Jouw plan voor meer cyberveiligheid

EERSTE HULP BIJ EEN CYBERAANVAL

Stel: jouw onderneming wordt aangevallen door cybercriminelen. Wat doe je? Hoe stop je de cyberaanval zo snel mogelijk? Dit 7-stappenplan helpt je op weg. Het plan is gebaseerd op advies van het Centrum voor Cybersecurity België.

STAP 1

Waarschuw iedereen

Zorg ervoor dat je in het cyberplan van jouw onderneming een collega aanduidt die verantwoordelijk is om als eerste actie te ondernemen bij een cyberaanval. Die collega brengt meteen iedereen die jouw IT-systemen beheert op de hoogte van de infectie, zodat alle aangetaste computers en servers van het netwerk ontkoppeld kunnen worden. Ontkoppel ook externe harde schijven om verdere infectie te voorkomen. Opgelet! Schakel de computers niet uit. Wie dat wel doet, kan belangrijke data verliezen die nodig zijn om de aanval te stoppen.

STAP 2

Zoek de oorzaak

Probeer vervolgens zo snel mogelijk te begrijpen waar de aanval vandaan komt. Stel jezelf of je collega's de volgende vragen:

- Heeft een medewerker op een link in een e-mail geklikt?
- Zijn het besturingssysteem, de applicaties of andere software niet up-to-date?
- Heeft iemand bewust of onbewust een virus geïnstalleerd?

STAP 3

Ruim de infectie op

Zoek naar sporen, doe bijvoorbeeld een virusscan. Ga ook na of hetzelfde incident op alle andere systemen in je IT-omgeving voorkomt. Vind je bijvoorbeeld software die externe toegang geeft, maar die niemand in je team installeerde? Dan check je of deze ook op andere computers of servers staat.

Als je gevonden hebt waar de infectie vandaan komt, voer dan een virusscan uit. Doe vervolgens een update van de besturingssystemen en software op alle systemen in je netwerk.

STAP 4

Herstart vanuit back-up

Het is risicovol om geïnfecteerde systemen terug aan het netwerk te hangen. Als de infectie zich nog verder kan verspreiden, zoals bij ransomware, doe je dit beter niet.

Een volledige herinstallatie en herstart van geïnfecteerde systemen is vaak nodig. Herinstalleer de laatste versie van de software. Let op! Als je geen back-up maakte van alle bestanden ben je jouw bestanden kwijt na een herinstallatie.

STAP 5

Verander wachtwoorden

Controleer vervolgens de toegangen. Cybercriminelen gebruiken soms oude accounts met zwakke wachtwoorden om binnen te geraken. Bekijk zeker welke gebruikers toegang hebben tot de clouddiensten waarop je organisatie een abonnement heeft. Het is belangrijk om alle accounts na te kijken en eventueel toegang te weigeren. Verander de wachtwoorden van alle accounts. Hiervoor gebruik je best een wachtwoordmanager.

STAP 6

Monitor je omgeving

Is de aanval gestopt? Wees nu extra waakzaam en hou je IT-omgeving continu in de gaten. Als je merkt dat de aanval opnieuw start, is de infectie niet volledig verwijderd.

STAP 7

Verwittig de autoriteiten

Als het incident ernstig is, meld dit dan bij de autoriteiten. Doe zo snel mogelijk aangifte bij de lokale politie. Geef vervolgens het nummer van het proces-verbaal door aan je bank en je verzekeraar. Vul ook een uitgebreid invulformulier van de het federale Computer Emergency Response Team - kortweg de CERT - in. Zo zijn de diensten die in België onderzoek doen naar cybercriminaliteit meteen en gedetailleerd op de hoogte.

Maak nu je plan tegen hackers

10 TIPS OM EEN CYBERAANVAL TE VOORKOMEN

Cybercriminelen vallen continu Vlaamse bedrijven aan. Voorkom dat jouw onderneming ook slachtoffer wordt. Maak een plan met deze 10 actiepunten voor een verhoogde beveiliging tegen hackers.

Het aantal Vlaamse bedrijven dat slachtoffer is van hackers loopt fors op. Toch kan je een cyberaanval voorkomen. Hoe? In dit artikel sommen we 10 actiepunten op van het Centrum voor Cybersecurity België. Aarzel niet om bij het uitvoeren van deze acties beroep te doen op externe expertise!

1 Schrijf een beveiligingsplan

Je moet de strijd op verschillende fronten voeren. Deze actieterreinen breng je samen in één strategisch actieplan voor je organisatie. Stel dit plan op in nauw overleg met leidinggevenden uit verschillende diensten. Deze zijn verantwoordelijk voor de veiligheid van informatie en moeten daarvoor organisatorische doelstellingen en ambities bepalen.

2 Inventariseer de IT-infrastructuur

Weet je vandaag welke machines, toestellen en mobiele apparaten er verbonden zijn met je bedrijfsnetwerk? Wie heeft toegang tot de software? Wie logt in op deze apparaten of bedient deze? Inventariseer de volledige IT-infrastructuur, inclusief de mobiele en private toestellen van medewerkers wanneer ze hiermee mailen, surfen of online werken voor je onderneming.

3 Update alle software

Softwarefabrikanten updaten voortdurend hun programma's. Ze verbeteren hun systemen en dichten zo ontdekte lekken. Haal deze updates binnen van zodra je er melding van krijgt of kies voor automatische updates.

4 Neem back-ups

Maak dagelijks een back-up van je belangrijke gegevens en software. Bewaar deze back-up op een fysiek andere plaats of vertrouw dit back-uppen toe aan een leverancier van cloud-back-upoplossingen. Kies daarbij voor een volledig automatische dienst. Zelfs wanneer je alle gegevens kwijt bent, is het mogelijk weer op te starten met deze back-up.

5 Splits het netwerk

Splits je netwerk in verschillende deelnetwerken. Cruciale diensten zoals productie, sales en logistiek mogen nooit direct aan elkaar gekoppeld zijn. Deze netwerksegmentatie vermijdt dat virussen zich ongehinderd verspreiden. Geef ook cloudtoepassingen een aparte sectie.

6 Scherm de toegang af

Vroeger volstonden robuuste firewalls rondom bedrijven. Vandaag is een meer slimme en flexibele beveiliging nodig die vlot digitaal werken mogelijk maakt, ook via mobiele en private toestellen. Denk aan antivirusprogramma's, next generation firewalls, beveiligingsoplossingen voor je cloudtoepassingen en all-in securitypacks.

7 Check je leveranciers

Steeds meer ondernemers, kmo's en grote organisaties vertrouwen op clouddiensten. Maar ook tussen bedrijven worden data uitgewisseld. Weet je hoe betrouwbaar je leveranciers zijn? Analyseer hun beveiliging. Check hoe gegevens met de leverancier uitgewisseld worden én eis de beste bescherming voor je data.

8 Beveilig je website

Vraag je webmaster naar het beveiligingssysteem dat bij het content management systeem van je website past. Voor websites van kleinere ondernemingen kan een eenvoudige plug-in volstaan.

9 Leid je mensen op

Technisch mag je onderneming uiterst beveiligd zijn, uiteindelijk is deze beveiliging zo sterk als de zwakste schakel. Bij cybercrimes blijken mensen vaak deze zwakste schakel te zijn. Eén verkeerde klik kan de deur voor hackers wijd openzetten. Organiseer cyberopleidingen. Informeer je mensen over alle mogelijke gevaren. Spreek vervolgens een eenvoudige gedragscode af.

10 Verbeter continu

Zoals cybercriminelen steeds slimmer te werk gaan, moet je je onderneming ook alsmaar intelligenter beveiligen. Evalueer en verbeter daarbij voortdurend. Neem hiervoor een specialist onder de arm en informeer naar ondersteunende maatregelen.

Heel wat werk op de plank maar je staat er niet alleen voor!

Op **vlaio.be/cybersecurity** ontdek je op welke financiële steun je beroep kan doen en ook welke interessante advies- en begeleidingstrajecten het VLAIO Netwerk aanbiedt. Je cybersecurity versterken doe je echt niet alleen!

vlaio.be/cybersecurity

Verantwoordelijke uitgever: VLAIO