Capgemini invent

VAN STRATEGIE TOT SCHILD: DE ROL VAN DE NIS2-RICHTLIJN BIJ HET BESCHERMEN VAN HET (NATIONALE) CYBERLANDSCHAP


RANSOMWARE
DETECTED

In juli 2021 werd de wereld opgeschrikt door de verstrekkende gevolgen van een grootschalige cyberaanval gericht op de wereldwijde supply chain[1]. Het incident draaide om de inzet van ransomware door de hackersgroep REvil. Deze ransomware maakte misbruik van kwetsbaarheden in de software van bedrijfsnetwerken om deze netwerken vervolgens te infiltreren. De impact van deze aanval op de supply chain bleef niet beperkt tot de virtuele wereld. Fabrieken kwamen tot stilstand, supermarkten worstelden met tekorten, en de gebeurtenis diende als herinnering aan het feit dat cyberdreigingen zich niet meer beperken tot het veroorzaken van enkel digitale overlast.

Eens te meer werd het duidelijk dat de hedendaagse dreigingen in staat zijn om juist dié technologieën die de samenleving in haar voordeel gebruikt te ondermijnen en exploiteren. Daarnaast is het onwaarschijnlijk dat het huidige traject van cyberincidenten in de nabije toekomst zal veranderen. Consumentengegevens, kritieke assets en intellectueel eigendom staan allemaal op het punt potentiële doelwitten te worden in een steeds sterker onderling verbonden en digitaal afhankelijkere wereld.

De Europese commissaris voor de Digitale Markt benadrukte de ernst van de situatie door aan de bel te trekken. Uit dit appèl kwam naar voren dat er in het afgelopen jaar een duizelingwekkende toename van 140% in het aantal cyberaanvallen is geweest. Deze escalerende trend van digitale gevaren en belangen wordt jaarlijks gedocumenteerd door het EU-Agentschap voor Cybersecurity (ENISA) in het Threat Landscape Assessment[2].

Het rapport benadrukt drie belangrijke observaties: ten eerste de proliferatie van social engineering Aanvallen, mogelijk gemaakt door de vooruitgang op het gebied van kunstmatige intelligentie, met name via Large Language Models, ten tweede de toenemende impact van aanvallen op de supply chain als gevolg van de toegenomen verbondenheid tussen organisaties, en ten slotte een angst die samengaat met ransomware aanvallen, namelijk een data lek waarbij gevoelige informatie buit wordt gemaakt. De gevolgen hiervan voor een bedrijf zijn desastreus en lopen uiteen van het verlies van een goede concurrentiepositie tot diefstal van bedrijfsgeheimen en reputatieschade.

De samenloop van de bovenstaande bedreigingen gepaard met de groeiende afhankelijkheid van onze samenleving van digitale systemen en infrastructuur dienen als waarschuwing voor wat er kan gebeuren als rapporten met digitale gevaren niet aanzetten tot verandering in de vorm van richtlijnen en best practices.

DE NIS2-RICHTLIJN: EEN HOOG GEMEENSCHAPPELIJK NIVEAU VAN CYBERSECURITY IN DE EU

Lang voordat de supply chain aanval door REvil een feit was introduceerde de Europese Commissie in 2016 de NIS1-richtlijn (Network and Information System) met als doel de verantwoordelijkheid van de kritieke infrastructuur te vergroten om maatregelen te nemen richting hun eigen cyberweerbaarheid.

In 2022 volgde de herziening op deze richtlijn genaamd NIS2. Deze richtlijn biedt een nieuwe visie op cybersecuritycybersecurity, afgestemd op de opkomst van digitale dreigingen en een uitgebreide verantwoordingsplicht voor organisaties. Bovendien worden kritieke marktspelers onderverdeeld in 'essential' en 'important' entiteiten. Hierbij is het belangrijkste verschil dat essential entiteiten proactief gemonitord worden en 'important' entiteiten enkel reactief gemonitord worden naar aanleiding van een incident. De autoriteiten die zorg zullen dragen voor deze monitoring zijn nog nader te bepalen per lidstaat en.

De invulling aan het aantal en soort autoriteiten ligt ook bij de lidstaten. De eerdergenoemde 'essential' entiteiten onder de NIS1-richtlijn hebben betrekking op vitale sectoren zoals energie, transport, banken, afvalwaterzuivering, gezondheidszorg en overheidsinstanties. NIS2 breidt uit naar onder meer Managed Security Service Providers (MSSPs), datacentra en Cloud computing-service providers. De opvallendste aanpassing ten opzichte van NIS1 is de toevoeging van digitale dienstverleners bij de 'essential' entiteiten, wat gepaard gaat met een hogere maat van toezicht van buitenaf. Dit benadrukt de ambitie van de Europese Unie om de veiligheid van de gehele (digitale) keten te versterken. Andere 'important' entiteiten volgens de NIS2-richtlijn zijn onder andere bedrijven in het afvalbeheer, onderzoek en de voedselproductie. In totaal behoren de bedrijven binnen 17 marktsectoren tot de categorie 'essential' of 'important' entiteit. Gezamenlijk vertegenwoordigen deze bedrijven een aanzienlijk deel van de nationale economie van iedere lidstaat.

De NIS2 is in januari 2023 in werking getreden en zal van toepassing zijn vanaf oktober 2024, wat tevens de datum is waarop lidstaten de wetgeving nationaal moeten omzetten. Tot die tijd moet de Europese Commissie haar uitvoeringsrichtlijnen nog definiëren, ondersteund door verdere richtlijnen van het EU-agentschap voor cybersecurity (ENISA) en de NIS-samenwerkingsgroep. Tijdens de nationale vertaling van de NSI2-richtlijn kan elk land eisen toevoegen aan specifieke sectoren.

1. https://securityintelligence.com/posts/revil-ransomware-kaseya-supply-chain-attack/
2. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

CYBER SECURITY EN DE RAAD VAN BESTUUR

Deze Europese wetgeving biedt een unieke kans voor iedere CISO (Chief Information Security Officer), cybersecurityprofessional en cybersecuritystrateeg om cyber security op bestuursniveau – en daarmee in de gehele organisatie – onder de aandacht te brengen.

Vanuit een organisatorisch perspectief begint de implementatie van NIS2 met het begrijpen en erkennen van cyber security risico's op bestuursniveau. Dat wil zeggen dat cyber security in overweging moet worden genomen bij de haalbaarheid van een nieuw innovatief project, bij het definiëren van een meerjarige bedrijfsstrategie, of bij het aangaan van nieuwe relaties met IT-leveranciers.

In dit opzicht is het onderwerp digitale veiligheid een aanvulling op de huidige visie voor het vaststellen van de organisatiestrategie. Doorgaans wordt risicobeheer, zowel operationeel als financieel al uitgevoerd en beveiliging van activa is in de meeste gevallen al aanwezig. Het grote verschil tussen de implementatie van NIS2 en de situatie ervoor is dat de digitale veiligheid niet langer een taak is die in zijn geheel op de IT-afdeling geschoven kan worden onder de verantwoordelijkheid van de Chief Information Officer (CIO) of CISO. Organisatie brede cyber security is met de komst van NIS2 het nieuwe normaal en is een bestuursaangelegenheid geworden, die tot uiting komt in het dagelijks bestuur van een organisatie.

Het is de plicht van het leiderschap van de organisatie om toezicht te houden op de naleving van de cybersecurityregels – vanwege hun verantwoordelijkheid voor het beperken van cyber security risico's en het bieden van adequate training voor de gehele organisatie. Deze plicht en vergrootte verantwoordelijkheid komt voort uit het in de NIS2 opgenomen artikel dat C-level management persoonlijk aansprakelijk spelt bij bewezen nalatigheid in het geval van een cyberincident of bij het niet tijdig investeren in benodigde organisatorische en cybersecuritymaatregelen. Hieruit vloeit ook voort dat het business line management of afdelingshoofd cyberbedreigingen moet opnemen in de huidige risicobeheerprocessen, een grondige identificatie van de kritieke digitale activa moet definiëren en goede cyberhygiëne onderdeel moet maken van de manier van werken in de teams. Buiten hun eigen speelveld moeten organisaties zich bewust zijn van hoe hun ecosysteem de cybersecurity bij het leveren van hun diensten beheert.

Deze uitgebreide reikwijdte van NIS2 manifesteert zich ook in de opname van Managed Cyber Security Service Providers en digitale infrastructuren onder de entiteiten waar nationaal toezicht op wordt gehouden. Daarnaast vallen overheidsdiensten, zoals gemeentes en uitvoerende organisaties zoals arbeidsbureaus of de belastingdienst ook onder NIS2. De motivatie voor deze uitbreiding is de noodzaak voor deze entiteiten om hun netwerk- en informatiesystemen – die gevoelige gegevens van burgers beheren – te beschermen. Deze toevoegingen onder NIS2 maakt het niet onwaarschijnlijk dat er op den duur een certificaat zal komen dat de naleving van de richtlijn voor burgers garandeert.

Een redelijke verwachting is dat de supply chain het due diligence-onderzoek zal zien toenemen, omdat klanten toenemend rekening moeten gaan houden met cyberpraktijken of de kwaliteit en veerkracht van producten en diensten van derden. Bovendien zal de naleving van NIS2 door organisaties overslaan naar andere domeinen dan alleen cybersecurity. Het zal organisaties dwingen de coördinatie- en communicatielijnen binnen de organisatie te verbeteren en te herzien als gevolg van de crisismanagement-vereisten die in NIS2 zijn vastgelegd, die verder gaan dan cybersecurity.

Organisaties die voldoen aan NIS2, zullen na verloop van tijd grondiger worden in hun cybersecuritybeheer en -afspraken.

Op Europees niveau begon in 2016 de ontwikkeling van Information Sharing and Analysis Centers (ISACs), gestimuleerd door de NIS1-richtlijn. In een ISAC gaan CISO's met elkaar in gesprek in een vertrouwde omgeving. Dit verbetert het situationele bewustzijn van individuele organisaties en bevordert een cultuur waarin vergelijkbare bedrijven kennis over kwetsbaarheden kunnen uitwisselen. Daarnaast biedt het een platform om te waarschuwen en gewaarschuwd te kunnen worden voor mogelijke escalerende bedreigingen die zijn geïdentificeerd.

Een ander initiatief dat voortkomt uit de NIS2-richtlijn is de EU-CyCLONe. Dit nieuwe samenwerkingsnetwerk brengt alle lidstaten samen om de coördinatie van grootschalige incidenten te ondersteunen, het situationeel bewustzijn voor grootschalige incidenten te bevorderen en de paraatheid voor grens- of sector overschrijdende samenwerking bij aanvallen te vergroten. Dit is een belangrijke beweegreden voor de lidstaten om getraind te worden en voorbereid te zijn op een aantal ernstige scenario's.

Voor organisaties uit dit zich in het vereiste om niet alleen hun omgeving, maar ook hun communicatieprocedures regelmatig te testen op de belangrijkste dreigingsscenario's. Dit omvat onder meer een regelmatige training van het bestuur in het nemen van beslissingen onder druk van een cyber aanval en de kennis en bewustzijn over hoe er naar behoren gecommuniceerd moet worden, hetzij intern, met de autoriteiten, of richting de maatschappij.

STRENGERE RAPPORTAGE AAN DE AUTORITEITEN

determined per sector in all Nationale autoriteiten – die nog nader bepaald zullen worden per lidstaat en per sector – zullen proactief toezicht houden op de naleving van NIS2 door de essentiële entiteiten.

Cyberincidenten die als "significant" worden geclassificeerd moeten door elke organisatie op grond van de NIS2-richtlijn worden gerapporteerd aan het nationale Computer Security Incident Response Team (CSIRT). Daarnaast zullen entiteiten hun rapportage richting de autoriteiten binnen vastgestelde termijnen moeten uitvoeren: 72 uur in geval van een cyberincident en 24 uur in geval van vermoedelijke kwaadwillige cyberactiviteit.

Dit vereist een robuuste organisatie van de cybersecurityafdeling met duidelijk afgestemde rollen en verantwoordelijkheden. Bovendien moet er sprake zijn van duidelijke interne communicatie, mitigatie van bedreigingen die escaleren binnen de organisatie of naar andere sectoren, en een goed zicht op bedreigingen. Dit betekent dat de toezichthouder begeleiding, informatie en training zal moeten bieden om de markt te ondersteunen en voor te bereiden.

Een fundamenteel verschil in de manier waarop NIS2 wordt gehandhaafd ten opzichte van eerdere richtlijnen is de introductie van financiële sancties in de nasleep van een cybersecurity incident. In gevallen waarin nalatigheid bij het uitvoeren van passende cybersecurity- en organisatorische maatregelen door de nationale autoriteiten wordt bewezen kan een administratieve boete opgelegd worden van maximaal 10 miljoen euro of 2% van de totale mondiale omzet (afhankelijk van welke van de twee het hoogste is). Daar komt bij dat dergelijke nalatigheid ook kan leiden tot een tijdelijk werkverbod voor leidinggevend personeel en de aanwijzing van toezichthoudende functionarissen die belast zijn met het toezicht op en het uitvoeren van maatregelen om de situatie te verzachten.

Sinds de introductie van NIS1 in 2016 is het publieke bewustzijn over cybersecurity aanzienlijk gegroeid. Mede als gevolg van uitgebreide mediaberichtgeving over grootschalige aanvallen en datalekken. Het nieuws heeft de ernst van de situatie benadrukt, niet alleen bij individuen, maar ook bij bedrijven en organisaties. Dit heeft geleid tot een groter bewustzijn van de toenemende risico's en de steeds verdergaande technieken die cybercriminelen en door de staat gesponsorde aanvallers gebruiken.

De omzetting van de NIS2 naar nationale wetgeving door de lidstaten is dé kans voor Europese regeringen om hun standpunt over cyberveiligheid te manifesteren en te verspreiden. Het kan ook een instrument van onschatbare waarde zijn om burgers voor te lichten en te betrekken in de algehele digitale weerbaarheid van de Europese Unie. Het dergelijk gebruik van wetgeving als instrument is geen nieuwe praktijk. Denk bijvoorbeeld aan de impact die de introductie van de Algemene Verordening Gegevensbescherming (AVG) heeft gehad bij het informeren van burgers over de Europese waarden met betrekking tot privacy en de bescherming van persoonsgegevens. Die waarden hebben zich vertaald in nieuwe rechten en terminologie zoals "gegevensbeheerder" en "gegevensverwerker" met als doel een gedeeld bewustzijn te creëren.

DE TOEKOMST

De agenda van de EU op het gebied van cybersecurity gaat verder dan NIS2. Sectorale wetgevingen vormen een aanvulling op de NIS2-richtlijn. Voorbeelden hiervan zijn de Critical Entities Resilience Act (CER) die rekening houdt met de fysieke beveiliging van kritieke infrastructuren en de Digital Operational Resilience Act (DORA) die cybersecurity als onderdeel van de financiële veerkracht van de financiële sector beschouwt. De Cyber Resilience Act (CRA) werd in november 2022 gepresenteerd. Deze legt de basis voor meer regulering van de cybersecurity van 'connected' producten en software en legt de aansprakelijkheid bij de fabrikanten van deze producten. De kern van de discussies naar aanleiding van de CRA zal de vraag naar de daadwerkelijke oorsprong van het product zijn.

Kijkend naar het grotere geheel maken deze wetgevingen allemaal deel uit van het EU-cybersecurity framework dat is ontworpen met als doel ''cybersecurity by design'' in te prenten in organisaties en 'connected' producten en apparaten die op de EU-markt circuleren. Onlangs werd dit opnieuw bevestigd door de Europese Commissie met de vrijgave van het Cyber Shield voor een collectieve veerkracht en weerbaarheid. Cybersecurity by design is op de lange termijn dé duurzaamste benadering van cybersecurity, omdat het kwetsbaarheden minimaliseert en daarmee minimaal kans biedt aan aanvallers. Met de blik op de toekomst moeten organisaties vandaag beginnen met het overwegen van dit langetermijndoel en hun activiteiten aanpassen aan de NIS2-richtlijn, die zonder meer de toon voor de toekomst van cybersecurity in de EU heeft gezet.

CONCLUSIE

De organisaties binnen de omvang van de NIS2-richtlijn hebben de verantwoordelijkheid gekregen om hun kernprocessen veilig te stellen als deze van belang zijn voor de nationale stabiliteit, veerkracht en de economie. Het daadwerkelijke succes van de NIS2-richtlijn zal echter bepaald worden door de reactie van zowel de particulieren als de publieke sector. Het risico bestaat echter dat organisaties de NIS2 zullen zien als een oefening in compliance in, in plaats van een actiegerichte oproep om de volwassenheid van cybersecurity te vergroten. Dit zou een vergissing zijn. Om aan de NIS2 te voldoen, zijn sterk gecoördineerde inspanningen van de hele organisatie nodig die verder gaan dan de gebruikelijke controlebeoordeling. Alle onderdelen van de organisatie (van de juridische afdeling tot aan HR) zullen zij aan zij moeten werken om het voorgeschreven niveau van volwassenheid op het gebied van cybersecurity te bereiken.

Voor organisaties is het uur U gekomen om bewustzijn te creëren en kennis te vergroten over wat cybersecurity inhoudt voor het dagelijks functioneren van de organisatie. Daarnaast is het een uitgelezen kans om goede gewoontes aan te nemen die niet alleen de organisatie maar ook de hele samenleving zullen beschermen. Op het eerste gezicht lijkt dit rigoureus, maar terugkijkend naar de REvil-ransomwareaanval – en de gevolgen die zo een aanval kan hebben voor de voedsel-, energie- of transportsector – wordt het belang van NIS2 des te meer benadrukt. Na de implementatie in nationale wetten – en zelfs daarvoor – zal NIS2 de drijfveer worden om de volwassenheid van de digitale veiligheid van organisaties, die het meest cruciaal zijn voor onze samenleving, te versnellen. De NIS2 richtlijn en de sectorale toepassingen hiervan zijn een ambitieuze poging om het soms ordeloze digitale tijdperk veiliger te maken, van nationaal tot op individueel niveau.

OVER DE AUTEURS

Ana-Isabel Llacayo, CISM
NIS2 Lead Advisor and Data Security Manager, Capgemini Invent
Ana-Isabel is gespecialiseerd in EU-cyberbeleid en adviseert publieke en private organisaties over EU-regelgeving om het bewustzijn over cyberrisico's te vergroten.
ana.isabel.llacayo@capgemini.com

Emir Hajduk
Management consultant data security, Capgemini Invent
Emir houdt zich bezig met governance op het gebied van beveiliging, digitale criminaliteit en adviseert over gedragsverandering op het gebied van cyberbeveiliging.
emir.hajduk@capgemini.com

Met dank aan

Roeland de Koning voor zijn inzichten en review.

About Capgemini Invent

As the strategy, innovation, design and transformation brand of the Capgemini Group, Capgemini Invent enables CxOs to envision and shape the future of their businesses. Located in more than 36 offices and 37 creative studios around the world, it comprises a 10,000+ strong team of strategists, data scientists, product and experience designers, brand experts and technologists who develop new digital services, products, experiences and business models for sustainable growth.Capgemini Invent is an integral part of Capgemini, a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 360,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2022 global revenues of €22 billion.

Capgemini Invent
Postbus 2575 - 3500 GN Utrecht
Tel. + 31 30 203 05 00
www.capgemini.nl/invent

06-049.23