindingen met het bedrijfsnetwerk.

55 Zie woordenlijst.

56 Zie woordenlijst.

57 Zie woordenlijst.

58 Zie woordenlijst.

4.3.12. Actie 12. Zorg voor een bedrijfscontinuïteitsplan (BCP) en voor een incidentbeheerplan.

- Beschik over een incidentbeheersplan om op een incident te reageren en voer regelmatig (ten minste eenmaal per jaar) oefeningen uit om de effectiviteit ervan te testen.
- Zorg voor een bedrijfscontinuïteitsplan om de activiteiten in stand te houden.
- Evalueer en test deze plannen jaarlijks.
- Installeer noodapparatuur voor nutsvoorzieningen (elektriciteit, telefoon, internet,...).
- Overweeg het nut van een verzekering tegen cybersecurityincidenten.

Voor meer informatie over deze acties kunt u de website van het Centre for Cybersecurity Belgium (CCB) raadplegen, evenals de publicaties over incident management op de ENISA-website en de Gids voor Incidentbeheer van de Cyber Security Coalition.

5. Top 10 van incidenten

Elk jaar publiceren de verschillende Computer Emergency Response Teams (CERT[59]) van de lidstaten statistieken van incidenten die zich hebben voorgedaan op hun grondgebied.

Het ENISA (European Network and Information Security Agency) compileert vervolgens de informatie en publiceert een jaarverslag waarin de bedreigingen worden voorgesteld die in Europa werden vastgesteld. Sommige grote categorieën (malware) kunnen ook andere soorten incidenten omvatten (ransomware, phishing, ...).

Dit is de top 10 van de incidenten die het meest werden vastgesteld in Europa in 2017 alsook een aantal goede reflexen die u zich eigen kunt maken op basis van het type incident.

5.1. Malware

De malware[60] die het meest voorkwam in 2017 was ransomware[61] en informatiediefstal, maar er zijn er nog vele andere: Trojaanse paarden[62] (Trojans), PUPs[63] (Potentially

59 of Computer Security Incident Response Team ("CSIRT").

60 Zie woordenlijst.

61 Zie woordenlijst.

62 Zie woordenlijst.

63 Zie woordenlijst.

Unwanted Programs), droppers[64], Command & Control[65] (C&C), key loggers[66], backdoors, ...

De goede reflexen zijn vooral:

- vertrouw niet op een enkele antimalware (geef de voorkeur aan multiscanner/multikanaalsystemen);
- voorzie een detectie op de verschillende gebruikte kanalen (intranet, internet, platformen, pc, gsm, ...);
- voorzie een veiligheidsbeleid en een incident management plan met een punt over malware;
- voorzie analysetools voor malware en blijf op de hoogte van de nieuwste trends;
- doe regelmatig tests en installeer een monitoring.

64 Zie woordenlijst.

65 Zie woordenlijst.

66 Zie woordenlijst.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

5.2. Web-based attacks

"Web-based attacks" zijn aanvallen op browsers[67] (Google, Mozilla, Safari, ...) en hun extensies en op de systemen voor inhoudsbeheer (Content Management Systems of CMS zoals WordPress, Drupal, Joomla, ...).

De goede reflexen zijn met name:

- voer regelmatig updates uit (patches) om de veiligheidsverbeteringen te kunnen toepassen;
- voorzie een beveiliging tegen software waarvan geweten is dat die kwetsbaar is en waarvoor geen patches beschikbaar zijn;
- geef de voorkeur aan een identificatie met verschillende factoren (wachtwoordbeleid, ...);
- wijzig de standaardprefix van de database (bijvoorbeeld wp_ voor WordPress);
- voorzie een regelmatig herstelpunt;
- detecteer en filter de browserplugins[68] (die niet afkomstig zijn van officiële sites).

5.3. Web application attacks

"Web application"-aanvallen zijn aanvallen op webapplicaties en webdiensten. Ze maken meestal misbruik van verkeerde configuraties of zwakke punten in de componenten of in de infrastructuur.

De vaakst voorkomende aanvallen zijn injecties van SQL-code, PHP-injecties, Local File Inclusions (FLI), cross site scriptings (XSS), ...

De goede reflexen zijn met name:

- werk een veiligheidsbeleid uit over de ontwikkeling en het in productie nemen van applicaties;
- gebruik legalisatie- en autorisatiesystemen die werken volgens de regels van de kunst;
- installeer een web application firewalling (WAF)[69] waarmee u HTML-, HTTPS-, SOAP-, XML-RPC-gegevens kunt controleren;

67 Zie woordenlijst.

68 Zie woordenlijst.

69 Zie woordenlijst.

- filter het verkeer door de prestaties op de verschillende kanalen (intranet, internet, e-mails, ...) te verifiëren;
- scan regelmatig en voer inbraakdetectietests uit.

Voor meer informatie raadpleeg

- de website securitymadein.lu
- het witboek van CERT.eu

5.4. Phishing

Phishing[70] ("hengelen") is een type aanval in de vorm van een waarschuwende e-mail (annuleren van uw account, dringende betaling van een factuur met dreiging van inbeslagname, ...) die afkomstig lijkt te zijn van een bekende en vertrouwde onderneming (banken, openbare instellingen, dienstenleveranciers, ...).

De bedoeling is om persoonlijk informatie los te peuteren van de gebruiker (bankgegevens, namen van de accounts van de onderneming, ...).

70 Zie woordenlijst.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Soms stuurt een e-mail met een kopie van het logo van de gekraakte onderneming het slachtoffer door naar een website die eveneens werd gekraakt of wordt het slachtoffer gevraagd om een geïnfecteerde bijlage te openen. De e-mail en de website lijken authentiek en in sommige gevallen is ook het URL-adres zodanig gemaskeerd dat het helemaal correct lijkt.

Uit het lijstje goede reflexen onthouden we vooral:

- sensibiliseren van de werknemers over phishing (zie Cyber Security KIT voor kmo's;
- filteren van e-mails;
- DNS-controle;
- detectie en verwijderen van geïnfecteerde bijlagen;
- detectie van de kenmerken van kwaadaardige URL-links;
- detectie van fraude en van anomalieën op het netwerk;
- verplichte authenticatie o.b.v. meerdere factoren voor alle kritieke elementen (beheer van bankrekeningen, ...).

Meld pogingen tot phishing via de volgende link: verdacht@safeonweb.be

Wanneer u het adres van een phishingsite doorgeeft, wordt elke website gevalideerd. Als het daadwerkelijk gaat om een poging tot phishing, worden de browsers op de hoogte gebracht en blokkeren ze de probleemadressen in hun browseprogramma's. Op die manier draagt u uw steentje bij om de impact te verminderen van dit soort praktijken en vermijdt u dat andere internetgebruikers het slachtoffer worden van fraude.

U kunt ook via dit instrument een URL-adres controleren.

5.5. SPAM

Dit type aanval maakt het vaakst gebruikt van een botnet[71] om massaal kwaadaardige e-mails te versturen met malware (exe-bestanden,...).

Spam is in 2017 kwalitatief beter geworden door bv. een combinatie van informatie waarmee het slachtoffer sneller in de val loopt en een beroep doen op bepaalde technieken om antispamfilters te ontwijken.

71 Zie woordenlijst.

Het merendeel van spam heeft een inhoud gelinkt aan een van de volgende categorieën:

- volwassen inhoud (seksuele aard);
- kettingbrieven;
- gezondheid en pseudofarmaceutische producten;
- IT en pseudovirussen die uw systeem hebben geïnfecteerd;
- bankzaken ("dringende" vragen waarbij bankgegevens verzonden moeten worden);
- winnaar van een valse loterij;
- Nigeriaanse oplichting (hulp wordt gevraagd bij het bewegen/transfert van monetaire buitenlandse fondsen);
- educatie (belofte van beurzen in grote universiteiten, ...).

Uit het lijstje goede reflexen onthouden we met name:

- maak een lijst van gekende spammers[72] en blokkeer alle e-mail inkomend van hun botnet;
- geschikte filters gebruiken (content filtering en reputatie, realtime blacklist (RBL), antispam, antimalware, enz.);
- blokkeer uitvoerbare bestanden (.exe) toegevoegd aan e-mails;
- verhinder de automatische uitvoering van codes, macro's, grafieken, enz.;
- sensibiliseer medewerkers (geen bijlagen openen uit verdachte e-mails...);
- scan en filter e-mails met bijlagen.

5.6. DDoS

Distributed Denial of Service-aanvallen zijn gericht tegen een website of een server en willen vermijden dat die op een correcte manier kan werken en dat legitieme gebruikers van een dienst die normaal kunnen gebruiken. Om doeltreffend te zijn, berust dit soort aanvallen meestal op een groot aantal besmette geconnecteerde objecten (botnet[73]). Door de toestroom van een enorme hoeveelheid informatie kan de aangevallen website of server deze talloze verzoeken niet meer behandelen en is hij ook dus niet meer bereikbaar.

72 Een lijst met de 10 meest gekende spammers ter wereld wordt regelmatig bijgewerkt en staat gratis ter beschikking op de website SPAMHAUS.

73 Zie woordenlijst.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Door het steeds groter wordend aantal geconnecteerde objecten (IoT, Internet of Things)[74], allemaal mogelijke zwakke schakels waarop cyberaanvallers hun oog kunnen laten vallen, bestaat jammer genoeg het vermoeden dat dit soort aanvallen in de toekomst wel vaker zal voorkomen.

Uit het lijstje goede reflexen, onthouden we met name:

- voorzie een veiligheidsbeleid en een Incident Management Plan met een punt over DDoS-aanvallen;
- ga bij voorkeur in zee met een leverancier van internettoegang (FAI of ISP) die beschermingsmaatregelen implementeert tegen DDoS-aanvallen;
- gebruik specifieke instrumenten: Firewall based, Access Control Lists (ACLs), Load Balancer, IPS/WAF, Intelligent DDoS mitigation systems (IDMS), Cloud-based DDoS mitigation service, ...
- controleer en test de maatregelen die door de onderneming worden genomen en haar reactievermogen;
- voorzie een Intrusion Prevention System (IPS) want sommige DDoS-aanvallen kunnen een inbraakpoging maskeren.

Voor meer informatie, lees:

- het witboek van Cert.be: DDoS Proactive and Reactive measures
- de pagina DDos attacks: how to protect yourself.
- Het witboek van Cert.eu: DDOS: Overview and Response Guide (2017)

5.7. Ransomware

Ransomware is een schadelijk programma dat gegevens versleutelt op het geïnfecteerde toestel en dat belooft om de gegevens opnieuw toegankelijk te maken mits de betaling van losgeld (in bitcoins).

Meer informatie vindt u terug op:

- de website No more ransom!
- de website Ransomfree.cybereason

74 Zie woordenlijst.

© zephy_P - Fotolia.com

Uit het lijstje goede reflexen onthouden we met name:

- zorg voor een goed back-upbeheer (reservekopie, bij voorkeur elders bewaard);
- zorg voor een doeltreffend antivirusprogramma;
- update uw besturingssysteem (OS) en de programma's;
- activeer de functie "Extensie weergeven van de bestandsnamen" in de configuratie van het besturingssysteem (OS)[75] van uw computer. Op die manier spoort u makkelijker mogelijk kwaadaardige bestanden op. Wees voorzichtig met extensies zoals ".exe", ".vbs" en ".scr". Mensen met slechte bedoelingen kunnen verschillende extensies gebruiken om een kwaadaardig bestand te camoufleren als een video, een foto of een document (zoals hot-chics.avi.exe of doc.scr);
- wanneer u een verdacht of onbekend proces ontdekt op uw machine, verbreek dan onmiddellijk de verbinding met internet of verbreek elke netwerkconnectie (zoals de wifi van de onderneming); zo vermijdt u dat infecties zich verspreiden terwijl u wacht op de interventie van een technisch team;

75 Zie woordenlijst.

- denk eraan om gespecialiseerde websites te raadplegen waar u vaak handige tips en tricks vindt over preventie en om besmette toestellen weer schoon te maken, bv.
  - » https://www.nomoreransom.org/
  - » https://ransomfree.cybereason.com/

Meer informatie vindt u ook in de gids "Ransomware. How to protect and respond" van het CERT.

5.8. Botnets

Een botnet is een netwerk van geconnecteerde objecten ("een leger van zombie-apparaten") die worden gebruikt - vaak zonder dat de eigenaars zich daar bewust van zijn - om websites of servers van bedrijven en organisaties aan te vallen door deze te bestoken met verzoeken of met malware (zie DDoS, e-mails met schadelijke bijlagen, ...).

Om het even welk object dat verbonden is met internet kan deel uitmaken van een botnet. Dit is het verloop: een kwaadaardig programma besmet een object dat verbonden is met internet maar blijft onzichtbaar. Het wacht op een opdracht van de cybercriminelen. Zodra de cybercriminelen voldoende geconnecteerde objecten hebben besmet, geven ze de opdracht aan die geïnfecteerde objecten om een bepaalde website of server te bestoken. Botnets kunnen ook worden verhuurd aan andere cybercriminelen via het darkweb.

Uit het lijstje goede reflexen onthouden we met name:

- installatie en configuratie van het netwerk en van een firewall;
- analyse van de prestaties van het verkeer op alle gebruikte kanalen (intranet, internet, e-mails, ...);
- installatie van zwarte lijsten met gedetecteerde besmette IP-adressen[76];
- installatie van Botnet Sinkholing (door de detectie van een aanval via botnet kunnen de aanvallen worden afgeleid naar een soort van bliksemafleiderserver die dan gebruikt wordt om allerlei gegevens te verzamelen over de uitgevoerde aanval).

76 Een lijst van 's werelds toonaangevende botnets wordt regelmatig bijgewerkt en is vrij beschikbaar op de website van SPAMHAUS.

5.9. Insider Threat

De Insider Threat[77] of "interne bedreiging" is meestal het resultaat van een onachtzaamheid of gewoon een onhandigheid, maar het kan ook gaan om een kwaadwillige daad van een van uw (ex-) werknemers.

Uit het lijstje goede reflexen onthouden we met name:

- beperkte administratoraccounts en implementering van een Privileged Identity Management (PIM)[78];
- invoering van een Identity and Access Management (IAM)[79](definitie van de functies);
- sensibilisering van uw werknemers over wat ze wel en niet mogen doen met de werkinstrumenten die hen worden toevertrouwd;
- een veiligheidsbeleid waarin aandacht wordt besteed aan een bijzonder punt in het geval van het ontslag van een of meerdere van uw werknemers;
- organisatie van een risicobeheer op basis van de verschillende functies;
- instrumenten voor de analyse van gegevens;
- monitoring van de gebruikers (misbruik van vaste rechten) en regelmatige audit.

5.10. Fysieke beschadiging, verlies of diefstal

Fysieke beschadigingen zijn dan wel geen echt cyberrisico, ze vormen wel een belangrijke bedreiging.

Het kan hier gaan om het verlies/de diefstal van USB-sticks waarop al dan niet versleutelde belangrijke informatie staat, de diefstal van servers (onbeveiligde zaal), diefstal van gsm's waarop dossiers of e-mails staan met belangrijke informatie, het niet-verlengen van onderhoudscontracten met als gevolg defecte servers, noodbatterijen die niet aangaan bij een stroomonderbreking, ...

77 Zie woordenlijst.

78 Zie woordenlijst.

79 Zie woordenlijst.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Uit het lijstje goede reflexen onthouden we met name:

- het versleutelen van alle informatie die op mobiele dragers (gsm, USB-sticks, ...) staat, en ook op uw netwerk;
- een tabel bijhouden van de onderhoudscontracten met een retroplanning om die op tijd te kunnen vernieuwen;
- een lijst bijhouden van toegestane dragers (en andere dragers verbieden);
- procedures uitwerken voor de werknemers opdat ze zouden weten hoe ze moeten reageren bij diefstal van materiaal (pc, gsm, USB, ...) en uw personeel sensibiliseren;
- eventueel een aangepaste verzekering afsluiten tegen diefstal en cyberrisico's.

Voor meer informatie raadpleeg CIRCLean - USB key sanitizer.

Kijk ook eens op websites die gespecialiseerd zijn in technische alarmmeldingen om mee te zijn met de nieuwste trends op het vlak van kwetsbaarheden en bedreigingen:

- ENISA
- CERT.be
- US-CERT
- CASES

6. Een incident doet zich voor ... Wat moet u doen?

Hebt u een aangepast plan (Incident Management Plan, Disaster Recovery Plan, ...), pas dan de regels toe die voorzien zijn op basis van het soort incident (Zie ook punt 8. Belangrijkste normen).

Neem meteen contact op met het CERT.be[80].

WIE CONTACTEREN?

Politie

Aarzel niet om een klacht in te dienen bij de lokale politie. Die geeft de informatie vervolgens door aan de bevoegde politieautoriteiten, met name de Federal Computer Crime Unit (FCCU) of de Regional Computer Crime Unit (RCCU) waar u van afhangt.

U kunt ook naar uw wijkcommissariaat gaan of contact opnemen met de politie op de volgende nummers: 112 of 101.

80 Zie de rubriek "Wie contacteren?"

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Computer Emergency Response Team (CERT)

Ongeacht of u nu een klacht indient bij de politie, moet u steeds contact opnemen met het Computer Emergency Response Team dat u de eerste tips geeft bij een incident.

Officiële website: https://www.cert.be/nl.html
E-mail: cert@cert.be
Telefoon: +32 2 501 05 60 (werkdagen tussen 9 en 17 uur).

Gegevensbeschermingsautoriteit

De Gegevensbeschermingsautoriteit is de nationale autoriteit die bevoegd is voor alle inbreuken op de verwerking van persoonsgegevens.

Door de gepaste technische en organisatorische beschermingsmaatregelen kan snel worden achterhaald of zich een schending van persoonlijke gegevens heeft voorgedaan en zo ja, stellen deze maatregelen de onderneming die verantwoordelijk is voor de verwerking van gegevens in staat om snel te reageren en onmiddellijk de Gegevensbeschermingsautoriteit en, in voorkomend geval, de betrokken personen op de hoogte te brengen.

Bent u verwerker in de zin van de bepalingen met betrekking tot de bescherming van de privacy, vergeet dan niet om ook onmiddellijk de verwerkingsverantwoordelijke te verwittigen!

De Gegevensbeschermingsautoriteit moet onmiddellijk op de hoogte gebracht worden van de gegevensschending en ten laatste binnen 72 uur na de ontdekking van het incident met de persoonsgegevens.

Officiële website: https://www.gegevensbeschermingsautoriteit.be/

Adres:

Gegevensbeschermingsautoriteit
Drukpersstraat 35
1000 Brussel

Tel.: +32 2 274 48 00 of +32 2 274 48 79
Fax: +32 2 274 48 35
E-mail: contact@apd-gba.be

De kantoren van de Gegevensbeschermingsautoriteit zijn alle werkdagen toegankelijk op afspraak. U kunt evenwel steeds hun onlinecontactformulier gebruiken.

Nationale autoriteit verantwoordelijk voor uw sector

Op basis van de sector waar u van afhangt, ziet u of u de nationale autoriteit moet verwittigen die verantwoordelijk is voor uw sector (BIPT, NBB, ...).

7. Meer weten? Actoren en nuttige links

Wilt u meer informatie over de verschillende actoren op het vlak van cyberveiligheid?

Actoren

In België

Gegevensbeschermingsautoriteit

CERT.be

Politie, FCCU/RCCU: contacteer uw wijkpolitie

In Europa en geallieerde landen

ECSO: vereniging zonder winst (vzw) opgericht op initatief van de Europese Commissie, die het mogelijk maakt voor de private en de publieke sector om hun standpunten te overleggen in het kader van cybersecurity.

ENISA: of "European Union Agency for Network and Information Security", publiceert talrijke documenten m.b.t. cybersecurity t.a.v.ondernemingen, m.n. richtlijnen over de verwerking van persoonsgegevens (AVG/GDPR) of het beheer van clouddiensten. Zie ook de woordenlijst, de quiz over cybersecurity en de bescherming van persoonlijke levenssfeer alsook de oefeningen gericht aan de cyberexperts in uw onderneming.

CERT.eu: of het Europees "Computer Emergency Response Team", produceert richtlijnen (guidelines) en witboeken (white papers) in het kader van cybersecurity. Zij identificeren ook de voornaamste cyberbedreigingen op Europees niveau.

Nuttige links

ANSSI: officiele Franse cybersecuritysite. Het ANSSI biedt gratis een online cybersecurityopleiding aan en onderhoudt ook een lijst met cyberproducten die met succes gecertificeerd zijn.

BIPT: stelt publieke informatie m.b.t. telecommunicatie ter beschikking (bv. de dekking van de verschillende netwerken,...).

CASES (LU): officiële Luxemburgse cybersecuritysite. Zie vooral de tool voor auto-evaluatie, het systeem START/FIT/TOP en de risicoanalyse MONARC.

CCB: of Centrum voor Cybersecurity België.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

CNIL (FR): officiële Franse website welke adviezen, documenten en tools aanbiedt om de Algemene Verordening Gegevensbescherming (AVG/GDPR) correct te implementeren. CNIL heeft ook een gids gepubliceerd voor kmo's/micro-ondernemingen alsook documenten m.b.t. de impactanalyse voor de bescherming van gegevens (DPIA) en een lijst met beveiligingstools die hun nut bewezen hebben.

CyberSecurity Coalition: de coalitie biedt een cybergids aan, een sensibiliseringskit m.b.t. cybersecurity, een eerste vragenlijst om uw matuurheid m.b.t. de GDPR te meten, ...

FOD Economie: van het oprichten van domeinnamen, tot aan de verzekering, de FOD Economie begeleidt kmo's in het opstellen van hun digitale strategie.

IA SME: Engelse website (UK) welke andere vragenlijst voor auto-evaluatie aanbiedt.

ICC The International Chamber of Commerce heeft een ICC Guide to Cybersecurity for Businesses gepubliceerd waarop deze handleiding is gebaseerd voor de Onderneming 1.0 sectie.

INFO SEC: een expertengroep welke evenementen organiseert in het kader van verschillende problematieken inzake cybersecurity (cryptografie, 5G, IoT, ...).

NCSC (NL): officiële Nederlandse cybersecuritysite. Zie m.n. de sensibilisatiecampagne "Cyber Save Yourself".

NCSC (UK): officële cybersecuritysite van het Verenigd Koninkrijk. Naast talrijke richtlijnen, biedt deze site ook wekelijkse rapporten aan m.b.t. aangetroffen bedreigingen.

NIST: of "National Institut of Standard and Technologies", een site uit de Verenigde Staten die talrijke publicaties, workshops en webinars aanbiedt.

UCM: voert enquêtes uit en volgt de uitdagingen m.b.t. cybersecurity voor kmo's.

UNIZO

VBO: biedt een cybsersecuritygids aan, een publicatie m.b.t. GDPR en organiseert talrijke events gelinkt aan cybersecurity.

Afhankelijk van het gewest waar u woont, kunt u ook het agentschap voor steun aan ondernemingen dat op u betrekking heeft, contacteren. Uw agentschap kan u eveneens kostbare informatie geven over financiering.

8. Belangrijkste normen

Voor meer informatie over de verschillende normen raadpleeg het ENISA-rapport Information security and privacy standards for SMEs.

8.1. Informatieveiligheid

ISO/IEC 27001:2013 Information security management systems – Requirements

ISO/IEC 27002:2013 Code of practice for information security controls

ISO/IEC 27003:2010 Information security management system implementation guidance

ISO/IEC 27004:2009 Information security management – Measurement

ISO/IEC 27013:2012 Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

ISO/IEC 27014:2013 Governance of information security

ISO/IEC TR 27016:2014 Information security management - Organisational economics

ISO/IEC 27032:2012 Guidelines for information security

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

ISO/IEC 27033-1:2009 Network security - Part 1: Overview and concepts

ISO/IEC 27033-2:2012 Network security - Part 2: Guidelines for the design and implementation of network security

ISO/IEC 27033-3:2010 Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues

ISO/IEC 27033-4:2014 Network security - Part 4: Securing communications between networks using security gateways

ISO/IEC 27033-5:2013 Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

ISO/IEC 27034-1:2011 Application security - Part 1: Overview and concepts

ISO/IEC 27039:2015 Selection, deployment and operations of intrusion detection systems (IDPS)

ISO/IEC 27040:2015 Storage security

CSA Cloud Controls Matrix

BSI PAS 555:2013 Cyber security risk. Governance and management.

PCI Data Security Standard

ISF The Standard of Good Practice for Information Security

UK Gov. Security policy framework

UK Gov. Cyber essentials scheme

ETSI GS ISI 001 Part 1: A full set of operational indicators for organisations to use to benchmark their security posture

ETSI TR 103 305 Critical Security Controls for Effective Cyber Defence

BSI 100-1 Information Security Management Systems (ISMS)

BSI 100-2: IT-Grundschutz Methodology

8.2. Risicobeheer

ISO/TR 31004:2013 Risk management - Guidance for the implementation of ISO 31000

ISO/IEC 27005:2011 Information security risk management

ISO/IEC 31000 Risk management - Risk assessment techniques

IEC 31010:2009 Risk management - Risk assessment techniques

BSI BIP 0076 Information Security risk management (Handbook for ISO/IEC 27001)

BSI 100-3: Risk Analysis based on IT - Grundschutz

8.3. Business Continuity Plan

ISO 22301:2012 Business continuity management systems – Requirements [3]

ISO 22313:2012 Business continuity management systems – Guidance

ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity

100-4: Business Continuity Management

8.4. Bescherming van persoonsgegevens

ISO/IEC 27018:2014 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 29100:2011 Privacy framework

ISO/IEC 29101:2013 Privacy architecture framework

BSI BS 10012:2009 Data protection. Specification for a personal information management system

CEN CWA 16113:2010 Personal Data Protection Good Practices

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

8.5. Incident Management Plan

ISO/PAS 22399:2007 Societal security - Guideline for incident preparedness and operational continuity management

ISO/IEC 27035:2011 Information security incident management

ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence

8.6. Relaties met derden

ISO/IEC 27036-1:2014 Information security for supplier relationships - Part 1: Overview and concepts

ISO/IEC 27036-2:2014 Information security for supplier relationships - Part 2: Requirements

ISO/IEC 27036-3:2013 Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security

8.7. Specifieke normen (sectoraal)

ISO/TR 13569:2005 - Financial services - Information security guidelines [Financial Services]

ISO/IEC TR 27015:2012 - Information security management guidelines for financial services [Financial Services]

ISO/IEC TR 27019:2013 - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry [Energy]

ISO 27799:2008 - Information security management in health using ISO/IEC 27002 [Healthcare]

ISO 22307:2008 Financial services - Privacy impact assessment [Financial Services].

Vooruitgangstraat 50
1210 Brussel
Ondernemingsnummer: 0314.595.348
https://economie.fgov.be