Samen tegen cybercrime

Stappenplan voor IT-specialisten

« waakzaam en dienstbaar »

Samen tegen cybercrime

Bent u slachtoffer van een cyberaanval? In deze brochure leest u stap voor stap hoe u informatie verzamelt die kan leiden tot de daders.

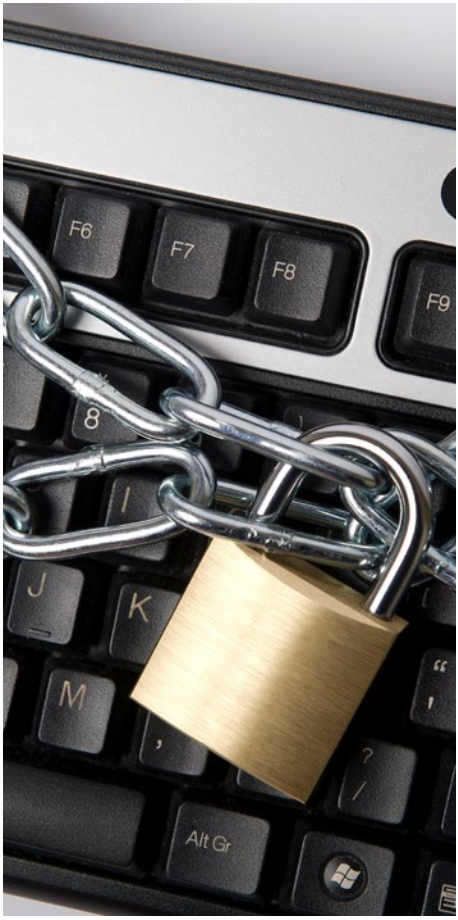
Digitale beveiligingsincidenten bestaan in allerlei vormen. Met hacken bijvoorbeeld bedoelen we het inbreken in computers. We spreken van een datalek als er daarna gegevens gestolen zijn. Of denk aan ransomware: bij dit soort malware zijn uw gegevens geblokkeerd en eist de dader losgeld in ruil voor uw gegevens. Het zijn allemaal vormen van cybercrime. Samen met u kunnen we cybercrime bestrijden.

Waarom is uw informatie belangrijk?

Met uw informatie kunnen we samenwerken in het opsporen van de cybercriminelen. Dit kan nieuwe aanvallen voorkomen. Zo kunnen we andere ondernemers waarschuwen of servers met schadelijke software uitschakelen.

Als u slachtoffer bent geworden van cybercrime

Als u een cyberaanval ontdekt, trek dan nooit zomaar de stekkers uit uw machines. Essentiële digitale sporen kunnen zo verdwijnen. Opsporing, bedrijfscontinuïteit en het voorkomen van meer schade kunnen tegenstrijdige belangen zijn. Ga daarom altijd eerst in overleg met de politie. Gaat u wel direct over tot actie en schakelt u ons pas later in? Houd dan alle handelingen schriftelijk bij, inclusief wie wat op welk tijdstip uitvoerde.



Zo voorkomt u verlies van bewijsmateriaal

- Schakel een geraakt systeem niet uit, maar verbreek wel de netwerkverbinding.
- Maakt u gebruik van virtuele machines? Maak daar dan een kopie van inclusief het werkgeheugen.
- Gebruik voor de herinstallatie van een geraakt systeem een nieuwe harde schijf en bewaar het origineel voor politieonderzoek.
- Heeft een geraakt systeem een logboek? Bewaar deze dan op een andere, veilige plek.
- Kijk ook verder dan alleen de aanleiding van dit incident. Wat zijn bijvoorbeeld onderliggende oorzaken? Raadpleeg hiervoor de uitleg over het opstellen van een 'incident response plan' in deze brochure.

Zevenstappenplan – Zo verzamelt u informatie over het incident

Heeft u bepaalde gegevens niet? Ga dan verder met de volgende stap.

Stap 1 – Logbestanden

Begin bij de meest vluchtige informatie. Vaak zijn dit logbestanden. Cybercriminelen laten namelijk digitale sporen achter en met de logbestanden kunnen specialisten van de politie deze sporen vinden. Deze logbestanden heeft u nodig:

- Tijdstippen
- IP- en MAC-adressen
- Account- en locatiegegevens
- User agents
- Netwerkpoorten

Afhankelijk van uw systeem vindt u deze informatie hier:

- Active directory
- Domain controller
- Domain name system-server of -recursor
- Firewall-verbindingen
- Het dynamic host configuration protocol (als u DHCP gebruikt voor de toewijzing van IP-adressen)
- Het virtual private network van uw organisatie
- Overige gegevens

Verzamel alle logbestanden die u heeft. Heeft u iets niet gelogd? Ga dan verder met de volgende stap.

Stap 2 – Communicatie

Communicatie van een bedrijfsnetwerk naar buiten toe is het belangrijkst, maar communicatie binnen een netwerk kan óók sporen bevatten. Die kunnen de politie bijvoorbeeld veel inzicht geven in de modus operandi van cybercriminelen.

Leg daarom de netflow vast, dat is het netwerkverkeer tussen machines. De netflow legt u vast door bijvoorbeeld de bron en bestemming van datapakketjes inzichtelijk maken. Zo kan het verband tussen de aanval op uw systeem en de criminelen die hiervoor verantwoordelijk zijn zichtbaar worden.

Stap 3 – Netwerksegmenten

Leg vast welke netwerksegmenten er zijn en hoe deze met elkaar zijn verbonden. Geef ook aan waar de firewalls zich bevinden. Maak hier een actueel gehouden netwerktekening van, het liefst in een diagram en het liefst voor een incident kan plaatsvinden. Het diagram is onderdeel van het 'incident response plan'. Verderop in de brochure leest u daar meer over.

Probeer bij het maken van de netwerktekening ook antwoorden te vinden op deze vragen:

- Welke IP-subnets gebruiken de netwerksegmenten?
- Welke proxies worden (eventueel) gebruikt?
- Welke andere services zijn te onderscheiden? Denk aan: webservers, single sign-on, virtual private networks, et cetera

De volgende vragen zijn lastiger, maar zeker waardevol:

- In welke vLAN's is uw netwerk geconfigureerd?
- Hoe is de toegangscontrole ingericht?
- Welke poorten staan open en welke zijn geblokkeerd?

Naast uw netwerktekening kunnen de configuratiebestanden van het systeem op een

centrale server helpen om de oorzaak van het probleem te vinden. Meestal vindt u deze in de Configuration Management Database. Een netwerkbeheerder kan hierbij helpen. Bij twijfel kan de netwerkbeheerder ook contact opnemen met uw contactpersoon bij de politie.

Stap 4 – Infrastructuur
Een overzicht van uw digitale infrastructuur geeft een aanvullend beeld van de verbindingen tussen machines. Als u zicht hebt op de digitale infrastructuur, heeft u ook zicht op de reikwijdte van de cyberaanval.

Zorg dat u bekend bent met verbindingen tussen deze machines:
- Routers
- Switches
- Servers
- Computers
- Printers en scanners
- IP-telefoons
- Overige met het internet verbonden apparaten

Stap 5 – Systeemlijst
De systeemlijst is een aanvulling op het overzicht van de infrastructuur. Deze lijst beschrijft de systemen van uw organisatie.

Per machine legt u deze gegevens vast:
- Contactgegevens van de afdeling of persoon die verantwoordelijk is
- Fysieke locaties
- Besturingssystemen (liefst met versie en patchniveau)
- Geïnstalleerde software (liefst met versie)
- Asset roles
- Provisioning dates
- Netwerkconfiguraties

Stap 6 – Images
Hoe konden criminelen inbreken en wat was hun doel? Voor het antwoord op deze vragen heeft u vaak de images van uw hardware nodig. Maak een kopie van het geheugen van getroffen systemen of neem voor het veiligstellen van uw gegevensdragers contact op met een digitaal specialist van de politie via 0900 - 8844. Deze specialist kan een inschatting maken van welke apparaten onderzocht moeten worden.

Stap 7 – Inloggegevens
Moet uw hardware worden meegenomen voor onderzoek? Houd er dan rekening mee dat de inloggegevens van deze machines nodig zijn.

Waarom aangifte doen?

Het doen van aangifte is een officieel startpunt voor politieonderzoek naar strafbare feiten. Zo'n onderzoek kan uiteindelijk leiden tot de strafrechtelijke vervolging van daders.
Ook het Nationaal Cyber Security Centrum adviseert om **altijd aangifte te doen**. Wilt u geen aangifte doen maar alleen een melding maken? Ook dat is mogelijk.

Doet u aangifte bij de politie? Dan geldt altijd: hoe meer informatie, hoe beter. Want ook informatie die niet belangrijk lijkt, kan zeer waardevol zijn voor het onderzoek. U kunt ook een it-specialist van uw organisatie vragen om meer toelichting te geven over de technische details.

Probeer zoveel mogelijk informatie uit het zevenstappenplan aan te leveren. Daarnaast geeft u ook deze informatie:

- Naam aangever, adres en woonplaats, organisatie en functie en contactgegevens
- Machtiging om namens de rechtspersoon aangifte te doen
- Een schatting van de schade en de herstelkosten, waaronder economische en imagoschade en de hoeveelheid (persoons) gegevens die getroffen zijn
- Welke beveiligingsmaatregelen al genomen zijn

Slachtoffer van Cybercrime?
Deel uw informatie met ons.
Bel 0900 - 8844 en vraag naar een digitaal coördinator
Telefonisch komt u het snelst in contact met een cybercrimespecialist. Dit kan een opsporingsambtenaar van een regionaal cybercrimeteam zijn of een rechercheur van het Team High Tech Crime. Ook online via politie.nl/aangifte-of-melding-doen of bij een politiebureau kunt u melding of aangifte doen.

Wat doet de politie met uw informatie?

We nemen uw informatie op in de politiesystemen. Uit ervaring weten we dat bedrijven het soms moeilijk vinden om informatie te delen over een beveiligingsincident, maar we benadrukken dat dit het enige juiste is wat u kunt doen. Zo neemt u zelf verantwoordelijkheid. En vergeet daarbij niet dat iedereen slachtoffer kan worden van cybercrime.

Zo herkent u een cyberaanval

Let op deze mogelijke signalen van een cyberaanval:

- Uw vertrouwelijke gegevens verschijnen op internet
- In uw logboeken staat opvallend veel verkeer geregistreerd
- Systemen maken verbinding met verdachte internetadressen
- Systemen vertonen een ongewone activiteit, bijvoorbeeld extreem veel activiteit
- Systemen zijn geblokkeerd en u wordt losgeld gevraagd om weer toegang te krijgen tot uw gegevens (ransomware)
- Een concurrent heeft gevoelige bedrijfsinformatie van u
- Uw website is beschadigd
- Bestanden of databases zijn gewist of gewijzigd
- Uw website is niet bereikbaar door grote hoeveelheden inkomend dataverkeer (DDoS-aanval)
- De e-mailserver functioneert niet vanwege een grote spamaanval
- Systemen zijn ontoegankelijk gemaakt.
- Er worden onrechtmatig bedragen van uw rekening afgeschreven
- Er worden onrechtmatig e-mails uit naam van uw bedrijf verstuurd


POLITIE
POLITIE
Coffee
Coffee

Hoe maakt u een incident response plan?

Een goede voorbereiding op incidenten geeft de nodige rust tijdens crises. Ons advies? Neem in deze procedure voor incidentopvolging ook het veiligstellen van bewijs en het doen van aangifte mee. Door de onderdelen die voor de politie relevant zijn op te nemen in dit plan voorkomt u dat bewijs verloren gaat. Met als gevolg dat u als bedrijf voorbereid bent op een cybercrime-incident.

Om cybercrime-incidenten goed het hoofd te kunnen bieden, kan uw organisatie processen en procedures inrichten over hoe hiermee wordt omgegaan. Voor het inrichten van processen voor incidentopvolging en –afhandeling voor informatiebeveiligingsincidenten en voor bedrijfscontinuïteitsbeheer zijn diverse normen en leidraden voorhanden, zoals de NEN-ISO/IEC 27002, NEN-ISO/IEC 27035 en NEN-ISO/IEC 22313 standaarden. (Commerciële) dienst-verleners op het vlak van informatiebeveiliging kunnen behulpzaam zijn bij het inrichten van de benodigde processen en systemen.

Ook kunt u denken aan het opstellen van een incident response plan. Dit is een intern document wat inzicht geeft in de te nemen stappen na het ontdekken van een cybercrime delict of beveiligingsincident. Zo bent u maximaal voorbereid op het moment dat u slachtoffer wordt van een dergelijk incident en kunnen de benodigde stappen snel genomen worden. Dit is van belang om het onderzoek te starten en de bedrijfsvoering zo snel mogelijk te laten hervatten. Een incident response plan, gebaseerd op het SANS Incident Response Process, kan de volgende onderdelen bevatten:

1. Voorbereiding
Maak een lijst met alle apparaten binnen het bedrijf waarin onder andere de servers, het netwerk, applicaties en critical endpoints inzichtelijk worden. Vervolgens wordt de lijst ingedeeld op mate van belangrijkheid. Hierbij is het van belang dat er een basis gelegd wordt in het gebruikelijke verkeer als zijnde een nulmeting, zodat afwijkingen snel gedetecteerd kunnen worden.

Begin het incident response plan met een meldprocedure. Wanneer een medewerker een incident constateert, is het van belang dat dit snel doorgegeven wordt aan de gemandateerde persoon. Bedenk welke personen geïnformeerd moeten worden over het incident en stel een team samen van mensen en welke rollen ze vervullen. Denk hierbij ook aan externe partijen, waaronder de politie.

2. Aangiftebeleid
Organisaties kunnen beleid opstellen waarin beschreven staat in welke gevallen er aangifte zal worden gedaan bij de politie. Een belangrijk onderdeel hiervan is beleid over het op verantwoordelijke wijze melden van kwetsbaarheden in ICT-producten en software door bijvoorbeeld ethische hackers. Denk aan een lek in uw website. Hiervan hoeft u uiteraard geen aangifte te doen. Een uitgebreide leidraad voor het opstellen van een dergelijk beleid is te vinden op www.ncsc.nl, onder 'responsible disclosure'.

3. Ideztificatie
In deze fase is een incident gedetecteerd en geïdentificeerd. Dit is tevens de fase waarin de data welke van belang is voor de aangifte, veilig gesteld moet worden*. Onderzoek wat er gebeurd is, wat de omvang is en wie er bij betrokken zijn. Schakel in deze fase ook overeenkomstig met het aangiftebeleid de politie in. Zij kunnen de getroffen apparaten forensisch veiligstellen voor verder onderzoek.

4. Isolatie
Nadat duidelijk is wat er gebeurd is en welke apparaten getroffen zijn. Hierbij is het van belang dat geïnfecteerde computers niet uitgeschakeld worden, maar geïsoleerd worden van het netwerk.

5. Eliminatie
Nu de kwetsbaarheid geïsoleerd is en het bewijs is veiliggesteld, start de politie met het onderzoek. De getroffen apparaten zullen veelal in beslag genomen worden voor onderzoek. Wanneer deze niet in beslag genomen worden, is het van belang dat de getroffen systemen grondig onderzocht worden en waar nodig opnieuw ingesteld om te voorkomen dat er sporen van het delict achterblijven. De bedrijfsprocessen kunnen nu weer opgestart worden en eventuele backups teruggezet worden.

6. Herstel
De bedrijfsprocessen kunnen herstart worden terwijl de politie of een ICT bureau onderzoek doet naar de oorzaak van het cybercrime-incident. Bepaal welke stappen intern genomen dienen te worden om de werkzaamheden te kunnen hervatten, eventueel met uitsluiting van de getroffen apparaten.

7. Evaluatie
Hoe kon het beveiligingslek ontstaan en wat dient er aangepast te worden om dit in de toekomst te voorkomen. Evalueer hoe het proces van detecteren, isoleren en herstel verlopen is.

Wat kunt u doen om cyberaanvallen te voorkomen?

Zorg dat u voorbereid bent op een digitaal beveiligingsincident. Een kleine fout of onoplettendheid kan grote gevolgen hebben. Bij een incident zijn twee zaken het belangrijkst: snel handelen en data veiligstellen voor politieonderzoek.

Meer tips om een cyberaanval te voorkomen:

- Zorg voor een up-to-date besturingssysteem (Windows, MacOS, Linux, OSX et cetera).
- Laat uw medewerkers inloggen met een tweestapsauthenticatie.
- Maak regelmatig backups van belangrijke bestanden en bewaar deze op een locatie buiten het bedrijf.
- Train uw personeel op het herkennen van cybercrime. Houd bijvoorbeeld een campagne over het herkennen van phishing e-mails.

* Zie hiervoor het zevenstappenplan in deze brochure.

Wetgeving: hoe staat cybercrime te boek in de wet?

Onderstaand zijn de meest voorkomende cybercrimedelicten inclusief indicaties en strafbaarstelling opgesomd:

(D)DoS aanval:
De infrastructuur van een bedrijf of webserver platleggen door het bedrijf met grote hoeveelheden data te bestoken.

Vorm en delict	*Indicaties*
Belemmeren geautomatiseerd werk Delict: Artikel 138b Wetboek van Strafrecht	• De website van uw organisatie is niet langer bereikbaar door grote hoeveelheden inkomend dataverkeer (DDoS-aanval). • De e-mailserver van uw organisatie functioneert niet meer vanwege een grote spamaanval. • Systemen van uw organisatie zijn ontoegankelijk gemaakt. • Uw systeem vertoont ongewone activiteit, zoals ongewoon hoge belasting. • Het netwerk is ongebruikelijk traag. • U heeft een bericht ontvangen waarin geld gevraagd wordt om de aanval te doen stoppen.

Hacken:
Toegang verschaffen tot systemen waartoe de gebruiker niet gemachtigd is.

Vorm en delict	*Indicaties*
Computervredebreuk: Binnendringen in een geautomatiseerd werk Delict: Artikel 138ab Wetboek van Strafrecht	• Er is zonder toestemming (wederrechtelijk) ingelogd op systemen van uw organisatie. • Vertrouwelijke gegevens van uw organisatie zijn op het internet verschenen. • In logboeken van uw (web-)servers staan aanvallen geregistreerd. • Systemen van uw organisatie maken verbinding met verdachte internetadressen. • Er is door een kwaadwillende een remote acces tool op computers van uw organisatie geïnstalleerd.

Phishing:
Het doel van een phishing aanval is veelal het vergaren van inloggegevens of toegang verschaffen tot computersystemen om van hieruit verdere actie te ondernemen.

Vorm en delict
Oplichting

Delict:
Artikel 326 Wetboek van Strafrecht

Indicaties
- Werknemers ontvangen e-mails met een niet gepersonaliseerde aanhef.
- Er wordt gevraagd om op een link te klikken en hier persoonlijke gegevens achter te laten.
- Werknemers ontvangen e-mails van een onbekend e-mail-adres wat op het oog gelijkenissen vertoond met een bekend e-mailadres.
- E-mails bevatten onbekende bijlagen zoals bestanden met een .exe-extentie of Office documenten met macro's ingeschakeld. Dit kan duiden op malware.

Ransomware:
Het gijzelen van computersystemen om gebruikers of bedrijven af te persen tot het betalen van grote sommen geld voor het ontgrendelen van de systemen.

Vorm en delict
Afpersing, opzettelijke computersabotage, computervredebreuk

Delict:
Artikel 317, 350a lid 1, 2 en 3 en 138ab Wetboek van Strafrecht

Indicaties
- Uw webbrowser of computer is vergrendeld en er is een bericht zichtbaar wat aangeeft te moeten betalen om uw bestanden te ontgrendelen.
- De bestanden op de computers hebben een andere extensie dan gebruikelijk of kunnen niet geopend worden. Bestanden die vergrendeld zijn door ransomware hebben vaak geen extensie of iets wat lijkt op .crypted of .cryptor.
- De bestanden zijn gecodeerd en de inhoud van de bestanden bevat onleesbare content.

Malware:
Malware kan verschillende doelen hebben waaronder het bespioneren van de gebruiker om zo belangrijke informatie te vergaren, het verspreiden van een virus of om het systeem deel uit te laten maken van een groter netwerk van aanvalscomputers. Malware is lastig te herkennen vanwege zijn vele verschijningsvormen.

Vorm en delict	*Indicaties*
Malware: Delict: Artikel 350a lid 3 Wetboek van Strafrecht	• De geïnfecteerde computer wordt als traag ervaren wegens op de achtergrond draaiende onbekende processen. • De geïnfecteerde computer loopt regelmatig vast. • Er is ongewenste content zichtbaar binnen browsers zoals pop-ups en add-on's.

Bij cybercrime staat vaak het juridische begrip "geautomatiseerd werk" centraal
In het algemeen valt alle ICT-apparatuur met een processor en geheugen onder deze omschrijving, zoals computers, laptops en servers, maar ook smartTVs, smartwatches, tablets, smartphones en steeds meer apparaten van het internet der dingen (IoT). Een misdaad wordt als cybercrime gekwalificeerd wanneer het gaat het om misdaad gepleegd met ICT, gericht op ICT.

Aantekeningen

www.politie.nl

« waakzaam en dienstbaar »

20605