

Het belang van Cyber Security

Cyber Security is een belangrijk onderwerp op maatschappelijk niveau.

forvis mazars

Het internet, computernetwerken en systemen vormen als het ware het zenuwstelsel van onze samenleving. Uitval, verstoring en manipulatie kan grote en serieuze consequenties hebben. Een concreet voorbeeld is ransomware, wat veel bedrijven en organisaties treft en tot (aanzienlijke) schade leidt.

De dynamiek en snelheid op het gebied van informatietechnologie en cybersecurity is groot. Voorbeelden hiervan zijn: Cloud computing, zelfrijdende auto's, artificalintelligence en toenemende cybercriminaliteit. De geboden kansen en mogelijkheden zijn eveneens groot. Zonder goed risicomanagement en bijbehorende cybersecurity maatregelen kunnen deze kansen echter bedreigingen worden.

Het inzetten van kwaadaardige software, middelen en technieken wordt steeds eenvoudiger en cybercriminelen bieden hun diensten zelfs aan in de vorm van een servicemodel (inclusief bijbehorende ondersteuning). Een voorbeeld hiervan is ransomware als een service.

Omdat de afhankelijkheid van IT op maatschappelijk, bedrijfsmatig en persoonlijk vlak alleen maar aan het toenemen is, worden ook steeds meer eisen gesteld vanuit toezichthouders en overheden op het gebied van cybersecurity en de genomen maatregelen.

De noodzaak voor Cyber Security Testing

Met een IT penetratie wordt een systeem en/of netwerk getest op de aanwezigheid van kwetsbaarheden en of deze kunnen worden misbruikt door een aanvaller. Een dergelijke test wordt meestal gedurende een korte periode uitgevoerd en richt zich op een beperkt deel van een systeem en/of infrastructuur. Onder een red team actie wordt verstaan het uitvoeren van een simulatie van een waarheidsgetrouwe cyberaanval die langere periode duurt om de daadwerkelijk werking van cyber security beveiligingsmaatregelen binnen een organisatie te testen. Dit wordt bijvoorbeeld vanuit de Nederlandse Bank toegepast op basis van de Threat Intelligence Based Ethical Redteaming(Tiber) filosofie om belangrijke financiële instituten in Nederland periodiek te testen. Recent heeft de DNB een lichtere variant aan toegevoegd genaamd: ART (Advanced Red Teaming). Deze test aanpak gaat ook gebruikt worden in andere sectoren zoals binnen de overheid en de zorg.

IntelligenceDriven Computer Network Defense

Red team testing en Tiber zijn gebaseerd op het zogenaamde IntelligenceDriven Computer Network Defenseconcept. Dit is een moderne vorm van risicomanagement op het gebied van cyber security en heeft als doel het creëren van daadwerkelijke weerbaarheid op het gebied van cyber security voor een organisatie. De kern van dit concept is eenvoudig en wordt gevormd door het principe van meten = weten.
Om een goede risico inschatting te kunnen maken worden zaken zoals: dreigingen, dreigingsactoren, aanvalstechnieken geïncorporeerd in een security test. Cruciaal is om te begrijpen wat een tegenstander / aanvaller kan en hoe deze werkt.

Concrete uitwerkingen van het IntelligenceDriven Computer Network Defense concept zijn toepassen van: threatmodelling en intelligence, IT pentesting en red teaming, monitoring & detectie en incident response. Hierbij staat de lerende organisatie centraal. Forvis Mazars kan samen met haar klanten deze onderwerpen vorm geven en realiseren.

Red teaming

Het is belangrijk om te beseffen dat de aard en uitvoering van een Red team test op een aantal punten verschilt van een ITpenetratietest. Een penetratietest wordt meestal uitgevoerd in periode van een aantal dagen, vindt plaats in overleg met het securityteam van een klant en detectie van testactiviteiten is veelal geen probleem.

Bij een Red team test wordt het beveiligingsteam van een klant niet geïnformeerd en het is de[1] [2] bedoeling om niet gedetecteerd / gevonden te worden

[1] Bron: https://www.dnb.nl/voor de sector/betalingsverkeer/tiber nl/
[2] Bron: https://www.lockheedmartin.com/content/dam/lockheedmartin/rms/documents/cyber/LM White Paper Intel Driven Defense.pdf

door dit team. Dit stelt andere eisen aan de aanpak, middelen en kennis en expertise van de uitvoerders van de test.

100 procent veiligheid bestaat niet. Forvis Mazars kan haar klanten helpen een optimale balans te realiseren op het gebied van: weerbaarheid, risicomanagement en cyber security. Hierbij wordt een effectieve mix van defensieve en offensieve beveiligingsmaatregelen ingezet, met als het optimale uit de situatie te halen.

Cybersecurity Governance, Compliance & Riskmanagement

In de moderne bedrijfsomgeving is cybersecurity cruciaal om gegevens te beschermen tegen cyberaanvallen en datalekken. Het veilig houden van een dergelijke complexe digitale omgeving vereist meer dan alleen technologie. Cybersecurity Governance gaat over het geheel aan beheersmaatregelen, regelgeving, verantwoording en sturing op menselijk gedrag waarmee we ervoor kunnen zorgen dat het veilig blijft.

Strategische Cybersecurity Governance

Forvis Mazars begrijpt dat cybersecurity begint bij het bestuur. Onze experts helpen bij het opzetten van een robuust governance kader. Dit omvat het definiëren van verantwoordelijkheden, het vaststellen van beleid en het creëren van een cultuur van beveiligingsbewustzijn. Op basis van onze dienstverlening kunt u risico's identificeren, terugbrengen tot een voor uw organisatie acceptabel niveau en voldoen aan wet- en regelgeving. Zo blijft uw organisatie veerkrachtig en vertrouwd. Ook staan we u graag bij met strategische vraagstukken op het gebied van cybersecurity en hebben de kennis en expertise in huis om op te treden als vertrouwd adviseur.

NIS 2 en DORA

De Europese Network and Information Security Directive 2 (NIS2) is in Nederland geïmplementeerd via de Cyberbeveiligingswet (Cbw), die op 15 augustus 2026 in werking is getreden en de Wet beveiliging netwerk- en informatiesystemen (Wbni) vervangt. De Cbw geldt voor essentiële en belangrijke entiteiten in 18 sectoren. Organisaties moeten zelf vaststellen of zij onder de wet vallen en hebben, indien van toepassing, onder meer een registratieplicht, zorgplicht en meldplicht voor significante incidenten.

Daarnaast is het bestuur eindverantwoordelijk voor de beheersing van cyberrisico's en moeten bestuurders over voldoende kennis beschikken en passende training volgen. Om de toepasselijkheid te beoordelen, is een online NIS2-zelfevaluatie beschikbaar via regelhulpenvoorbedrijven.nl/NIS-2-NL/.

DORA is sinds 17 januari 2025 van toepassing op een brede groep gereguleerde financiële instellingen in de Europese Unie. De verordening introduceert een geharmoniseerd kader voor digitale operationele weerbaarheid en stelt eisen aan ICT-risicomanagement, het melden van ernstige ICT-gerelateerde incidenten, digitale weerbaarheidstesten, informatie-uitwisseling en het beheer van ICT-risico's bij derden. Financiële instellingen blijven verantwoordelijk voor uitbestede ICT-diensten en moeten onder meer hun contractuele afspraken, leverancierssketens en kritieke of belangrijke functies beheersen. Kritieke ICT-dienstverleners kunnen daarnaast rechtstreeks onder Europees toezicht worden geplaatst.

Slimme Complianceoplossingen

Forvis Mazars kent de complexe wereld van compliance. Of het nu gaat om AVG, ISO27001, DORA, NIS2 of andere wetten en securitynormen, wij helpen onze klanten te voldoen aan de gekozen normen en verplichte wet- en regelgeving.

Onze consultants voeren gapanalyses en audits uit, optimaliseren processen, helpen u bij het opstellen van benodigde policies en procedures en bieden concrete en praktische adviezen.

Beveiligingscultuur en Bewustzijn

Wij geloven in een mensgerichte aanpak. Onze trainingen en workshops vergroten het beveiligingsbewustzijn van uw medewerkers.

Een sterke beveiligingscultuur is een belangrijke factor tot succes van uw organisatie. Samen bouwen we aan een veilige digitale omgeving.

Cyber security specialisten netwerk Forvis Mazars

Forvis Mazars is een internationale organisatie. Hierdoor kunnen we in meerdere landen cyber security dienstverlening aanbieden. Samenwerken en bundelen van aanwezige kennis, expertise en middelen zorgt ervoor dat u als klant beter en indien nodig internationaal geholpen en ondersteund kan worden.

Neem contact met ons op om meer te weten te komen over wat wij voor u kunnen betekenen.

Contacts

René Ewals
Partner
Tel: +31 (0)88 277 18 61
rene.ewals@forvismazars.com

Jeffrey de Bruijn
Director Cyber Security & Data p
rotection
Tel:
+31 (0)88 277 11 27
jeffrey.debruijn@forvismazars.com

Jacques Tuin
Senior Spectialist Cyber Security & Ethical Hacker
Tel:
+31 (0)88 277
11 37
jacques.tuin@forvismazars.com

Imane Azrioual
Manager Cyber Security & IT Advisory
Tel:
+31 (0)88 277 20 51
imane.azrioual@forvismazars.com

Forvis Mazars is wereldwijd leider op het gebied van audit & assurance, outsourcing, tax, advisory en consulting. Wij zijn actief in meer dan 100 landen. Met ons team van professionals streven wij ernaar om een ‘unmatched client experience’ te bieden. Met diepgaande kennis van regels en gedegen inzicht in de markt helpen wij onze klanten toekomstgericht en met vertrouwen te ondernemen.