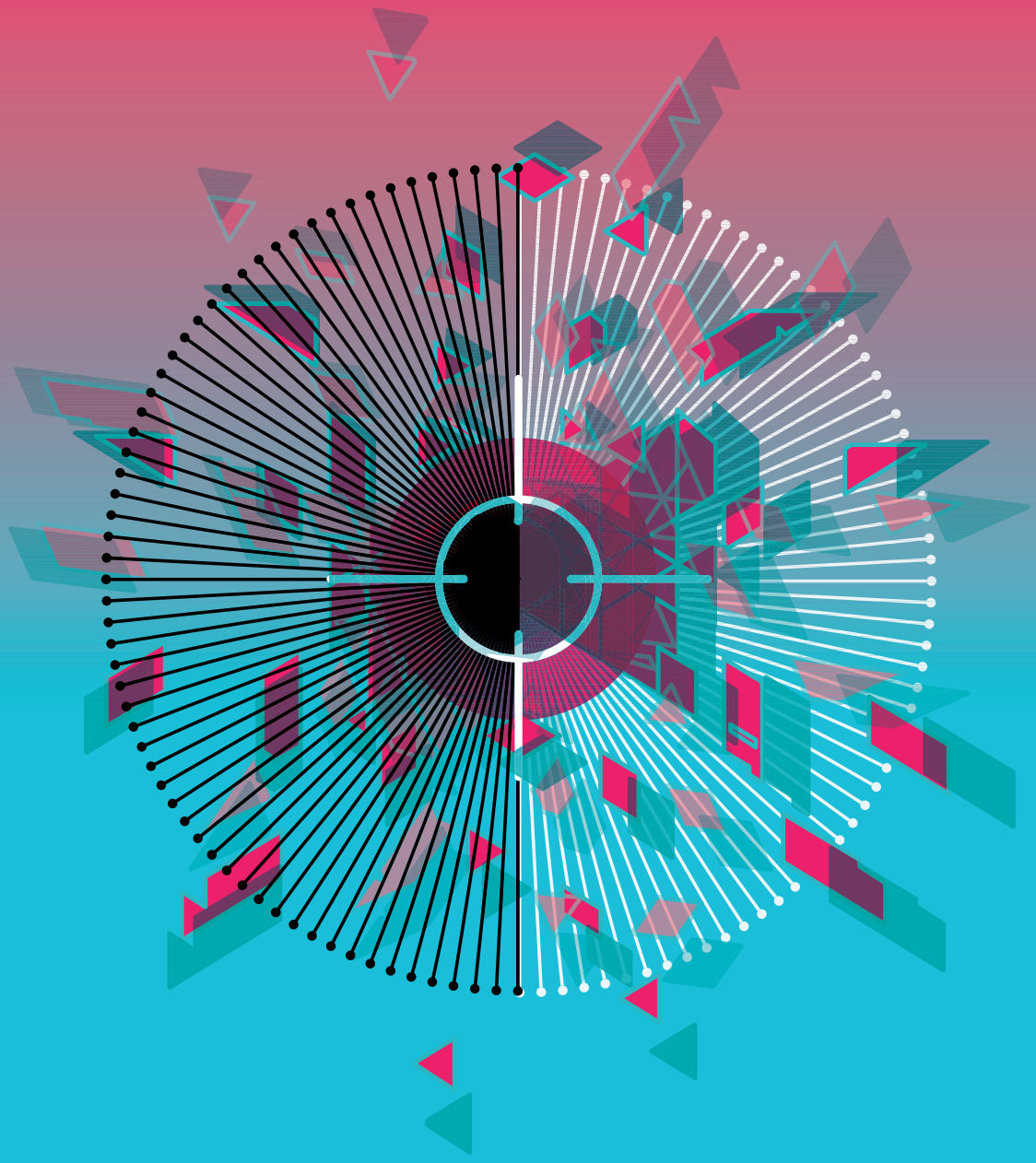
CENTRE FOR
CYBER SECURITY
BELGIUM

CYBER SECURITY
COALITION.be

CYBERVEILIGHEID
GIDS VOOR INCIDENTBEHEER

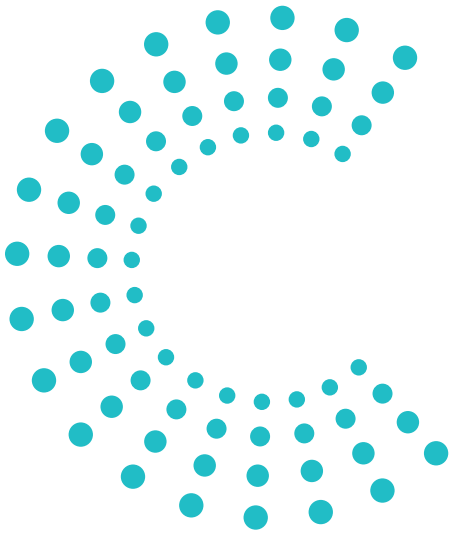


OVER DE CYBER SECURITY COALITION

De Cyber Security Coalition is een uniek samenwerkingsverband tussen spelers uit de academische wereld, de publieke sector en het bedrijfsleven, met als doel de krachten te bundelen tegen cybercriminaliteit. Meer dan 100 kernspelers uit deze drie sectoren zijn op dit moment actief lid. Zij dragen bij aan de missie en de doelstellingen van de Coalition.

De Coalition biedt een antwoord op de dringende behoefte aan een samenwerking over alle sectoren heen om kennis en ervaring te delen, om concrete multidisciplinaire initiatieven te starten, te organiseren en te coördineren, **om burgers en organisaties te sensibiliseren**, om de ontwikkeling van expertise te promoten en om aanbevelingen te geven voor een efficiënter beleid en betere regelgeving.

Met deze gids willen we zowel kleine als grote bedrijven laten inzien hoe belangrijk het is om het beheer van cyberveiligheidsincidenten vooraf te plannen.



SAMEN-VATTING

Deze gids wil de aandacht vestigen op het belang om tijdig te plannen hoe cyberveiligheidsincidenten zullen worden aangepakt.

Het beheer van cyberveiligheidsincidenten is geen lineair proces maar een cyclus die bestaat uit een **voorbereiding**, **detectie** incident**inperking**, **risicobeperking en herstel**. De laatste fase is er een van lessen trekken uit het incident om het proces te verbeteren en zich **voor te bereiden op toekomstige incidenten**. Tijdens deze cyclus is **communicatie** met zowel interne als externe belanghebbenden uiterst belangrijk.

Vele organisaties beschikken intern niet over de nodige expertise en vaardigheden om gepast te reageren op een cyberveiligheidsincident. Wanneer ze met een incident worden geconfronteerd, moeten ze mogelijk een beroep doen **op experts** om het incident onder controle te krijgen en/of forensisch onderzoek uit te voeren. Dit betekent niet dat ze zelf niets kunnen doen. Integendeel, er zijn heel wat zaken die kunnen en moeten gebeuren voor er zich een echt incident voordoet.

Een eerste belangrijke stap in de aanpak van cyberveiligheidsincidenten is het opstellen van een **incidentresponsplan** voor de organisatie. Het is ook van groot belang dat het **topmanagement dit plan goedkeurt** en **betrokken** is bij elke stap in de cyclus van de aanpak van de cyberveiligheidsincidenten.
De volgende elementen dienen te worden opgenomen in het incidentresponsplan voor cyberveiligheidsincidenten:

- Wat er moet worden beveiligd? Welke informatie, systemen, netwerk, producten, …?;
- Identificatie en toewijzing van **verantwoordelijkheden**;
- **Interne bekwaamheden** of contracten met **externe experts** voor de aanpak van incidenten en/of forensisch onderzoek;
- De **apparatuur en technologie**;
- **Een basisinperkingsstrategie**: de systemen onmiddellijk loskoppelen om zo snel mogelijk te herstellen? Of de tijd nemen om bewijzen te verzamelen?
- Een **communicatie**strategie voor zowel interne als externe belanghebbenden en voor autoriteiten zoals ordehandhavers, de Gegevensbeschermingsautoriteit en de bevoegde instanties voor het melden van Netwerk- en informatiebeveiligings-incidenten.

Aanbieders van essentiële diensten en digitaledienstverleners, zoals beschreven in de Belgische Netwerk- en Informatiebeveilingswet van 7 april 2019, zijn onderworpen aan specifieke verplichtingen inzake de beveiliging van hun informatiesystemen en het wapenen tegen en melden van incidenten. De informatie in deze gids kan helpen om de juiste maatregelen te treffen om aan dit laatste te kunnen voldoen.

Ten slotte kunnen organisaties overwegen om een cyberverzekering af te sluiten. De kosten van cyberveiligheidsincidenten lopen vaak op tot honderdduizenden of zelfs miljoenen euro's. Een betrouwbare cyberverzekering dekt in elk geval een deel van deze kosten.

INHOUD

SAMENVATTING 3

VOORWOORD 5

BASISBEGINSELEN EN -DEFINITIES 6

01 ZICH VOORBEREIDEN OP EEN CYBERVEILIGHEIDSINCIDENT 8

I. Een incidentresponsplan voor cyberveiligheidsincidenten opstellen en up-to-date houden
II. Inhoud van een incidentresponsplan voor cyberveiligheidsincidenten
III. Verantwoordelijkheden toewijzen en een incidentresponsteam voor cyberveiligheidsincidenten samenstellen
IV. Externe experts
V. Is uw organisatie uitgerust om een cyber-veiligheidsincident aan te pakken?
VI. Uw communicatiestrategie voorbereiden
VII. Cyberverzekering

02 CYBERVEILIGHEIDSINCIDENTEN DETECTEREN EN IDENTIFICEREN 20

I. Categorieën van incidenten
II. Methodes om incidenten te detecteren

03 EEN INCIDENT AANPAKKEN: ONDER CONTROLE KRIJGEN, VERWIJDEREN EN HERSTELLEN 22

I. Uw incidentresponsteam voor cyberveiligheidsincidenten bijeenroepen
II. Beeldvorming
III. Een cyberveiligheidsincident onder controle krijgen
IV. Eliminering en sanering
V. Herstellen

04 COMMUNICATIE TIJDENS EEN CYBERVEILIGHEIDSINCIDENT 29

I. Middelen
II. Incidentspecifiek communicatieplan

05 NABESPREKING EN AFSLUITING VAN HET INCIDENT: LESSEN TREKKEN VOOR DE TOEKOMST 36

I. Evaluatie van geleerde lessen en toekomstige acties: organiseer een nabespreking van het incident
II. Opvolgen van en rapporteren over incidenten

WOORDENLIJST 38

BIBLIOGRAFIE 40

DANKBETUIGING 41

BIJLAGE 42

VOORWOORD

Er zijn slechts twee soorten bedrijven, zij die gehackt zijn en zij die gehackt zullen worden.

Robert Mueller

Het internet heeft een revolutie teweeggebracht in de manier waarop we zaken doen: de hoeveelheid gegevens die we via het internet verzenden en onze afhankelijkheid van de beschikbaarheid ervan worden elke dag groter. Het is overduidelijk dat onze verbinding met de wereld niet alleen geweldige mogelijkheden oplevert, maar ook nieuwe risico's met zich brengt. Cybercriminaliteit is 'big business' en zelfs de kleinste kwaadwillige aanval kan zware schade toebrengen aan de reputatie, productiviteit, ICT-systemen enz. van een organisatie.

Geen enkele organisatie mag denken dat ze veilig is voor cybercriminaliteit. Cybercriminelen richten zich niet alleen op grote organisaties. Integendeel, een kleine organisatie kan een veel interessanter slachtoffer zijn wegens de informatie die ze verwerkt of zelfs de partners waar ze mee samenwerkt.

Deze gids vestigt de aandacht op hoe belangrijk het is te beseffen dat uw organisatie vandaag of morgen het doelwit kan zijn van een cyberaanval. En wanneer dat gebeurt, bent u best goed voorbereid. Een goed responsplan voor cyberveiligheidsincidenten kan het verschil uitmaken tussen een cyberveiligheidsincident en een cyberveiligheidscrisis. De snelheid waarmee een organisatie een incident kan herkennen, analyseren en erop kan reageren, heeft immers een belangrijke impact op de grootte van de schade en de herstelkosten.

Een dergelijk responsplan voor cyberveiligheidsincidenten mag niet beperkt blijven tot technologie alleen. Processen, mensen en andere organisatorische aspecten zijn ook belangrijke elementen waarmee rekening moet worden gehouden.

Verwacht echter niet dat u na het lezen van deze gids meteen een expert wordt in de aanpak van cyberveiligheidsincidenten. Waarom niet? De reden is eenvoudig: het vraagt tijd en ervaring om de nodige expertise te verwerven om cyberveiligheidsincidenten efficiënt te kunnen aanpakken. Incidentbeheer is een leerproces dat gepaard gaat met vallen en opstaan.

Jan De Blauwe
Voorzitter van de Cyber Security Coalition

Miguel De Bruycker
Directeur van het Centrum Cyberveiligheid België (CCB)

BASISBEGINSELEN & -DEFINITIES

Wanneer u deze Gids voor incidentbeheer leest, moet u de volgende basisbeginselen en -definities in gedachten houden.

BASISDEFINITIES

Aan het einde van deze gids vindt u een volledige woordenlijst. Hierna geven we enkele belangrijke definities, die nodig zijn om het toepassingsgebied en de inhoud van deze gids te begrijpen.

CYBERVEILIGHEIDSEVENT
Een wijziging in de cyberveiligheid die een invloed kan hebben op activiteiten van de organisatie (inclusief missie, mogelijkheden of reputatie).

CYBERVEILIGHEIDSINCIDENT
Eén of een reeks ongewenste of onverwachte cyberveiligheidsevents die waarschijnlijk de activiteiten van de organisatie in het gedrang brengen.

BEHEER VAN CYBERVEILIGHEIDSINCIDENTEN
Processen voor het voorbereiden, detecteren, rapporteren, beoordelen van, reageren op, behandelen van en leren uit cyberveiligheidsincidenten.

1.

Een oplossing op maat

Elke organisatie is anders. Als het om cyberveiligheid gaat, **is er geen oplossing die voor iedereen werkt**. Wat werkt voor uw organisatie, hangt af van uw missie en doelstellingen, het type infrastructuur en informatie die u beveiligt, de beschikbare middelen enz. Besef ten slotte dat u sommige technieken alleen kunt leren beheersen door **tijd en ervaring**. Dit mag u er echter niet van weerhouden om ermee van start te gaan!

2.

Engagement van het topmanagement

Cyberveiligheidsincidenten zijn een risico dat vervat moet zijn in het algemene risicobeheerbeleid van uw organisatie. Bovendien gaat de aanpak van cyberveiligheidsincidenten verder dan het louter toepassen van technologie. Het vereist ook de ontwikkeling van een plan dat in de bestaande processen en structuren van de organisatie wordt geïntegreerd, zodat het de kritieke bedrijfsfuncties mogelijk maakt in plaats van hindert. Daarom moet het topmanagement **actief worden betrokken** bij het opstellen van het plan van de organisatie voor cyberveiligheidspreventie en de respons op incidenten. De uitdrukkelijke steun van het topmanagement via de gepaste interne communicatie en de **toewijzing van personeel en financiële middelen** is van het grootste belang voor het welslagen van het plan.
Een goed ingelichte topmanager is zich bewust van zowel de risico's van cybercriminaliteit als van zijn eigen **voorbeeldfunctie** in het aanmoedigen van alle werknemers van de organisatie om hun verantwoordelijkheid op te nemen.

3.

Elke werknemer van uw organisatie betrekken

Er wordt vaak gezegd dat mensen de zwakste schakel vormen als het over cyberveiligheid gaat. Anderzijds moeten we ook beseffen dat de werknemers van uw organisatie u in grote mate kunnen helpen bij het detecteren en identificeren van cyberveiligheidsincidenten. Zorg ervoor dat elke medewerker van uw organisatie **uw incidentresponsplan voor cyberveiligheidsincidenten en zijn eigen rol** daarin kent, zelfs als dit alleen betekent dat hij de juiste persoon moet inlichten over ICT-anomalieën die hij toevallig opmerkt.

4.

Houd de documenten die u nodig hebt tijdens een incident ook offline beschikbaar

Tijdens een cyberveiligheidsincident hebt u niet noodzakelijk altijd toegang tot de bestanden op uw computer. Het is altijd een goed idee om een **gedrukt exemplaar/ offline kopie** te bewaren van elk document dat u tijdens een cyberveiligheidsincident of -crisis waarschijnlijk nodig zult hebben.

5.

Back-ups horen niet verbonden te zijn met de rest van uw systeem

Als het om back-ups gaat, is het niet alleen van het grootste belang dat ze bestaan. Het is ook heel belangrijk om een **back-up te hebben die op geen enkele manier met de rest van uw systeem is verbonden**. Als uw back-up met uw systeem is verbonden, is de kans groot dat de besmetting van uw systeem uitbreidt naar uw back-up, zodat uw back-up nutteloos wordt.

6.

Het is belangrijk om logs te maken en ze bij te houden gedurende een bepaalde tijd (tot zes maanden lang)

Logs kunnen u helpen bij het vinden van de bron van het cyberveiligheidsincident. Dit is niet alleen belangrijk om de cybercrimineel te kunnen identificeren; het kan uw organisatie ook helpen om zo snel mogelijk haar normale activiteiten te kunnen hernemen.

7.

Houd uw incidentresponsplan en alle verwante informatie en documenten up-to-date!

8.

Zorg ervoor dat u met alle juridische aspecten rekening houdt wanneer u een cyberveiligheidsincident aanpakt

Bewijzen worden in rechtbanken alleen aanvaard als ze werden verkregen in overeenstemming met alle toepasselijke wetten en voorschriften. Bovendien hebt u in sommige gevallen een meldingsplicht ten aanzien van de autoriteiten of betrokken personen bv. de Belgische Gegevensbeschermingsautoriteit of de betreffende bevoegde instantie voor het melden van Netwerk- en informatiebeveiligingsincidenten .

9.

Elke stap van een cyberveiligheidsincident documenteren

Vertrouw in tijden van crisis niet uitsluitend op uw geheugen! Noteer elke ondernomen actie, zoals het rapporteren van het incident, het verzamelen van bewijzen, gesprekken met gebruikers, systeemeigenaars en anderen enz. Deze documentatie is uw 'tijdmachine'. Wanneer iets fout loopt, stelt deze documentatie u in staat om terug te kijken en te bepalen waar en waarom het probleem is ontstaan. Bovendien zorgt documentatie over de respons op het cyberveiligheidsincident ervoor dat de kennis over wat er aan de hand is zich niet tot enkele mensen beperkt.

01 ZICH VOORBEREIDEN OP EEN CYBERVEILIGHEIDSINCIDENT

I. EEN INCIDENTRESPONSPLAN VOOR CYBERVEILIGHEIDS-INCIDENTEN OPSTELLEN EN UP-TO-DATE HOUDEN

Wanneer een organisatie geconfronteerd wordt met een cyberveiligheidsincident, moet ze snel en gepast kunnen reageren. Daarom is het belangrijk om reeds bij voorbaat te beslissen hoe u met bepaalde situaties zult omgaan, in plaats van wanneer u ze voor het eerst tijdens een incident tegenkomt. Stel een plan op (op papier, niet alleen in uw hoofd) om de schade te beperken, de kosten en de hersteltijd in te perken en om te communiceren met de belanghebbenden zowel binnen als buiten uw organisatie.

UW RESPONSPLAN VOOR CYBERVEILIGHEIDSINCIDENTEN HERZIEN

Een responsplan voor cyberveiligheidsincidenten (hierna 'incidentresponsplan') is geen statisch document. Het is belangrijk om het responsplan in uw bedrijfsprocessen te integreren en het regelmatig te herzien en bij te werken, op jaarbasis en als onderdeel van de nabespreking van een incident.

INCIDENTRESPONSPROCEDURES VOOR CYBERVEILIGHEIDS-INCIDENTEN

Op basis van uw incidentresponsplan kunt u een aantal standaardprocedures opstellen voor veel voorkomende incidenten waarvan de kans groot is dat ze uw organisatie zullen treffen. Deze procedures moeten stap voor stap uitleggen hoe een specifiek probleem kan worden aangepakt. Op die manier is er voor de aanpak van de meest voorkomende scenario's een beknopte en praktische handleiding. Zorg ervoor dat deze eenvoudig toegankelijk zijn.

BELANGRIJKSTE ELEMENTEN VAN EEN RESPONSPLAN VOOR CYBERVEILIGHEIDSINCIDENTEN

II. INHOUD VAN EEN INCIDENTRESPONSPLAN VOOR CYBERVEILIGHEIDSINCIDENTEN

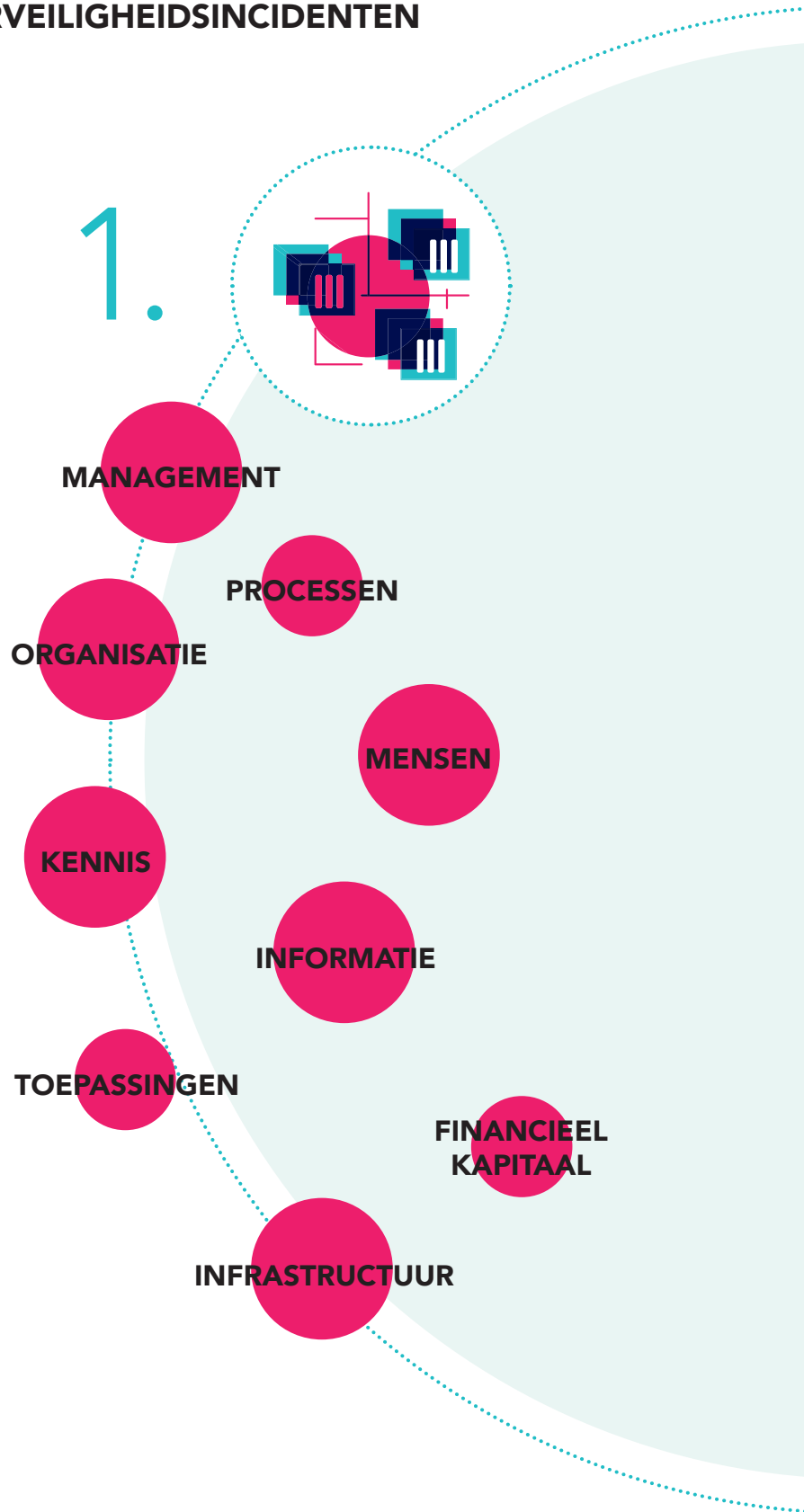
WAT BEVEILIGEN?

Uw activa en mogelijke bedreigingen identificeren

Wanneer er zich een incident voordoet, zijn de eerste vragen die gesteld worden: welke activa (informatie, kennis, processen, ...) lopen een risico? En welke van die activa zijn van cruciaal belang voor uw bedrijfsactiviteit? U dient te beslissen welke activa eerst uw aandacht vereisen om uw activiteiten te kunnen voortzetten en de schade aan uw bedrijf zo beperkt mogelijk te houden.

Daarom is het ontzettend belangrijk dat u de zaken die voor de goede werking van uw organisatie onmisbaar of zelfs vitaal zijn, **identificeert, documenteert en categoriseert**: de activa waarvan uw organisatie afhangt om haar kernactiviteiten uit te voeren. Dit helpt u te bepalen waar welke beschermingsmaatregelen moeten worden getroffen en om snelle en gemotiveerde beslissingen te nemen tijdens het incidentbeheerproces.

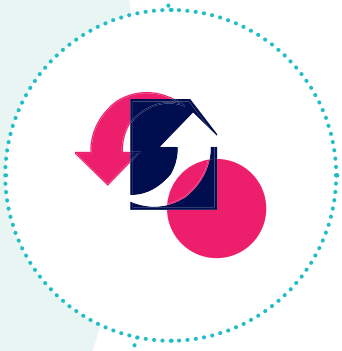
De volgende opsomming geeft u een idee van wat die 'vitale zaken' kunnen zijn: management, organisatie, processen, kennis (bv. intellectuele eigendom werd gestolen), mensen, informatie (bv. gegevens werden gestolen of gewijzigd), toepassingen (bv. website is onbereikbaar of aangetast), infrastructuur (bv. systeemen/ of netwerkverbindingen zijn uitgeschakeld), financieel kapitaal (bv. bankrekeningen).
Het is ook een goed idee om kwetsbaarheden en mogelijke dreigingen te identificeren.



2. Hoe de vitale zaken, kwetsbaarheden en mogelijke bedreigingen van uw organisatie identificeren, documenteren en categoriseren?

A. Identificeer de te beveiligen activiteiten en middelen

- Bepaal wat de kernactiviteiten van uw bedrijf zijn, die activiteiten die de basis vormen van uw organisatie, waardoor ze haar bedrijfsdoelstellingen kan realiseren en waaruit ze haar inkomsten haalt: goederen produceren, goederen verkopen, goederen leveren enz.
- Voor elk van die activiteiten bepaalt u door welke ICT-systemen (databases, toepassingen, besturingssystemen) en netwerkverbindingen ze wordt ondersteund.
- Bepaal ook waar deze ICT-systemen zich bevinden: op uw eigen servers of in de cloud.
- Wanneer u deze activa identificeert, mag u de informatiestromen naar derde partijen (leveranciers, klanten enz.) of industriële besturingssysteemstromen niet vergeten.



B. Uw kroonjuwelen identificeren

Bepaal nu welke activa, gegevens, processen of netwerkverbindingen zo belangrijk voor uw organisatie zijn dat u in grote problemen zou geraken of zelfs failliet gaat als u er de controle over zou verliezen, of ze zou kwijtraken.

C. Wijs prioriteiten toe voor herstel

Deze prioriteiten bepalen de volgorde waarin de systemen worden hersteld. In de meeste gevallen heeft het onderliggende netwerk de hoogste prioriteit, aangezien niet alleen uw systeembeheerders via deze weg toegang hebben tot uw systemen, maar het ook de weg is die de cybercriminelen gebruiken om uw systemen aan te vallen. Zolang criminelen gebruik kunnen maken van uw netwerkverbindingen, kunnen ze elke andere herstelactiviteit tenietdoen. Wanneer verschillende activa even prioritair zijn, kunnen parallelle herstelactiviteiten worden overwogen.

D. Documenteer hoe uw systemen werken en houd deze documentatie up-to-date

Zorg ervoor dat de manier waarop uw systemen werken gedocumenteerd is en dat deze informatie up-to-date wordt gehouden en beschikbaar is in de documentatiesystemen van het incidentresponsteam. Vooral de volgende documenten zijn belangrijk:

Een netwerkschema dat de netwerkarchitectuur weergeeft met de interne netwerksegmentatie en de verschillende gateways naar gebruikte externe netwerken, DMZ, VPN, IP-adresbereiken. In dit schema moeten ook de gebruikte beveiligingsapparaten worden opgenomen die mogelijk loginformatie van netwerkactiviteit (firewalls, (reverse) proxyservers, inbraakdetectiesystemen, beheersystemen voor beveiligingsincidenten) bevat. Voor grotere bedrijven met complexe netwerken is het ook nodig om een high-level versie van de netwerkarchitectuur te hebben zodat men bij een noodgeval snel kan zien hoe het netwerk in elkaar zit.

Een inventaris van apparatuur en diensten. Deze inventaris omvat, voor de vitale activa in uw omgeving, alle verschillende servers en de netwerkcomponenten die worden gebruikt voor het leveren van de verschillende bedrijfsdiensten. Aangezien enkele van deze (fysieke) servers mogelijk meerdere bedrijfsfuncties bedienen, is het belangrijk te weten welke diensten van welke server gebruikmaken.

Lijsten van accounts en toegangen. Het is belangrijk om op elk moment te weten wie er toegang heeft tot uw netwerk en de verschillende systemen erin, en wie ervan gebruikmaakt en/of het beheert. Zo kan u tijdens een incident elke verdachte of misbruikte toegang gemakkelijk detecteren.

Uw systemen zijn niet louter een hoop kabels en computers! Het is van cruciaal belang dat uw systeembeheerder weet hoe uw netwerk werkt en dit kan uitleggen aan experts, politie, enz.

III. VERANTWOORDELIJKHEDEN TOEWIJZEN EN EEN INCIDENTRESPONSTEAM VOOR CYBERVEILIGHEIDSINCIDENTEN SAMENSTELLEN

VERANTWOORDELIJKHEDEN EN FUNCTIES TOEWIJZEN AAN MENSEN MET DE JUISTE VAARDIGHEDEN

Het is belangrijk dat de functies en verantwoordelijkheden in geval van een cyberveiligheidsincident gedocumenteerd zijn in uw incidentresponsplan. Wanneer u de beschrijving van deze functies en verantwoordelijkheden opstelt, moet u zichzelf de volgende vragen stellen:

1. Wie is de interne contactpersoon voor cyberveiligheidsincidenten? En hoe kan met hem contact worden opgenomen?
2. Wat zijn de verschillende incidentresponstaken? En wie is verantwoordelijk voor wat?
3. Wie beheert het incident aan de bedrijfs-/technische kant? Dit moet iemand binnen uw bedrijf zijn met beslissingsbevoegdheid, die het incident van het begin tot het einde volgt.
4. Wie onderhoudt het contact met het topmanagement?
5. Wie kan de externe incidentresponspartner erbij betrekken?
6. Wie kan een klacht indienen bij de autoriteiten/de toezichthouders inlichten?
7. Wie is belast met de communicatie met de pers en externe partijen?

U moet beseffen dat er om een cyberveiligheidsincident correct aan te pakken, verschillende vaardigheden nodig zijn om de verschillende verantwoordelijkheden en nodige functies op te nemen om op efficiënte wijze op het incident te reageren.

VAARDIGHEDEN	VERANTWOORDELIJKHEDEN	FUNCTIES
Incidentbeheer	Het cyberveiligheidsincident beheren vanaf het ogenblik van detectie tot de afsluiting.	Incidentresponsmanager
Bevoegdheid om zakelijke beslissingen te nemen	De impact op het bedrijf beoordelen en dienovereenkomstig handelen. De juiste middelen inzetten. Beslissingen nemen over hoe verder te gaan, bv. beslissen of de internetverbinding van een aangetast systeem kan worden uitgeschakeld en op welk ogenblik dat het meest aangewezen is. Beslissen wanneer de herstelactiviteiten moeten starten. Beslissen of al dan niet een klacht moet worden ingediend.	Management
Netwerkbeheer	Technische knowhow over het netwerk van de organisatie (firewall, proxy's, IPS, routers, switches …). De gegevensstroom van en naar uw netwerk analyseren, blokkeren of beperken. Informatiebeveiliging van IT-activiteiten en bedrijfscontinuïteit	ICT-personeel voor technische ondersteuning
Bevoegdheid voor het beheer van werkstations en servers (beheerrechten)	Aangetaste werkstations en servers analyseren en beheren.	ICT-personeel voor technische ondersteuning
Juridisch advies	De contractuele en juridische impact van een incident beoordelen. Verzekeren dat incidentresponsactiviteiten binnen de wettelijke, reglementaire en organisatorische beleidsgrenzen blijven. Een klacht indienen.	Juridische afdeling/ bedrijfsjurist
Communicatievaardigheden	Op een gepaste manier communiceren naar alle betrokken groepen van belanghebbenden. Vragen van klanten, aandeelhouders en de pers onmiddellijk beantwoorden.	Communicatie- of PR-afdeling
Forensische vaardigheden	Op een gepaste manier bewijzen verzamelen en analyseren, d.w.z. zodat het bewijsmateriaal door een rechtbank kan worden aanvaard.	ICT-personeel voor technische ondersteuning
Fysieke veiligheid	De aspecten van het incident behandelen die gekoppeld zijn aan • de fysieke toegang tot de bedrijfsruimten • de fysieke beveiliging van de cyberinfrastructuur.	Veiligheidsmanager
Crisisbeheer	Crisisbeheer	Crisismanager

RESPONSTEAM VOOR CYBERVEILIGHEIDSINCIDENTEN

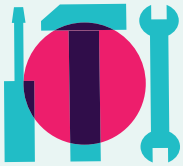
In een ideale wereld beschikt elke organisatie over een responsteam voor cyberveiligheidsincidenten (hierna 'incidentresponsteam') dat bij elk incident wordt samengeroepen. Uiteraard bepaalt de grootte van het bedrijf de grootte en structuur van het incidentresponsteam. Kleinere bedrijven die niet over de middelen voor een echt team beschikken, kunnen een eerste aanspreekpunt – idealiter iemand met beslissingsbevoegdheid – aanstellen onder het personeel. In geval van een cyberveiligheidsincident moet hij of zij extern hulp zoeken, maar blijft hij of zij de uiteindelijke verantwoordelijke voor de incidentrespons binnen de organisatie.

De samenstelling van dit incidentresponsteam wordt ook bepaald door de verschillende vaardigheden die nodig zijn om een incident aan te pakken (zie ook: tabel op pagina 11). Bij kleinere bedrijven kan het nodig zijn om enkele van deze vaardigheden buiten de organisatie te zoeken en neemt het eerste aanspreekpunt contact op met die mensen.

EEN MINIMAAL INCIDENTRESPONSTEAM BEVAT DE VOLGENDE FUNCTIES

INCIDENTRESPONSMANAGER

De persoon die het incident beheert vanaf het moment dat hij erover is ingelicht, tot het is bedwongen en opgelost. Hij onderhoudt het contact met het management en mogelijk met ander intern personeel en externe hulp om het incident aan te pakken. Deze persoon dient kennis te hebben van de bedrijfsactiviteiten van uw organisatie omdat hij de eerste is die zakelijke beslissingen zal nemen.



ICT-PERSONEEL VOOR TECHNISCHE ONDERSTEUNING

Deze persoon dient een goede kennis te hebben van uw ICT-infrastructuur aangezien hij verantwoordelijk is voor het onderzoek van de aanwijzingen, de bevestiging van het incident en de ontwikkeling van de technische oplossingen om het incident aan te pakken.

DE GROOTTE EN AARD VAN UW ORGANISATIE BEPALEN OF ER MEER FUNCTIES NODIG ZIJN

Kleinere organisaties hebben vaak de flexibiliteit om zich voor de aanpak van het incident snel tot het ondernemingsbestuur te wenden. Dit is niet het geval voor grotere organisaties. Daar zullen incidentresponsteams de meeste incidenten op een meer autonome wijze moeten behandelen, zodat de bedrijfstop alleen in geval van een bijzonder ernstig incident bij incidentresponsacties wordt betrokken.

Grotere organisaties. Hoe groter uw organisatie, hoe gedifferentieerder de samenstelling van uw incidentresponsteam moet zijn. In grotere organisaties kan er naast een incidentresponsteam ook een crisisbeheerteam worden samengesteld uit vertegenwoordigers van het ondernemingsbestuur die bij ernstige incidenten de verantwoordelijkheid opnemen voor de strategische en bedrijfsbeslissingen en de communicatie hierover. Op deze manier kan de incidentresponsmanager zich meer richten op de technische kwesties van het incident.

BEPAALDE ORGANISATIES MOETEN EEN FUNCTIONARIS VOOR GEGEVENSBESCHERMING OF CONTACTPUNT AANDUIDEN

De Algemene Verordening Gegevensbescherming (AVG) verplicht bepaalde organisaties een functionaris voor gegevensbescherming aan te duiden (ook Data Protection Officer of 'DPO' genoemd). Het gaat meer bepaald over organisaties die belast zijn met de verwerking van persoonsgegevens en die regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen, of belast zijn met grootschalige verwerking van bijzondere categorieën van gegevens, bijvoorbeeld gezondheidsgegevens, of strafrechtelijke veroordelingen en strafbare feiten.

De wet Netwerk- en Informatiebeveiliging (NIS), legt aanbieders van essentiële diensten (AED) en Digitale Dienstverleners (DDV) op om een contactpunt voor de beveiliging van netwerk -en informatiesystemen aan te duiden om een vlotte communicatie met de bevoegde autoriteiten toe te laten in geval van incidenten.

IV. EXTERNE EXPERTS

EXPERTS INCIDENTRESPONS

Of uw organisatie nu een kmo of een grote organisatie is, het is een dure zaak om alle nodige expertise en vaardigheden voor incidentrespons in huis te ontwikkelen en te onderhouden. Dit is vooral het geval voor forensisch en juridisch advies bij cyberveiligheidsincidenten. Het kan dus goedkoper en doeltreffender zijn om een beroep te doen op externe partners voor het aanpakken van cyberveiligheidsincidenten en zo de leemten in de vaardigheden van uw organisatie te dichten.

- Hun professionele incidentresponders kunnen met hun kennis van mogelijke dreigingen en scenario's de **tijd** verkorten die nodig is voor de diagnose van het incident.
- Ze werken op een forensisch degelijke manier zodat alle bewijzen worden beveiligd en gedocumenteerd op een **juridisch geldige** manier en de bewijsketen gegarandeerd is. Dit bewijs kan dan later indien nodig aan een rechtbank worden voorgelegd.
- Ze hebben de ervaring om de zaken in de juiste volgorde uit te voeren en beschikken over **middelen** om sporen te vinden in het RAM-geheugen, in virtuele machines, op harde schijven en in netwerken.
- Deze experts helpen u **de oorzaken** van het incident te bepalen en bieden advies om het incident in te perken, te vernietigen en op te lossen.

WANNEER CONTACT OPNEMEN MET EEN EXPERT?

A. TIJDENS DE VOORBEREIDINGSFASE versus B. WANNEER ZICH EEN CYBERVEILIGHEIDS-INCIDENT VOORDOET

U kunt tijdens de voorbereidingsfase een responspartner voor cyberveiligheidsincidenten inhuren of wachten tot er zich een echt cyberveiligheidsincident voordoet. Houd er hier rekening mee dat het inhuren van zo iemand tijd en moeite kost. Als u er zeker van bent dat u externe hulp nodig zult hebben, is het beter om niet te wachten. Zo wint u waardevolle tijd bij het begin van het cyberveiligheidsincident. Verschillende gespecialiseerde adviesbureaus voor incidentresponsdiensten en advocatenkantoren bieden abonnementen die hun incidentrespons ter beschikking houden van de abonnee. Bovendien omvatten de meeste van deze abonnementen opleidingssessies met uw incidentresponsteam zodat de onderlinge samenwerking gemakkelijker verloopt in geval van een incident.

BEPAALDE OVERHEIDSINSTANTIES KUNNEN HELPEN BIJ UW ONDERZOEK

Andere partijen zoals sectorale toezichthouders, de Gegevensbeschermingsautoriteit, Centrum Cyberveiligheid België (CCB), Afdeling CERT.be, en de ordehandhavende instanties (politie en magistraten) kunnen belangrijk zijn wanneer u wordt geconfronteerd met een cyberveiligheidsincident van criminele aard of in geval van een lek van persoonsgegevens. Sommige wetgeving verplicht u zelfs om deze partijen in te lichten wanneer u een incident van specifieke aard hebt gedetecteerd (zie ook: pagina 31 Rapporteren aan autoriteiten).

Deze partijen kunnen vaak helpen met informatie over de dreiging en met praktische richtlijnen op basis van vorige incidenten die ze hebben behandeld. Houd er rekening mee dat de ordehandhavers de aanvaller willen identificeren en vatten. Het is niet hun taak om uw bedrijf opnieuw operationeel te maken. Het is ook mogelijk dat de doeltreffendste manier om de aanvaller te vatten niet de snelste manier is voor uw organisatie om haar gewone werkzaamheden te hervatten.

Bovendien vallen de meeste van deze onderzoeken onder het beroepsgeheim, zodat het relatief moeilijk is om informatie over hun resultaten te verkrijgen. Mogelijk geven ze echter informatie vrij die u helpt bij de identificatie van de aanvaller en zijn manier van werken, wat mogelijk de analyse van uw cyberveiligheidsincident kan versnellen.

De politie kan uw organisatie vragen om uw systeem niet onmiddellijk uit te schakelen. Als u dat wel doet, dan merkt de aanvaller dit op en verdwijnt hij, wat het vaak onmogelijk maakt om hem nadien nog op te sporen. Het systeem onmiddellijk uitschakelen en met een schone lei starten kan de snelste manier zijn voor uw organisatie om haar gewone activiteiten te hervatten.

V. IS UW ORGANISATIE UITGERUST OM EEN CYBER-VEILIGHEIDSINCIDENT AAN TE PAKKEN?

UW NETWERK VAN EXPERTS – EEN LIJST MET CONTACTPERSONEN MAKEN

Het is van cruciaal belang dat u tijdens een incident op het juiste ogenblik hulp kunt vragen aan de juiste professionals, aangezien dit de schade aan de infrastructuur en het imago van uw bedrijf kan beperken. Een lijst met contactpersonen waarop al deze mensen of organisaties staan, zal u hierbij helpen. Deze lijst bevat de namen, functies, contact- en back-upgegevens van de verschillende leden van het incidentresponsteam, de externe partijen die stand-by zijn, de ordehandhaving enz.

De contactgegevens die moeten worden genoteerd, zijn de vaste en mobiele telefoonnummers, zakelijke e-mailadressen (inclusief openbare codeersleutels voor de vertrouwelijkheid en integriteit van de communicatie) en fysieke adressen voor traditionele post en pakketten. Zorg ervoor dat u ook over alternatieve contactopties beschikt (secundaire e-mailadressen, faxnummers), omdat het mogelijk is dat het incidentresponsteam tijdens het incident geen gebruik kan maken van het interne netwerk.
Deze contactgegevens moeten beschikbaar zijn in een centrale, offline locatie, zoals op papier in een farde of op een offline computer. Naast de 'ruwe' contactgegevens dienen deze noodgegevens ook de escalatieprocedures te bevatten. Deze informatie moet zowel onmiddellijk beschikbaar zijn als fysiek uiterst veilig worden bewaard. Een manier om deze informatie te beveiligen en onmiddellijk beschikbaar te houden is ze te versleutelen op een speciale beveiligde draagbare computer die in een veilige kluis zit en waarbij de toegang tot de kluis is beperkt tot enkele mensen zoals het hoofd van het incidentresponsteam en de Chief Information Officer (CIO) of de Chief Technology Officer (CTO).

Voor een uitgebreid invulformulier, zie **Sans Institute**

NAAM	ORGANISATIE	FUNCTIE	CONTACTGEGEVENS
Mw. Incident Responsmanager	Intern/extern	Responsbeheer voor cyberincidenten	Adres Telefoon E-mail **Weekend- en back-up** contactgegevens
Dhr. Jurist	Intern/extern	Juridisch expert	
Mw. Forensisch deskundige	Extern	Forensisch expert	
Dhr. Politie	Ordehandhaving	Ordehandhaving	

HARDWARE EN SOFTWARE VOOR HET BEHEER VAN CYBERVEILIGHEIDSINCIDENTEN

Om de ervaring en de efficiëntie van het incidentresponsteam te verhogen, moet u over de gepaste hulpmiddelen beschikken. Het is belangrijk dat het incidentresponsteam beschikt over autonome systemen en hulpmiddelen zodat het een incident kan behandelen, zelfs als het bedrijfsnetwerk is aangetast. Dit betekent dat zelfs wanneer de systemen of netwerken van uw organisatie niet langer beschikbaar zijn, het systeem van het incidentresponsteam wel nog beschikbaar is. Op deze systemen dienen procedures voor incidenten en lijsten met contactgegevens beschikbaar te zijn.

VI. UW COMMUNICATIE-STRATEGIE VOORBEREIDEN

Communicatie is een **vitaal onderdeel** van elke stap van incidentrespons. U wilt de communicatiestroom beheersen om ervoor te zorgen dat **de juiste informatie** wordt gecommuniceerd op het **juiste ogenblik** door de **juiste personen** naar de **juiste belanghebbenden**. Dit geldt zowel voor interne communicatie als voor communicatie naar de buitenwereld. We adviseren om alle externe communicatie af te stemmen zowel met de juridische afdeling als met de communicatie- of PR-afdeling.

WAT COMMUNICEREN EN AAN WIE?

Het type incident en zijn (mogelijke) impact bepaalt het type communicatie dat nodig is. Bijvoorbeeld, een ***intern*** fraudegeval of een ***interne*** poging tot hacking is hoogstwaarschijnlijk geen reden tot communicatie met de media. Maar wanneer de persoonsgegevens van de klanten van een organisatie gelekt zijn, dan is het een goed idee om ten minste met die klanten en de Gegevensbeschermingsautoriteit contact op te nemen en om een persbericht voor te bereiden. Verder moet alle communicatie het midden houden tussen openheid en bescherming. In de meeste gevallen is interne communicatie opener dan externe communicatie. Maar zelfs bij interne communicatie dient alleen de noodzakelijke informatie te worden meegedeeld.

INTERNE EN EXTERNE BELANGHEBBENDEN IDENTIFICEREN

Tijdens de incidentreponsactiviteiten hebben vele verschillende belanghebbenden voortdurend informatie nodig. Elk van hen heeft behoefte aan een andere soort informatie. Maak uw eigen lijst van mogelijke belanghebbenden en zorg ervoor dat de juiste contactgegevens beschikbaar zijn! (zie ook: tabel op pagina 15). Merk op dat deze contactgegevens beschikbaar moeten zijn in de organisatie maar dat men per incident dient te bekijken naar welke partijen moet worden gecommuniceerd.

WIE? INTERNE BELANGHEBBENDEN	WELKE SOORT INFORMATIE HEEFT DEZE BELANGHEBBENDE NODIG?
Topmanagement	Welke activiteiten of activa worden getroffen? Wat is de respons? Wat is het verwachte resultaat en wanneer verlopen de activiteiten opnieuw normaal?
Betrokken bedrijfsmanagers	Wanneer worden de normale activiteiten hervat?
Werknemers	Wat moet een werknemer doen? Hoe lang zal deze situatie naar verwachting aanhouden?

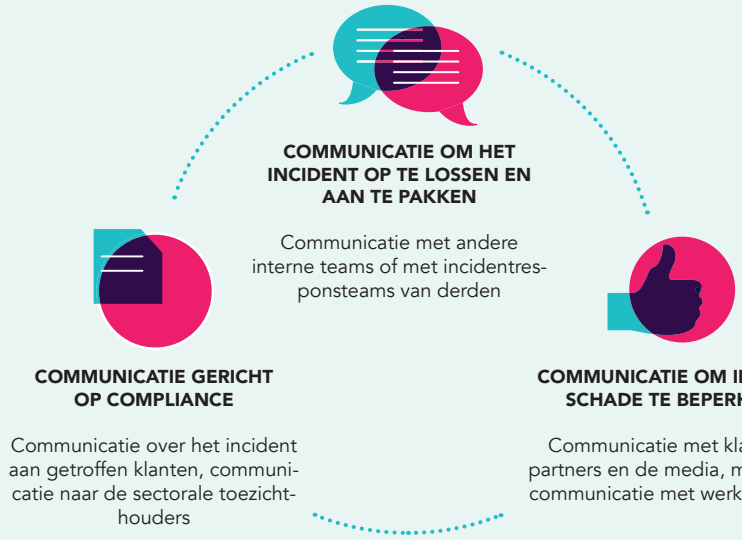
WIE? EXTERNE BELANGHEBBENDEN	WELKE SOORT INFORMATIE HEEFT DEZE BELANGHEBBENDE NODIG?
Media	Een officiële verklaring over het incident en zijn impact. In het geval van bedrijven en/of incidenten waarvoor veel aandacht bestaat, kunnen de media worden betrokken. Aandacht van de media bij een veiligheidsincident is zelden wenselijk, maar is soms onvermijdelijk. Door media-aandacht kan uw organisatie een proactieve houding aannemen bij de communicatie van het incident en zo uw engagement en vermogen tonen om het incident aan te pakken. Het communicatieplan moet duidelijk aangeven wie bevoegd is om met de media te spreken (meestal de PR- of juridische afdeling).
Klanten	Kunnen ze worden getroffen door het cyberveiligheidsincident? Gingen hun (persooons)gegevens verloren of werden ze gestolen? Vormen ze mogelijk het eerste doelwit van de aanval? In sommige gevallen is er een wettelijke verplichting om contact op te nemen met de sectorale toezichthouder (zie ook: pagina 31 Rapporteren aan autoriteiten).
Leveranciers	Kunnen ze worden getroffen door het cyberveiligheidsincident? Vormen ze mogelijk het eerste doelwit van de aanval?
Andere cyberveiligheidteams	Communicatie met andere incidentresponsteams kan technische hulp bieden en zo zorgen voor een snellere oplossing (bv. ze hebben dit soort incident misschien eerder gezien/ behandeld). Dit type van communicatie bevat meestal technische gegevens van het gevonden bewijsmateriaal.
Internetservice-provider	Communicatie met uw internetserviceprovider kan technische hulp bieden en zo voor een snellere oplossing zorgen (bv. ze hebben dit soort incident misschien eerder gezien/ behandeld). Dit type van communicatie bevat meestal technische gegevens van het gevonden bewijsmateriaal.

WIE? OFFICIËLE BELANGHEBBENDEN	WELKE SOORT INFORMATIE HEEFT DEZE BELANGHEBBENDE NODIG?
Gegevensbeschermingsautoriteit	Was er een inbreuk in verband met persoonsgegevens? Om welke gegevens gaat het? In sommige gevallen is er een wettelijke verplichting om contact op te nemen met de Gegevensbeschermingsautoriteit (telecomwetgeving en de AVG). (Zie ook: pagina 31 Rapporteren aan autoriteiten)
CCB (Afdeling CERT.be)	Technische gegevens van het gevonden bewijsmateriaal
Politie	Wilt u een klacht indienen? Als de gebeurtenis een aanzienlijk impact had en er een vermoeden van crimineel opzet is, dan wilt u het incident mogelijk rapporteren aan de ordehandhavende instanties. Zij hebben juridische en technische informatie nodig.
Sectorale toezichthouders en overheden	Welke soort incidenten? Wat is de status van het incident? In sommige gevallen is er een wettelijke verplichting om contact op te nemen met bepaalde overheden of de sectorale toezichthouders (zie ook: pagina 31 Rapporteren aan autoriteiten).

Organisaties moeten er rekening mee houden dat een partij, zodra ze wordt ingelicht, regelmatig om nieuws over het betreffende incident zal verzoeken. Het gaat niet om een eenmalige communicatie en het communicatieplan moet rekening houden met deze nood aan periodieke updates.

DE IMPACT VAN HET INCIDENT BEPAALT DE DOELSTELLINGEN VAN DE COMMUNICATIE

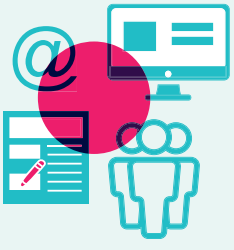
Om te weten wat aan wie moet worden gecommuniceerd, moet een organisatie de (mogelijke) impact van het cyberveiligheidsincident beoordelen: bv. betreft het alleen interne of ook externe belanghebbenden? Werden er gegevens gelekt? Afhankelijk van deze impact heeft uw communicatie over het cyberveiligheidsincident verschillende doelstellingen, bijvoorbeeld:



ZORG ERVOOR DAT MEERDERE COMMUNICATIEKANALEN BESCHIKBAAR ZIJN

Het incident kan een impact hebben op bestaande communicatiekanalen (bv. e-mailsystemen aantasten). Als organisatie moet u beschikken over alternatieve, veilige communicatiekanalen. Er zijn diverse communicatiemethodes beschikbaar en het is aan de organisatie om de meest geschikte methode te kiezen voor een specifiek incident.

Een **beste praktijk** die door vele organisaties wordt gebruikt, is gebruikmaken van een conferencecallnummer dat onmiddellijk kan worden geïnstalleerd. Het incidentresponsteam en alle belanghebbenden moeten worden ingelicht over de toegangsnummers maar niet over het controlenummer dat nodig is om een vergadering te beleggen. Dit wordt meestal voorbehouden aan een crisismanager die verantwoordelijk is voor het beheren, onder controle houden en organiseren van crisisgesprekken.



MOGELIJKE COMMUNICATIEMETHODES

- E-mail (bij voorkeur met behulp van PGP voor de vertrouwelijkheid en integriteit van de communicatie)
- Website (intranet voor werknemers, publieke website …)
- Telefoongesprekken
- Persoonlijk (bv. dagelijkse briefings)
- Papier (bv. mededelingen plaatsen op borden en deuren, mededelingen overhandigen bij alle toegangspunten).

VII.

CYBERVERZEKERING

Bepaalde verzekeraars bieden aangepaste verzekeringspolissen die altijd worden voorafgegaan door een analyse van de risico's die eigen zijn aan de organisatie in kwestie. Met deze analyse kan de organisatie bepalen of en in welke mate ze een cyberverzekering nodig heeft. De risicoanalyse wordt ook gebruikt door de verzekeraar om de vereiste dekking te bepalen. Factoren waarmee rekening wordt gehouden, zijn:

- blootstelling van het bedrijf: hoogwaardige technologie met een exclusief productieproces en doorgedreven Onderzoek & Ontwikkeling
- type distributienetwerk: e-commerce
- hoeveelheid en soort gegevens (kritiek of niet), het bestaan van een juridisch kader.

KOSTEN VAN HERSTEL IN GEVAL VAN VERLIES VAN GEGEVENS

MOGELIJK OMZETVERLIES

EXTRA KOSTEN VOOR DE DETECTIE, ONDERZOEK EN OPLOSSING VAN INCIDENTEN, MET INBEGRIP VAN LOSGELD EN KOSTEN VAN ONDERHANDELINGEN, CLAIMS VAN DERDEN EN VERZEKERBARE BOETES

COMMUNICATIEKOSTEN, JURIDISCHE EN FORENSISCHE BIJSTAND IN GEVAL VAN EEN INCIDENT

Een compensatie wordt uitbetaald boven een eigen risico dat met de verzekeringshouder werd onderhandeld. De verzekerde bedragen per claim en/of per verzekerd jaar worden altijd bepaald volgens de behoeften van het bedrijf en de mogelijkheden van de verzekeringsmaatschappij.

02 CYBERVEILIGHEIDSINCIDENTEN DETECTEREN EN IDENTIFICEREN

I. CATEGORIEËN VAN INCIDENTEN

CYBERVEILIGHEIDSINCIDENT EN VERWANTE TERMEN DEFINIËREN

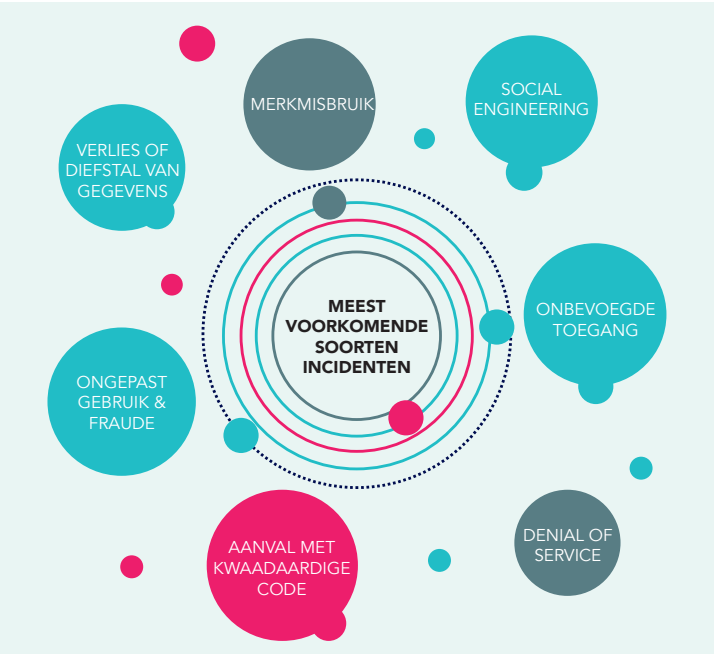
Om te beginnen is het een goed idee om 'cyberveiligheidsincident' en verwante termen te definiëren binnen uw organisatie. Dit zorgt voor een veel vlottere communicatie over de incidenten. U kunt voor deze definities inspiratie vinden in het inleidende hoofdstuk van deze gids over basisbeginselen en -definities. U moet bijvoorbeeld beslissen wanneer een cyberveiligheidsevent een cyberveiligheidsincident wordt voor uw organisatie. Met andere woorden, welke cyberveiligheidsevents hebben waarschijnlijk een negatieve impact op de activiteiten van uw organisatie?

MOGELIJKE CATEGORIEËN VAN CYBERVEILIGHEIDSINCIDENTEN IDENTIFICEREN

Om cyberveiligheidsincidenten te kunnen detecteren en identificeren, moet u minstens een idee hebben van waar u naar moet zoeken. Daarom is het geen luxe om te beschikken over een lijst met categorieën van de cyberveiligheidsincidenten waarvan de kans het grootst is dat ze uw organisatie zullen treffen. Bovendien is het, wanneer u een cyberveiligheidsevent detecteert, vaak moeilijk om vanaf het begin reeds te weten hoe erg de gevolgen zullen zijn. Dit verandert echter niets aan het feit dat u moet optreden. Met categorieën van incidenten kunt u prioriteiten vaststellen voor cyberevents en dienovereenkomstig beslissingen nemen. Dit deel biedt een typologie van een aantal cyberveiligheidsincidenten. Het is niet de bedoeling om een 'definitief' overzicht van alle soorten incidenten te geven, wel om u eenvoudigweg een idee te geven van de meest voorkomende incidenten (op het moment van opstellen van deze gids). Incidenten kunnen tot meer dan één categorie behoren. Een uitvoerigere uitleg van deze soorten incidenten vindt u in de Bijlage.

USB-STICK OF USB-SPION?
In 2013 trad Rusland op als gastheer van een vergadering van de staatshoofden van de G20. Op het einde van de bijeenkomst kregen alle deelnemers, onder wie Herman Van Rompuy, een USB-stick en een lader voor mobiele telefoons. Hoewel het Kremlin het altijd heeft ontkend, zouden beide apparaten in staat zijn geweest om informatie te downloaden, zoals e-mails, tekstberichten en telefoongesprekken van laptops en telefoons.

EEN CRYPTOLOCKER KAN OOK UW BACK-UP VERSLEUTELEN
Een bedrijf ontvangt een e-mail met een factuur in bijlage die lijkt op die van een van hun leveranciers. De boekhouder van het bedrijf klikt op de bijlage en enkele seconden later verschijnt een bericht op zijn scherm: "Al uw informatie werd versleuteld! Als u de sleutel wenst om de versleuteling ongedaan te maken, moet u me 1000 Bitcoins betalen." Het bedrijf wil de cybercrimineel niet betalen. Er is immers geen enkele garantie dat hij de verloren gegevens zal terugplaatsen zodra hij het losgeld heeft ontvangen. Om de gegevens terug te krijgen, beslist het bedrijf een back-up terug te plaatsen. Wanneer het bedrijf dit wil doen, merken de werknemers dat de back-up ook werd versleuteld omdat die aan het systeem was gekoppeld...



II. METHODES OM INCIDENTEN TE DETECTEREN

HET PERSONEEL VAN UW ORGANISATIEIS IN STAAT OM TE DETECTEREN

Mensen worden vaak als de zwakste schakel beschouwd met betrekking tot cyberveiligheid. Ze beschikken echter ook over het grootste potentieel om een organisatie te helpen bij het detecteren en identificeren van cyberveiligheidsincidenten. Zorg ervoor dat elke werknemer van uw organisatie zich bewust is van cyberveiligheidsrisico's en van de rol die hij kan spelen bij de detectie ervan. Maak van uw werknemers een menselijke firewall! Elke werknemer in uw organisatie moet weten hoe men kan melden dat men iets abnormaals op een computer of een mobiel apparaat heeft opgemerkt. Zorg ervoor dat de contactgegevens hiervoor eenvoudig ter beschikking staan en dat de manier om contact op te nemen met deze persoon laagdrempelig is.

Hoe kunt u de rapportering van incidenten door het personeel (en andere partners) concreet organiseren?
- Een telefoonnummer voor het melden van noodgevallen
- Een e-mailadres voor het informeel rapporteren van incidenten
- Een internetformulier voor het formeel rapporteren van incidenten

TECHNOLOGIE- EN ENDPOINTBEVEILIGING

Technologie

Technologie is een van de belangrijkste elementen waarmee u de detectie, het onderzoek, het elimineren en het herstel bij incidenten mogelijk maakt. Wanneer zich een incident heeft voorgedaan, is het ad hoc inzetten van technologie nog altijd mogelijk, maar uw onderzoek beperkt zich dan vaak tot de actuele gebeurtenissen. Als u tijdens de voorbereidingsfase de juiste technologie inzet, krijgt u een uitgebreid beeld van de gebeurtenissen nu en in het verleden. Dit geeft uw organisatie een betere kans om het incident tot aan zijn oorsprong te traceren.

Houd uw software, virusscanners enz. up-to-date om kwaadaardige code te vermijden!
Werk uw software regelmatig bij of installeer updates wanneer deze beschikbaar zijn.

Gebruik geen niet-ondersteunde softwareversies zoals Windows XP en Windows 2003. Niet-ondersteund betekent dat de software niet langer wordt bijgewerkt zodat uw computer niet langer beveiligd is tegen nieuwe, bekende malware.

Endpointbeveiliging

Een endpoint is een apparaat dat verbonden is met het netwerk van uw organisatie, zoals laptops, smartphones enz. Elk van deze apparaten vormt een mogelijke toegang voor cybercriminelen. Daarom is het belangrijk dat al deze apparaten goed beveiligd zijn.

DETECTIEMIDDELEN

Elk detectiemiddel (bv. IDS) heeft zijn specifiek doel en kan vanuit een verschillend standpunt controles uitvoeren: netwerkgebaseerd of hostgebaseerd. Door de verscheidenheid aan soorten dreigingen moeten de detectiemiddelen correct geconfigureerd worden.

Netwerkgebaseerde detectiemiddelen

Een goede start is het inzetten van een inbraakpreventiesysteem, zoals een Snort-netwerk IDS-sensor, op de internetuplink. Daarnaast beschikken veel organisaties al over heel wat informatie die, zonder dat ze het beseffen, kan worden gebruikt om een incident te detecteren. Denk bijvoorbeeld aan:
- toegangslogs van servers en toestellen;
- operationele logs van systemen (bv. procescreatie);
- firewall-logs.

Deze gegevens kunnen worden gebruikt om regels en trends te creëren, die helpen bij het detecteren van onverwacht of ongeldig verkeer (bv. verkeer naar ongewone websites, aanmeldpogingen van niet-bestaande gebruikers enz.).

Hostgebaseerde detectiemiddelen

Antivirusoplossingen volstaan niet tegen geavanceerde aanvallen op endpoints. Veel malware is tegenwoordig polymorf (hij verandert naargelang het gedrag van de host), wat het moeilijk detecteerbaar maakt op basis van statische definities door klassieke antivirusprogramma's. Geavanceerde middelen voor endpointbeveiliging onderzoeken verdacht gedrag en kunnen zo in veel gevallen doeltreffender optreden.
Dit betekent echter niet dat er geen antivirusoplossingen moeten worden ingezet. Integendeel, een antivirusprogramma is nodig om de bekendste dreigingen op te vangen.

03 EEN INCIDENT AANPAKKEN: ONDER CONTROLE KRIJGEN, VERWIJDEREN EN HERSTELLEN

In dit hoofdstuk leest u wat u moet doen om opnieuw de controle te verwerven wanneer u een cyberveiligheidsincident hebt gedetecteerd. Er moeten belangrijke beslissingen worden genomen over hoe u het incident inperkt, hoe u het vernietigt en hoe u ervan herstelt. Het is absoluut noodzakelijk dat het topmanagement van uw organisatie deze beslissingen goedkeurt. Incidenten kunnen tot meer dan één categorie behoren.

I. UW INCIDENTRESPONSTEAM VOOR CYBERVEILIGHEIDSINCIDENTEN BIJEENROEPEN

Wanneer een daadwerkelijk incident wordt gedetecteerd, is het heel belangrijk om de risico's snel te beoordelen zodat de juiste maatregelen kunnen worden genomen. De cyberveiligheidsincidentmanager moet onmiddellijk op de hoogte worden gebracht en een vergadering beleggen van het incidentresponsteam, als uw organisatie over zulk team beschikt (zie ook: pagina 12 Responsteam voor cyberveiligheidsincidenten). De cyberveiligheidsincidentmanager en zijn team rapporteren aan de CEO, die hun beslissingen dient goed te keuren.

II. BEELDVORMING

Na de detectie van een incident is het belangrijk dat alle beschikbare informatie wordt verzameld over de activiteiten in de periode van het incident. De centrale verzameling en archivering van beveiligingsinformatie (bv. systeemlogs, firewall-logs) biedt de analist eenvoudige toegang tot deze informatie. Belangrijke factoren waarmee rekening moet worden gehouden, zijn de integriteit van de informatie en de indexering ervan.
Een forensisch onderzoek kan nodig zijn om alle artefacten te verzamelen en om de omvang en reikwijdte van de aanval te onderzoeken. Middelen om volledige schijfkopieën te maken en te analyseren, geheugendumps (op afstand) te nemen van een verdachte machine en write-blockers zijn nuttig bij de uitvoering van deze analyse.

Om de omvang van het incident te detecteren, kunnen de tijdens het aanvankelijk onderzoek verzamelde artefacten of indicatoren vervolgens worden gebruikt om te zoeken naar verdere grootschalige inbraken via alle beheerde apparaten. Dit proces kan worden versneld als er een centraal beheerpunt is dat dit kan uitvoeren. U dient ook na te gaan of er gegevens verloren zijn gegaan of gestolen werden.

RISICOBEPALING VAN PERSOONSGEGEVENSLEKKEN

Een kernelement in het omgaan met een persoonsgegevenslek is het bepalen van het risiconiveau van het lek in kwestie. Hoe ernstig is het lek en de mogelijke gevolgen voor de persoon wiens gegevens werden gelekt? Het antwoord op die vraag vormt een belangrijke factor in het bepalen van de stappen die gezet moeten worden. Elk risiconiveau (geen risico, risico, hoog risico), vereist een andere aanpak, in het bijzonder in het kader van de meldplicht. Daarom is een exacte en consistente risico-evaluatie de sleutel tot een doeltreffende aanpak van een persoonsgegevenslek. Zo kan men ervoor zorgen dat de juiste acties worden ondernomen om in overeenstemming te zijn met de wetgevende bepalingen.

Een beoordeling van een persoonsgegevenslek in zijn totaliteit, maakt het mogelijk een adequaat en realistisch risiconiveau te formuleren, en de juiste vervolgstappen te zetten. Om de risico's voor rechten en vrijheden van individuen te kunnen evalueren dient men rekening te houden met een aantal elementen. Hieronder staan de belangrijkste elementen beschreven:

Aard en gevoeligheid van persoons-gegevens	Gevoelige gegevens Des te gevoeliger de persoonsgegevens, des te hoger het risico voor schade aan de getroffen individuen. Publiciteit van de gegevens Naast de gevoeligheid van de gelekte gegevens is ook het niveau van publiciteit dat reeds aan de gegevens werd gegeven van belang. Men moet nagaan of de persoonsgegevens van het individu al (publiek) toegankelijk waren. Gekoppelde persoonsgegevens Datalekken met gezondheidsgegevens, identiteitsdocumenten, of financiële gegevens, zoals creditcardgegevens, kunnen elk op zichzelf al schade veroorzaken, maar gecombineerd met publiek toegankelijke informatie kunnen bovendien ernstige vergrijpen worden gepleegd, zoals identiteitsfraude. Om die reden vormen gekoppelde persoonsgegevens een hoger risico dan een geïsoleerde categorie van persoonsgegevens.
Hoeveelheid persoonsgegevens en aantal getroffen individuen	Dit element kijkt naar de hoeveelheid informatie waarop het lek betrekking heeft en het totaal aantal individuen wiens gegevens zijn getroffen. Hoe meer gegevens en individuen getroffen werden, des te hoger de risico's.
Gemak van identificatie van de individuen	Dit element richt op hoe gemakkelijk het zal zijn voor een partij met toegang tot de geschonden persoonsgegevens om een persoon te identificeren (eventueel na het vergelijken met aanvullende beschikbare informatie). Het risico hangt ervan af of individuen direct kunnen worden geïdentificeerd zonder enkele andere persoonsgegevens, of dat er aanvullende informatie uit andere gegevenscategorieën nodig is om de individuen te identificeren.
Ernst van de gevolgen	De potentiële schade berokkend aan de individuen, en de ernst van de schade moeten worden vastgesteld. Datalekken kunnen buitengewoon schadelijk zijn in gevallen als identiteitsfraude, fysieke schade, psychologische stress, vernedering of reputatieschade. Als het lek persoonsgegevens betreft van kwetsbare individuen, (bijv. patiënten, kinderen), kan een hoger risico tot schade worden toegekend.
Bestaande mitigerende maatregelen	Mitigerende maatregelen die reeds van kracht zijn tijdens het datalek, moeten in acht worden genomen bij de algehele risicobepaling; door mee te wegen of, en hoe, deze maatregelen de getroffen individuen beschermen.

Register van datalekken

Omwille van het aansprakelijkheidsprincipe, dienen alle overwegingen en conclusies van de risicobepaling te worden gedocumenteerd in een datalekkenregister. In dit register moeten ten minste onderstaande zaken zijn opgenomen:

Datum en tijd van het datalek	De exacte datum en tijd waarop de organisatie zich bewust werd van het persoonsgegevenslek. Deze informatie is van belang om het nakomen van de 72-uursdeadline voor notificatie van de Gegevensbeschermingsautoriteit, en eventuele datasubjecten.
Tijdslijn en beschrijving van het datalek	Omschrijvingen van gebeurtenissen omtrent het persoonsgegevenslek: wanneer het lek gerapporteerd werd, wanneer het lek (vermoedelijk) plaatsvond, een overzicht van de getroffen systemen, en overige beschrijvingen.
Contactpersoon	Het is van belang een centraal contactpersoon te hebben, die geïnformeerd is over de omstandigheden van het persoonsgegevenslek, die gecontacteerd kan worden in geval van vervolgvragen. Meestal is de persoon die het lek heeft gerapporteerd, de functionaris voor gegevensbescherming, of de zakelijk leider van het getroffen departement.
Betrokken externe partijen	Bevat informatie over de aard en de rol van de organisatie (verwerkingsverantwoordelijke, verwerker, gezamenlijke verwerkingsverantwoordelijke) en de derde partijen die getroffen kunnen zijn en derhalve moeten worden ingelicht.
Risicobepaling – motivatie en conclusie	Gedetailleerde risicoanalyse en de totale risicobepaling, gebaseerd op de elementen voor het bepalen van het risiconiveau, (zie sectie op pagina 23).
Bestaande controlemiddelen en remediërende acties	Een lijst van de bestaande technische en organisatorische maatregelen, en de maatregelen die zullen worden genomen om bestaande risico's te beperken voor de getroffen individuen.
Meldingen	Een overzicht van meldingen die hebben plaatsgevonden, en aan wie (Gegevensbeschermingsautoriteit, getroffen individu, derde partijen).

III.

EEN CYBERVEILIGHEIDSINCIDENT ONDER CONTROLE KRIJGEN

SNEL HERSTELLEN OF BEWIJZEN VERZAMELEN?

Een cyberveiligheidsincident onder controle krijgen heeft alles te maken met het beperken van de schade en het stoppen van de aanvaller. U moet een manier vinden om tegelijkertijd het risico voor uw organisatie te beperken en de activiteiten ervan verder te zetten. U dient te verhinderen dat het incident uitbreidt naar andere systemen, apparaten en netwerken binnen uw organisatie of daarbuiten.

In het begin van deze fase moet uw organisatie een belangrijke strategische beslissing nemen: de systemen onmiddellijk loskoppelen om zo snel mogelijk haar gewone activiteiten te kunnen hervatten? Of de tijd nemen om bewijzen te verzamelen tegen de cybercrimineel die het systeem binnendrong?

In vele gevallen zal de oplossing ergens tussen deze twee opties in liggen. Welke beslissing uw organisatie neemt, hangt af van het bereik, de grootte en impact van het incident. De volgende criteria kunnen u helpen bij het beoordelen daarvan:

1. Wat kan er gebeuren als het incident niet onder controle raakt?
2. Brengt de aanval of inbreuk onmiddellijke zware schade toe?
3. Is er (mogelijke) schade aan en/of diefstal van activa?
4. Is het nodig om bewijzen bij te houden? Zo ja, welke bronnen van bewijsmateriaal moet de organisatie verzamelen? Waar worden de bewijzen opgeslagen? Hoe lang moet het bewijsmateriaal worden bewaard?
5. Is het nuttig dat de hacker voorlopig niet weet dat hij gedetecteerd werd?
6. Moet u zorgen voor de beschikbaarheid van diensten of is het aanvaardbaar om het systeem offline te brengen? (denk bijvoorbeeld aan diensten aan externe partijen)

In sommige gevallen is het onmogelijk om de normale activiteiten van uw organisatie (onmiddellijk) te hernemen. Wanneer dit gebeurt, zal het onder controle krijgen van het incident erin bestaan om al het mogelijke te doen om ervoor te zorgen dat de basisfunctionaliteiten van het systeem blijven werken en dat de bevoegde gebruikers hun toegang behouden. Tezelfdertijd dient men achter de schermen te proberen om de aanvaller zo snel mogelijk de toegang tot het systeem te ontzeggen.

Tijdens een incident is de druk groot om snel te handelen. Om onnodige fouten te voorkomen, is het heel belangrijk om een stap terug te zetten en na te denken voor u iets onderneemt!

HET ONDERZOEK: BEWIJZEN VERZAMELEN

Als u het probleem bij de bron wilt aanpakken en de dader wilt identificeren om hem te kunnen vervolgen, dan moet u de bewijzen bewaren. Om bewijsmateriaal te verzamelen moet forensisch **onderzoek** worden uitgevoerd voor u het incident vernietigt. Als u niet over de nodige interne expertise beschikt om het forensisch onderzoek zelf uit te voeren, moet u een beroep doen op externe experts die over de juiste middelen beschikken om de bewijzen op een rechtsgeldige manier te verzamelen (zie ook: pagina 13 Experts incidentrespons).
Houd in het achterhoofd dat u, zelfs als uw organisatie over een uiterst deskundig ICT-team beschikt, nog steeds externe hulp nodig kunt hebben in het geval van een complex cyberveiligheidsincident. Dit betekent niet dat uw ICT-professionals hebben gefaald; integendeel, het betekent dat ze tijdig hebben ontdekt dat het incident zo complex is dat extra expertise nodig is.

EEN DDOS-AANVAL AANPAKKEN VEREIST ERVARING

Een DDOS-aanval is een gerichte aanval om uw systeem uit te schakelen. Concreet houdt dit in dat zo'n aanval een belangrijke impact kan hebben op de beschikbaarheid van uw systeem. DDOS-aanvallen zijn heel gesofisticeerd en het is moeilijk om ervan af te raken. De meeste organisaties zullen niet in staat zijn om zelf een DDOS-aanval op te lossen en moeten een beroep doen op externe experts wanneer ze door een dergelijke aanval worden getroffen.

Belangrijk: om in de rechtbank te worden aanvaard, moet bewijsmateriaal verzameld worden volgens procedures die alle van kracht zijnde wetten en voorschriften naleven. Zorg er dus voor dat u geen bewijzen aantast. Het is bijvoorbeeld geen goed idee om

UW SERVER ONMIDDELLIJK UIT TE SCHAKELEN

- U kunt de oorzaak van het incident of de dader mogelijk niet identificeren. Als u de server uitschakelt, maakt u het geheugen op de server leeg. Dit betekent dat u geen forensisch onderzoek van het geheugen kunt uitvoeren omdat er niets meer te analyseren valt.
- U vernietigt dan misschien cruciaal bewijsmateriaal omdat het RAM-geheugen vaak heel wat sporen van malware bevat. Voor u uw server uitschakelt, moet die worden gedumpt op een USB-schijf.

DE SERVER ONMIDDELLIJK LOS TE KOPPELEN VAN HET INTERNET

- U vernietigt dan misschien cruciaal bewijsmateriaal. Door een onmiddellijke uitschakeling kan de omvang van de aantasting van uw infrastructuur niet worden bepaald, omdat een server die werd uitgeschakeld en van het internet werd losgekoppeld niet langer communiceert met zijn commando- en besturingsserver op het internet, noch met andere besmette werkstations/servers in uw netwerk.
- U kunt zo de cybercrimineel alarmeren. Hij zal weten dat u hem op het spoor bent en in deze fase is dat nog geen goed idee.

UW SYSTEEM TE HERSTELLEN VANAF EEN BACK-UP, ALS U NIET ZEKER BENT DAT DE BACK-UP ZELF NIET IS BESMET

Uw back-up kan besmet zijn: APT's kunnen langere tijd in uw netwerk aanwezig zijn zonder dat u het merkt. Daarom is de kans op een besmette back-up reëel. Een besmette back-up installeren kan voor een nieuwe besmetting zorgen.

OPNIEUW TE INSTALLEREN OP DEZELFDE SERVER ZONDER EEN FORENSISCHE KOPIE

MEEST VOORKOMENDE SOORTEN INCIDENTEN

Op dit ogenblik komt de lijst met categorieën van de cyberveiligheidsincidenten die het meeste kans maken om uw organisatie te treffen (zie ook: pagina 20 Mogelijke categorieën van cyberveiligheidsincidenten identificeren) van pas. Een goed opgestelde lijst voorziet enerzijds welke soorten incidenten uw organisatie zouden kunnen treffen en anderzijds ook de basisinstructies om deze typische incidenten op te lossen. Een voorbeeld vindt u in de Bijlage.

IV.

ELIMINERING EN SANERING

Zodra het onderzoek is afgerond, kunt u de eliminering starten. In deze fase moet u alle componenten met betrekking tot het incident en alle door de aanvaller achtergelaten artefacten (kwaadaardige code, gegevens enz.) verwijderen en alle gaten en kwetsbaarheden die door de hacker werden gebruikt om binnen te dringen, verwijderen.

Start de sanering niet voor u een volledig overzicht van het incident hebt! Dit betekent dat u moet beginnen met het bepalen van de grondoorzaak. Dit is geen gemakkelijke opdracht. Bovendien moet u ervoor zorgen dat u ten minste naar alle machines met dezelfde kwetsbaarheid hebt gekeken; deze kunnen ook besmet zijn. Wanneer de beslissing wordt genomen om het incident uit te roeien, is het belangrijk om snel, gesynchroniseerd en grondig te werk te gaan zodat de tegenstander zo weinig mogelijk de kans krijgt (idealiter geen kans) om te reageren.

De vernietiging kan vele vormen aannemen. Het gaat vaak om acties zoals:
- Een virus- of spywarescanner gebruiken om de kwaadaardige bestanden en services te verwijderen
- Handtekeningen bijwerken
- Malware verwijderen
- Aangetaste gebruikersaccounts uitschakelen
- Wachtwoorden van aangetaste gebruikersaccounts wijzigen
- Alle uitgebuite kwetsbaarheden identificeren en verhelpen
- Gaten in de veiligheid identificeren en herstellen
- Werknemers inlichten over de dreiging en hen instructies geven over wat in de toekomst moet worden vermeden
- Externe belanghebbenden zoals de media en uw klanten inlichten (zie ook: pagina 29 Communicatie tijdens een cyberveiligheidsincident)

Belangrijk ook: het topmanagement moet worden ingelicht over de resultaten van de eliminering en sanering en over de status van het netwerk.

Individuele bestanden kunnen worden gedetecteerd, in quarantaine geplaatst of van systemen verwijderd door de antivirusoplossing. Deze oplossing moet specifieke virusdefinities kunnen accepteren die door u worden geleverd.

Phishing-e-mails kunnen op de mail gateway worden tegengehouden door te blokkeren op basis van afzender, het mailrelay of onderdelen van de inhoud.

IP- en domeingebaseerde indicatoren kunnen worden geblokkeerd op basis van netwerkverkeer, door ze toe te voegen aan toegangslijsten, firewallregels of proxyregels. Daarom is het belangrijk om over de nodige capaciteit te beschikken om deze wijzigingen op een ad-hocmanier in te voeren.

V.

HERSTELLEN

Wanneer we het over herstellen hebben, bedoelen we het herstellen van het systeem (de systemen) om terug te keren naar een normale werking en (indien van toepassing) kwetsbaarheden oplossen om soortgelijke incidenten te verhinderen. Er zijn verschillende manieren om te herstellen na een cyberveiligheidsincident. Ze hebben allemaal een andere impact op de hersteltijd, de kostprijs van het herstel of gegevensverlies:

	HERSTELTIJD	KOSTEN	GEGEVENSVERLIES	OPMERKINGEN
De kwaadaardige artefacten schoonmaken en de aangetaste bestanden vervangen door schone versies	Snel	Rendabel		U laat mogelijk onontdekte artefacten achter
Herstellen vanaf een back-up	Middelmatig	Rendabel		Dit is alleen mogelijk als u over een betrouwbare back-up beschikt. In sommige gevallen is het moeilijk om de exacte tijd van het initiële incident te bepalen, of het incident is al heel lang aan de gang en er is geen back-up meer van de periode vóór het incident.
De systemen of omgeving vanaf nul heropbouwen	Traag, niet tijdsefficiënt	Heel duur	Kans op gegevensverlies	Dit is echter de enige manier om er 100% zeker van te zijn dat u van de aanvaller bent verlost.

Uit statistieken blijkt dat incidenten heel vaak pas na verschillende maanden aan het licht komen. Hoe ver gaat de back-up van uw organisatie terug?

Welk type herstel het meest aangewezen is voor een specifiek incident, hangt niet alleen af van de tijd en de financiële middelen die u ter beschikking hebt. Het hangt ook af van de schade die het incident aan uw infrastructuur heeft veroorzaakt. Het is bijvoorbeeld mogelijk dat u geen onbesmette back-up hebt, omdat zelfs uw oudste back-up werd gemaakt nadat de aanvaller uw systeem binnendrong. Daarom is het belangrijk om uw back-up te controleren op virussen, rootkits en achterpoortjes voor u hem gebruikt om te herstellen. Als er geen betrouwbare back-up kan worden gevonden, dan moet het systeem helemaal opnieuw worden geïnstalleerd (inclusief het besturingssysteem!). Na het herstellen van het systeem dient u de kwetsbaarheden op te lossen waardoor de dader in uw systeem kon binnendringen.

Dit omvat acties zoals: patches installeren, zowel op het niveau van het besturingssysteem, als op dat van applicaties, wachtwoorden wijzigen, accounts wijzigen, de beveiliging van de netwerkperimeter verbeteren door bv. de firewall te wijzigen, controlelijsten voor routertoegang enz., en diensten vergrendelen.

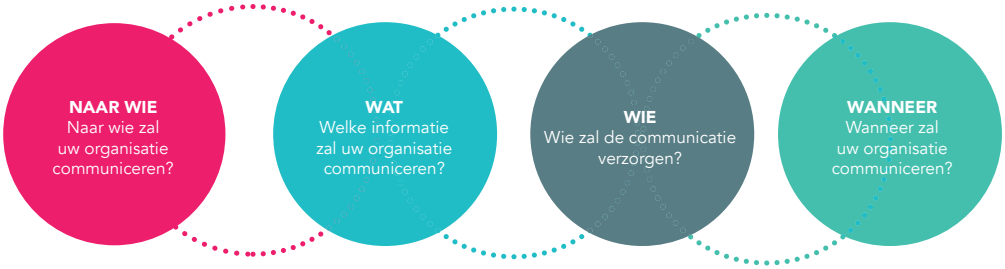
U moet er ook rekening mee houden dat zodra een tool met succes werd aangevallen, de kans bestaat dat het opnieuw zal worden aangevallen, of dat andere tools in uw organisatie op een soortgelijke manier kunnen worden aangevallen. Daarom moet u overwegen om uw verdediging te verbeteren, bijvoorbeeld door systeemlogging of netwerktoezicht op een hoger niveau.

Ten slotte moet het systeem, voor het opnieuw online wordt geplaatst, worden goedgekeurd voor zowel veiligheids- als bedrijfsfuncties. Op het vlak van beveiliging kan uw systeem worden goedgekeurd door het te scannen met een tool dat controleert op overblijvende kwetsbaarheden. Om de bedrijfsfuncties te valideren, moet de bevoegde persoon controleren of alle functies die nodig zijn voor het bedrijf naar behoren werken.

Vergeet zeker niet: als u niet over de nodige expertise beschikt binnen uw organisatie, doe dan een beroep op externe experts. En vergeet niet na te gaan of uw cyberverzekering deze kosten dekt.

04 COMMUNICATIE TIJDENS EEN CYBERVEILIGHEIDSINCIDENT

Wanneer er zich effectief een cyberbeveiligingsincident voordoet, moet er onmiddellijk een concreet communicatieplan opgesteld worden voor dit specifieke incident door het incidentresponsteam. Dit communicatieplan bouwt verder op de voorbereidingen die reeds getroffen zijn in de voorbereidende fase (zie ook: pagina 16 Uw communicatiestrategie voorbereiden). Het is sterk aanbevolen om het opstellen van alle externe communicatie af te stemmen zowel met de juridische afdeling als met de communicatie- of PR-afdeling. In essentie moeten de volgende vragen beantwoord worden:



I. MIDDELEN

Als u goed voorbereid bent, dan heeft uw incidentresponsteam al enkele middelen ter beschikking. Tijdens de voorbereiding heeft uw organisatie een lijst van alle mogelijke belanghebbenden (interne en externe belanghebbenden en officiële instanties) opgesteld waarmee contact moet worden opgenomen, evenals een lijst met hun contactgegevens (een specifiek persoon en zijn back-up) (zie ook: pagina 16 Uw communicatiestrategie voorbereiden).

II. INCIDENTSPECIFIEK COMMUNICATIEPLAN

NAAR WIE COMMUNICEREN EN WAT TE COMMUNICEREN NAAR ELKE CATEGORIE VAN BELANGHEBBENDEN

De eerste stap in uw incidentspecifieke communicatieplan is bepalen naar wie u zult communiceren. Om dit te doen, moet u identificeren welke betrokkenen mogelijk (negatief) worden getroffen door het cyberveiligheidsincident waarmee u wordt geconfronteerd en of u wettelijk gebonden bent bepaalde instellingen in te lichten, zoals de Gegevensbeschermingsautoriteit – dat is de Belgische commissie voor de bescherming van de persoonlijke levenssfeer – of de sectorale toezichthouder.

- Interne belanghebbenden: topmanagement, getroffen managers, werknemers
- Externe belanghebbenden: media, klanten, betrokken leveranciers, andere partners enz.
- Officiële belanghebbenden: Gegevensbeschermingsautoriteit, sectorale toezichthouder, CCB (Afdeling CERT.be), Nationaal Crisiscentrum (NCCN), politie

Een goede basisregel om in acht te nemen wanneer bepaald wordt wat er gecommuniceerd zal worden en naar wie, is om enkel te communiceren op basis van 'need-to-know'. Er zijn belanghebbenden naar wie u wilt communiceren om het cyberveiligheidsincident te beheersen en er zijn belanghebbenden naar wie u moet communiceren, ofwel omdat ze u onder druk zetten om informatie te verkrijgen (bv. de media) of omdat u wettelijk verplicht bent hen in te lichten (bv. Gegevensbeschermingsautoriteit, sectorale toezichthouder, de mensen van wie de gegevens werden gelekt).

Persoonsgegevens

Wanneer persoonsgegevens zijn verloren of gestolen (gegevenslek of inbreuk in verband met persoonsgegevens), is het raadzaam om de Gegevensbeschermingsautoriteit in te lichten. In sommige gevallen bent u daartoe wettelijk verplicht.
Bijvoorbeeld:

- Voor ondernemingen die elektronische communicatiediensten aanbieden die toegankelijk zijn voor het publiek is het wettelijk verplicht een inbreuk in verband met persoonsgegevens te melden aan de Gegevensbeschermingsautoriteit en aan de personen om wiens gegevens het gaat.
- Onder de AVG is het wettelijk verplicht om elke inbreuk in verband met persoonsgegevens die mogelijk een risico kan inhouden voor de personen wiens gegevens zijn gelekt, te melden zowel aan de Gegevensbeschermingsautoriteit (binnen de 72 uur) als aan de betrokken personen. [1]

Rapporteringsplicht: NIS-wetgeving

AED en DDV hebben de verplichting om alle incidenten met ingrijpende gevolgen te melden aan het CCB (afdeling CERT.be), het Nationaal Crisiscentrum en aan hun sectorale overheid via een beveiligd meldingsplatform. De CCB treedt op als nationale CSIRT. Of de gevolgen van een incident al dan niet ingrijpend zijn, moet worden beoordeeld in het licht van de beschikbaarheid, de vertrouwelijkheid, de integriteit of de authenticiteit van de informatiesystemen waarvan de informatiesystemen van de AED / DDV.

- Beschikbaarheid verwijst naar de mogelijkheid voor gebruikers om toegang te krijgen tot de diensten van de AED / DDV. Een DDoS aanval bijvoorbeeld kan het netwerk van een AED lamleggen en de beschikbaarheid van de dienst in het gevaar brengen.
- Een voorbeeld van een incident m.b.t. confidentialiteit is een "man in the middle attack" waarbij gegevens tussen de gebruikers en de AED / DDV worden onderschept. Een dergelijk incident kan ook aanleiding geven tot een meldingsplicht aan de Gegevensbeschermingsautoriteit (zie p. 29).
- Een integriteitsincident is voorhanden wanneer gegevens van een AED / DDV gedurende een systeem-crash worden vernietigd.
- Een incident inzake authenticiteit speelt zich bv. af wanneer een verstrekker van domeinnamen de authenticiteit van de domeinnamen niet meer met zekerheid kan waarborgen.

Het is mogelijk dat er per (deel)sector weerslagniveaus en/of drempelwaarden bepaald worden bij koninklijk besluit, maar dit is tot op heden nog niet het geval.

Wees ervan bewust dat zware administratieve en strafrechtelijke sancties kunnen worden opgelegd bij schending van de rapporteringsplicht.

WANNEER COMMUNICEREN?

Zogauw het beslist is naar wie er gecommuniceerd gaat worden en wat u hen gaat vertellen, moet er beslist worden wanneer u hen zal contacteren. De timing wordt bepaald door de doelstellingen van de communicatie (zie ook: illustratie op p. 18).

De timing is belangrijk:
- Sommige betrokkenen hebben de informatie zo snel mogelijk nodig omdat zij kunnen helpen bij het onder controle krijgen van het cyberveiligheidsincident (bv. het topmanagement, de werknemers van uw organisatie);
- Met andere belanghebbenden (bv. Gegevensbeschermingsautoriteit) moet binnen een wettelijk opgelegde termijn contact worden opgenomen;
- en ten slotte, kunnen anderen contact met u opnemen en in dat geval moet u uw antwoorden voorbereid hebben (bv. media).

Om te voorkomen dat de dader te weten komt dat u hem op het spoor bent, kan het noodzakelijk zijn om een **periode zonder communicatie** in te lassen vanaf het ogenblik van detectie van het incident tot het ogenblik waarop u een volledig overzicht van het incident en een actieplan hebt. Als de dader wordt gealarmeerd, zal hij zich waarschijnlijk terugtrekken en al zijn sporen wissen of, erger nog, ultieme schade aanbrengen zoals het stelen van het laatste deel van de kroonjuwelen van uw organisatie of achterpoortjes installeren. Om een lek tijdens deze periode zonder communicatie te voorkomen, kan er een lijst bijgehouden worden van mensen die op de hoogte zijn van het cyberveiligheidsincident. Dit maakt het gemakkelijker om te ontdekken wie verantwoordelijk is, wanneer blijkt dat informatie is gelekt. Er kunnen juridische stappen ondernomen worden tegen de persoon die informatie lekte.

Wat betreft het melden van NIS-incidenten, dient er onverwijld melding gemaakt te worden van het incident. Het is niet nodig om te wachten tot alle relevante informatie beschikbaar is. Wanneer het duidelijk is dat het incident gemeld moet worden, en wanneer er dus aan tenminste één criteria voldaan wordt, moet dit zo snel mogelijk gebeuren.

RAPPORTEREN AAN AUTORITEITEN

Rapporteren aan bevoegde instanties is een heel specifiek onderdeel van communicatie. Het is om diverse redenen belangrijk:
- Zoals hierboven reeds vermeld, is in sommige gevallen het rapporteren van een gegevenslek of andere cyberveiligheidsincidenten **wettelijk verplicht**.
- Bepaalde instanties kunnen u **helpen**. Het cyberveiligheidsincident waarmee u wordt geconfronteerd, is mogelijk geen alleenstaand geval. Overheidsdiensten kunnen over informatie beschikken waarmee u uw incident sneller onder controle kunt krijgen.
- Indien u een klacht wilt indienen tegen de crimineel die achter het cyberveiligheidsincident zit, moet u contact opnemen met de ordehandhavende instanties. In principe is dat **de politie**.
- Bovendien is het rapporteren aan de overheid een noodzakelijke stap waardoor de **cybercriminaliteit in het land kan worden geïnventariseerd en gemeten**. Betere kennis van en inzicht in het fenomeen en zijn verspreiding kunnen immers bijdragen tot de verbetering van het algemene veiligheidslandschap, bv. door het meebepalen van preventieve maatregelen en tegenmaatregelen.

1. Algemene verordening gegevensbescherming
2. Richtlijn voor Netwerk- en informatiebeveiliging (NIS)

CCB (Afdeling CERT.be) stelt steun en expertise kosteloos, in alle confidentialiteit ter beschikking, helpt om de eerste brand te blussen en geeft advies om te komen tot een oplossing. Rapporteer een cyberveiligheidsincident via cert@cert.be of, als u dat verkiest, telefonisch via: +32 (0)2 790 33 85 (elke werkdag van 8 tot 18 uur).

Na uw melding krijgt u een ontvangstbevestiging en een incidentnummer. Met dit incidentnummer kunt u steeds naar uw melding verwijzen. CCB (Afdeling CERT.be) neemt zo snel mogelijk contact met u op om uw vragen te beantwoorden.

NL **EN** **FR**

Vrijwillig rapporteren aan het CCB (Afdeling CERT.be)

Organisaties moeten altijd ernstig overwegen om cyberveiligheidsincidenten te rapporteren aan het federale cyber emergency team, het CCB (Afdeling CERT.be). Om aanvallen op andere computersystemen te verhinderen, is het CCB (Afdeling CERT.be) vooral geïnteresseerd in wat ze 'Indicators Of Compromise' (IOCs) noemen. Dit zijn artefacten die worden gevonden op een netwerk of besturingssysteem en die erop wijzen dat er heel waarschijnlijk een inbreuk is geweest. Rapporteren aan het CCB (Afdeling CERT.be) is van vitaal belang om te kunnen bepalen of het incident een alleenstaand geval is of niet, en om de trends in België in kaart te brengen.
Het CCB (Afdeling CERT.be) zal informatie en advies verstrekken over het incident, die het slachtoffer helpen om efficiënte tegenmaatregelen te treffen. Meer nog, de informatie die uw organisatie verschaft, kan mogelijks aanvallen op andere computersystemen voorkomen.

DE VOLGENDE INFORMATIE MOET WORDEN GERAPPORTEERD

1. Uw contactgegevens
2. Het type incident
3. De datum van het incident
4. Is het incident nog aan de gang?
5. Hoe merkte u het incident op?
6. Wat is de impact van het incident?
7. Hebt u al acties of maatregelen ondernomen? Zo ja, welke?
8. Beschikt u over logs of andere nuttige gegevens?
9. Wie hebt u al ingelicht?
10. Wat verwacht u van uw melding?

Verplicht rapporteren van NIS-incidenten

Melding moet gedaan worden via het NIS-meldingsplatform (https://nis-incident.be/). Het platform is toegankelijk via internet door middel van een beveiligde verbinding en een voor elke AED en DDV unieke identificatiesleutel (login/gebruikersnaam en wachtwoord). Indien het platform niet beschikbaar is, moet het incident gemeld worden via de website van het CCB (https://cert.be/nl/een-incident-melden). Het platform zorgt ervoor dat de melding bij het CCB, het Nationaal Crisiscentrum en bij de sectorale overheid terechtkomt.

Hieronder is voor elke sector de respectievelijke sectorale overheid opgesomd.

SECTOR	SECTORALE OVERHEID
Energie	Federale Minister bevoegd voor Energie (FOD Economie DG Energie)
Vervoer	Federale Minister bevoegd voor Vervoer of Maritieme Mobiliteit (FOD Mobiliteit en Transport)
Gezondheidszorg	Federale Minister bevoegd voor Volksgezondheid (FOD Volksgezondheid)
Drinkwater	Nationaal Comité voor de beveiliging van de levering en distributie van drinkwater
Digitale infrastructuren	Federale Minister bevoegd voor Economie (BIPT)
Financiën	NBB (financiële instellingen); FSMA (financiële handelsplatformen

De melding omvat alle beschikbare informatie die toelaat de aard, de oorzaken, de effecten en de gevolgen van het incident te bepalen:
- de naam en contactgegevens van de aanbieder en de door hem verleende dienst;
- de datum en het tijdstip waarop het incident plaatsvond;
- de duur van het incident;
- de omvang van het geografische gebied dat door het incident is getroffen en de eventuele grensoverschrijdende aard ervan;
- het aantal getroffen gebruikers;
- informatie over de aard van het incident;
- de omvang van de gevolgen van het incident, met name voor maatschappelijke en economische activiteiten;
- het belang van de systemen of van de betrokken informatie;
- de gevolgen van het incident voor in België gevestigde internationale organisaties;
- de ondernomen acties;
- de beschrijving van de huidige situatie.

De initiële melding, die zo snel mogelijk dient te gebeuren, is één fase in de meldingsprocedure. In totaal kan de procedure drie fasen omvatten:

- De initiële melding moet onverwijld plaatsvinden, zelfs indien de AED of DDV nog niet over alle relevante informatie beschikt. Doel van deze initiële melding is het CCB, de sectorale overheid of haar sectorale CSIRT, en het NCCN te wijzen op het incident en de mogelijke gevolgen ervan.

- Bijkomende meldingen moeten regelmatig worden verstuurd of zodra de AED of DDV over nieuwe informatie beschikt. Doel van deze bijkomende meldingen is het CCB, de sectorale overheid of haar sectorale CSIRT, en het NCCN op de hoogte te houden van de status van het incident. De AED of DDV doet dan een nieuwe melding op het platform, waarbij hij enkel de nieuwe gegevens en het referentienummer van de initiële melding vermeldt.

- Een eventueel eindverslag (op verzoek van een van de voornoemde overheden) met alle informatie die naar het CCB, de sectorale overheid of haar sectorale CSIRT, en het NCCN is gestuurd. Doel van dit eindverslag is een overzicht te geven van het incident en er conclusies uit te trekken.

De AED of DDV moet het CCB en de sectorale overheid, of in voorkomend geval het sectorale CSIRT, op de hoogte houden van de evolutie van het incident en de ondernomen remediërende acties.

Een klacht indienen bij de ordehandhaving

De ordehandhavende instanties moeten zo snel mogelijk na de ontdekking van het cyberbeveiligingsincident geïnformeerd worden, gezien de vluchtigheid van sporen en de acties die moeten worden ondernomen (internetidentificatie enz.). Voor een succesvolle gerechtelijke vervolging moeten de bewijsstukken verkregen worden op een juridisch geldige manier. Dit houdt in dat het bewijsmateriaal onmiddellijk na de detectie van het incident intact moet bewaard worden.
De gerechtelijk instanties dienen over de informatie over het incident te beschikken om de kwalificatie van het misdrijf te maken en over te gaan tot de identificatie van de verdachte. De informatie die aan de politie moet worden gegeven in geval van internetfraude (een 'klassiek' misdrijf dat met behulp van elektronische middelen wordt gepleegd) is mogelijk niet helemaal dezelfde als de informatie die de politie nodig heeft in geval van een ICT-misdrijf (hacking, sabotage, spionage). In de loop van het onderzoek zal er bijkomende informatie gevraagd, verzameld en gezocht worden door de speurders. Het is van het allergrootste belang dat uw diensten de bijstand en inbreng leveren die door de ordehandhavende instanties gevraagd worden, om het onderzoek vooruit te helpen.

U dient sowieso naar uw plaatselijke politiekantoor of het politiekantoor van uw keuze te gaan. Informatie over politiezones vindt u hier:

NL FR

I. Politie

Als uw organisatie geconfronteerd wordt met een incident en aldus het slachtoffer is geworden van een misdrijf, kunt u beslissen om een klacht in te dienen. U gaat hiervoor naar uw plaatselijke politiekantoor of naar een politiekantoor van uw keuze. Voor complexere zaken krijgt de lokale politie bijstand van de Regional Computer Crime Units (RCCU), die gespecialiseerd zijn in ICT-misdrijven (hacking, sabotage, spionage), en/of de Federal Computer Crime Unit (FCCU). Indien het gaat om kritieke infrastructuur of het een sector betreft met specifieke regelgeving, is er mogelijk een speciale procedure van toepassing.

II. Onderzoeksrechter

Het is ook mogelijk om rechtstreeks bij een magistraat (onderzoeksrechter) een klacht in te dienen. Dit is een uitzonderlijke maatregel. Bovendien zal uw organisatie waarschijnlijk bij voorbaat de kosten van het onderzoek moeten betalen, omdat de magistraat het onderzoek op uw specifieke verzoek voert.

KENNISGEVING VAN EEN GEGEVENSLEK AAN DE GEGEVENSBESCHERMINGSAUTORITEIT

Bepaalde lekken van persoonsgegevens, dienen gemeld te worden aan de Gegevensbeschermingsautoriteit. Ter herinnering: met persoonsgegevens bedoelt men alle gegevens die betrekking hebben op een natuurlijk persoon die rechtstreeks of onrechtstreeks geïdentificeerd wordt of kan worden. Ook een nummer, zoals een IP-adres, zal dus in heel wat gevallen als een persoonsgegeven beschouwd worden.

Kennisgeving aan de Gegevensbeschermingsautoriteit gebeurt via een beveiligd elektronisch formulier. Meer uitleg is terug te vinden in de handleiding van het meldingsformulier.

NL FR

De meldingsplicht betreft lekken die een risico inhouden voor de rechten en vrijheden van de betrokkenen. Een voorbeeld daarvan is het verlies van confidentialiteit van een communicatie waardoor factuurgegevens, adressen,…, tijdelijk zichtbaar worden voor derden. In beginsel is de meldingstermijn 72 uur nadat het gegevenslek wordt vastgesteld.

Dankzij de melding door uw organisatie kan de Gegevensbeschermingsautoriteit de impact van het gegevenslek inschatten samen met de verantwoordelijke voor de verwerking van de gelekte gegevens, en kan zij aanbevelingen doen over de wettelijke regels rond gegevensverwerking en de beveiliging daarvan. Bovendien zullen de verantwoordelijke(n) voor gegevensverwerking de wijze waarop de gegevensverwerking georganiseerd en beveiligd wordt, nu en in de toekomst, opnieuw moeten bekijken. Organisaties in specifieke sectoren, zoals ondernemingen die financiële diensten of elektronische communicatiediensten aanbieden, moeten er rekening mee houden dat zij reeds verplicht zijn om elk incident met een inbreuk op persoonsgegevens, te melden aan de Gegevensbeschermingsautoriteit.

KENNISGEVING AAN DE PERSONEN VAN WIE DE GEGEVENS GELEKT ZIJN

Indien het gegevenslek een hoog risico meebrengt voor de betrokkenen, dient een kennisgeving te worden verricht aan de personen van wie de gegevens gelekt zijn. De verantwoordelijke voor de gegevensverwerking moet het gegevenslek melden aan de betrokken personen met communicatiemiddelen die garanderen dat de informatie snel wordt ontvangen. Als het onmogelijk is om de benadeelde personen te identificeren, kan de verantwoordelijke die personen inlichten via de media, hoewel hij ondertussen moet blijven proberen om de identiteit van die personen te achterhalen zodat zij ook individueel geïnformeerd kunnen worden.

De kennisgeving aan de betrokken personen moet duidelijk en makkelijk te begrijpen zijn. De Gegevensbeschermingsautoriteit beveelt aan om tenminste de hiernavolgende informatie te verstrekken:

- naam van de verantwoordelijke voor de gegevensverwerking;
- contactgegevens waar bijkomende informatie kan worden verkregen;
- samenvatting van het incident dat de persoonsgegevens heeft aangetast;
- (vermoedelijke) datum van het incident;
- aard en strekking van de betrokken persoonsgegevens;
- denkbare gevolgen van het gegevenslek voor de betrokken personen;
- omstandigheden waaronder het gegevenslek plaatsvond;
- de maatregelen die de verantwoordelijke heeft genomen om dit gegevenslek te verhelpen;
- de maatregelen die de verantwoordelijke aan de betrokken personen aanbeveelt om de mogelijke schade in te perken.

GEGEVENSLEK

Rex Mundi heeft toegang tot de gegevens van uw bedrijf gekregen. Deze bevatten gevoelige informatie over uw klanten, hun privacy staat dus op het spel. Hij dreigt ermee alles op het internet te plaatsen via zijn Twitter-account.

05

NABESPREKING EN AFSLUITEN VAN HET INCIDENT: LESSEN TREKKEN VOOR DE TOEKOMST

Net als elk ander incident moeten alle cyberveiligheidsincidenten correct worden afgesloten. Bovendien is het heel belangrijk dat er uit elk incident lessen worden getrokken om in de toekomst verbeteringen te kunnen doorvoeren.

EVALUATIE VAN GELEERDE LESSEN EN TOEKOMSTIGE ACTIES: ORGANISEER EEN NABESPREKING VAN HET INCIDENT

Een nabespreking van het incident levert een bijzonder nuttig document omdat het de feitelijke gegevens en echte impact weergeeft. Dit kan van nut zijn voor uw organisatie bij de beoordeling van uw incidentresponsplan en de herziening van het budget.

DOELSTELLING
Alle cyberveiligheidsincidenten moeten formeel worden besproken nadat het incident is opgelost om na te gaan of beveiligingsmechanismen of risicobeperkende controles moeten worden ingevoerd of aangepast om soortgelijke incidenten in de toekomst te vermijden.

WAAROM?
Cyberveiligheidsincidenten kunnen wijzen op belangrijke tekortkomingen in uw beveiligingsstrategie of -praktijk. Elk belangrijk incident moet worden geanalyseerd om te beoordelen of er lessen uit kunnen worden getrokken voor toekomstige verbeteringen.

HOE MOET DE NABESPREKING VAN HET INCIDENT ERUITZIEN?
Een nabespreking van het incident en mogelijke geleerde lessen moeten een onderdeel vormen van de aanpak van elk cyberveiligheidsincident.
Checklist met vragen die bij de evaluatie kunnen helpen:

- Werden de aanpak en de procedures voor cyberveiligheidsincidenten gevolgd? Waren die geschikt? Moet het plan op bepaalde punten worden aangepast?
- Was de informatie op tijd beschikbaar? Zo nee, zou het mogelijk zijn geweest om die sneller te hebben en hoe?
- Hebt u stappen of acties ondernomen die het herstel mogelijk hebben gehinderd?
- Kan het delen van uw informatie met andere organisaties worden verbeterd?
- Welke corrigerende acties kunnen soortgelijke incidenten in de toekomst voorkomen?
- Zijn er voortekens of indicatoren die in de gaten kunnen worden gehouden om soortgelijke incidenten in de toekomst gemakkelijker te detecteren?
- Welke extra middelen zijn nodig om toekomstige cyberveiligheidsincidenten te detecteren, analyseren en beperken?
- Beschikte het responsteam voor cyberveiligheidincidenten over de juiste bevoegdheiden binnen de organisatie om te kunnen reageren op het incident? Dient u meer mensen aan te werven of een adviesbureau, jurist enz. ter beschikking te houden in geval van een toekomstig cyberveiligheidsincident?

II. OPVOLGEN VAN EN RAPPORTEREN OVER INCIDENTEN

Het is belangrijk om elk incident en de ondernomen acties te documenteren en al deze informatie bijeen te houden. Soortgelijke incidenten kunnen opnieuw plaatsvinden en vereisen mogelijk dezelfde behandelingsprocedures, of een klein incident kan een onderdeel blijken van een groter incident dat later ontdekt wordt. Bovendien is het ook nodig om het incident aan de relevante interne en externe belanghebbenden te rapporteren. Gebruik de resultaten van uw post-incidentevaluatie om te bepalen met welke belanghebbenden contact moet worden opgenomen. Intern moet het topmanagement van de organisatie altijd als relevante belanghebbende worden beschouwd en dus een gedocumenteerd verslag ontvangen over wat er is gebeurd, welke acties er werden genomen, waar het goed/fout liep enz.

DOELSTELLING

VOLGEN
Alle cyberveiligheidsincidenten en hun afwikkeling moeten worden gedocumenteerd.

RAPPORTEREN
Alle cyberveiligheidsincidenten en hun afwikkeling moeten worden gerapporteerd aan het topmanagement en, als deze functie binnen uw organisatie bestaat, aan de informatiebeveiliger (Information Security Officer).

WAAROM?

OPVOLGEN
Soortgelijke incidenten kunnen opnieuw plaatsvinden en vereisen mogelijk dezelfde behandelingsprocedures, of een klein incident kan een onderdeel blijken van een groter incident dat u later ontdekt.

RAPPORTEREN
Het topmanagement en/of de mensen binnen uw organisatie die de risico's van uw organisatie analyseren (bv. Het Comité operationeel risico of gelijkwaardig) moeten op de hoogte zijn van cyberveiligheidsincidenten.

HOE MOET DE NABESPREKING VAN HET INCIDENT ERUITZIEN?

Een gedocumenteerd verslag moet worden geschreven voor alle cyberveiligheidsincidenten en worden bijgehouden bij verslagen over cyberveiligheidsincidenten. U kunt dit verslag baseren op de conclusies van de nabespreking van het incident.
Alle grote veiligheidsincidenten moeten onmiddellijk aan het topmanagement worden gerapporteerd. Ten minste één keer per jaar moeten alle cyberveiligheidsincidenten worden gerapporteerd aan en toegelicht voor het topmanagement en de mensen die binnen uw organisatie belast zijn met de risicoanalyse van de organisatie.

WOORDENLIJST

Achterpoortje In software of een computersysteem is dit een methode om de beveiligingsmechanismen te omzeilen. Het kan op wettige wijze worden gebruikt door systeembeheerders of programmeurs. Maar in deze gids hebben we het over de onwettige wijze, namelijk een geheim portaal waarvan hackers en intelligentiediensten gebruik maken om ongemerkt onwettige toegang te verkrijgen tot computersystemen.

Activa Elk middel of elke mogelijkheid. De activa van een serviceprovider zijn alles wat kan bijdragen aan de verstrekking van een dienst. Activa kunnen van de volgende types zijn: management, organisatie, proces, kennis, mensen, informatie, toepassingen, infrastructuur en financieel kapitaal.

APT APT is de afkorting van Advanced Persistent Threat (geavanceerde aanhoudende bedreiging). Dit is een reeks heimelijke en continue computerhackingprocessen. In geval van een APT maakt de dader gebruik van meerdere fasen om in een netwerk in te breken, om detectie te verhinderen en om op lange termijn waardevolle informatie te verzamelen.

Artefact Een artefact is een voorwerp van digitaal archeologisch belang.

Back-up Back-upprocedures worden gebruikt om bestanden te kopiëren naar een tweede medium, zoals een schijf, tape of de cloud. Back-upbestanden moeten op een offsite locatie worden bewaard. Back-ups worden meestal geautomatiseerd met behulp van commando's van het besturingssysteem of back-upprogramma's. De meeste back-upprogramma's comprimeren de gegevens zodat er voor de back-ups minder media nodig zijn.

Botnet Een verzameling computers (vaak tienduizenden) die door een of meer mensen (botmasters genoemd) worden bediend met behulp van malware (kwaadaardige software). Botnets kunnen worden gebruikt om spam te verzenden, een DDOS-aanval te starten, malware te verspreiden enz.

Commando- en controleserver Een gecentraliseerde server die commando's kan verzenden en informatie kan ontvangen van de computers die deel uitmaken van een botnet. Met de commando- en controleserver kan een botmaster de groep computers in zijn botnet vanop afstand bedienen.

DDOS DDOS is de afkorting van Distributed Denial of Service. In het geval van een DDOS geeft een botmaster aan de computers van zijn botnet de opdracht om een bepaalde website te bezoeken. De server van deze website raakt overbelast en werkt niet langer correct.

DMZ DMZ is de afkorting van 'demilitarised zone' (gedemilitariseerde zone) en verwijst naar het fysieke of logische subnetwerk (zone) dat een interne LAN (Local Area Network) scheidt van andere niet-vertrouwde netwerken, zoals het internet. Met een DMZ wil men een extra beveiligingsniveau toevoegen. De naam is afgeleid van de term 'demilitarised zone' (gedemilitariseerde zone), een gebied tussen twee naties waarin militaire operaties niet zijn toegestaan.

Host Een computer die een website of andere gegevens bevat die via het internet kunnen worden geraadpleegd of die andere diensten aan een netwerk levert.

IDS	IDS is de afkorting van Intrusion Detection System (Inbraakdetectiesysteem). Dat is een geautomatiseerd systeem om hacking of onbevoegde toegang tot een computersysteem of netwerk te detecteren.
IP-adres	IP-adres is de afkorting van Internet Protocol-adres. Het is een numeriek label dat wordt toegewezen aan elk apparaat dat deel uitmaakt van een computernetwerk. IP-adressen worden gebruikt om het apparaat te identificeren en te lokaliseren.
Kwetsbaarheid	Een zwakte in een systeem, toepassing of netwerk die kan worden uitgebuit of misbruikt.
Netwerk	Een telecommunicatienetwerk waarmee computers of andere apparaten gegevens kunnen uitwisselen. Het bekendste computernetwerk is het internet.
Patch	Een patch is een klein stukje software dat vaak ontwikkeld is door de ontwikkelaars van specifieke software om deze software bij te werken, te herstellen (van fouten of kwetsbaarheden) of te verbeteren. Hiermee kunt u de software wijzigen zonder die helemaal opnieuw te installeren.
PGP	PGP is de afkorting van Pretty Good Privacy. Dat is een computerprogramma voor het coderen en decoderen van gegevens dat cryptografische beveiliging en verificatie voor datacommunicatie levert. PGP kan worden gebruikt voor het ondertekenen, coderen en decoderen van teksten, e-mails, bestanden, mappen, en hele schijfpartities en om de veiligheid van e-mailcommunicatie te verbeteren.
RAM	RAM is de afkorting van Random Access Memory. RAM is de meest voorkomende vorm van gegevensopslag in computers en andere apparaten zoals printers. In een RAM-apparaat kunnen alle gegevens in (bijna) dezelfde hoeveelheid tijd worden geraadpleegd, ongeacht waar de gegevens zich fysiek in het geheugen bevinden.
Rootkit	Een verzameling van computersoftware, vaak kwaadaardig, ontworpen met een dubbele bedoeling: (1) om een toegang te krijgen tot een computer of delen van zijn software die anders niet is toegestaan en tegelijkertijd (2) zijn bestaan of het bestaan van andere software maskeren. De detectie van rootkits is moeilijk omdat een rootkit in staat kan zijn om de software te ontwrichten die wordt gebruikt om de rootkit te vinden.Verwijdering kan ingewikkeld of nagenoeg onmogelijk zijn.
SNORT	Snort is een gratis opensourcesysteem voor de preventie en detectie van netwerkinbraak. www.snort.org
Spoofing	Een spoofingaanval is een situatie waarin een persoon of programma zich met succes uitgeeft voor een ander door gegevens te vervalsen en zo een onwettig voordeel te verkrijgen. Zo is e-mailspoofing bijvoorbeeld het aanmaken van e-mailberichten met een vervalst adres van de afzender.
VPN	VPN is de afkorting van Virtual Private Network. Dit is een groep computers die in een netwerk zijn verbonden via een openbaar netwerk zoals het internet. Bedrijven maken gebruik van VPN om op afstand verbinding te maken met datacenters of om werknemers toe te laten om veilig toegang te krijgen tot het intranet van het bedrijf wanneer ze niet op kantoor zijn.
Werkstation	Een computer (hardware).

BIBLIOGRAFIE

CERT-EU (2012), *Guidelines of the CERT-EU for data acquisition for investigation purposes*
Gehaald uit http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_12_04_Guideline_DataAcquisition_v1_4_4.pdf

CREST (2013), *Cyber Security Incident Response Guide*
Gehaald uit http://www.crest-approved.org/wp-content/uploads/CSIR-Procurement-Guide.pdf

ENISA (2010), *Good Practice Guide for Incident Management*
Gehaald uit https://www.enisa.europa.eu/activities/cert/support/incident-management

FEB, ICC, B-CCENTRE, *Isaca, EY, Microsoft (2013), Belgische Gids voor Cyberveiligheid*
Gehaald uit https://www.b-ccentre.be/wp-content/uploads/2014/05/B-CCENTRE-BCSG-NL.pdf

ISO/IEC 20000-1 (2011), *Information technology - Service management - Part 1: Service management system requirements*
Gehaald uit http://www.iso.org/iso/catalogue_detail?csnumber=51986

ISO/IEC 27001 (2013), *Information technology - Security techniques - Information security management systems - Requirements*
Gehaald uit http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

MARSH (2015), *European 2015 Cyber Risk Survey Report*
Gehaald uit http://belgium.marsh.com/Portals/95/Documents/15%2010-023%20European%20Cyber%20survey%20report.pdf

Microsoft TechNet, *Responding to IT Security Incidents*
Gehaald uit https://technet.microsoft.com/en-us/library/cc700825.aspx

NIST (2012), *Framework for Improving Critical Infrastructure Cyber Security – Version 1.0*
Gehaald uit http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

NIST (2012), *Computer Security Incident Handling Guide – Recommendations of the National Institute of Standards and Technology*
Gehaald uit http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

SANS Institute, *SCORE Security Checklist on APT Incident Handling*
Gehaald uit https://www.sans.org/media/score/checklists/APT-IncidentHandling-Checklist.pdf

SANS Institute (2003), *Sample Incident Handling Forms*
Gehaald uit https://www.sans.org/score/incident-forms/

SANS Institute (2007), *An Incident Handling Process for Small and Medium Businesses*
Gehaald uit https://www.sans.org/reading-room/whitepapers/incident/incident-handling-process-small-medium-businesses-1791

SANS Institute (2008), *Incident Handling for SMEs (Small to Medium Enterprises)*
Gehaald uit https://www.sans.org/reading-room/whitepapers/incident/incident-handling-smes-small-medium-enterprises-32764

SANS Institute (2008), *Security Incident Handling in Small Organizations*
Gehaald uit https://www.sans.org/reading-room/whitepapers/incident/security-incident-handling-small-organizations-32979

DANKBETUIGING

ONTWERP- & REVISIEGROEP

Cathy Suykens, Cyber Security Coalition
Anneleen Dammekens (VBO)
Daniel Letecheur (BOSA - formerly FEDICT)
Georges Ataya (Solvay Brussels School)
Luc Beirens (Deloitte)
Ferdinand Casier (Agoria)
Phédra Clouner (CCB)
Walter Coenraets (FCCU)
Miguel De Bruycker (CCB)
Dirk De Nijs (ICT CONTROL)
Pedro Deryckere (CCB - Afdeling CERT.be)
Nathalie Dewancker (Proximus)
Steven Goossens (Proximus)
Ann Mennens (European Commission, formerly B-CCENTRE)
Philippe Mermuys (Allianz)
Benoit Montens (Assuralia)
Ronny Tronquo (KBC Groep)
Erik Van Buggenhout (Nviso)
Geoffrey Schreiber (KPMG Advisory)
Kara Segers (KPMG Advisory)
Mathieu Tulpinck (Legal consultant)

VERANTWOORDELIJKE UITGEVER

Jan De Blauwe
Stuiversstraat 8
1000 Brussel
info@cybersecuritycoalition.be
www.cybersecuritycoalition.be

DATUM VAN EERSTE VERSCHIJNING

Januari 2016

DATUM VAN TWEEDE VERSCHIJNING

September 2021

BIJLAGE

Meest voorkomende types incidenten en hoe ze te neutraliseren

TYPE INCIDENT	DEFINITIE	MOGELIJK DOELWIT	KWETSBAARHEDEN DIE KUNNEN WORDEN UITGEBUIT	MOGELIJKE REACTIES
Social engineering: (spear) phishing, vishing (phone phishing)	Iemand manipuleren en bedriegen zodat hij informatie vrijgeeft (bv. wachtwoord of financiële informatie) die kan worden gebruikt om systemen of netwerken aan te vallen.	CEO Boekhouding		
(spear) phishing, vishing (phone phishing)	Een poging om gevoelige informatie te verkrijgen van klanten (bv. gebruikersnamen en wachtwoorden van klanten) door zich uit te geven voor een gewettigde en vertrouwde persoon of organisatie.			
Onbevoegde toegang	Wanneer iemand zonder toestemming logische of fysieke toegang tot een netwerk, systeem, toepassing, gegevens of een andere IT-bron verkrijgt.	Klanteninformatie kredietkaartinformatie Toepassingen voor het aanmaken of verwerken van betalingen Websites en diensten	Gekraakt of afgeluisterd wachtwoord Ongepatchte kwetsbaarheden van het systeem Social engineering Onzorgvuldige gebruikers of zwakke procedures	Kwetsbaarheden patchen of uitbuiting blokkeren Controleren op malware (rootkits, achterpoortjes, trojans…) Wachtwoorden wijzigen of accounts buiten werking stellen Verzamelen van forensische bewijzen (Netwerk) toegang tot de geviseerde middelen blokkeren
Denial of service	Elke aanval die het bevoegde gebruik van netwerken, systemen of toepassingen verhindert of schaadt door de middelen uit te putten.	Mailsysteem Netwerkapparaten Applicatieservers Websites en diensten	Zwaktes van spamfilter Ongepatchte kwetsbaarheden van het systeem Zwakke configuratie van systemen of apparaten	Verkeer blokkeren Contact opnemen met ISP De verbinding met besmette systemen verbreken
Aanval met kwaad-aardige code **Ransomware:** is een soort malware die de toegang beperkt tot het computersysteem dat het heeft besmet en losgeld vraagt dat aan de makers van de malware moet worden betaald om de beperking op te heffen. Sommige soorten ransomware coderen bestanden op de harde schijf van het systeem terwijl andere gewoon het systeem vergrendelen en berichten vertonen die de gebruiker tot betaling moeten overhalen.	Een aanval met kwaadaardige code is elke (grootschalige) infectie of infectiedreiging door een virus, worm, trojan of andere kwaadaardige entiteit op basis van code.	Elke server of zelfs apparaat in het netwerk kan het doelwit vormen van een aanval met kwaadaardige code, maar sommige systemen hebben een hoger risicoprofiel (bv. systemen die rechtstreeks of onrechtstreeks verbonden zijn met de buitenwereld). Alle werkstations van eindgebruikers kunnen het doelwit vormen via e-mail, USB-opslagapparaten, bezoeken aan websites en internettoepassingen enz.	Ongepatchte kwetsbaarheden van het systeem (bv. Flash of JavaScript) Antivirussoftware niet geïnstalleerd, niet actief of handtekeningenbestand niet up-to-date Ongepast of onvoorzichtig gedrag van de gebruiker (bv. gebruikt een besmet USB-geheugenapparaat)	Kwaadaardig internetverkeer blokkeren Patches toepassen Antivirus bijwerken van het handtekeningenbestand Schoonmaaktool voor virussen gebruiken indien beschikbaar Tool voor de inschatting van kwetsbaarheden gebruiken om de kwetsbare middelen te inventariseren Besmet systeem volledig opnieuw installeren Kwetsbare diensten uitschakelen Besmette systemen uitschakelen of de verbinding ermee verbreken

TYPE INCIDENT	DEFINITIE	MOGELIJK DOELWIT	KWETSBAARHEDEN DIE KUNNEN WORDEN UITGEBUIT	MOGELIJKE REACTIES
Ongepast gebruik	Een incident met ongepast gebruik is elk incident waarbij een interne medewerker of contractant een gedragscode of computerbeleid schendt. Ongepast gedrag is niet altijd kwaadwillig en gericht. Soms handelt een gebruiker gewoon onzorgvuldig of is hij zelfs helemaal niet op de hoogte van het beleid dat of de gedragscode die hij heeft geschonden. Het ongepaste gedrag is soms een ernstig veiligheidsincident op zich, maar het kan ook de oorzaak of trigger zijn van een ernstig incident (zoals besmetting met malware, verlies van kritieke gegevens)	Betalingstransacties Kredietkaartinformatie Commerciële en persoonlijke informatie van klanten Vertrouwelijke informatie in het algemeen	Zwak beheer of controle van vertrouwelijke gegevens Slecht wachtwoordbeheer Gebrek aan scheiding van functies, accumuleren van toegangsrechten Gebrek aan beveiliging van of toezicht op toepassingen Gebrek aan procedures of controle om beleid en gedragscodes af te dwingen	Raadplegen en advies vragen van de afdeling Compliance en/of de juridische afdeling Gebruikers op non-actief stellen of toegangsrechten intrekken Forensische kopieën maken van logs en andere cruciale informatie om op te sporen en te bewijzen wat er is gebeurd Logs en andere informatie controleren op sporen van de inbreuk
Fraude	Fraude is een soort ongepast gedrag dat inherent kwaadaardig van aard is en gericht is op persoonlijke verrijking door misbruik van bedrijfssystemen, toepassingen of informatie.			
Verlies of diefstal van gegevens	Dit is een incident dat betrekking heeft op het verlies of de diefstal van vertrouwelijke informatie. Informatie kan vertrouwelijk zijn wegens de waarde die ze voor het bedrijf heeft, of omdat ze beveiligd is door interne of externe regelgeving. Incidenten met verlies van gegevens kunnen een grote financiële impact hebben wegens de mogelijke financiële aansprakelijkheid of de schade aan het imago van het bedrijf, mocht de informatie zelf of het feit van het verlies openbaar worden of bekend raken bij de foute mensen.	Persoonlijke informatie over werknemers of klanten (beschermd door privacywetten) Kredietkaartinformatie Commerciële informatie van klanten Vertrouwelijke balansgegevens Vertrouwelijke informatie over de bedrijfsstrategie, lopende projecten en beslissingen enz.	Onjuist gebruik van draagbare opslagapparaten (USB- geheugenstick, cd, back- uptape enz.) Onjuist gebruik van mobiele apparatuur (laptop, smartphone enz.) Onjuist gebruik van gedrukte vertrouwelijke informatie Schending van het 'clean desk'-beleid	Het niveau van gegevensbescherming evalueren, als die er is (versleuteling (encryptie), wachtwoordbeveiliging, specifiek apparaat vereist om de gegevens te lezen) Raadplegen en advies krijgen van de afdeling Compliance en/of de juridische afdeling of van uw externe juridisch adviseur De communicatie-afdeling en het management inlichten, een communicatiestrategie bepalen De eigenaar van de verloren of gestolen gegevens inlichten
Merkmisbruik	Dit is een incident waarbij iemand uw merk en gedeponeerde handelsmerken misbruikt.	Registratie van DNS-namen die het merk bevatten Spoofing van websiteontwerpen Spoofing van e-mailadressen en e-mailsjablonen	Niet van toepassing	De politie inlichten (in geval van diefstal) Verzoeken om de website offline te halen Klanten inlichten over het bestaan hiervan

VBO
Verbond van Belgische Ondernemingen

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

ICT CONTROL
Your Trusted Advisor

BNP PARIBAS FORTIS

Solvay Brussels School
Economics & Management

proximus

Deloitte.