ICT TriOpSys
Part of ICT Group

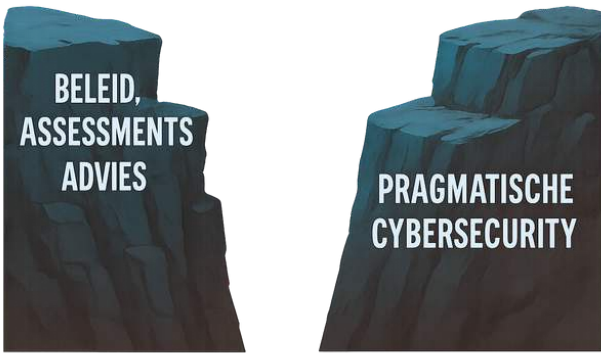
Cyber Improve

Van advies naar actie, van risico naar resultaat

Cybersecurity staat bij veel organisaties hoog op de agenda, maar de praktijk laat zien dat het verbeteren van de digitale weerbaarheid vaak moeilijk van de grond komt. Niet omdat de risico's onduidelijk zijn, integendeel. Ransomware-aanvallen, datalekken en compliance-issues domineren steeds meer de nieuwsberichten. De uitdaging zit in de uitvoering: de vertaling van strategisch besef naar pragmatische implementatie en borging.

Cyberkloof

Organisaties hebben vaak uitdagingen in de capaciteit, ervaring of specialistische kennis om cybersecuritymaatregelen op het juiste moment en op de juiste manier door te voeren. IT-afdelingen zijn overbelast, securityspecialisten zijn schaars en veel projecten blijven steken in analyses of abstract beleid. Dat is geen onwil, maar een logisch gevolg van beperkte middelen en kennis in een complex landschap. Daardoor ontstaat er een structurele kloof tussen wat nodig is en wat daadwerkelijk wordt gerealiseerd.



ICT TriOpSys ondersteunt organisaties bij het daadwerkelijk verbeteren van hun cybersecurity, niet alleen met (beleids)advies, maar met technisch uitvoerbare oplossingen, uitgevoerd door mensen die de materie snappen én in de praktijk brengen.

Van plan naar uitvoering

Veel organisaties hebben de afgelopen jaren fors geïnvesteerd in strategisch advies over cybersecurity. Risicoanalyses zijn uitgevoerd, maturity assessments gedaan, frameworks gespiegeld aan NIST of ISO 27001, en uitgebreide rapporten zijn opgemaakt vol aanbevelingen.

Toch blijft de praktijk achter. Projecten komen niet van de grond. Aanbevelingen worden niet door vertaald naar concrete acties. Engineers weten niet waar ze moeten beginnen. Beveiliging blijft steken in abstracte termen als "zero trust", "continuous monitoring" of "defence in depth", zonder dat er duidelijkheid is over wie wat moet doen in welke systemen. Een heldere roadmap ontbreekt vaak.

"De risico's zijn duidelijk, de wil is er vaak ook, maar zonder gerichte actie blijft digitale weerbaarheid een goed voornemen."
– Security Consultant

Deze kloof, tussen hoogover advies en concrete (technische) uitvoering, is precies waar ICT TriOpSys het verschil maakt. Wij helpen organisaties niet aan nóg een rapport, maar aan tastbare verbeteringen om risico's te mitigeren: De netwerksegmentatie klopt niet. Firewallregels zijn ooit organisch gegroeid maar nooit opgeschoond. MFA is deels geïmplementeerd, maar niet afdwingbaar op alle systemen. Back-ups zijn er wel, maar worden niet getest. Incident response leeft op papier, maar niemand weet wie wat doet als het misgaat.

Flexibele vorm

Onze aanpak is modulair en schaalbaar, zodat we aansluiten bij uw organisatie, of u nu een concreet project wilt uitvoeren of structureel wilt verbeteren.

1. Programmamanagement

We nemen de regie over bredere verbetertrajecten, zorgen voor overzicht, afstemming met stakeholders, en vertalen securitydoelen naar haalbare implementatie-stappen.

2. Projectteams

We stellen multidisciplinaire teams samen, bestaande uit securityspecialisten, netwerkengineers en consultants, die werken aan afgebakende projecten zoals het opmaken van een security roadmap, een EDR-implementatie of IAM-inrichting.

3. Flexibele inzet van experts

Heeft u op korte termijn behoefte aan specifieke expertise? Wij leveren tijdelijke versterking: bijvoorbeeld een security engineer voor hardening, of een consultant voor compliance-advies.

4. Quick wins & verbeterworkshops

We starten waar de impact het grootst is. Denk aan workshops waarin we met IT én business prioriteiten bepalen, risico's identificeren en een verbeterplan opstellen.

Soorten projecten

Onze dienstverlening richt zich op (technische) domeinen waar verbetering het meeste oplevert en waar het vaak het lastigst is om zelfstandig tot structurele oplossingen te komen:

Netwerkbeveiliging: veel organisaties beschikken over firewalls, maar missen de juiste configuratie of monitoring. Wij helpen bij het opzetten en onderhouden van netwerk- en applicatiefirewalls en het logisch segmenteren van netwerken (bijv. met VLAN's of DMZ's), zodat risico's daadwerkelijk worden beperkt in plaats van verplaatst.

Identity & Access Management (IAM): toegang is een van de meest kwetsbare schakels in IT. Wij helpen organisaties met het instellen van Multi-Factor Authenticatie (MFA), het inrichten van Role-Based Access Control (RBAC) en de implementatie van IAM-oplossingen die passen bij de schaal en complexiteit van de organisatie.

Endpointbeveiliging: ondanks centrale firewalls zijn eindgebruikerssystemen vaak het werkelijke aanvalspunt. Wij ondersteunen bij het implementeren van geavanceerde EDR-oplossingen die proactief verdachte activiteiten opsporen op werkstations en laptops.

Server- en besturingssysteembeveiliging: veel systemen draaien standaardconfiguraties die onnodige risico's met zich meebrengen. Met gerichte systeem-hardening zorgen we dat ongebruikte diensten worden uitgeschakeld en instellingen worden afgestemd op het dreigingsniveau.

Back-ups en Disaster Recovery: back-ups zijn er vaak, maar worden zelden getest of offsite veiliggesteld. Wij helpen organisaties bij het opstellen, inrichten én testen van Disaster Recovery Plans (DRP's) en het implementeren van bijvoorbeeld Disaster Recovery as a Service, zodat beschikbaarheid gegarandeerd is, ook als het misgaat.

Incident Response en Monitoring: een cyberincident is geen kwestie van "of", maar van "wanneer". Wij helpen organisaties met het opstellen van een Incident Response Plan en begeleiden de aansluiting op een Security Operations Center (SOC) voor continue monitoring en snelle actie bij incidenten.

Al deze onderwerpen vereisen niet alleen technische kennis, maar ook overzicht, prioritering en regie. En juist dat ontbreekt vaak in organisaties waar cybersecurity 'erbij' wordt gedaan in plaats van integraal wordt aangepakt. Onze rol is helder: wij verbeteren uw cybersecurityomgeving technisch, operationeel én organisatorisch met concrete oplossingen, schaalbare inzet en bewezen methodes.

"We zien een groeiend strategisch besef rond cybersecurity, maar de vertaalslag naar dagelijkse processen blijft achter."
– Security Consultant

ICT TriOpSys als partner

Bij ICT TriOpSys staat veiligheid voorop. De kern van onze dienstverlening is simpel: we zorgen dat securitymaatregelen echt worden doorgevoerd, technisch correct, documenteerbaar en overdraagbaar. Daarbij houden we altijd rekening met bestaande capaciteit, tooling en infrastructuur. We bouwen dus niets dat uw team niet kan beheren.

Onze mensen zijn niet alleen adviseurs, maar engineers en specialisten die configureren, scripten, testen, migreren en afronden. We werken nauw samen met interne IT-teams en zorgen voor kennisoverdracht zodat u na afloop verder kunt. We kunnen tijdelijk capaciteit leveren, projecten volledig uitvoeren, of fungeren als technische partner in bredere securityprogramma's.