ICT TriOpSys
Part of ICT Group

Cybersecurity Trainingsdag

Beveiliging begint bij bewustwording

De wereld van cybersecurity verandert razendsnel. Organisaties worden steeds vaker geconfronteerd met digitale dreigingen die direct invloed hebben op continuïteit, reputatie en vertrouwen. Bestuurders spelen hierin een cruciale rol: niet als technici, maar als leiders. Bent u voorbereid en kent u uw verantwoordelijkheden in een steeds digitaler dreigingslandschap?

In controle

Voor organisaties is de grootste uitdaging op het gebied van cybersecurity de vraag; Hoe weet ik als organisatie dat ik in controle ben en wanneer ben ik veilig genoeg? Als bestuurder wilt u weten wat er speelt, hoe uw organisatie ervoor staat en wat uw specifieke taken zijn om de cyberveiligheid van de organisatie te waarborgen. Dit vereist een begrip van de complexiteit van moderne cyberontwikkelingen en de impact ervan op uw organisatie. Het is een voortdurende uitdaging om als bestuurder op de hoogte te blijven van het snel evoluerende cybersecurity-landschap en om te weten hoe je kunt, en soms moet, anticiperen op nieuwe potentiële dreigingen en uitdagingen. Daarnaast schrijft de huidige NIS2-richtlijn voor dat bestuurders kennis hebben van cybersecurity en weten hoe hun organisatie er op dat gebied voor staat. Het delegeren aan een CISO of security-verantwoordelijke is hierbij niet meer voldoende.

Onze training is speciaal ontworpen om bestuurders hierin te ondersteunen. U ontwikkelt praktische kennis over cyberdreigingen, compliance en bestuurlijke verantwoordelijkheid met als doel: structureel grip op digitale veiligheid.

“Cybersecurity is geen IT-vraagstuk, maar een leiderschapsverantwoordelijkheid. De veiligheid van je organisatie begint in de bestuurskamer.”
– Principal Cybersecurity Consultant

Doel van de training

Bestuurders hebben als taak om effectief te (be)sturen op de veiligheid van de organisatie. Het begrijpen van cybersecurity is hierin cruciaal om de juiste keuzes te kunnen maken. Tijdens deze training gaan wij in op bewustwording en kennisoverdracht over het thema cybersecurity. Voor bestuurders komen daar specifieke uitdagingen bij kijken zoals taakverantwoordelijkheid, waar stuur ik op, wat betekend de aankomende Cyberbeveiligingswet voor mij? Tijdens deze training zullen wij hier antwoorden op geven en bestuurders pragmatische tips meegeven.

De training is bedoeld voor alle belanghebbenden met betrekking tot cybersecurity binnen de organisatie op strategisch niveau. Een diverse groep stimuleert eenieder beter inzicht te krijgen in elkaars kennis én verantwoordelijkheden. Bovendien biedt de training de gelegenheid voor bestuurders om vragen te stellen, ideeën uit te wisselen en samen te werken met andere belanghebbende in de organisatie. Dit kan resulteren in waardevolle discussies om de effectiviteit van bestaand beleid en procedures te evalueren en beter voorbereid te zijn op cyberdreigingen.

Waar bestaat de training uit?

De trainingsdag begint met een kennissessie over de complexiteit van cybersecurity, trends en ontwikkelingen in de wereld, het dreigingsbeeld en risicoprofiel voor uw organisatie. Op basis van verscheidende modules kunt u een eigen trainingsdag op maat samenstellen. Hierbij kunt u denken aan inhoudelijke presentaties, het behandelen van thema's zoals NIS2, een praktijkgerichte tabletop crisis oefening en een rondetafelgesprek. De training is zo opgebouwd dat naast de theoretische kennissessie, belanghebbende door interactieve sessies praktische ervaring opdoen in het omgaan met echte cybersecurity-situaties.

Table-top (crisis)oefening

Een realistische crisissimulatie naar keuze (bijv. ransomware aanval) om de bewustwording te vergroten wat te doen tijdens een crisis. Hierbij worden deelnemers als geheel getest op de kennis van hun rol en verantwoordelijkheden.

Lagerhuis debat

Verschillende stellingen waarbij deelnemers worden ingedeeld in twee teams; voor en tegen. Hierbij worden deelnemers gestimuleerd vanuit een ander perspectief na te denken over het onderwerp en hier onderbouwd een discussie over te voeren.

Stellingen

Verschillende (prikkelende) stellingen worden behandeld om een discussie op gang te brengen over gerelateerde security onderwerpen. Hierbij worden deelnemers gestimuleerd hun keuze te beargumenteren en kritisch na te denken over het onderwerp.

Rondetafelgesprek

Een open gesprek over ervaringen, uitdagingen en best practices binnen de organisatie. Dit versterkt het collectieve inzicht en de samenhang in de cybersecuritycultuur binnen uw organisatie.

Specifiek onderwerp

Een verdiepend blok over een specifiek onderwerp, zoals de aankomende Cyberbeveiligingswet (NIS2), keten-verantwoordelijkheid, of risicobeoordeling.

Mogelijk onderwerp naar keuze – NIS2

De NIS2-richtlijn, die momenteel wordt omgezet in de Nederlandse Cyberbeveiligingswet (Cbw), introduceert een reeks strengere en meer uitgebreide verplichtingen voor organisaties die opereren binnen vitale en essentiële sectoren. Waar de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni) al eisen stelde aan cybersecurity, gaat NIS2 een stap verder door bestuurders expliciet verantwoordelijk te maken voor het actief sturen op risico's. Dit betekent dat niet alleen de IT-afdeling, maar het gehele bestuursorgaan betrokken moet zijn bij het waarborgen van de digitale veiligheid.

Daarnaast verplicht NIS2 organisaties tot een proactieve houding ten aanzien van cyberincidenten. Dit houdt onder meer in dat incidenten tijdig en op een gestructureerde manier gemeld moeten worden aan de bevoegde autoriteiten, zodat risico's voor de continuïteit van cruciale diensten worden beperkt. De wet stelt ook strengere eisen aan het nemen van aantoonbare maatregelen, zoals het implementeren van robuuste technische en organisatorische beveiligingsmaatregelen, periodieke risicoanalyses en het trainen van medewerkers om bewustwording te vergroten.

De implementatie van NIS2 in Nederland staat gepland voor 2026, wat organisaties ruim de tijd geeft om zich voor te bereiden. Echter, de complexiteit en impact van de nieuwe regels vragen om een grondige aanpak. Daarom bieden wij tijdens onze training een vertaling van de juridische en beleidsmatige kaders naar praktische handvatten. We helpen bestuurders inzicht te krijgen in hun rol en verantwoordelijkheid, en bieden strategieën aan om niet alleen te voldoen aan de wettelijke eisen, maar ook om de cyberweerbaarheid van hun organisatie structureel te versterken.

"Hackers zoeken niet naar firewalls. Ze zoeken naar zwakke schakels in beslissingen. Zorg dat je als directie niet de opening bent."
– Principal Cybersecurity Consultant

ICT TriOpSys als partner

Bescherm de continuïteit, het vertrouwen en de reputatie van uw organisatie. Investeer in uw leiderschap en maak cybersecurity tot een krachtig onderdeel van uw bestuursfunctie. ICT TriOpSys staat klaar om samen met u een op maat gemaakte training te organiseren, afgestemd op de unieke context van uw organisatie.