OpenNovations

Navigeren door cybersecurity compliance

Hans de Raad, Brenno de Winter

De Winter Information Solutions

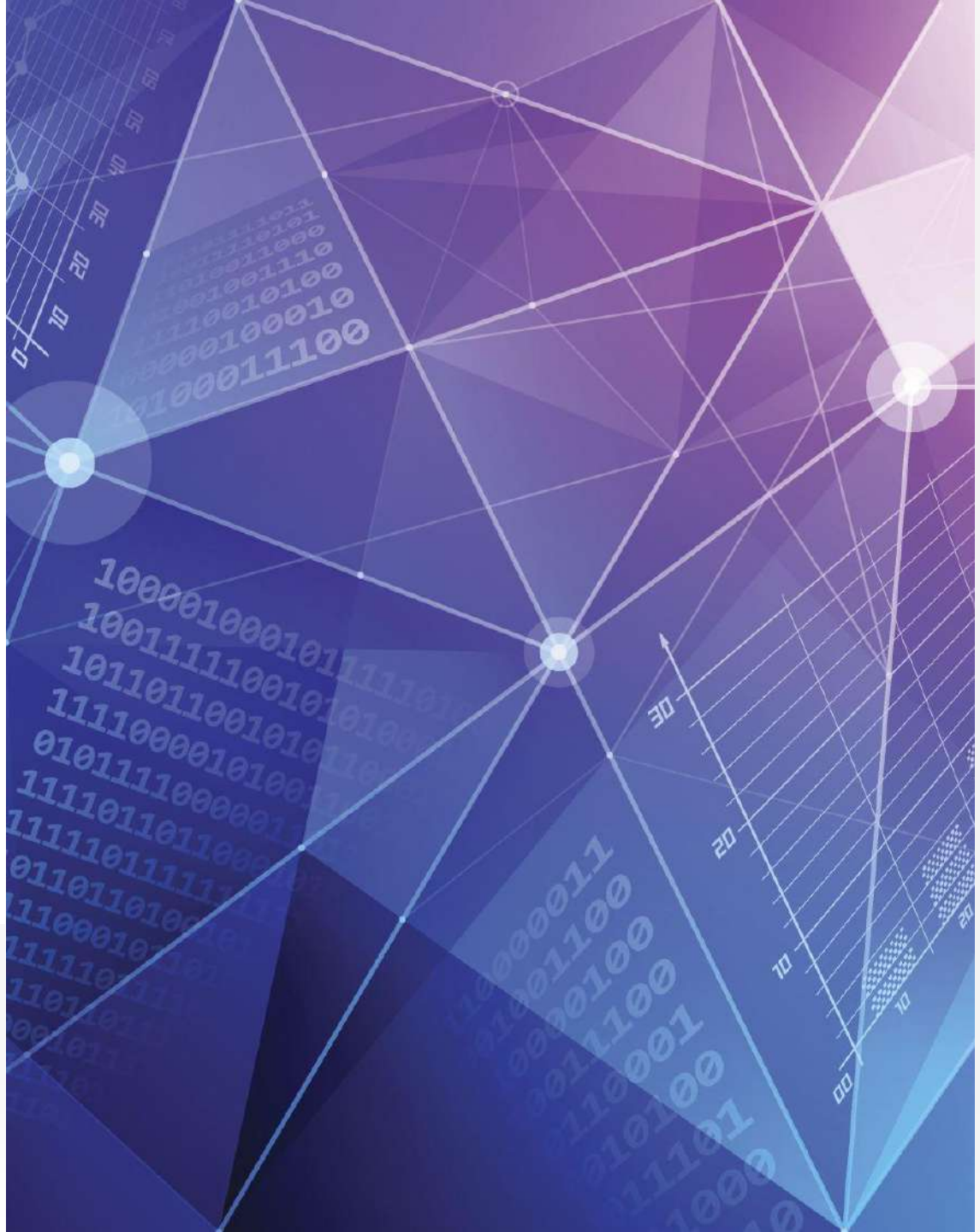
Welkomstwoord en introductie

- Welkom deelnemers
- Introductie van sprekers:
- Hans de Raad, OpenNovations, DARQA / RQA, ETSI
- Brenno de Winter, cybersecurity expert, voormalig lid Rijksbrede NIS2 werkgroep, geestelijk vader OpenKAT en MIAUW
- Doel van de sessie: Inzicht geven in de belangrijkste principes en nieuwste regelgeving op het gebied van cyberbeveiliging, en hoe geavanceerde beveiligingstools kunnen worden ingezet voor compliance.

De Winter Information Solutions

OpenNovations

Sectie 1: Overzicht van Cybersecurity Normen en Regelgeving



De Winter Information Solutions

OpenNovations

Wat Europa aan het doen is

- Risicogebaseerde aanpak
- Er moeten echte stappen worden gezet (aantonen dat je in control bent)
- Geen ruimte voor magie
- Klaar met eigen bs standaarden van 1 bedrijf
- De onderneming bewijst dat ze in control zijn

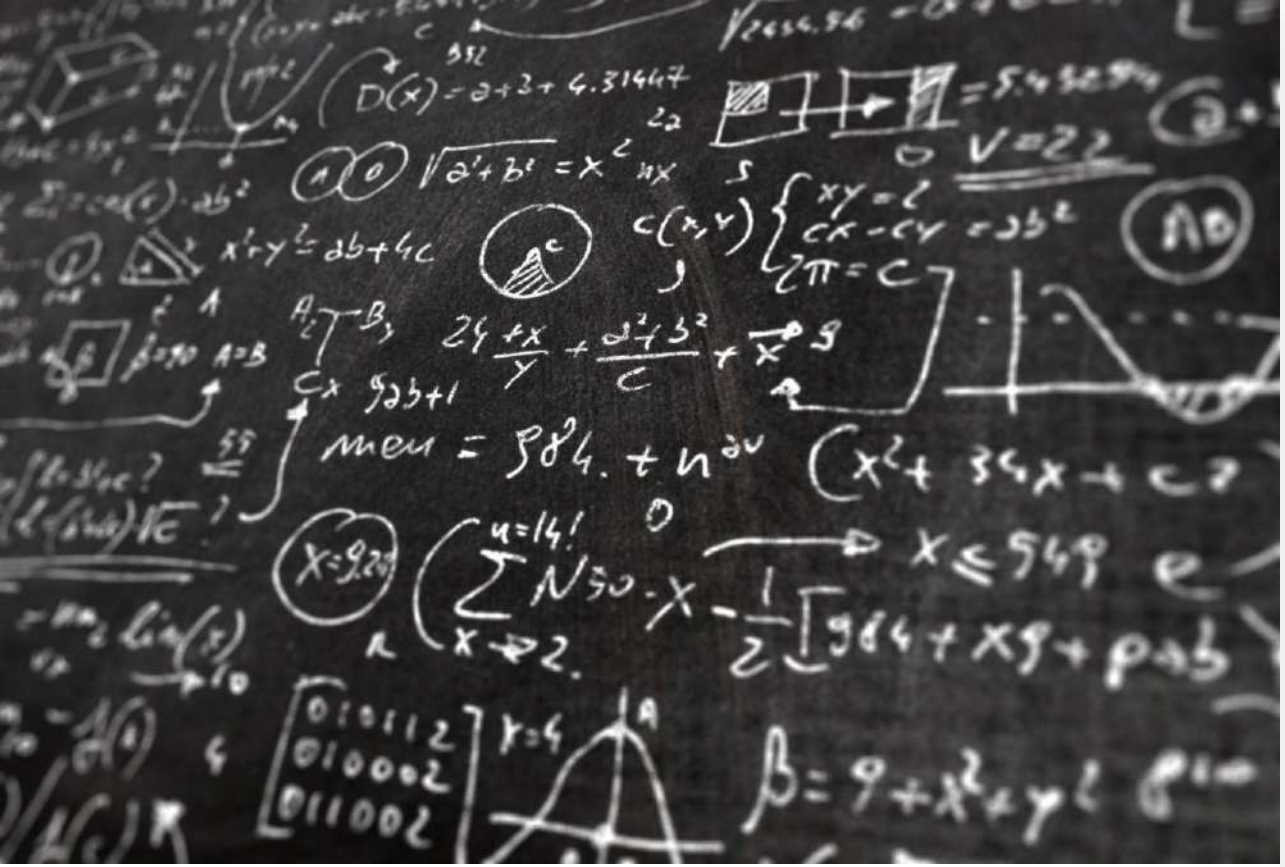
De Winter Information Solutions

OpenNovations

ISO 27001 en NEN7510

De Winter Information Solutions

OpenNovations



Kernprincipes van ISO 27001

- Risicomanagement: ISO 27001 benadrukt het belang van een systematisch risicobeheerproces om informatiebeveiligingsrisico's te identificeren, evalueren en beheersen.
- Beleidsvorming en Organisatie: Het vereist de vaststelling van een duidelijk informatiebeveiligingsbeleid en het definiëren van rollen en verantwoordelijkheden binnen de organisatie.

De Winter Information Solutions

OpenNovations

Kernprincipes van ISO 27001 (2)

- Continue Verbetering: ISO 27001 moedigt aan om de informatiebeveiligingsmaatregelen voortdurend te monitoren, evalueren en verbeteren om nieuwe bedreigingen en kwetsbaarheden aan te pakken.
- Documentatie en Controle: Het vereist gedetailleerde documentatie van alle processen en controles die binnen het informatiebeveiligingsmanagementsyst eem (ISMS) worden geïmplementeerd.

Implementatie van NEN7510 in de Gezondheidszorg

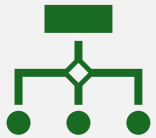
- Bescherming van Patiëntgegevens: NEN7510 richt zich specifiek op het beschermen van persoonlijke gezondheidsinformatie en het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van deze gegevens.
- Veiligheidsbeleid en -procedures: Het stelt dat zorginstellingen duidelijke veiligheidsbeleid en -procedures moeten hebben om te voldoen aan de wettelijke en reglementaire vereisten.

Implementatie van NEN7510 in de Gezondheidszorg (2)

- Bewustzijn en Training: Implementatie van NEN7510 vereist regelmatige training en bewustzijnsprogramma's voor medewerkers om de beveiligingspraktijken en -procedures te begrijpen en na te leven.
- Technische en Fysieke Maatregelen: Zorginstellingen moeten zowel technische als fysieke beveiligingsmaatregelen implementeren, zoals toegangscontroles, encryptie en beveiligde netwerkomgevingen.

Nieuwe Horizonten: ISO 18974

Wat is ISO 18974?



Raamwerk voor het opzetten en onderhouden van een beveiligingsprogramma voor open source software.

Belangrijke veranderingen en impact op organisaties

Europese Wetgeving: EU Cyber Resilience Act, Cybersecurity Act en NIS2

De Winter Information Solutions

OpenNovations

EU Cyber Resilience Act

Doel en Reikwijdte:

Richt zich op het versterken van de cyberweerbaarheid van producten met digitale elementen in de EU.

Biedt een kader voor het verbeteren van beveiligingsmaatregelen gedurende de gehele levenscyclus van een product.

Verplichtingen voor Fabrikanten:

Fabrikanten moeten zorgen voor robuuste beveiligingsmaatregelen en regelmatige updates om kwetsbaarheden te verhelpen.

Verplicht om veiligheidsincidenten te melden aan de relevante autoriteiten binnen vastgestelde termijnen.

EU Cyber Resilience Act

- Doel en Reikwijdte:
  - Richt zich op het versterken van de cyberweerbaarheid van producten met digitale elementen in de EU.
  - Biedt een kader voor het verbeteren van beveiligingsmaatregelen gedurende de gehele levenscyclus van een product.
- Verplichtingen voor Fabrikanten:
  - Fabrikanten moeten zorgen voor robuuste beveiligingsmaatregelen en regelmatige updates om kwetsbaarheden te verhelpen.
  - Verplicht om veiligheidsincidenten te melden aan de relevante autoriteiten binnen vastgestelde termijnen.

EU Cyber Resilience Act (2)

Certificering en Conformiteit:

Introduceert verplichte certificeringsprogramma's voor kritieke producten en diensten.

Certificeringen moeten aantonen dat producten voldoen aan de EU-beveiligingsnormen.

Handhaving en Sancties:

Strenge handhavingsmechanismen en zware sancties voor niet-naleving van de wetgeving.

Samenwerking tussen nationale en EU-autoriteiten voor effectieve handhaving.

Cybersecurity Act

Versterking van ENISA:

De Europese Cybersecurity Act versterkt de rol van het EU Agentschap voor Cybersecurity (ENISA).

ENISA krijgt meer middelen en verantwoordelijkheden om cyberdreigingen te bestrijden.

Europese Cybersecurity Certificering:

Introduceert een Europees kader voor cybersecurity certificering van producten, processen en diensten.

Certificering moet zorgen voor vertrouwen in de digitale markt binnen de EU.

Cybersecurity Act (2)

Harmonisatie van Beveiligingsnormen:

- De wet streeft naar harmonisatie van beveiligingsnormen over de hele EU.
- Beoogt het creëren van een uniforme markt voor cybersecurity producten en diensten.

Beveiliging van Kritieke Infrastructuur:

- Specifieke aandacht voor de beveiliging van kritieke infrastructuur zoals energie, transport, en gezondheidszorg.
- Verplichte risicobeheermaatregelen en incidentmeldingen voor operators van essentiële diensten.

NIS2: Verantwoordelijkheden en Vereisten

Uitgebreide Toepassingsgebied:

NIS2 breidt het toepassingsgebied uit naar meer sectoren en entiteiten, waaronder openbare administraties en aanbieders van digitale diensten.

Strengere beveiligingsvereisten voor deze entiteiten om cyberweerbaarheid te verbeteren.

Versterkte Risicobeheervereisten:

Verplichting voor organisaties om uitgebreide risicobeheerpraktijken te implementeren.

Periodieke beoordelingen en audits van cybersecurity maatregelen vereist.

NIS2: Verantwoordelijkheden en Vereisten (2)

Incidentmeldingsverplichtingen:

Strikte verplichtingen voor het melden van significante incidenten aan nationale bevoegde autoriteiten.

Rapportage moet snel en gedetailleerd zijn om de respons op cyberdreigingen te verbeteren.

Samenwerking en Informatie-uitwisseling:

Bevordert samenwerking en informatie-uitwisseling tussen EU-lidstaten en relevante instanties.

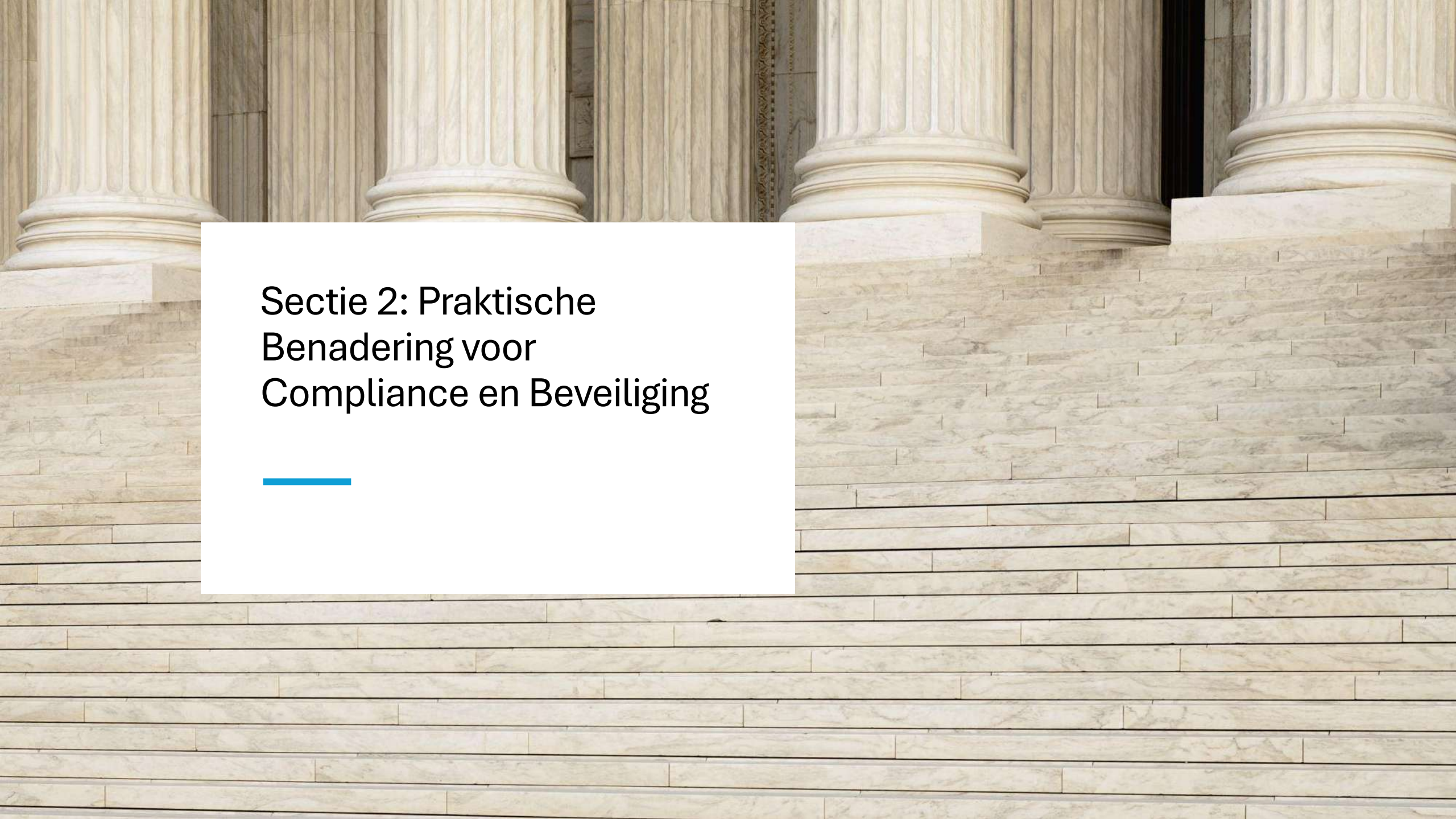
Oprichting van een EU-brede samenwerking groep voor cyberveiligheid om best practices te delen en gezamenlijke bedreigingen aan te pakken.

De Winter Information Solutions

OpenNovations

Tien maatregelen uit de NIS2

- Een risicoanalyse en beveiliging van informatiesystemen
- Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van assets
- Maatregelen op het gebied van bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen
- Incidentenbehandeling
- Basis cyberhygiëne en trainingen op het gebied van cyberbeveiliging
- Beveiliging bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen, inclusief de respons op en bekendmaking van kwetsbaarheden
- Beveiliging van de toeleverancierssketen
- Beleid en procedures over het gebruik van cryptografie en encryptie
- Het gebruik van multifactorauthenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen
- Beleid en procedures om de effectiviteit van beheersmaatregelen van cyberbeveiligingsrisico's te beoordelen



Sectie 2: Praktische Benadering voor Compliance en Beveiliging

Inventarisbeheer van Bedrijfs “assets”

- Gedetailleerde Inventarisatie: Zorg voor een uitgebreide inventaris van alle bedrijfsmiddelen binnen de organisatie, inclusief hardware, software, en netwerkapparatuur.
- Gebruik van Discovery Tools: Maak gebruik van actieve discovery tools om alle bedrijfsmiddelen binnen de organisatie te identificeren en bij te houden.
- DHCP-Logging: Gebruik DHCP-logging om de inventaris van bedrijfsmiddelen automatisch bij te werken en zo real-time zichtbaarheid te behouden.
- Regelmatige Updates: Voer regelmatige controles en updates uit van de inventaris om ervoor te zorgen dat deze altijd up-to-date is en alle veranderingen binnen de infrastructuur weerspiegelt.

De Winter Information Solutions

OpenNovations

Gegevensbescherming

- Firewalls en VPN’s: Implementeer firewalls en virtual private networks (VPN’s) om de gegevens binnen het netwerk te beschermen tegen ongeautoriseerde toegang.
- Authenticatie en Autorisatie: Gebruik sterke authenticatie- en autorisatiemechanismen om de toegang tot gevoelige gegevens te beheren en te controleren.
- Access Control Lists (ACLs): Pas access control lists (ACLs) toe om te bepalen wie toegang heeft tot welke gegevens en om ongeautoriseerde toegang te voorkomen.
- Intrusion Detection Systems (IDS): Implementeer intrusion detection systems om verdachte activiteiten binnen het netwerk te detecteren en hierop te reageren.
- Versleuteling van Gegevens: Implementatie van sterke encryptieprotocollen voor gegevensoverdracht en -opslag om de vertrouwelijkheid en integriteit van gevoelige informatie te beschermen.

De Winter Information Solutions

OpenNovations

Beveiligde Configuratie van Software

- Veilige Configuratieprocessen: Stel een formeel proces in voor de configuratie van alle bedrijfsmiddelen en software, waarbij security een prioriteit is.
- Automatische Sessievergrendeling: Configureer automatische sessievergrendeling op alle bedrijfsmiddelen om ongeautoriseerde toegang tijdens inactiviteit te voorkomen.
- Firewallbeheer op Servers: Implementeer en beheer firewalls op servers om inkomend en uitgaand netwerkverkeer te reguleren en te beschermen.
- Regelmatige Beoordelingen en Updates: Voer regelmatige beoordelingen en updates van de configuraties uit om nieuwe kwetsbaarheden aan te pakken en de beveiliging te verbeteren.

De Winter Information Solutions

OpenNovations

Accountbeheer

- Proces voor Gebruikersaccountbeheer: Stel een duidelijk proces in voor het beheren van gebruikersaccounts, inclusief het aanmaken, wijzigen en deactiveren van accounts.
- Sterke Wachtwoordbeleid: Implementeer een sterk wachtwoordbeleid dat vereist dat gebruikers complexe wachtwoorden gebruiken en deze regelmatig veranderen.
- Multi-factor Authenticatie: Gebruik multi-factor authenticatie om een extra beveiligingslaag toe te voegen voor de toegang tot kritieke systemen en gegevens.
- Regelmatige Accountreviews: Voer regelmatige reviews van gebruikersaccounts uit om te controleren op ongeautoriseerde of inactieve accounts en deze te verwijderen of bij te werken.

De Winter Information Solutions

OpenNovations

Toegangsbeheer

Rolgebaseerde Toegangscontrole (RBAC)

- Definitie: Toegangsrechten worden toegekend op basis van de rollen die gebruikers binnen een organisatie vervullen.
- Doel: Vereenvoudigt het beheer van toegangsrechten door rechten toe te kennen aan rollen in plaats van aan individuele gebruikers.

Kenmerkgebaseerde Toegangscontrole (ABAC)

- Definitie: Toegangsbeslissingen worden gebaseerd op een combinatie van attributen van de gebruiker, het systeem, de omgeving en de acties die worden uitgevoerd.
- Doel: Biedt fijnmazige controle over toegangsrechten door het gebruik van meerdere attributen in toegangsbeslissingen.

Discretionaire Toegangscontrole (DAC)

- Definitie: De eigenaar van de gegevens bepaalt wie toegang heeft tot zijn of haar gegevens en kan deze rechten aan anderen delegeren.
- Doel: Geeft gebruikers meer controle over hun eigen gegevens en wie daar toegang toe heeft.

Continu monitoren van Kwetsbaarheden

Proces voor kwetsbaarhedenbeheer en remediering

Anti-malware software

Incidentresponsplan: Een gedetailleerd incidentresponsplan om snel en effectief te reageren op beveiligingsincidenten, inclusief regelmatige testen en oefeningen om de effectiviteit te waarborgen.

Periodieke Risicobeoordelingen: Uitvoeren van regelmatige risicobeoordelingen en penetratietesten om potentiële kwetsbaarheden te identificeren en proactief maatregelen te nemen om deze aan te pakken.

De Winter Information Solutions

OpenNovations

Beheer van Auditlogs

Noodzaak van Auditlogs:

Auditlogs zijn essentieel voor het monitoren en registreren van gebeurtenissen binnen IT-systemen. Ze helpen bij het opsporen van ongeautoriseerde toegang en mogelijke beveiligingsinbreuken.

Ze dienen als bewijs voor naleving van wettelijke en regelgevende vereisten, zoals GDPR en ISO-normen.

Bewaren en Beheren van Logs:

Auditlogs moeten veilig worden bewaard en beschermd tegen onbevoegde toegang en manipulatie.

Logs moeten gedurende een bepaalde periode worden bewaard om te voldoen aan de wettelijke vereisten en om historische analyses mogelijk te maken.

Proces voor Auditlogbeheer

Loggeneratie en -verzameling:

- Definieer welke gebeurtenissen en activiteiten moeten worden vastgelegd. Dit omvat gebruikersactiviteiten, systeemgebeurtenissen en beveiligingsincidenten.
- Gebruik geautomatiseerde tools en systemen om loggegevens te verzamelen en te consolideren vanuit verschillende bronnen.

Bewaking en Analyse:

- Voer continue monitoring en analyse van auditlogs uit om verdachte activiteiten snel te detecteren en hierop te reageren.
- Gebruik SIEM (Security Information and Event Management) systemen om loggegevens te correleren en inzicht te krijgen in potentiële bedreigingen.

Proces voor Auditlogbeheer (2)

Beveiliging van Auditlogs:

Implementeer maatregelen om de integriteit en vertrouwelijkheid van auditlogs te waarborgen, zoals encryptie en toegangscontrole.

Zorg ervoor dat alleen geautoriseerde personen toegang hebben tot de auditlogs en dat alle toegangspogingen worden geregistreerd.

Periodieke Review en Rapportage:

Voer regelmatige reviews uit van de auditlogbeheerprocessen om ervoor te zorgen dat ze effectief blijven en voldoen aan veranderende beveiligings- en nalevingseisen.

Documenteer en rapporteer bevindingen uit de auditloganalyses aan relevante belanghebbenden en gebruik deze informatie om het beveiligingsbeleid te verbeteren.

Verzameling van Gebeurtenissen

Identificatie van Kritieke Gebeurtenissen:

Bepaal welke gebeurtenissen als kritieke veiligheidsincidenten moeten worden beschouwd, zoals inlogpogingen, wijzigingen in toegangsrechten, en systeemfouten.

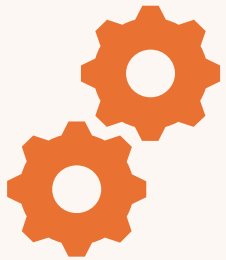
Zorg ervoor dat deze gebeurtenissen consistent en nauwkeurig worden vastgelegd.

Gebruik van Standaarden en Best Practices:

Volg industriestandaarden en best practices voor het verzamelen van loggegevens, zoals het gebruik van gestandaardiseerde formaten en protocollen.

Dit vergemakkelijkt de integratie van loggegevens uit verschillende systemen en verhoogt de betrouwbaarheid van de gegevens.

Verzameling van Gebeurtenissen (2)



Automatisering en Efficiëntie:

Maak gebruik van geautomatiseerde tools om het proces van logverzameling te stroomlijnen en te zorgen voor real-time gegevensverzameling.

Automatiseer ook het proces van logbeheer om fouten te minimaliseren en de efficiëntie te verbeteren.

Compliance en Verantwoording:

Zorg ervoor dat de verzameling van gebeurtenissen voldoet aan de wettelijke en regelgevende vereisten, zoals GDPR en andere relevante regelgeving.

Houd gedetailleerde documentatie bij van alle verzamelde loggegevens en de bijbehorende beheersprocessen om naleving aan te tonen tijdens audits.

Sectie 3: Praktische Casussen en Voorbeelden

De Winter Information Solutions

OpenNovations

Casus: Pentesting en Incidenten

- Voorbeeld: Hof van Twente ransomware aanval
- Analyse van pentesting-methoden en tekortkomingen

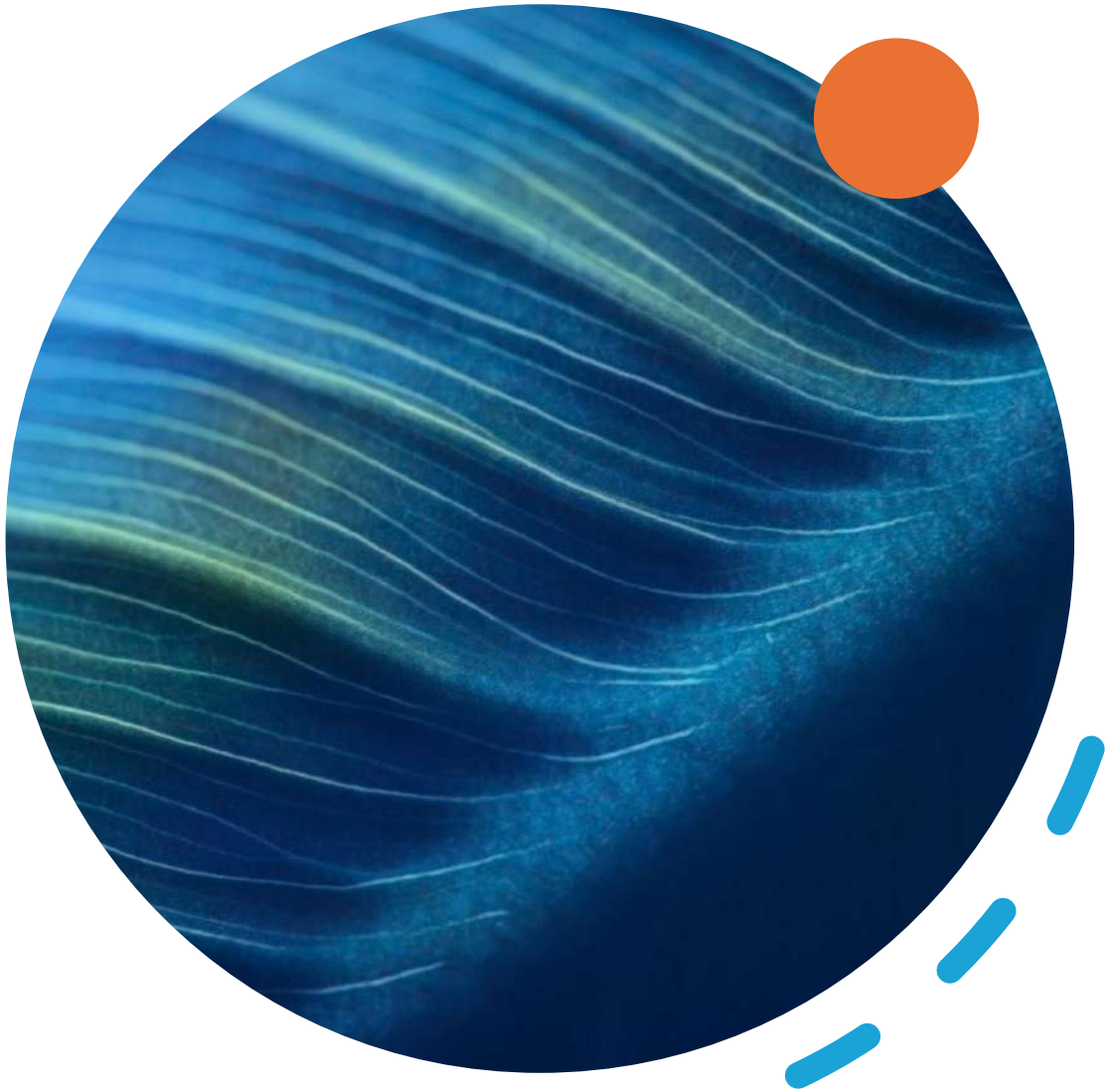
De Winter Information Solutions

OpenNovations

Casus: Corona-technologie

Privacy-first ontwerp en beveiligingsprincipes

Verificatie- en validatieprocessen



De Winter Information Solutions

OpenNovations

Coronamelder: privacy first, security first

Design

- Decentraal systeem
- Geen informatie vragen aan gebruikers
- Strakke retentie
- Zo moeilijk mogelijk te linken aan persoon
- Geen herleidbaar naar apparaat
- Alleen noodzakelijke data
- Alleen data doorgeven na verificaties
- App ziet geen codes

Gevalideerd

- Doelbinding in de wet
- Strafbepaling
- Geen statistieken feest
- Cryptografisch correct (alles signen)
- Geen back-ups maken
- Detecteren op misbruik

De Winter Information Solutions

OpenNovations

Hoe het vaak gaat:
de Magie van de Penetratietest

- Hoe we het doen is magie
- Wat we doen is bedrijfsgeheim
- Wat we opleveren mag je niet zomaar verspreiden
- En aan onze testen kun je geen rechten ontlenen

De Winter Information Solutions

OpenNovations

Over magie gesproken

Magie of toverij is de vermeende kunst van het manipuleren van de werkelijkheid met behulp van speciale objecten, spreuken en rituelen op basis van verborgen krachten. Berust op 3 pijlers:

1. Magiërs, de specialisten met een speciale status.
2. Magische handelingen: in de traditie gewortelde rituelen en daarmee verbonden voorschriften en symbolen.
3. Handelingen van de magiër overeenstemmend met magische voorstellingen van de werkelijkheid, de ideeën en geloofsovertuigingen.

En vaak is dit de realiteit

rijfsauto's
t

Bedrijfsauto's
zwaar

Driewielige
motorrijtuigen

Aanhangwagens

Landbou
bosbouw

Uniform pentesten

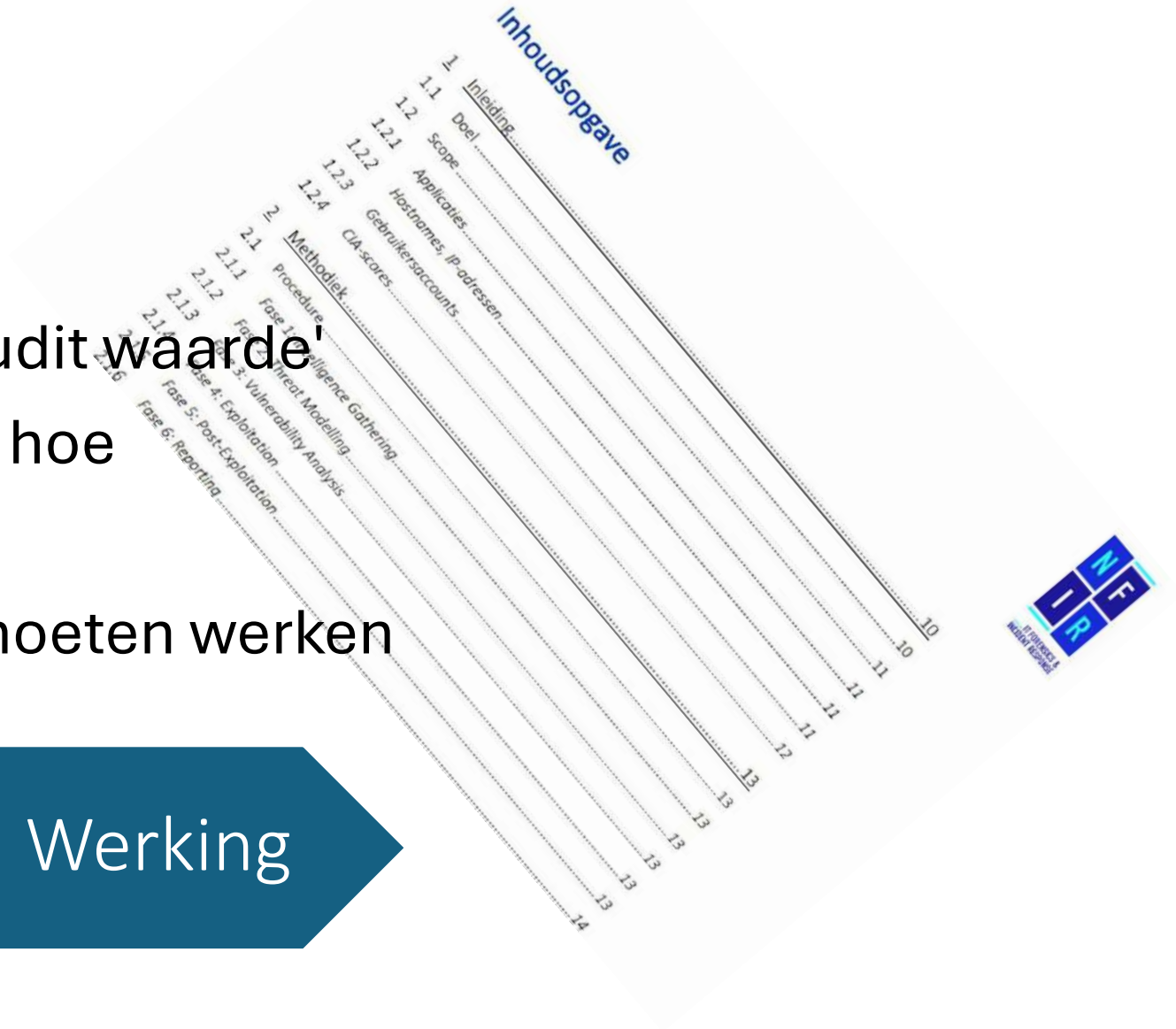
- Uniforme eisen voor inkoop van pentesten
- Alle bevindingen langs dezelfde meetlat (CVSS)
- Een minimale set aan eisen:
  - OWASP TOP-10
  - MSTG/WSTG
  - CIS
- Uniforme manier van presenteren van bevindingen: PTES
- Reproduceerbaarheid van het onderzoek
- Het rapport wordt openbaar

De Winter Information Solutions

OpenNovations

Andere aanpak

- Pentest als container begrip met 'audit waarde'
- Bewijzen wat je hebt onderzocht en hoe
- Inkoopeisen
- Standaard hoe documentatie zou moeten werken



Opzet → Bestaan → Werking

De Winter Information Solutions

OpenNovations

Later … toen een aanbieder van coronatests werd gehacked

rtlnieuws

RTL Nieuws
Tip ons

Nieuws Economie Sport Entertainment Tech Lifestyle EditieNL Uitzendingen

11° 0 files • 0 km 8 OV

CoronaCheck-app

ALLE 47 ARTIKELEN

EXCLUSIEF

Groot lek testbedrijf: iedereen kon valse toegangsbewijzen in app CoronaCheck krijgen

18 juli 2021 10:14
Aangepast: 20 juli 2021 14:28

De Winter Information Solutions

OpenNovations

Aansprakelijkheden bij gebruik software

- Artikel 82 AVG, eerste lid
  - Eenieder die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk op deze verordening, heeft het recht om van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen voor de geleden schade.
- Artikel 82 AVG, derde lid
  - Een verwerkingsverantwoordelijke of verwerker wordt van aansprakelijkheid op grond van lid 2 vrijgesteld indien hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit.

Bij ons is alles veilig!

- 'We hebben hackers laten kijken'
- 'We laten ons inspireren door de standaarden'
- Wat onze mensen doen is magie
- Wat een pentest is, tja dat is wat wij doen!
- Ze kwam er niet doorheen
- Zelfs hackers kregen het niet stuk

De Winter Information Solutions

OpenNovations


Zes maanden later ...

Hof van Twente

- 1 december 2020 – boodschappen op scherm, veel VM's niet bereikbaar
- Mei/Juni 2020 was een infrastructuur pentest uitgevoerd
- Er waren self assessments voor DigiD uitgevoerd
- Leverancier beheersdiensten doet eerste fasen onderzoek
- Daarna forensisch bureau
- Losgeldclaim: plm. €750.000
- Kosten 'in de miljoenen'
- Veel gemeentelijke diensten niet mogelijk

De Winter Information Solutions

OpenNovations

REGIO ALGEMEEN SPORT VIDEO OPINIE FUN

Switch wil reputatieschade door hack privé verhalen op burgemeester Hof van Twente

HOF VAN TWENTE/ENSCHEDE - Switch IT Solutions in Enschede stelt burgemeester Ellen Nauta van Hof van Twente persoonlijk aansprakelijk voor de reputatieschade die het bedrijf lijdt als gevolg van uitlatingen die Nauta heeft gedaan over de veronderstelde rol van Switch bij de cyberaanval op de systemen van de gemeente in december.

Redactie 28-04-21, 17:44 Laatste update: 29-04-21, 09:06

De leverancier claimt te hebben gewaarschuwd

- Geen risk letters
- Gedeeld user beheer tussen gemeente en leverancier

De Winter Information Solutions

OpenNovations

Maar alles was veilig?

- Mei/Juni 2020 was
  een infrastructuur pentest uitgevoerd
  - Geen signaal dat iets serieus speelde
  - Ging over deels de zaken die bij ransomware speelden
  - Poorten die misbruikt zijn stonden niet open
- Er waren assessments
  voor DigiD uitgevoerd

De Winter Information Solutions

OpenNovations

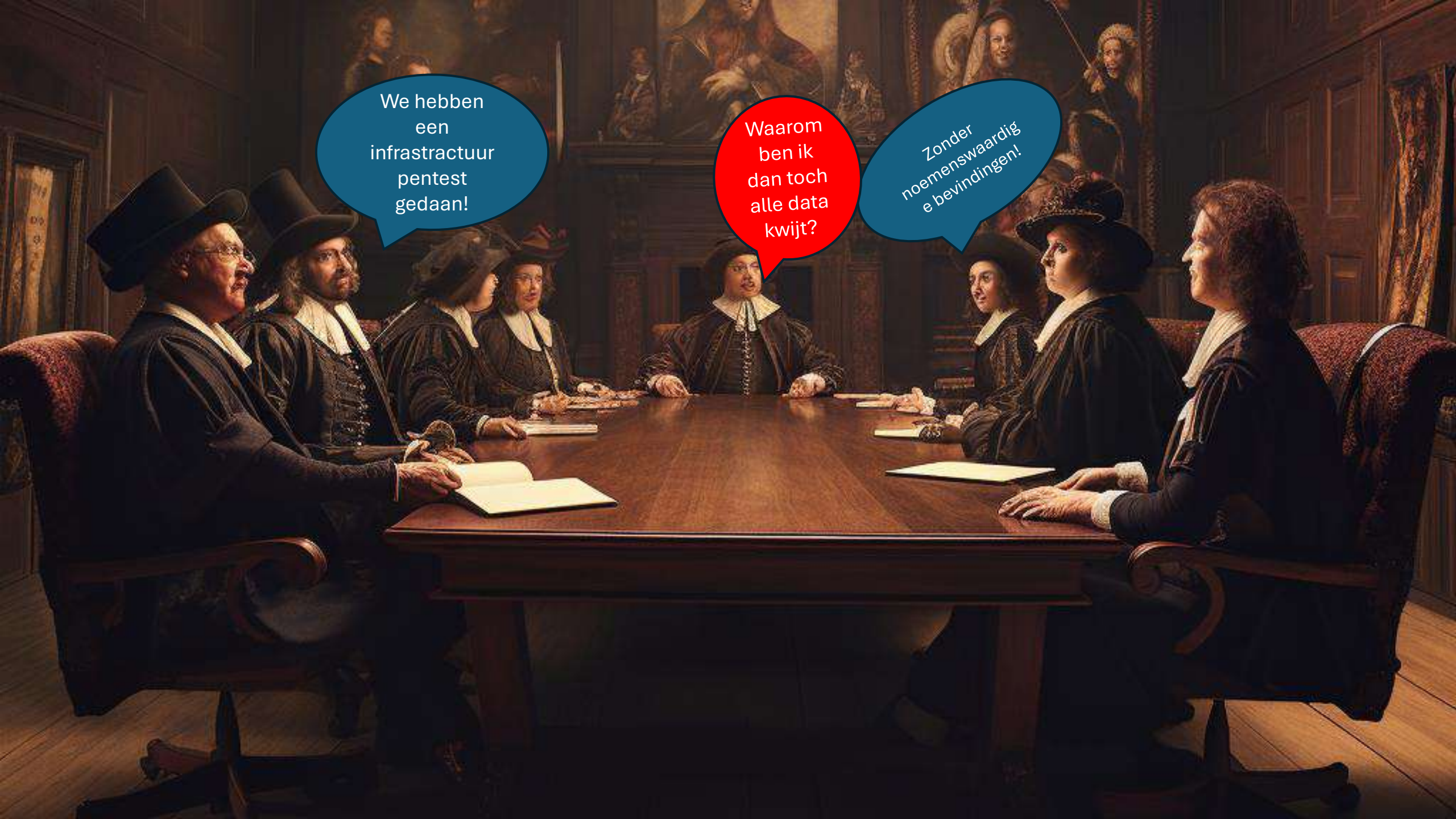
Vraagtekens

- De point of entry op patient zero stond dicht volgens de pentest
  - Of de poort is later open gezet
  - Of de poort was al open
- Via openbare bronnen werd duidelijk dat de poort al open stond
- Waarom staat dit anders in de pentest?
- Onduidelijk wat er nu precies wel of niet is gedaan

Als dit niet klopt, wat klopt dan wel?

De Winter Information Solutions

OpenNovations


We hebben een infrastractuur pentest gedaan!
Waarom ben ik dan toch alle data kwijt?
Zonder noemenswaardig e bevindingen!

Te goed van vertrouwen?

- Professionele beheerspartij
- Geen riskletters van beheerder
- Pentest die er ogenschijnlijk goed uitziet
- DigiD assessments gaven een gerustellend beeld
- Blijven vertrouwen op leverancier
- Raad heeft het over functioneren van de burgemeester

SECURITY

Ophef over pentest bij gemeente Hof van Twente

IT-dienstverlener en pentester zouden niet op orde hebben.

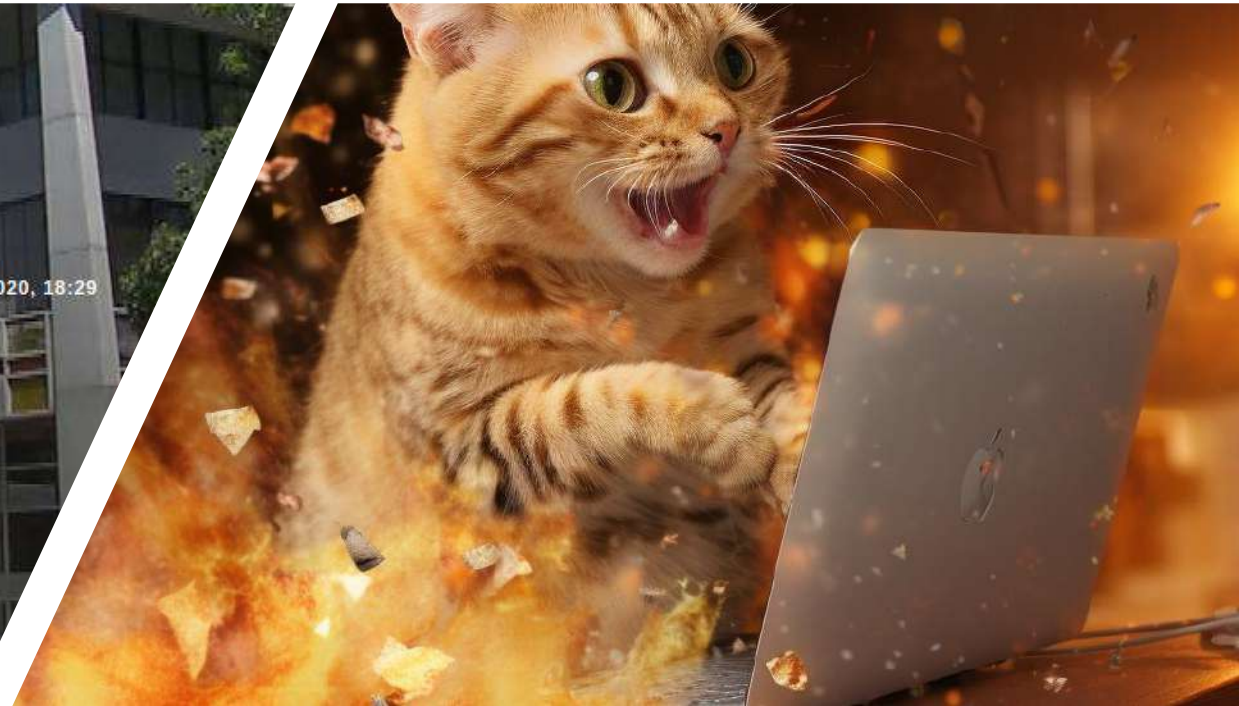
De door ransomware getroffen gemeente Hof van Twente h
forensisch onderzoeksrapport in ontvangst genomen. In he
meerdere misstanden geconstateerd. Waaronder een vor
pentest waarbij een IP-adres zou zijn gemist waarlangs

Hoe grondig is de vereiste pentest voor coronatestbedrijven?

Lek in Testcoronanu had met pentest gevonden moeten worden, maar dat gebeurde niet.

NOS NIEUWS • BINNENLAND • TECH • 06-06-2020, 16:04 • AANGEPAST 06-06-2020, 18:29

Lek in RIVM-coronasite: gegevens van gebruikers makkelijk in te zien



Sectie 4: Implementatie en Best Practices

De Winter Information Solutions

OpenNovations


Compliance is ....

De basis – theorie – denk in risico’s

- C – confidentiality (vertrouwelijkheid – lees niet delen met anderen / systemen)
  - S – security (o.a. electronisch maar ook de kast op slot)
  - P – privacy (o.a. doel beperking, niet naar anderen)
- I – integrity (getrouwheid – juist/nauwkeurig, tijdig, volledig)
- A – availability (beschikbaarheid – in de ogen van de gebruiker)
- *-> beheersing – controls? <-*

De Winter Information Solutions

OpenNovations

Veel EU-regelgeving in tien jaar tijd (tot 2026)

- Artificial Intelligence Act (AIA)
- Artificial Liability Directive (AIL)
- Cyber Security Act (CSA)
- Data Act (DA)
- Digital Markets Act (DMA)
- Digital Operation Resilience Act (DORA)
- Digital Services Act (DSA)
- Directive on liability for defective products
- General Data Protection Regulation (GDPR)
- Network and Information Security Directive 2 (NIS2)
- Radio Equipment Directive
- Resilience of Critical Entities Directive (RCE)

De Winter Information Solutions

OpenNovations

Bonus

Denk aan de jaarrekening

SOC1 vs SOC2

TRANSACTION & SECURITY PROCESSING CONTROLS FOCUS

Essential for revenue software

SECURITY CONTROLS FOCUS

Essential for all service organizations including CLOUD service providers

TYPE 1	TYPE 2	TYPE 1	TYPE 2
• Organization system & controls	• Organization system & controls	• Organization system & controls	• Organization system & controls
• At a specific time point	• Period of time	• At a specific time point	• Period of time
• Key security issues	• Opinion on design & operating effectiveness of controls	• Focus on security	• Opinion on design & operating effectiveness of controls
• Opinion on design of controls			

Denk aan ISO 27001/2

Type 1 – opzet en bestaan

Type 2 – werking

De Winter Information Solutions

OpenNovations

De bredere vraag
Hoe voer je een audit uit?

- **Is dat het toetsen van een claim?**
- **Is het terugkijkend?**
- **Is het vooruitkijkend?**

Waar stuur je op?

De Winter Information Solutions

OpenNovations

Waar kijkt de auditor nou eigenlijk naar?

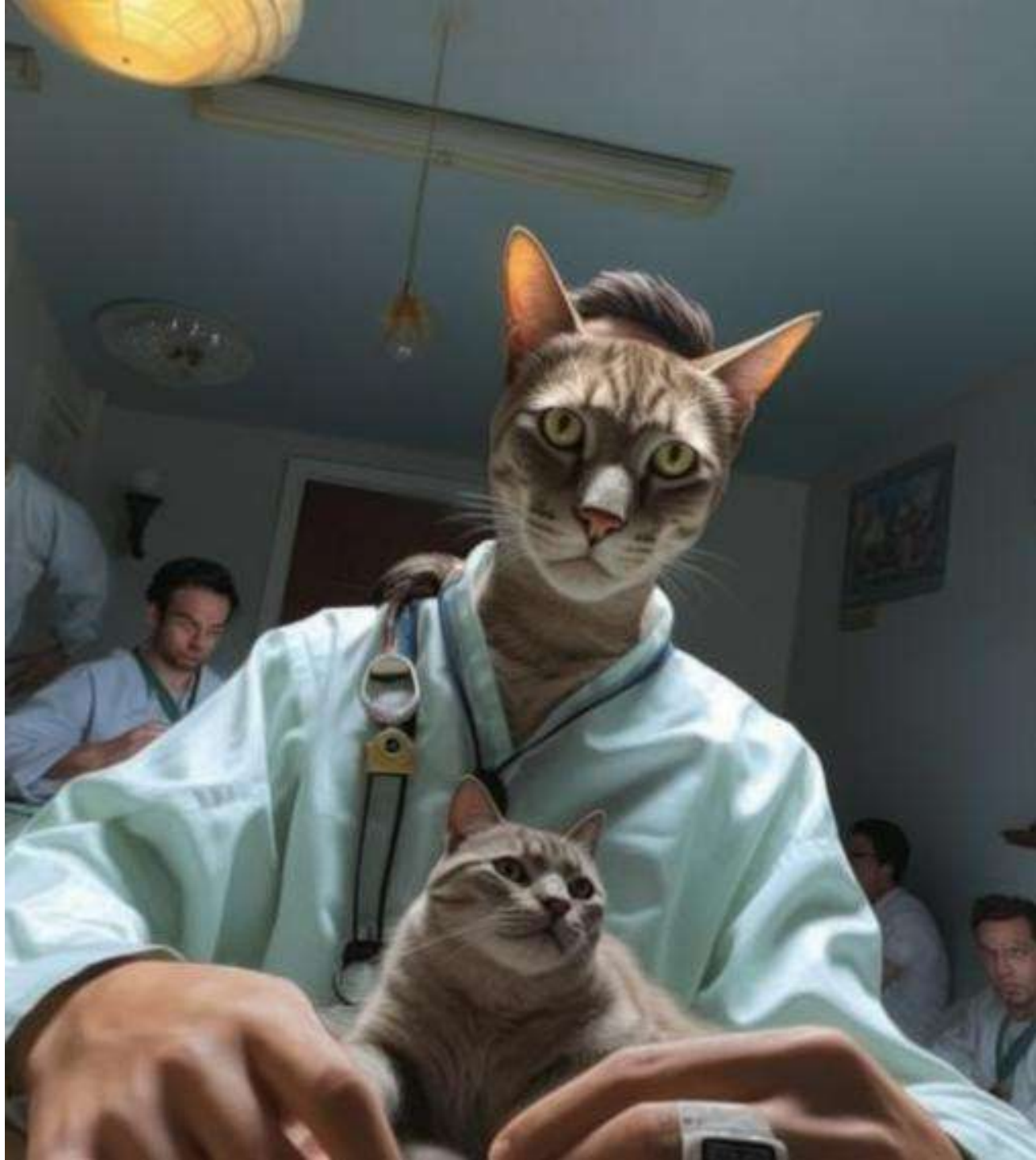
- 'We hebben hackers laten kijken' - geen vastgesteld kennisniveau
- 'We laten ons inspireren door de standaarden' - niet gestandaardiseerde tests
- Wat onze mensen doen is magie – dark magic
- Wat een pentest is, tja dat is wat wij doen! - geen kader

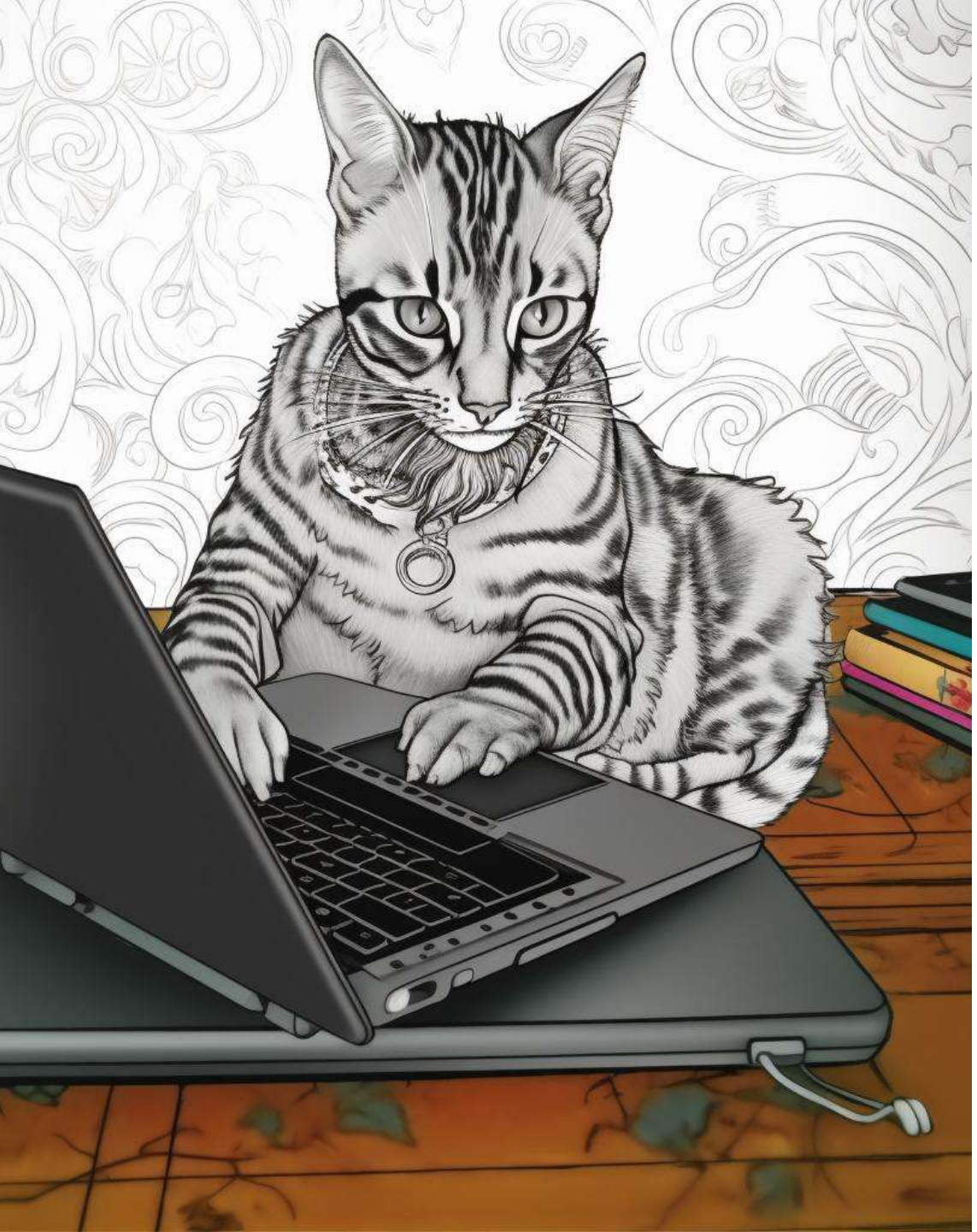
De NIS2 eist meer helderheid

- NIS2 (artikel 32): De lidstaten zorgen ervoor dat de bevoegde autoriteiten bij de uitoefening van hun toezichthoudende taken met betrekking tot essentiële entiteiten de bevoegdheid hebben om deze entiteiten te onderwerpen aan ten minste:
    - (g) **verzoeken om bewijs van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van beveiligingsaudits die door een gekwalificeerde auditor zijn uitgevoerd en de respectieve onderliggende bewijzen.**
- NIS2 (artikel 33): De lidstaten zorgen ervoor dat de bevoegde autoriteiten bij de uitoefening van hun toezichthoudende taken met betrekking tot belangrijke entiteiten de bevoegdheid hebben om deze entiteiten te onderwerpen aan ten minste:
    - (f) verzoeken om bewijs van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van beveiligingsaudits die door een gekwalificeerde auditor zijn uitgevoerd en de respectieve onderliggende bewijzen.

Fixbaar met wat chirurgische ingrepen

- Minder magie
- Meer zekerheid bieden
- Bewijs aanleveren





Duidelijkheid
Definitie pentest

Penetratietest. Een penetratietest (pentest) is “een door eigen personeel of derden uit te voeren **offensief veiligheidsonderzoek**, waarbij **gecontroleerd** wordt gezocht naar kwetsbaarheden in een of meer beveiligde netwerk- en informatiesystemen of onderdelen daarvan, die kunnen worden gebruikt voor **het inbreken** in deze systemen en/of die **zonder opzet en autonoom de gegevensverwerking** van de onderzochte organisatie **kunnen verstoren** of anderszins **nadelige gevolgen** kunnen hebben”.

De 'hacker' … nee … onderzoeker kan dingen

De pentester kan dingen en heeft een relevante certifcering

- OffSec Certified Professional (OSCP)
- OffSec Experienced Pentester (OSEP)
- OffSec Offensive Security Certified Expert (OSCE of OSCE^3)
- OffSec Web Expert (OSWE)
- Web application Penetration Tester eXtreme (eWPTX)

Andere aanpak

- Pentest als container begrip met 'audit waarde'
- Bewijzen wat je hebt onderzocht en hoe
- Inkoopeisen
- Standaard hoe documentatie zou moeten werken

Onderzoeken volgens minimale set aan tests

- Uniforme eisen voor inkoop van pentesten
- Alle bevindingen langs dezelfde meetlat (CVSS) gewogen
- Duidelijke afspraken hoe je bevindingen opschrijft
- Een minimale set aan eisen:
  - OWASP TOP-10
  - MSTG/WSTG
  - CIS Controls (ETSI TR 103 305)
- Uniforme manier van presenteren van bevindingen: PTES
- Reproduceerbaarheid van het onderzoek
- De onderliggende tests worden meegeleverd
- Optioneel: Het rapport moet openbaar kunnen worden

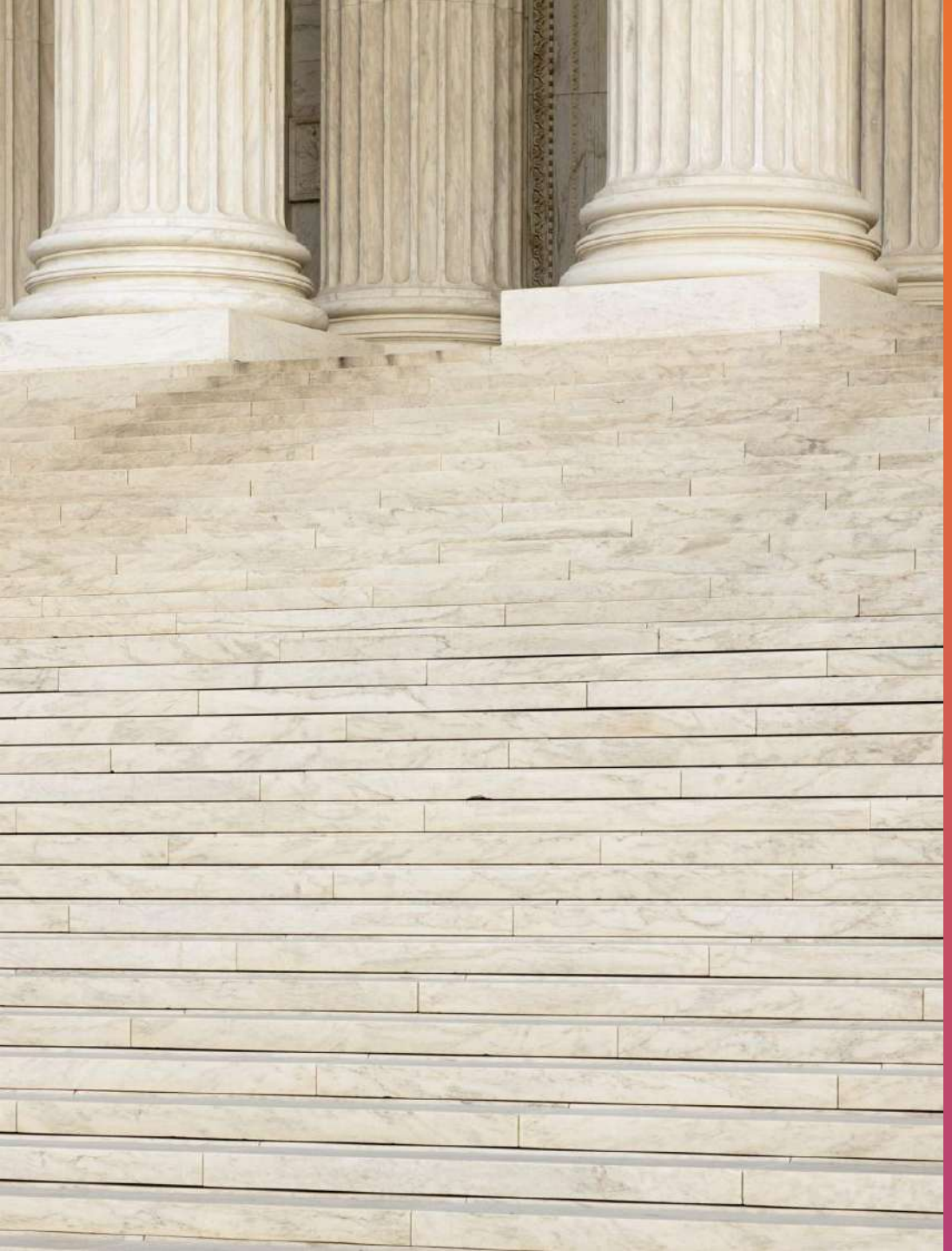
Beveiligingsonderzoeken

- Vulnerabilityscan
- Penetratietest
- Red Teaming
- Code review
- Security Assessment
- Zelf Conformiteitsbeoordeling
- Audit / Conformiteitsbeoordeling

Wat zegt iets over een product?

Informatiebeveiligingsonderzoek (security assessment)	
Security assessment	**Technisch onderzoeken**
Procesbeschrijving met inschaling (BIV)	**Vulnerabilityscan**
Dreigingsanalyse	**Penetratietest**
FMEA – Hoe kan het fout gaan	Code review
Threat modeling	

Methodiek voor informatiebeveiligingsonderzoek met auditwaarde



Compliance en Governance

Allemaal naar het zelfde kijken

- Helderheid wat er is onderzocht
- Helderheid over wat je niet hebt gekregen en wat dat betekent
- Helderheid of het onderzoek daadwerkelijk is uitgevoerd
- Reproduceerbaarheid

Op basis van feiten in control zijn

De Winter Information Solutions

OpenNovations

ANOVUM
ONDERZOEK | STANDAARDEN | KENNISCENTRUM

CONSULTANCY

eset
Digital Security
Progress. Protected.

Mathison
MR.V.A. DE POUS

SECURITY ACADEMY

OWASP®

tex

Innerheight
Internetdiensten BV

OpenNovations

DSEC CONSULTING

pinkroccade
TSS
LOCAL GOVERNMENT

PROTEON

De Winter Informatio n Solutions

Cynalytics

proxy

DIVD

Academy

UNICORN Security

MIAUW

GRÖEN OPLOSSINGEN

ZOLDER
applied security research

ZA CERT

Ministerie van Volksgezondheid, Welzijn en Sport

Rijksdienst voor Identiteitsgegevens
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

There is one more more thing

De Winter Information Solutions

OpenNovations


De Winter
Information
Solutions
OpenNovations

There is one more more thing

De Winter Information Solutions

OpenNovations

branie

Checklist: Checklist voor MIAUW

DEBUG

State: Deze certificeringen bieden een niveau van zekerheid dat de onderzoeker beschikt over een minimaal niveau aan opleiding en deze beschikt over voldoende kennis om een examen te kunnen doorstaan. Dat maakt de onderzoeker een professionele partner voor het onderzoek. De geselecteerde certificeringen zijn gebaseerd op het kwalificatieschema van het [CCV Keurmerk Pentesten](https://hetccv.nl/app/uploads/2023/09/20230921-Kwalificaties-pentester.pdf).

Section: 1, Step: 4

Kun je dit schema

De rapportage levert bewijs van de certificering in de vorm van een link naar een online validatieplatform om de authenticiteit van de geclaimde certificering te valideren of een kopie van het diploma, waardoor andere validatie mogelijk is. Bij digitale documenten is deze link niet aanklikbaar, bij papieren versie hoeft de link aanklikbaar te zijn.

State: Het is niet mogelijk om zekerheid vast te stellen of de door de rapporteur geclaimde competentie daadwerkelijk aanwezig is.

Section: 1, Step: 5

Benoemen van de versie van de rapportage

Er wordt in de sectie 'Over dit document' melding gemaakt van het versienummer van het document.

State: Het is niet mogelijk vast te stellen welke versie van de rapportage is geleverd, waardoor meerdere documenten verwarring kunnen zaaien.

Section: 1, Step: 6

Handtekening voor waarheidsgetrouwe rapportage

De rapportage wordt voorzien van een tekst, waaruit blijkt dat de rapportage:
1. accuraat en naar waarheid is opgesteld;
2. er een kwaliteitsreview op deze versie van het document heeft plaatsgevonden door andere een niet bij het onderzoek betrokken persoon.

Deze tekst voorzien van een handtekening van de rapporteur. Deze handtekening kan een fysiek gezette handtekening zijn of een digitale handtekening

De Winter Information Solutions

OpenNovations

Save Checklist

Share as PDF

Checklist voor MIAUW

Description: De onderzoeksrapportage wordt in digitale vorm verstrekt.

SOP code: (No SOP code)

Si	Title	Description	I	State
1	De onderzoeksrapportage wordt digitaal verstrekt.	De onderzoeksrapportage wordt in digitale vorm verstrekt.	N i	Het maakt het mogelijk in combinatie een digitale hash vast te stellen dat het document niet is veranderd. Daarnaast is het mogelijk om verwijzingen in het document als link op te nemen. Dit voorkomt fouten bij het valideren van de rapportage.
1	Aanwijzing en beschrijving rapporteur, opsteller of hoofdond erzoeker	De rapportage vermeldt de naam van de rapporteur.	N i	Dit maakt het mogelijk vast te stellen wie het onderzoek heeft uitgevoerd en wie professionele verantwoordelijkheid draagt. Het maakt het mogelijk te valideren dat deze persoon beschikt over voldoende certificering om professioneel te kunnen optreden.

	rs	hebben deelgenomen met inbegrip van de respectievelijke functies.	i	hebben genomen en betrokken kunnen worden bij de validatie.
2	Informatie verstrekking	Er wordt aangegeven welke informatie voor aanvang van het onderzoek moet worden aangeleverd.	N i	Een centraal overzicht van welke stukken benodigd zijn voorafgaand aan de penetratietest.
2	Beschrijving scope onderzoek	Er is een beschrijving van de scope van het onderzoek. Deze bevat de relevante selectie van onderdelen en objecten volgens sub 2.2.1 t/m 2.2.8. De scope komt overeen met de behoeftes uit het intakegesprek en past binnen de afgesproken tijdspanne.	N i	Inzage in de gemaakte afspraken met betrekking tot de scope van het onderzoek.
2	Scope - Aanvalsperspectieven	In de scopebeschrijving staan de aanvalsperspectieven opgenomen op basis van het intakegesprek, verdeeld onder: Greybox en Whitebox. Het uitvoeren van een blackbox-test valt nadrukkelijk niet onder deze methodiek	N i	Het is onduidelijk welke aanvalsperspectieven gebruikt zijn met tot gevolg het onnavolgbaar zijn van het onderzoek
2	Scope - Objecten	De objecten die naar voren zijn gekomen naar aanleiding van de intake, vormen de basis voor de scopeonderdelen en bijbehorende standaarden die van toepassing zijn in 2.2.3 tot en met 2.2.8. Alle standaarden die van toepassing kunnen zijn op het betrokken object, zijn in	N i	Indien de opdrachtnemer geen grey- of whitebox onderzoek kan doen, wordt belangrijke informatie voor het onderzoek achterhalen. Het ontdekken van zwakheden is dan lastiger en mogelijke aanvalsscenario's kunnen buiten beeld blijven.

Vraag en Antwoord

- Vragen?
- Oplossingen op maat voor specifieke compliance-uitdagingen
- Afsluiting

De Winter Information Solutions

OpenNovations

Samenvatting en Slotwoord

- Samenvatting van de belangrijkste punten
- Dankwoord aan de deelnemers en sprekers
- Informatie over verdere stappen en bronnen

De Winter Information Solutions

OpenNovations