

# Eerste hulp bij Hackers

## Wat te doen bij een cyberaanval?

Als er brand is, bel je de brandweer. Als er is ingebroken, bel je de politie. Maar wat doe je als je IT-systemen zijn getroffen door een cyberaanval?

Nog te weinig bedrijven bereiden zich hier goed op voor. Terwijl de kans erop vele malen groter is dan die op brand. Het gevolg? Tienduizenden euro's aan schade, reputatieverlies en het verlies van waardevolle data.

Wees daarom altijd voorbereid op een 'digitale brand'.



## Vorbereiding

Een aantal zaken moet je eigenlijk altijd op orde hebben, ook al lijken ze nog zo voor de hand liggend.



## Veilig back-upstelsysteem

Iedereen weet dat het verstandig is om op regelmatige basis een back-up te maken van je gegevens. En toch gebeurt het lang niet altijd consequent. Ons advies: zorg er samen met je ICT-dienstverlener voor dat in elk geval onderstaande drie punten in orde zijn.

- Maak geregeld een back-up.
- Bewaar de back-up zowel op een digitale als een fysieke locatie.
- Test je back-up regelmatig.

## Goede logging

Wil je snel kunnen reageren bij een digitale aanval? Dan zijn goede logfiles van groot belang. Zorg ervoor dat er altijd logfiles beschikbaar zijn van de belangrijkste componenten in je netwerk. En zorg ervoor dat deze niet besmet kunnen raken met het virus dat hackers op jouw stelsysteem plaatsen.

## Crisisprotocol

In een crisissituatie is er meestal geen tijd om rustig na te denken en te handelen. Je doet er daarom goed aan een crisisprotocol op te stellen. Dit bestaat meestal uit twee delen:

- Deel 1 richt zich op het besturen van de organisatie in een crisissituatie, ook wel het Business Continuity Plan (BCP) genoemd.
- Deel 2 richt zich op de in- en externe communicatie.

## Belangrijke informatie ook op papier beschikbaar

Hacking kan ervoor zorgen dat digitaal bijgehouden contactgegevens niet meer beschikbaar zijn en dat er geen toegang meer is tot het internet of het bedrijfsnetwerk om die op te zoeken. Het kan gebeuren dat een of meerdere communicatiekanalen niet meer werken. Maak daarom alle belangrijke informatie uit je crisisprotocol op papier beschikbaar. Denk daarbij zeker aan:

- personen die een rol spelen in het crisisteam;
- contactgegevens van alle medewerkers;
- contactgegevens van overheidsinstanties;
- contactgegevens van klanten (soms ben je onderdeel van een keten);
- contactgegevens van leveranciers (je kan onderdeel zijn van een keten);
- contactgegevens van je ICT-partner of security experts;
- de informatie die er op het darkweb beschikbaar is over jouw bedrijf.

## In het geval van een datalek moet je de contactgegevens van volgende instanties paraat hebben:

- **AVG ([www.gegevensbeschermingsauthoriteit.be](http://www.gegevensbeschermingsauthoriteit.be)) i.v.m. GDPR.**  
Hier maak je melding van een datalek of inbreuk.
- **CERT ([www.cert.be](http://www.cert.be))**
- **Lokale Politie**  
Voor het doen van een aangifte.

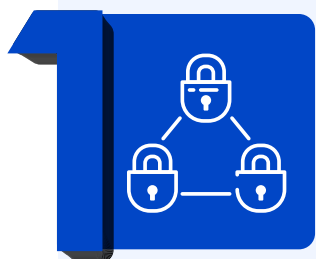
## Verzekering

Er zijn polissen die je verzekeren tegen (een gedeelte van) de schade die een cyberaanval kan veroorzaken aan je eigen organisatie en aan derden. Het is de moeite waard om te onderzoeken of een verzekering - en welke soort - nuttig is, rekening houdend met de werking en de risico's van je organisatie.

Bewaar, nadat je een verzekering hebt afgesloten, altijd de gegevens van je contactpersoon op papier.

# Wat als je slachtoffer bent van een aanval?

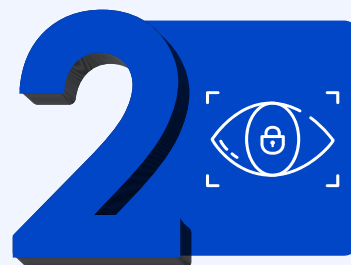
Als je ICT-systemen zijn gehackt, volg je best een standaardprocedure. Doorloop samen met een ICT-specialist die ervaring heeft met cyberaanvallen én een communicatiespecialist de hierna opgesomde stappen. Deze personen kunnen zowel in als externe personen zijn.



## VERSPREIDING BEPERKEN

---

Koppel de systemen waarop het virus is vastgesteld zo snel mogelijk los van het bedrijfsnetwerk. Het heeft de voorkeur om eveneens de gevrijwaarde systemen los te koppelen, zodat deze geen kans krijgen om besmet te raken. Zet nooit de computer uit want dit bemoeilijkt het onderzoek.



## ANALYSEER BESMETTING EN IMPACT

---

Onderzoek om welk virus het gaat, hoe het is binnengekomen en hoe ver het zich (mogelijk ook extern) heeft verspreid. Op basis daarvan wordt een eerste opzet gemaakt van de herstel mogelijkheden. Geef kritieke apparaten binnen je netwerk altijd prioriteit, zodat je weer snel up and running bent.



## ANALYSEER DE BACK-UP

---

Bij het terugplaatsen van de back-up dien je rekening te houden met de volgende elementen:

- **Kwaliteit**  
Is de back-up volledig en bevat het alle essentiële informatie?
- **Ouderdom**  
Hoe oud is de back-up? Hoeveel informatie ben je definitief kwijt bij het terugplaatsen?
- **Veiligheid**  
Is de back-up besmet door het virus?
- **Tijd**  
Hoelang duurt het voordat de systemen weer draaien?

### Terugplaatsen of opnieuw beginnen?

Na de analyse volgt een belangrijke beslissing: zetten we de back-up terug of installeren we alles vanaf nul? Neem in het crisisprotocol op wie deze beslissing op welk moment neemt en verdiep je alvast in een leverancier die snel nieuwe (of refurbished) hardware op locatie kan leveren.



## BETALEN OF NIET?

---

Als het terugplaatsen van een back-up geen optie blijkt, kom je voor de belangrijke keuze te staan: wel of geen 'losgeld' betalen voor de gehackte informatie? Hierin spelen een aantal belangrijke overwegingen mee:

- Hoe zeker is het dat je je gegevens terugkrijgt nadat je hebt betaald?
- Wie beslist of er wordt betaald?
- Wat is het maximumbedrag dat je wilt betalen?
- Wie voert de onderhandelingsgesprekken met de hackers?
- Omwille van de anonimiteit wordt vaak gevraagd te betalen in een digitale munt (bijv. Bitcoin). Hoe schaf je deze munten aan en hoe betaal je ermeer?



## IN- EN EXTERNE COMMUNICATIE

---

Over een ingrijpende gebeurtenis als een hack moet doordacht worden gecommuniceerd, zowel in- als extern. Het is slim om dit vooraf vast te leggen in het crisisprotocol. Hierin staan de antwoorden op vragen als:

- Hoe en wanneer brengen we onze medewerkers op de hoogte?
- Hoe doen we dat voor medewerkers die extern aan het werk zijn?
- Wanneer brengen we betrokken externen (leveranciers en klanten) op de hoogte?
- Zijn er andere in- en externe stakeholders die op de hoogte moeten worden gebracht voordat we naar de pers gaan?
- Hoe vermijden we dat de pers informatie ontvangt nog voordat we zelf iets naar de buitenwereld hebben gecommuniceerd?
- Welke informatie sturen we naar de pers en wanneer doen we dat?

## Klanten, leveranciers & overheid

Als je bedrijfsgegevens zijn gehackt, heeft een externe instantie toegang gekregen tot informatie die mogelijk ook betrekking heeft op personen en organisaties buiten jouw bedrijf.

Dit heeft gevolgen voor de Algemene Verordening Gegevensbescherming (AGV = GDPR). Stel een lijst op van bedrijven, organisaties en personen die op de hoogte moeten worden gebracht van het feit dat er mogelijk informatie van hen werd gelekt en om welke informatie het gaat. Neem bovendien binnen 72 uur contact op met de overheidsinstanties zoals eerder benoemd.



## Hulp van een specialist

De hierboven vermelde checklist geeft een goed beeld van de vele, soms moeilijke analyses die moeten worden gemaakt en de beslissingen die moeten worden genomen in het geval van een cyberaanval.

Het is raadzaam om een **ervaren security-expert** te betrekken bij de eerste stappen. Beschikt je huidige ICT-leverancier niet over zo'n expert? Zorg er dan voor dat je de gegevens hebt van een bedrijf dat is gespecialiseerd in cybersecurity.

## Stress en geld besparen?

Het is een cliché, maar voorkomen is nog altijd beter dan genezen.

Hoe maken we de kans op een cyberaanval zo klein mogelijk voor jouw organisatie?

Laten we rond de tafel gaan zitten. We kijken samen wat het beste past. Is dat een awareness training voor je medewerkers? Een security audit? Of misschien wel monitoring?

Wil jij jezelf stress en geld besparen? Neem dan gerust contact met ons op en we bekijken samen wat we voor jouw organisatie kunnen betekenen. Zo kan jij op beide oren slapen.



### **Secutec BV (HQ)**

Boomsesteenweg 41/11  
2630 Aartselaar  
Belgium

+32 (0)3 877 82 93  
info@secutec.com

### **Secutec Nederland BV**

Breda Business Park - Lijndonk 4  
4825 BG Breda  
The Netherlands

+32 (0)3 877 82 93  
info@secutec.com

### **Secutec GmbH**

Gewerbestrasse West 14  
4921 Hohenzell  
Austria

+43(0) 664 301 05 68  
office-dach@secutec.com

### **Secutec Canada**

4000-1 Place Ville Marie  
H3B4M4 Montréal  
Canada

+1 438 728 84 32  
info@secutec.com

### **Australia & New Zealand Region**

Sonny Bal  
+61 449 932 977  
sonny.bal@secutec.com