Cyber security

Michael Theuerzeit – Hudson Cybertec *(a Kiwa company)*

Kiwa Nederland B.V.

Partner for Progress

Voorstellen

Michael Theuerzeit

Hudson Cybertec B.V. (*a Kiwa company.)*

Lead consultant

Cyber security OT / IoT

> 10 werkzaam bij Hudson Cybertec B.V.

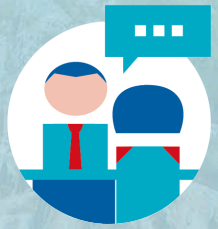
Over Kiwa:

Testen

Inspecteren

Certificeren

Training



Consultancy

Data services

Er is een strikte lijn tussen certificatie diensten en activiteiten zoals trainingen en consultancy.

De Erasmusbrug kleurde in 2010 geel bij de start van de Tour de France. © Marco de Swart

Lichtsysteem van Erasmusbrug gehackt: ‘Zat geen wachtwoord op’

Het lichtsysteem van de Erasmusbrug in Rotterdam is gehackt door journalist Daniël Verlaan. Dat meldt RTL Nieuws.

Eric Oosterom 10-11-20, 21:30

Zeeuwse gemalen te hacken via SCADA-lek

De SCADA-systemen van rioleringspompen en gemalen van de gemeente Veere blijken slecht beveiligd. Hackers kunnen de systemen manipuleren vanuit huis. De gemeente is geschrokken.

Door Bas Bareman |Webwereld | 14 feb 2012

De infrastructuur van de Zeeuwse gemeente Veere blijkt kwetsbaar. Dit bevestigt de gemeente naar aanleiding van een onthulling van actualiteitenrubriek EenVandaag. Dinsdagavond werd in de uitzending aangetoond hoe slecht beveiligd de SCADA-systemen voor de riolering en gemalen in de gemeente zijn. Hackers kunnen die systemen op afstand manipuleren.

Albert Heijn kampt met tekort aan voorverpakte kaas

Albert Heijn kampt met leveringsproblemen van haar voorverpakte kazen. Daardoor is er een tekort aan kaas ontstaan in de winkels. Dat geldt zowel voor de fysieke winkels als online.

Redactie Koken&Eten 09-04-21, 21:30 **Laatste update:** 10-04-21, 07:29

Dat meldt de supermarktgigant vrijdagmiddag op Twitter. De leveringsproblemen zouden door een storing bij een logistiek dienstverlener zijn ontstaan. Het gaat om voorverpakte kazen, zoals zakjes geraspte kaas en plakken voor op brood. De storing leidt inmiddels tot lege schappen in de winkels van Albert Heijn.

Hack

Het probleem zou veroorzaakt kunnen zijn door een hack. *Omroep Flevoland* wist donderdag te melden dat transportbedrijf Bakker Logistiek uit Zeewolde het afgelopen weekend doelwit is geweest van hackers. Daardoor zou het bedrijf minder ritten hebben kunnen rijden dan normaal. Bakker benadrukte dat het geen lege schappen zou opleveren.

Dat lijkt nu niet helemaal te kloppen. Volgens *Tweakers* is uitgerekend dit transportbedrijf verantwoordelijk voor de levering van voorverpakte kaas aan Albert Heijn. Daarmee zou het tekort het gevolg zijn van deze hack. Bakker logistiek kon geen vragen van *Tweakers* beantwoorden over de hack. Het is niet duidelijk om wat voor soort hack het precies gaat.

Stilleggen oliepijplijn VS veroorzaakt door gijzelsoftware van 'DarkSide'

onduidelijk. De gevolgen waren al wel direct zichtbaar: de vier hoofdleidingen werden dit weekend stilgelegd. Er is daarnaast een noodverordening afgegeven die vervoer over de weg mogelijk maakt en er dreigen tekorten aan benzine en gas.

De bron van de aanval is inmiddels bekend: de FBI heeft bevestigd dat het gaat om software gemaakt door DarkSide. Dit is volgens experts een relatief nieuwe groep, maar wel een die heel professioneel te werk gaat. Compleet met een klantenservice. Hun doel: veel geld verdienen. De werkwijze wordt *ransomware as a service* genoemd, wat zoveel betekent als dat de groep de gijzelsoftware ontwikkelt en anderen rekruteert om aanvallen uit te voeren. De groep krijgt vervolgens een percentage van het losgeld.

> **Ransomware is gewoon een heel interessant verdienmodel voor criminelen.**

Opmerkelijk: eenmaal binnen bij een potentieel doelwit, zou DarkSide eerst informatie verzamelen. Als blijkt dat ze zijn binnengedrongen bij een universiteit of ziekenhuis, dan zetten ze niet door, schrijft Cybereason. Zelf claimen ze daarnaast delen van de buit te hebben geschonken aan goede doelen, die dit niet zouden hebben geaccepteerd.

Ransomware group demands $51 million from Johnson Controls after cyber attack

Graham CLULEY
September 28, 2023

Johnson Controls, a multinational conglomerate that secures industrial control systems, security equipment, fire safety and air conditioning systems, has been hit by a massive cyber attack.

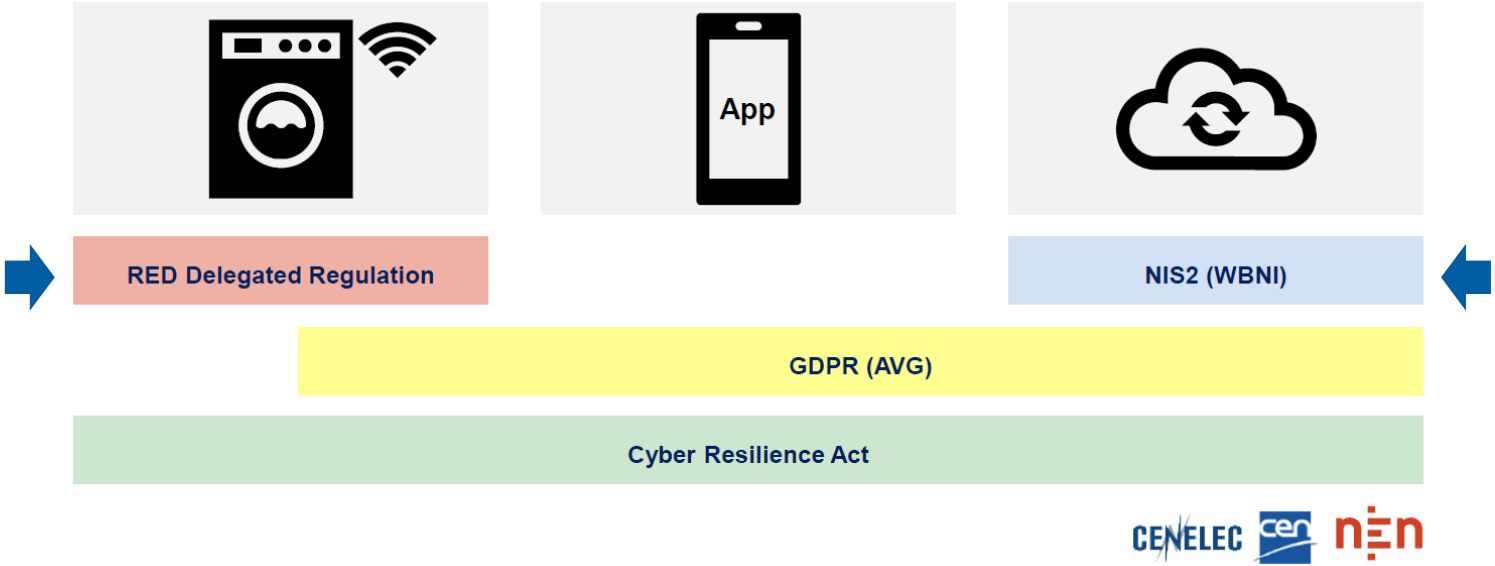
Casino Hacked by Fish-Tank: The Dangers of the Internet of Things

Internet of Things Driving Need for More Cybersecurity Professionals

At a recent event in London, it was reported by *The Hacker News* that Nicole Eagan, the CEO of cybersecurity company Darktrace, shared a story about an unnamed casino that was hacked through an internet-connected aquarium thermometer sitting in the lobby. What does that have to do with you? Plenty. That aquarium thermometer is no different from the thermostat in your home that you control through your smartphone.

Waar maakt u zich zorgen over ten aanzien van de cyberweerbaarheid van uw organisatie?

Toename van richtlijnen en regelgeving:



NIS II richtlijn (EU) 2022/2555

*“De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten **passende en evenredige technische, operationele en organisatorische maatregelen nemen** om de risico’s voor de beveiliging van de netwerk- en informatiesystemen die deze entiteiten voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken, te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken.”*

NIS II richtlijn (EU) 2022/2555

Essentieel:

- Sectoren bijlage 1
- >= 250 medewerkers
- Of jaaromzet > €50mln.

Belangrijk:

- Sectoren bijlage 1 & 2
- >= 50 medewerkers
- Of jaaromzet > €10mln

Kleine ondernemingen met kritieke functie op aanwijzing van minister.

Zorgplicht, meldplicht & toezicht.

Sectoren bijlage 1	Sectoren bijlage 2
Energie	Digitale aanbieders
Transport	Koeriersdiensten
Bankwezen	Afvalstoffen beheer
Financiële markt (infra)	Levensmiddelen
Gezondheidszorg	Chemische stoffen
Drinkwater	Onderzoek
Digitale infrastructuur	Manufacturing
Beheerders van ICT diensten	
Afvalwater	
Overheidsdiensten	
Ruimtevaart	

NIS II richtlijn (EU) 2022/2555

Wanneer van kracht:

- 27 december 2022 NIS II gepubliceerd in OJ.
- Consultatie Q1 2024
- **18 oktober 2024** nationale wetgeving van kracht.
  (voormalig WBNI)

Handvatten voor compliance:

- DTC website
- ISO 27001
- IEC 62443

Eisen (zorgplicht)
a) beleid inzake risicoanalyse en beveiliging van informatiesystemen;
b) incidentenbehandeling;
c. Bedrijfscontinuïteit
d. Beveiliging toeleveringsketen
e. Beveiliging verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen
f. Beleid en procedures t.b.v. beoordelen effectiviteit van maatregelen
g. Basispraktijken cyberhygiëne en opleiding
h. Beleid en procedures m.b.t. cryptografie
i. Beveiligingsaspecten personeel, toegangsbeleid en beheer van activa
j. Authenticatieoplossingen en noodcommunicatie

Selectie van regelgevingen & richtlijnen voor producten

MDR

KIWA

MID

RED

PED

MED

ATEX

Radio apparaten richtlijn 2014/54/EU (RED)

- **RED essentiële eisen**
  - Artikel 3.1a gezondheid & veiligheid
  - Artikel 3.1b EMC
  - Artikel 3.2 RF (efficient en effectief gebruik van het radio spectrum)

  - **Artikel 3.3 d: bescherming van netwerken**
  - **Artikel 3.3 e: bescherming van de persoonsgegevens en de privacy van de gebruiker**
  - **Artikel 3.3 f: bescherming tegen monetaire fraude**

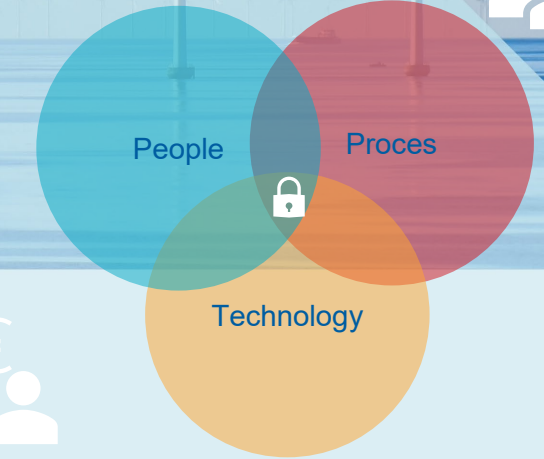

01 Augustus 2025

Hoe blijf je als organisatie cyberweerbaar?

De drie belangrijke pijlers in cyber security in de gehele keten.

Kiwa's aanpak

- Compliance based services
- Risk-based services
- Training




Compliance
based

ISO 27001:2022

INTERNATIONALE NORM

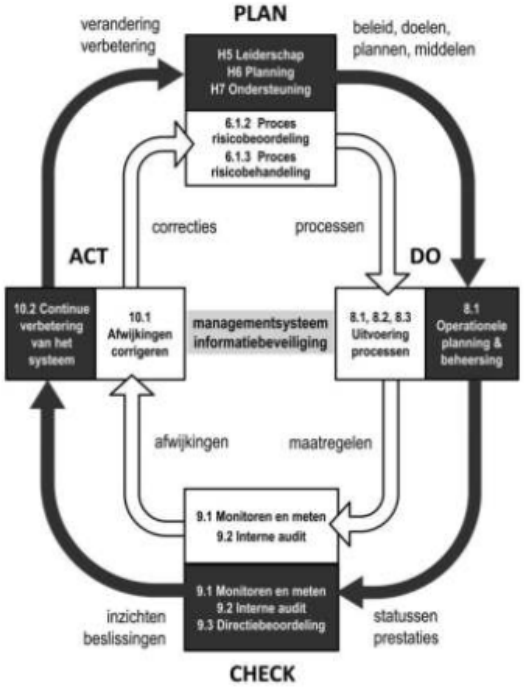
ISO/IEC 27001 (nl)

Derde editie
2022-10

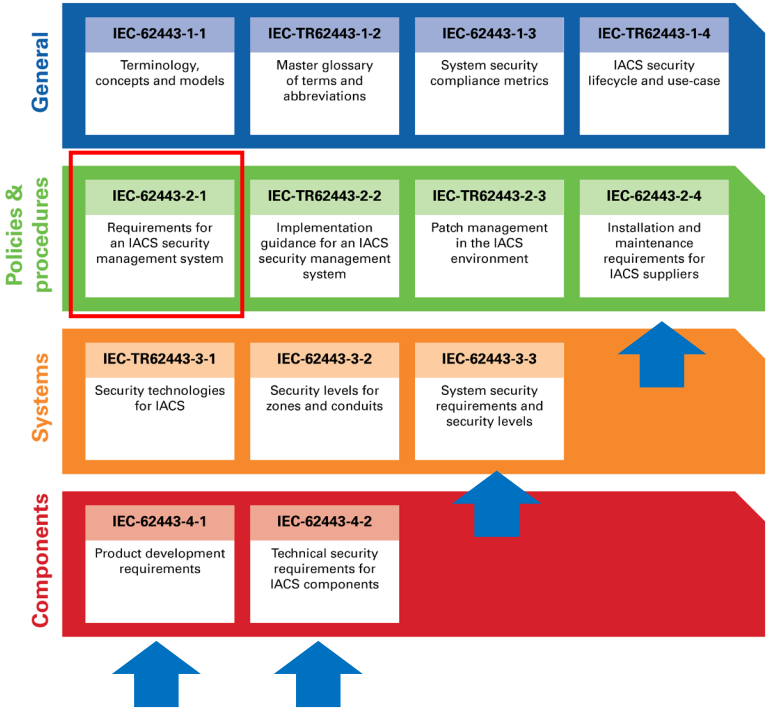
Informatiebeveiliging, cybersecurity en bescherming van de privacy – Managementsysteem voor informatiebeveiliging – Eisen

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences



IEC 62443 in de keten




Risk
Based

Penetratietesten

Penetratie testen

Gesimuleerde cyberaanval door ethische hackers.

Opzoek naar zwakheden in, people, processes & technology van een gehele organisatie.

1. Organisaties

2. Systemen & applicaties

Het vooral technisch beoordelen van applicaties, websites & systemen.

Penetratietesten met ethische hackers


Training

AVG, ISO 27001 & zorg specifieke training

Klassikaal
1 dag

Basiscursus ISO 27001: leg de basis voor structurele Informatiebeveiliging

In onze samenleving draait het steeds meer om data. In deze basiscursus ISO 27001 leer je alles wat nodig is om waardevolle bedrijfsdata structureel op een goede manier te beveiligen.

Lees meer →

Klassikaal
1 dag

Basiscursus NEN 7510: informatiebeveiliging in de zorg (ééndaagse)

In deze ééndaagse cursus maken we u vertrouwd met de NEN 7510, de Nederlandse standaard voor informatiebeveiliging in de zorg. U krijgt inzicht in het belang van...

Lees meer →

Klassikaal
1 dag

Werksessie: Aan de slag met de ISO 27001:2022

In de werksessie 'Aan de slag met de ISO 27001:2022' leren deelnemers alles over de wijzigingen in de ISO 27001:2022 en de vernieuwde beheersmaatregelen uit bijlage A van de norm. Zij...

Lees meer →

Klassikaal
1 dag

Praktische training AVG: Slim onderweg met de AVG

In de training 'Slim onderweg met de AVG' staat de praktische toepassing van de AVG centraal. Er is volop ruimte voor interactie, onder meer aan de hand van je eigen praktijkcases en...

Lees meer →

Klassikaal
1 dag

Training Slim onderweg met de AVG in de Zorg

Zorgprofessionals maken in hun dagelijks werk steeds meer gebruik van persoons- en andere informatie. Die gegevens zijn vrijwel altijd vertrouwelijk en dus vallen ook zorginstellingen onder...

Lees meer →

OT specifiek – IEC 62443 & CSIR

IEC 62443 Training "Cybersecurity voor OT"

Cyber Security for Industrial Automation & Control Systems (IACS)

"Take control over your security risks with the IEC 62443"

Er is een sterk groeiende behoefte aan ICS-professionals, die kennis hebben van cybersecurity binnen technische of procesautomatisering omgevingen. Om hierin te voorzien heeft Hudson Cybertec een complete cybersecuritytraining ontwikkeld voor iedereen, die betrokken is bij productie- en procesinstallaties, gebouw gebonden installaties, zoals gebouwbeheersystemen, HVAC, toegangscontrole, CCTV en inbraakbeveiligingssystemen. Deze training is bij uitstek ook interessant voor iedereen die interesse heeft, of betrokken is bij de ontwikkelingen rondom Smart Industry, Industry 4.0, Smart Cities, IoT of IIoT (Industrial Internet of Things).


Quiz

Het wereledwijd aantal cyberincidenten neemt in zijn totaliteit toe?

A. Waar
B. Niet waar.

Het wereledwijd aantal cyberincidenten neemt in zijn totaliteit toe?

A. Waar

B. Niet waar.

Waarom introduceert de Europese comissie de NIS II richtlijn?

A. Om cyberveiligheid van producten en systemen in de EU te garanderen.
B. Om het algemene niveau van cyberbeveiliging in de EU te verhogen.
C. Om organisaties op te zadelen met meer werk en kosten.

Waarom introduceert de Europese comissie de NIS II richtlijn?

A. Om cyberveiligheid van producten en systemen in de EU te garanderen.

B. Om het algemene niveau van cyberbeveiliging in de EU te verhogen.

C. Om organisaties op te zadelen met meer werk en kosten.

Wanneer ik beschik over een ISO 27001 certificaat voldoe ik aan de NIS II directive?

a. Waar
b. Niet waar

Wanneer ik beschik over een ISO 27001 certificaat voldoe ik aan de NIS II directive?

a. Waar

b. Niet waar

Wat kunt u doen om uw organisatie digitaal weerbaarder te maken?*

a. Het uitvoeren van een risico analyse.
b. Het nemen van risico mitigerende organisatorische, technische en proces gerelateerde maatregelen.
c. Een penetratietest laten uitvoeren.
d. Voldoen aan standaarden zoals de IEC 62443 en ISO 27001.

*Er zijn meerdere antwoorden mogelijk

Wat kunt u doen om uw organisatie digitaal weerbaarder te maken?

a. Het uitvoeren van een risico analyse.
b. Het nemen van risico mitigerende organisatorische, technische en proces gerelateerde maatregelen.
c. Een penetratietest laten uitvoeren.
d. Voldoen aan standaarden zoals de IEC 62443 en ISO 27001.

Meer weten?

Michael Theuerzeit
Lead consultant
Cyber security
Hudson Cybertec B.V. (a kiwa company)

Let’s connect!