

11 februari 2025

Europese regelgeving

En de impact hiervan op de samenwerking tussen jou
en je klanten en toeleveranciers

Cyberweerbaarheidscentrum Oost Nederland



Centrum voor
Veiligheid en
Digitalisering



+



Evelien Bras:

- Directeur-Bestuurder FERM Rotterdam
- The Cyber Partners B.V.
- Commissaris multinational(s)
- Voorzitter bestuur "CYRA: Cyber-Rating"
- Gastdocent "Corporate Governance"
- Penvoerder "Cyberweerbaarheidscentrum Oost Nederland"

Aangenaam kennis te maken.



Table 1: Overview of EU Legislation in the Digital Sector

Applicable law	Published in the Official Journal of the European Union
In negotiation	Proposal by the European Commission entered the legislative process.
Planned initiative	Mentioned by the European Commission as potential legislative initiative

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Media	Finance
Digital Europe Programme Regulation, (EU) 2021/694	Recovery and Resilience Facility Regulation, (EU) 2021/241	Frequency Bands Directive, (EEC) 1987/372	General Data Protection Regulation (GDPR), (EU) 2016/679	Database Directive, (EC) 1996/9	Regulation for a Cybersecurity Act, (EU) 2019/881	Law Enforcement Directive, (EU) 2016/680	Product Liability Directive (PLD), (EEC) 1985/374, 2022/0302(COD)	Unfair Contract Terms Directive (UCTD), (EEC) 1993/13	Technology Transfer Block Exemption, (EC) 2014/316	Satellite and Cable I Directive, (EEC) 1993/83	Common VAT system, (EC) 2006/112, 2022/0407(CNS)
Horizon Europe Regulation, (EU) 2021/695, (EU) 2021/764	InvestEU Programme Regulation, (EU) 2021/523	Radio Spectrum Decision, (EC) 2002/676	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies, (EU) 2018/1725	Community Design Directive, (EC) 2002/6, 2022/0391(COD)	Regulation to establish a European Cybersecurity Competence Centre, (EU) 2021/887	Directive on combating fraud and counterfeiting of non-cash means of payment, (EU) 2019/713	European Standardization Regulation, (EU) 2012/1025	E-commerce Directive, (EC) 2000/31	Company Law Directive, (EU) 2017/1132, 2023/0089(COD)	Information Society Directive, (EC) 2001/29	Payment Service Directive 2 (PSD2), (EU) 2015/2366, 2023/0209(COD)
Regulation on a pilot regime distributed ledger tech, market, (EU) 2022/858	Connecting Europe Facility Regulation, (EU) 2021/1153	Broadband Cost Reduction Directive, (EU) 2014/61, 2023/0046(COD)	Regulation on the free flow of non-personal data, (EU) 2018/1807	Enforcement Directive (IPR), (EC) 2004/48	NIS 2 Directive, (EU) 2022/2555	Regulation on terrorist content online, (EU) 2021/784	Radio Equipment Directive (RED), (EU) 2014/53	Unfair Commercial Practices Directive (UCPD), (EC) 2005/29	Market Surveillance Regulation, (EU) 2019/1020	Audio-visual Media Services Directive (AVMSD), (EU) 2010/13	Digital Operational Resilience Act (DORA Regulation), (EU) 2022/2554
	Regulation on High Performance Computing Joint Undertaking, (EU) 2021/1173	Open Internet Access Regulation, (EU) 2015/2120	Open Data Directive (PSI), (EU) 2019/1024	Directive on the protection of trade secrets, (EU) 2016/943	Information Security Regulation, 2022/0084(COD)	Temporary CSAM Regulation, (EU) 2021/1232, 2022/0155(COD)	eIDAS Regulation, (EU) 2014/910, 2021/0136(COD)	Directive on Consumer Rights (CRD), (EU) 2011/83	P2B Regulation, (EU) 2019/1150	Portability Regulation, (EU) 2017/1128	Crypto-assets Regulation (MiCA), (EU) 2023/1114
	Regulation on Joint Undertakings under Horizon Europe, (EU) 2021/2085, 2022/0033(INLE)	European Electronic Communications Code Directive (EECC), (EU) 2018/1972	Data Governance Act (DGA Regulation), (EU) 2022/868	Standard essential patents, 2023/0133(COD)	Cybersecurity Regulation, 2022/0085(COD)	E-evidence Regulation, 2018/0108(COD)	Regulation for a Single Digital Gateway, (EU) 2018/1724	e-Invoicing Directive, (EU) 2014/55	Vertical Block Exemption Regulation (VBER), (EU) 2022/720	Satellite and Cable II Directive, (EU) 2019/789	Digital euro, 2023/0212 (COD)
	Decision on a path to the Digital Decade, (EU) 2022/2481	Roaming Regulation, (EU) 2022/612	ePrivacy Regulation, 2017/0003(COD)	Design Directive, 2022/0392(COD)	Cyber Resilience Act, 2022/0272(COD)	Digitalization of travel documents	General Product Safety Regulation, (EU) 2023/988	Geo-Blocking Regulation, (EU) 2018/302	Digital Market Act (DMA Regulation), (EU) 2022/1925	Copyright Directive, (EU) 2019/790	Financial Data Access Regulation, 2023/0205 (COD)
	European Chips Act (Regulation), 2022/0032(COD)	Regulation on the Union Secure Connectivity Programme, (EU) 2023/588	European Data Act (Regulation), 2022/0047(COD)	Compulsory licensing of patents, 2023/0129(COD)	Cyber Solidarity Act (Regulation), 2023/0109(COD)		Machinery Regulation, (EU) 2023/1230	Digital content Directive, (EU) 2019/770	Regulation on distortive foreign subsidies, (EU) 2022/2560	European Media Freedom Act, 2022/0277(COD)	Payment Services Regulation, 2023/0210(COD)
	European critical raw materials act (Regulation), 2023/0079(COD)	.eu top-level domain Regulation, (EU) 2019/517	European Health Data Space (Regulation), 2022/0140(COD)				AI Act (Regulation), 2021/0106(COD)	Directive on certain aspects concerning contracts for the sale of goods, (EU) 2019/771	Horizontal Block Exemption Regulations (HBER), (EU) 2023/1066, (EU) 2023/1067		Revision of the late payments Directive
	Establishing the Strategic Technologies for Europe Platform (STEP), 2023/0199(COD)	New radio spectrum policy programme (RSPP 2.0)	Regulation on data collection for short-term rental, 2022/0358(COD)				Eco-design Regulation, 2022/0095(COD)	Digital Services Act (DSA Regulation), (EU) 2022/2065	Platform Work Directive, 2021/0414(COD)		
		Telecoms Act / Fair Share Initiative	Harmonization of GDPR enforcement 2023/0202(COD)				AI Liability Directive, 2022/0303(COD)	Right to repair Directive, 2023/0083(COD)	Single Market Emergency Instrument (SMEI), 2022/0278(COD)		
			Interoperable Europe Act, 2022/0379(COD)					Political Advertising Regulation, 2021/0381(COD)			
			Access to vehicle data, functions and resources					Multimodal digital mobility services (MDMS)			
			GreenData4all					Consumer protection: strengthened enforcement cooperation			
								Consumer rights: adapting ADR to digital markets			





AD



Foto ter illustratie. © Getty Images

Apple buigt voor de EU en daarom is er nu een porno-app voor de iPhone

Hans Nijenhuis
7 februari 2025, 22:02



3:46

Artikel luisteren

Dankzij Europese regels is er sinds deze week een porno-app beschikbaar voor de iPhone. Bijzonder, want Apple wil geen pornografie op zijn apparaten. De techgigant laat de nieuwe app dan ook alleen maar toe onder fel protest.

Advertentie

autoriteitpersoonsgegevens.nl

AUTORITEIT
PERSOONSGEGEVENS

Menu

[Terug naar AVG algemeen](#)

De AVG in het kort

Door de Algemene verordening gegevensbescherming (AVG) hebben organisaties die persoonsgegevens verzamelen en gebruiken meer verantwoordelijkheden gekregen. En de mensen van wie zij gegevens gebruiken hebben meer rechten gekregen. Houden organisaties zich niet aan de regels? Dan kunnen zij een boete krijgen.

OP DEZE PAGINA

↓ Voor wie de AVG geldt

↓ Basisprincipes (beginselen) AVG

↓ De betekenis van de AVG

↓ De rol van de AP

↓ Informatie en hulpmiddelen

newsbit.nl — Privé

Newsbit.



Jeroen van Welsenens · 20-12-2024 12:02 · 2 - 3 min

Noord-Koreaanse hackers stelen \$1,34 miljard aan crypto in recordjaar 2024

Noord-Koreaanse hackers hebben in 2024 een recordbedrag van \$1,34 miljard aan cryptocurrencies weten te stelen, aldus blockchain-onderzoeker Chainalysis. Dit bedrag werd verzameld in 47 verschillende hacks en vertegenwoordigt maar liefst twee derde van alle grote cryptodiefstallen wereldwijd. Hiermee blijft Noord-Korea een van de meest actieve en succesvolle groepen in de wereld van cryptocriminaliteit.

Het land, bekend om zijn gesloten beleid en dictatoriale regime, wordt steeds actiever en succesvoller in cybercriminaliteit. Het aantal hacks is meer dan verdubbeld ten opzichte van vorig jaar. Experts uit de Verenigde Staten hebben zelfs lof voor de effectiviteit van Noord-Koreaanse hackers en noemen hen "de beste bankrovers ter wereld".

De gestolen fondsen worden vermoedelijk gebruikt om het ballistische raket- en nucleaire programma van het regime te financieren. Volgens schattingen wordt ongeveer een derde van Noord-Korea's

Nieuws

Koersen

Kopen

Over crypto's

Meer



Twee onderwerpen:

- NIS-2
Network Information Security
Europese directive
- CRA
Cyber Resilience ACT
European regulation
- Samenvatting impact op je klanten en/of
toeleveranciers



De NIS-2 is een Europese richtlijn

Voor bedrijven van 50+ FTE
in een van 18 specifieke sectoren

en omvat:

- cyberrisicobeheersmaatregelen en
- rapportageverplichtingen

Naar schatting 8000 bedrijven in
Nederland gaan onder de NIS-2 vallen,
zijnde 'essentieel' of 'belangrijk'.

Zeer kritieke sectoren



Andere kritieke sectoren



De NIS-2 is een Europese richtlijn

Voor bedrijven van 50+ FTE
in een van 18 specifieke sectoren

en omvat:

- Cyberrisicobeheersmaatregelen (zorgplicht) en
- rapportageverplichtingen

Naar **schatting** 8000 bedrijven in Nederland gaan onder de NIS-2 vallen, zijnde 'essentieel' of 'belangrijk'.



Bron: ncsc.nl

Welke maatregelen moet ik nemen om aan de zorgplicht te voldoen?

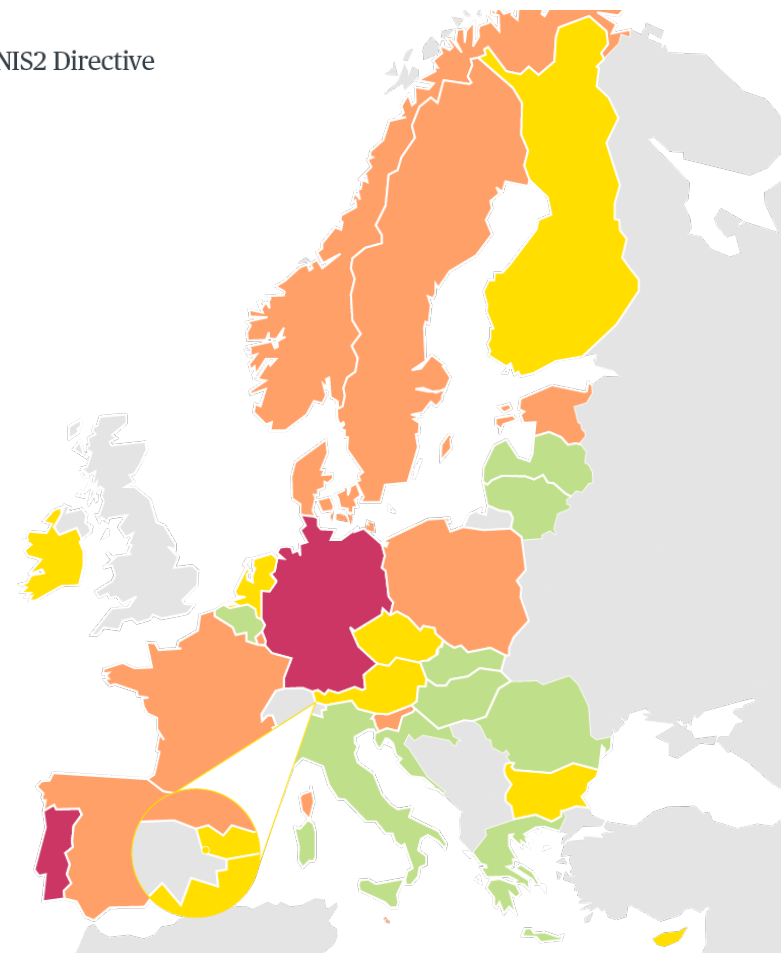
Onder de zorgplicht vallen ten minste:

1. Een risicoanalyse en beveiliging van informatiesystemen
2. (Beleid en procedures over) incidentenbehandeling
3. Maatregelen op het gebied van bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen
4. Beveiliging van de toeleveranciersketen
5. Beveiliging bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen, inclusief de respons op en bekendmaking van kwetsbaarheden
6. Beleid en procedures om de effectiviteit van beheersmaatregelen van cyberbeveiligingsrisico's te beoordelen
7. Basis cyberhygiëne en trainingen op het gebied van cyberbeveiliging
8. Beleid en procedures over het gebruik van cryptografie en encryptie
9. Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van activa
10. Het gebruik van multifactorauthenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit

Maar, wanneer precies?

NIS2 Directive

Status	
	Adoption of the national implementing act
	Publication of the proposal
	Consultation phase
	No developments



En, wat precies?

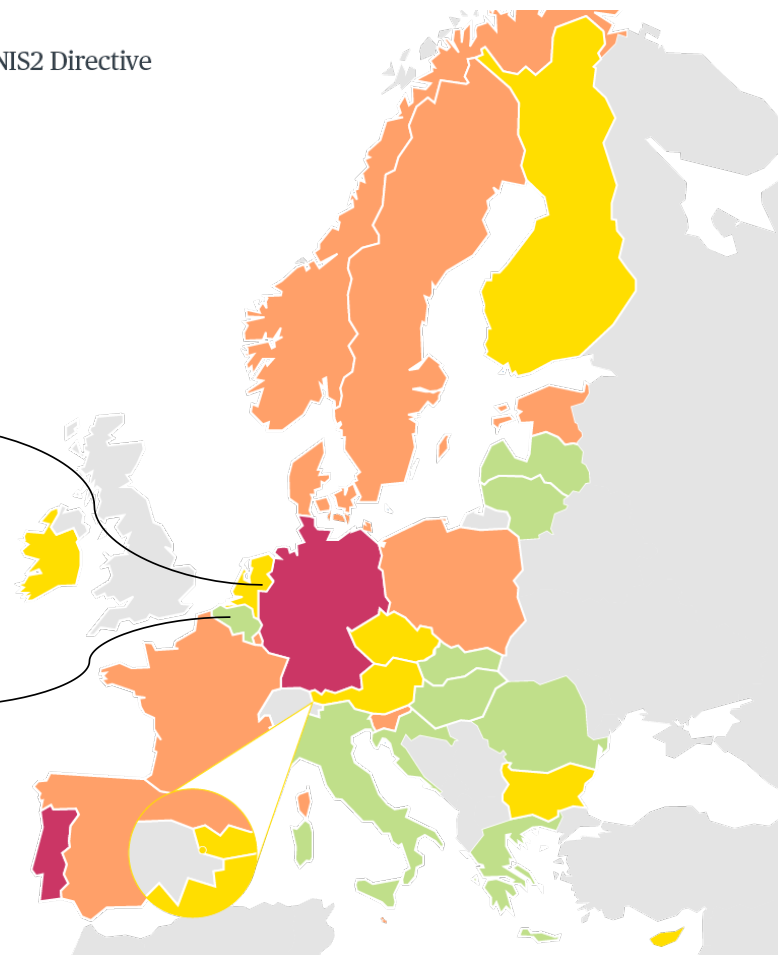
NIS2 Directive



Open norm



CyFun





Wat betekent de Nederlandse open norm?

Zorgplicht: Compliancy - Maturity

Aantoonbaarheid in de keten:

- Bedrijfsspecifieke vragenlijsten
- NIS-2-QM
- CYRA
- CYFUN
- ISO
- NIST SCF
- Branchespecifiek:
NEN7510, IEC62443, ABDO, TISAX...

Tip: volg het CCV op hetccv.nl

Meer weten over **Keurmerken** →

Brandbeveiliging →

Cybersecurity →

Inbraakbeveiliging →

Voertuigbeveiliging →

Veilig ondernemen →

Over certificeren →

Gekwalificeerde bedrijven →

CCV centrum voor
criminaliteitspreventie en
veiligheid



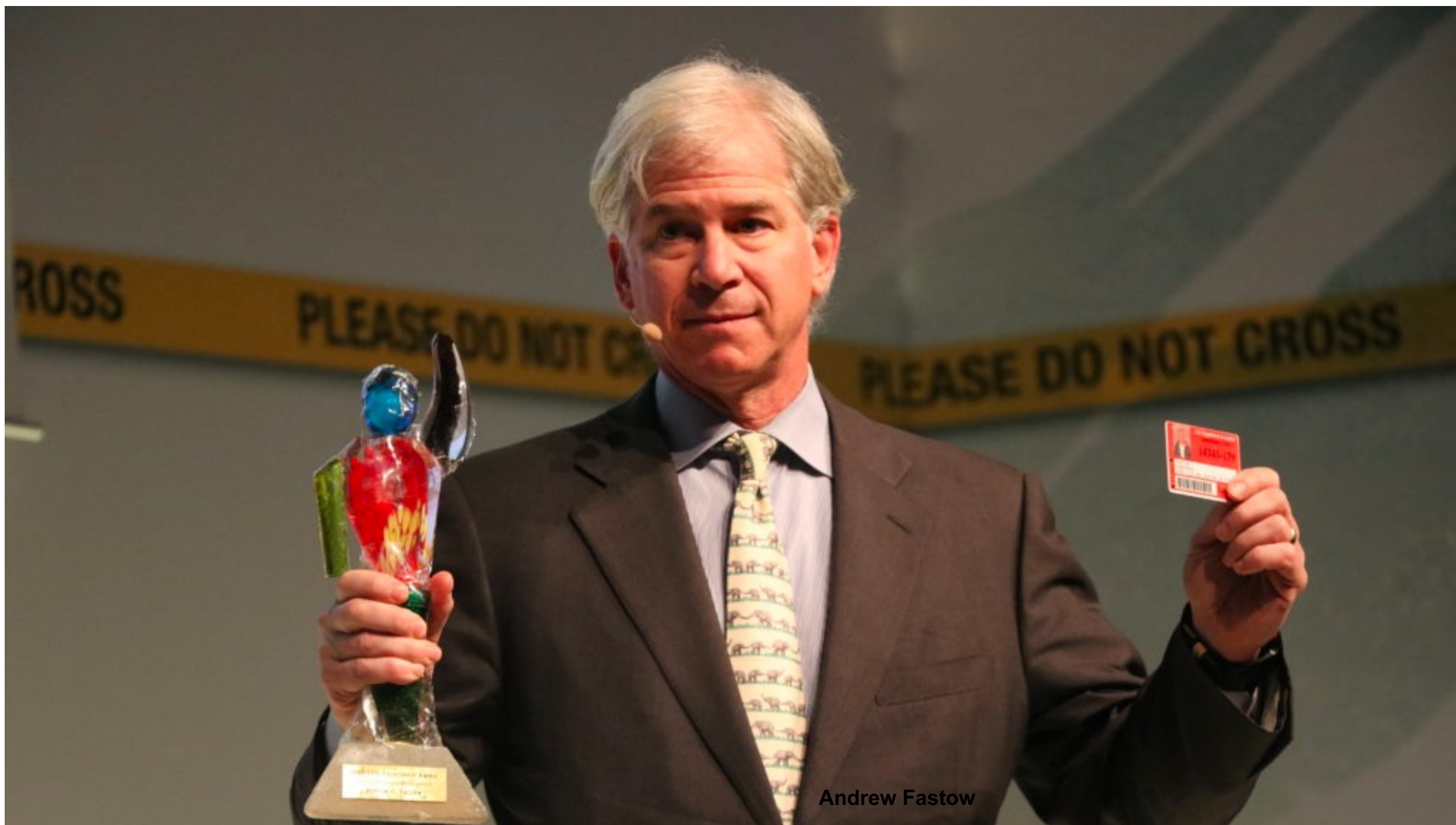
Cyber Resilience Act (CRA)

De Cyber Resilience Act (CRA) is een Europese verordening die zich richt op het verbeteren van de beveiliging van digitale producten en diensten. De verordening is gepubliceerd en eind 2024 in werking getreden.

Omdat de CRA een verordening is, hoeft deze niet vertaald te worden naar Nederlandse wetgeving, maar is deze direct van kracht. Eind 2027 moeten vervolgens alle producten met digitale elementen als inherent veilig ontworpen en geproduceerd zijn (zogenoeten security-by-design). Daarnaast geldt voor fabrikanten en andere partijen in de toeleveringsketen een zorgplicht, waaronder het aanbieden van ondersteuning en beveiligingsupdates en een meldplicht bij kwetsbaarheden en incidenten.

Welke producten moeten aan de CRA voldoen?

Alle producten met digitale elementen moeten vanaf 2027 voldoen aan de CRA. Dit zijn niet alleen fysieke producten zoals IoT-apparatuur, firewalls of netwerkkapapparaat, maar ook software zoals videogames, mobiele apps of besturingsystemen zoals Windows en componenten zoals videokaarten en software libraries.



Andrew Fastow

- 
- Werk risicogebaseerd aan cybervolwassenheid, ook voor de NIS-2
 - Een management workshop, leerkring, scan is een mooie start of vervolgstap. Betrek de bestuurder.
 - Bevraag in een vroeg stadium je klanten voor aantoonbaarheid.
Volg het CCV voor keurmerken, ook voor pentesten, awareness trainingen en ICT dienstenleveranciers.

Heb je iemand in je netwerk die je vertrouwt en de trends in de gaten kan houden?

Vragen?



Centrum voor
Veiligheid en
Digitalisering



+

