# Jouw cyberveiligheid onder de loep

**Bescherm jouw organisatie tegen cybercriminelen.**

**Samen met ACA.**

**Wat is de impact als je de toegang tot jouw ICT-omgeving verliest? Ineens geen toegang meer tot applicaties en data van je organisatie. Kun je dat voorstellen? Het legt jouw bedrijfsprocessen volledig stil. In beginsel is het probleem praktisch van aard (niet kunnen werken), maar al gauw ontstaat er financiële schade. Wat als jouw organisatie een dag, een week of zelfs een maand stil ligt?**

De beschikbaarheid van ICT heeft enorme invloed op de continuïteit van je organisatie. Cybercriminelen weten dat ook. In hoeverre is jouw organisatie (en jouw ICT-omgeving in het bijzonder) bestand tegen de grote variëteit aan aanvallen? Een proactieve aanpak is hierbij essentieel.

## Methodieken & Assessments

Voorkomen is beter dan genezen, dat wordt vaak gezegd. Bij cyberveiligheid gaat het nog een stap verder: voorkomen is een must, want genezen is niet altijd mogelijk of financieel gezien uiterst kostbaar. Hierbij zijn drie elementen belangrijk: beleid, techniek en de mens. Ze zijn onlosmakelijk met elkaar verbonden en dienen stuk voor stuk te worden geoptimaliseerd om de cyberveiligheid en continuïteit van de organisatie te bewaken.

- **Beleid:** in hoeverre zijn het beleid en IT-werkwijze van je organisatie passend om cyberaanvallen en te kunnen pareren en IT-risico's te voorkomen?
- **Techniek:** in hoeverre is jouw ICT-omgeving bestand tegen cybercriminaliteit en in staat om dataverlies en de beschikbaarheid van het bedrijfsnetwerk en applicaties te garanderen?
- **Mens:** in hoeverre beschikken jouw medewerkers over de kennis en faciliteiten om veilig (en bewust) met IT-middelen te werken en cyberaanvallen te herkennen en voorkomen?

Waar bevinden zich de zwakke plekken in jouw ICT-beveiliging? Het onderzoek begint bij een beoordeling van de huidige situatie. Hiervoor hanteren wij, afhankelijk van en toegepast op jouw situatie, diverse onderzoeksmethodieken. Deze kunnen onafhankelijk van elkaar of gecombineerd worden uitgevoerd.

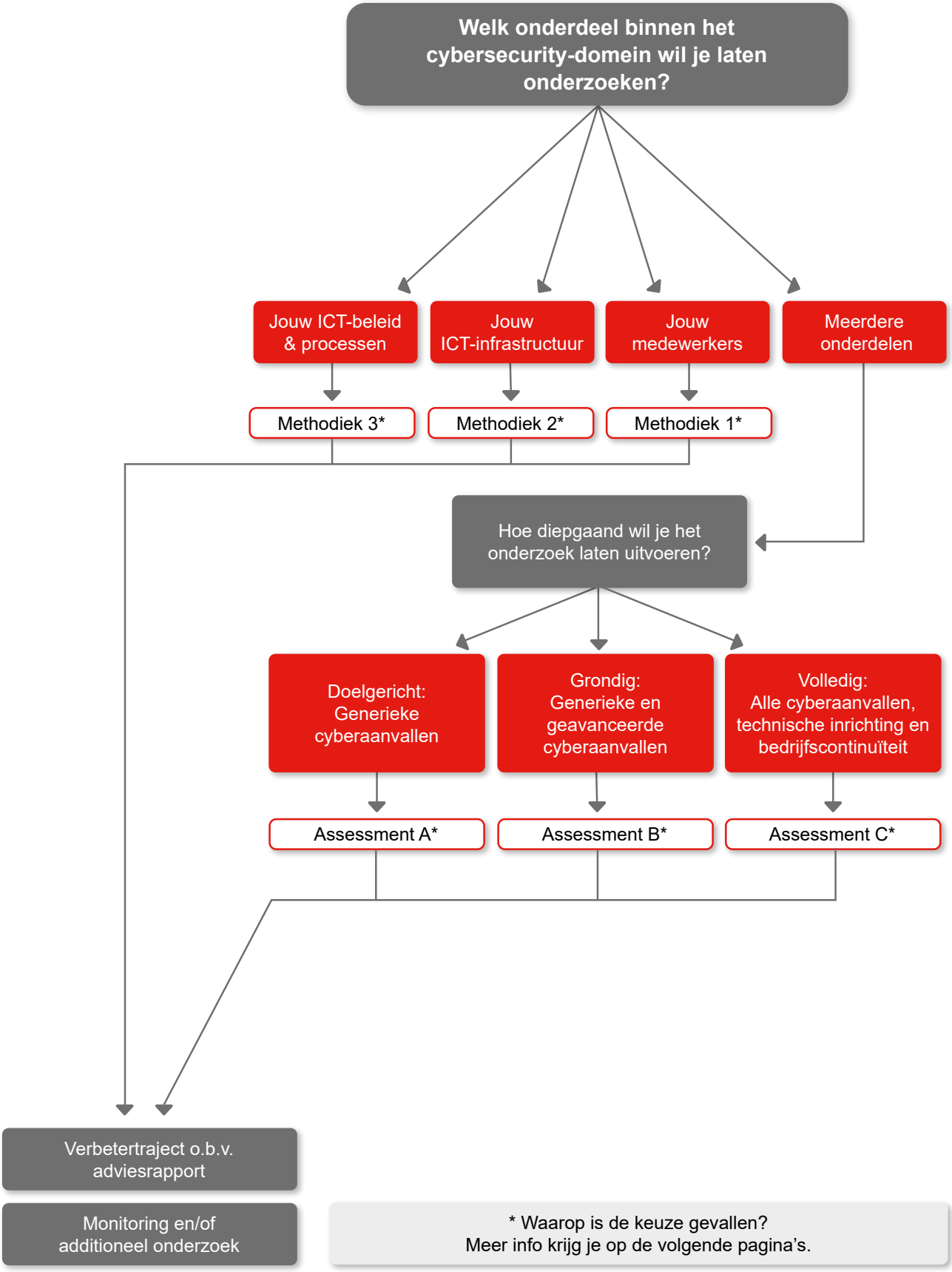
> Cybersecurity is niet langer alleen de verantwoordelijkheid van de IT-manager. Beleid, techniek én de medewerkers zijn schakels die allemaal even sterk dienen te zijn en naadloos op elkaar moeten aansluiten. Zo wordt een situatie gecreëerd die cybercriminelen doet besluiten een deur verder te gaan.

**Michael Waterman, Cybersecurity Specialist van ACA IT-Solutions**



Beukenlaan 40-50 | 5651 CD Eindhoven
T +31 (0)40 - 8 800 100 | info@aca-it.nl | www.aca-it.nl

## Keuzehulp flowchart




A·C·A IT-SOLUTIONS
ONDERDEEL VAN Crowe

Beukenlaan 40-50 | 5651 CD Eindhoven
T +31 (0)40 - 8 800 100 | info@aca-it.nl | www.aca-it.nl

## Vervolgstappen

De keuzehulp op pagina 3 geeft je richting om je cyberveiligheid naar een hoger niveau te brengen. Wil je op basis van de voorgestelde keuze graag een nadere toelichting, wil je van gedachten wisselen over de toepasbaarheid op de vraagstukken die spelen in jouw organisatie of wil je direct starten met je cybersecurity project? Ons Cybersecurity Team heeft alle specialisaties in huis om je bij te staan bij het optimaliseren van de cyberveiligheid binnen je organisatie, te beginnen met een methodiek of assessment (of een combinatie). Op basis van het opgeleverde adviesrapport krijg je concrete verbeterpunten voorgesteld die je zelfstandig of met onze ondersteuning kunt uitvoeren.

## Contact

Wil je meer informatie of een afspraak maken? Neem dan contact met ons op via onderstaande contactgegevens.

**Adresgegevens**
ACA IT-Solutions
Beukenlaan 40-50
5651 CD Eindhoven

**Contactgegevens**
040 - 8 800 100
info@aca-it.nl
www.aca-it.nl

# Methodieken

| | Methodiek 1 | Methodiek 2 | Methodiek 3 |
|---|---|---|---|
| | **Cyber Security Bewustwording** | **Cyber Security IT-Beschikbaarheid** | **Cyber Security Weerbaarheid** |
| |  |  |  |
| **Welke aanpak wordt gebruikt?** | In hoeverre kunnen jouw medewerkers een cyberaanval (phishing) herkennen?<br><br>Een specialist van ACA IT-Solutions neemt samen met je door welke medewerkers getraind moeten worden in het herkennen van phishing. Primaire doelen zullen personen zijn met autoriteit of toegang tot financiële middelen, maar ook een test voor alle medewerkers is mogelijk. De gesimuleerde aanval wordt op een moment uitgevoerd dat jij aangeeft. | In hoeverre is jouw ICT-omgeving bestand tegen cybercriminaliteit?<br><br>Een IT-specialist van ACA IT-Solutions neemt samen met jouw operationeel IT-verantwoordelijke de inrichting van de IT-infrastructuur onder de loep en beoordeelt of daarbij de juiste keuzes zijn gemaakt (proces en inrichting). Anders gezegd: een onderzoek ‘onder de motorkap’ dat plaatsvindt op jouw bedrijfslocatie. | In hoeverre zijn het beleid en IT-werkwijze van jouw organisatie passend om cyberaanvallen te kunnen pareren?<br><br>Op basis van een uitgebreid interview (150 vragen) door een IT Business Professional van ACA IT-Solutions met uw IT-management wordt de werkwijze van de organisatie duidelijk, alsook de hiaten en verbeterpunten op het vlak van cybersecurity en ICT. |
| **Wat is de diepgang?** | Generiek | Diepgaand | Generiek |
| **Welke methodiek wordt gehanteerd?** | Gesimuleerde phishing-aanval | Intakegesprek<br>Onsite research | Operationeel Interview |
| **Wat wordt onderzocht?** | Interne medewerkers | Interne Infrastructuur | Interne Processen |
| **Welk toetsgebied wordt onderzocht?** | Mens | Techniek | Beleid |
| **Welke normering is van toepassing?** | - | - | MSAT |
| **Wat krijg je opgeleverd?** | Adviesdocument bestaande uit een managementsamenvatting, testresultaten, conclusies en aanbevelingen. | Adviesdocument bestaande uit een managementsamenvatting, conclusies en aanbevelingen. Tevens wordt een ICT componenten inventarisatie opgeleverd. | Adviesdocument bestaande uit een managementsamenvatting, conclusies en aanbevelingen. |

Wil je meer informatie of een afspraak maken? Neem dan contact met ons op via onderstaande contactgegevens.
**ACA IT-Solutions** – Beukenlaan 40-50 – 5651 CD Eindhoven – T 040-8800100 – E info@aca-it.nl – I www.aca-it.nl

# Assessments

| | Assessment A | Assessment B | Assessment C |
|---|---|---|---|
| | **Cyber Security Assessment - Basis** | **Cyber Security Assessment - Uitgebreid** | **Cyber Security Assessment - Totaal** |
| |  |  |  |
| **Welke aanpak wordt gebruikt?** | Hoe kwetsbaar is jouw organisatie voor generieke cyberaanvallen?<br><br>Tijdens een geautomatiseerde scan onderzoeken we steekproefsgewijs hoe het gesteld is met de cyberweerbaarheid van jouw bedrijfsnetwerk en de status van patches/updates. Deze onderzoeksresultaten koppelen we aan het adviesdocument van de methodiek Cyber Security Weerbaarheid (prijs inbegrepen). | Hoe goed is jouw organisatie beschermd tegen cyberincidenten en geavanceerde cyberaanvallen?<br><br>In dit onderzoek passeren de onderzoeksmethodieken Cyber Security Weerbaarheid en Cyber Security Assessment - Basis, aangevuld met een grondig onsite onderzoek naar kwetsbaarheden, procedurefouten en risico's/zwakheden in de IT-Security omgeving. Daarbij wordt ook de compliance beoordeeld. | Hoe is het gesteld met de cyberveiligheid, technische inrichting en bedrijfscontinuïteit van jouw organisatie?<br><br>In dit volledige onderzoek worden alle methodieken en assessments zoals hiervoor beschreven ingezet en gecombineerd om tot een diepgaand en compleet adviesrapport te komen over de staat van jouw IT-omgeving, IT-beleid en de mate van cyberveiligheid op alle vlakken. |
| **Wat is de diepgang?** | Doelgericht | Grondig | Volledig |
| **Welke methodiek wordt gehanteerd?** | Operationeel Interview<br>Geautomatiseerde scan | Operationeel Interview<br>Geautomatiseerde scan<br>Onsite research | Operationeel Interview<br>Geautomatiseerde scan<br>Onsite research |
| **Wat wordt onderzocht?** | Interne Processen & Infrastructuur (geauthenticeerd) (max. 10 devices) | Interne & Externe Infrastructuur, Interne Processen | Interne & Externe Infrastructuur, Interne Processen, Open Source Intelligence & Publieke Websites |
| **Welk toetsgebied wordt onderzocht?** | Techniek & Beleid | Techniek & Beleid | Techniek & Beleid & Mens |
| **Welke normering is van toepassing?** | CIS | CIS | CIS |
| **Wat krijg je opgeleverd?** | Adviesdocument bestaande uit een managementsamenvatting, conclusies en aanbevelingen. Ook worden de data van de kwetsbaarheden scan opgeleverd. Deze data worden in het adviesdocument verwerkt. | Gedetailleerde, uitgebreide rapportage bestaande uit een managementsamenvatting, conclusies en aanbevelingen op basis van resultaten uit de systemen. Hiernaast wordt tevens de data van de kwestbaarheden scan geleverd. Deze data wordt in het advies document verwerkt. | Gedetailleerde, uitgebreide rapportage bestaande uit een management-samenvatting, conclusies en aanbevelingen op basis van resultaten uit de systemen. Hiernaast worden tevens de data van de geautomatiseerde scan geleverd. Deze data worden in het adviesdocument verwerkt. |

Wil je meer informatie of een afspraak maken? Neem dan contact met ons op via onderstaande contactgegevens.
**ACA IT-Solutions** – Beukenlaan 40-50 – 5651 CD Eindhoven – T 040-8800100 – E info@aca-it.nl – I www.aca-it.nl