Acto

Cyberweerbaarheid in de installatiebranche

6 tips om te starten met cyberweerbaarheid

Digitale veiligheid is niet vanzelfsprekend, en bedrijven zijn steeds vaker een doelwit van cyberaanvallen. De vraag is niet meer óf het gebeurd, maar wanneer. In deze whitepaper geven we je 6 cyberweerbaarheid tips die je als organisatie direct kunt implementeren.

Acto

Tip 1 | Maak een back-up van je bestanden

Als je bedrijf is aangevallen, is een reservekopie vaak het laatste redmiddel. Zorg daarom voor één of meerdere (versleutelde) kopieën van je bedrijfsgegevens, zoals klantdata en dossiers.

Let op!

Werk je in de cloud? Dit betekent niet dat er automatisch een back-up van je gegevens wordt gemaakt. Regel dit goed met je cloud provider of IT-manager intern.

Acto

Tip 2 | Maak inloggen in meerdere stappen verplicht

1 **Multifactor Authenticatie**

Ook wel 2-staps verificatie genoemd. Naast het invoeren van je wachtwoord, wordt er een extra verificatiemethode gebruikt, zoals een sms-code, een authenticatie-app of een biometrische verificatie.

2 **Gebruik wachtwoord manager**

Een wachtwoordmanager is een handig hulpmiddel om veilige wachtwoorden te bedenken en deze voor jou te onthouden.

3 **Sterke wachtwoorden**

Een sterk wachtwoord is niet te raden en moeilijk te kraken door een computer. Een belangrijke voorwaarde is hierbij dat de kracht van een sterk wachtwoord ook is dat deze uniek is. Een sterk wachtwoord dat bekend wordt, is direct zijn kracht kwijt.

Acto

Tip 3 | Voer altijd software updates uit

Updaten is het actueel houden van de software op je IT-systemen. Denk aan je besturingssysteem, e-mailprogramma, webbrowser of website.

Kijk verder dan je eigen computer. **Update regelmatig alle apparaten** waar software op staat. Zeker als ze een onlineverbinding hebben!

Een beveiligingsupdate, ofwel ‘security patch’, is vaak wel dringend. Die repareert kwetsbaarheden in je software. **Installeer security patches altijd meteen**. Dan verklein je het risico dat cybercriminelen je computernetwerk binnendringen.

Updates houden je software goedwerkend en veilig. In niet bijgewerkte software zitten mogelijk zwakke plekken. Hackers zijn daarvan op de hoogte en weten zo precies hoe ze makkelijk computersystemen kunnen binnendringen.

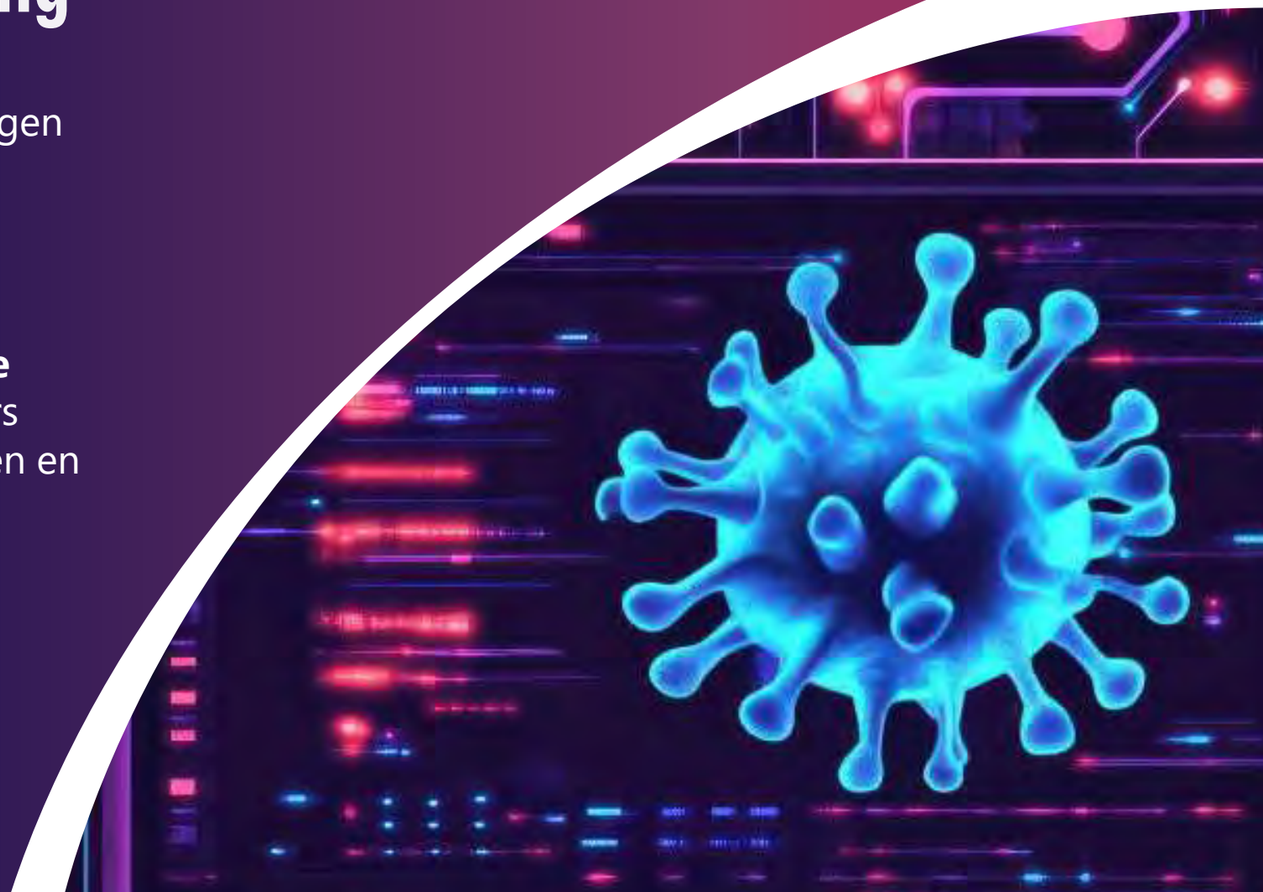
EXTRA TIP: Stel automatische updates in, of laat je IT manager dit inrichten voor jouw organisatie.

Acto

Tip 4 | Zorgvuldige antivirusbewaking

Een antivirusprogramma of antivirussoftware die je beschermt tegen internetvirussen en ‘malware’ is op veel apparaten inmiddels standaard aanwezig. Soms kun je ook zelf een antivirusproduct kiezen.

Installeer een antivirusprogramma en zorg dat deze software up-to-date blijft. Doe dit op alle computers, telefoons en servers binnen je bedrijf. Zo loop je minder risico op schade door virussen en andere malware.



Tip 5 | Hoe herken je phishing?

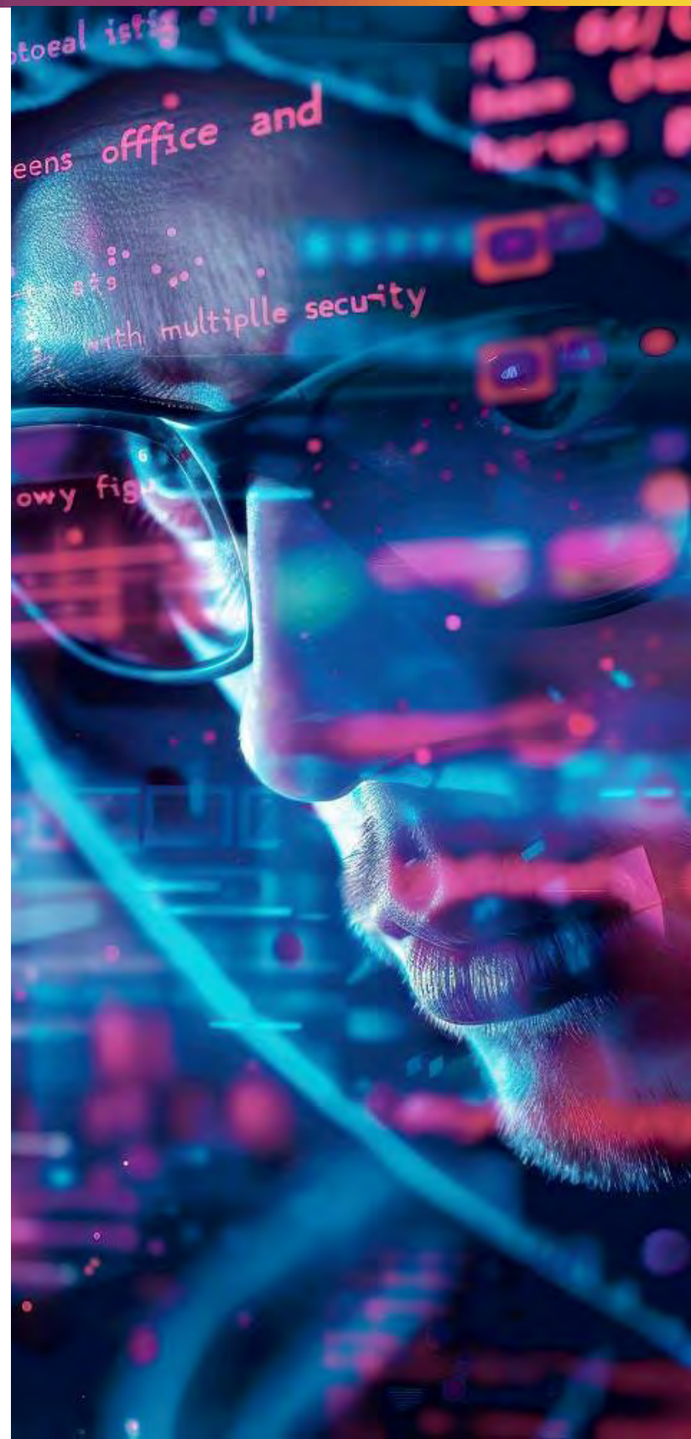
Controleer **altijd** het e-mailadres, de afzender en de inhoud van een e-mail bericht.

1. Controleer of de domeinnaam en het e-mailadres van de afzender hetzelfde zijn;

2. Controleer of de domeinnaam overeenkomt met het website-adres;

3. Let op details! Zie jij tussen *mail@31008mailers.nl* en *mail@3I008mailers.nl*?

4. Klik niet op een link als je het niet vertrouwt, maar beweeg (*hoover*) met de aanwijzer van je muis over de link. Zo ontdek je waar de link écht naar toe gaat!



Acto

Tip 6 | Maak een bellijst voor noodsituaties

Wanneer je door een cyberaanval geen toegang meer hebt tot je informatiesystemen, is er sprake van een noodgeval. Zorg dat er een bellijst ligt met daarop de contactgegevens van je IT-dienstverlener, softwareleverancier of securitybedrijf.

Heb je belangrijke klanten en (keten)partners? Zorg er dan ook voor dat jouw IT-dienstverlener bij hen geregistreerd staat als contactpersoon.

Acto

EXTRA TIPS

Wil je een stap verder gaan in het veilig digitaal ondernemen?

Voeg deze stappen dan toe aan je cyberweerbaarheidsplan.

Acto

EXTRA TIP 1 | Identificeer je kritieke systemen (1)

1

Breng alle systemen, netwerken en applicaties die je organisatie gebruikt in kaart.

Dit helpt om een overzicht van de gehele IT-omgeving te krijgen

2

Identificeer bedrijfsprocessen

Welke bedrijfsprocessen zijn essentieel voor de dagelijkse operaties van je organisatie? (bv. planning, klantbeheer en/of financiële transacties.

3

Beoordeel de impact

Analyseer wat de gevolgen zijn als een bepaald systeem uitvalt of wordt aangevallen.

Acto

EXTRA TIP 1 | Identificeer je kritieke systemen (2)

4

Voer een risicoanalyse uit

Dit kan met behulp van penetratietests of vulnerability scanners. Dit helpt om te zien welke systemen extra beveiliging nodig hebben.

5

Prioriteer op basis van risico

Rangschik systemen op basis van risico. Focus dan ook op het beveiligen van de meest kritieke systemen.

Acto

EXTRA TIP 2 | Bewustwording en opleiding van je medewerkers

- **Train met praktijkgerichte simulaties,** zoals bijvoorbeeld een Phishing test;
- **Stimuleer meldingen** van verdachte e-mails;
- Maak security continu **zichtbaar**
- Evalueer en verbeter je **awareness-programma**
- Maak security awareness **onderdeel van je dagelijkse bedrijfsvoering**

Acto

Extra tip van Acto | Wat als jouw organisatie toch een cybersecurity issue heeft?

Cyberincidenten zijn, ondanks het puin, leerzaam. Als het puin eenmaal is geruimd, het incident verholpen is en de bedrijfsprocessen weer door kunnen, is het tijd om na te gaan welke lessen daaruit getrokken kunnen worden.

- ✓ **Leg alles wat er gebeurd is vast**. Maak een tijdslijn met alle voorgevallen impact situaties;
- ✓ Doormiddel van een **evaluatie** kan je de eerste lessen in kaart brengen. Wanneer het een menselijke fout betreft, kan dit extra pijnlijk zijn. Kijk daarom ook wat er wel goed ging, zodat men bereid is én blijft om beter te leren;
- ✓ Leg alles vast in een **situatie verslag**, op deze manier bevorder je het herstel. En kan je je organisatie veiliger inrichten;
- ✓ **Zet de geleerde lessen om in de praktijk**, wees er – tot bepaalde hoogte – open over naar concullega's, medeondernemers of zelfs in de pers.

Samen staan we sterker in de strijd tegen cyberdreigingen!

Acto

Wil je meer weten

over hoe je als organisatie meer cyberweerbaar kan worden?

Door als organisatie meer cyberweerbaar te worden, ben je beter voorbereid zijn om met cyberdreigingen om te gaan. **Cyberweerbaarheid** is van essentieel belang in de moderne digitale wereld. Dreigingen evolueren voortdurend en aanvallen worden steeds geavanceerder.

Wil je meer weten of ben je benieuwd hoe wij als Acto met cybersecurity omgaan? Neem dan contact met ons op!

MEER INFORMATIE:

Acto Informatisering B.V.
Amsterdamseweg 51a
3812 RP Amersfoort

t (033) 422 68 00
e info@acto.nl
i www.acto.nl