Gemeente Geertruidenberg

De digitale weerbaarheid van de gemeente Geertruidenberg

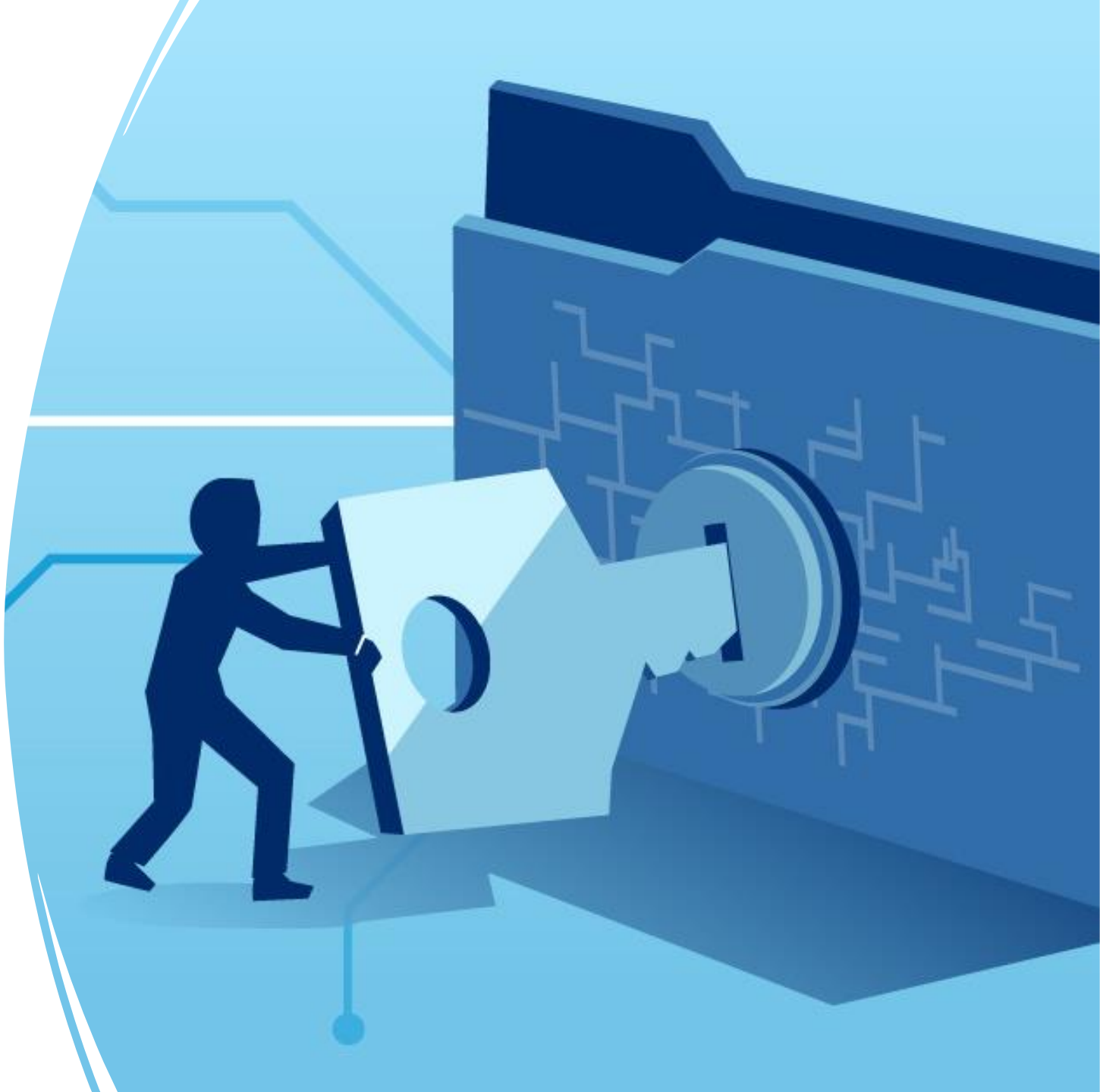


Max Aarts
CISO

3 oktober 2024

Inhoud

1. Wat is **digitale weerbaarheid**?
2. Wat is **informatiebeveiliging**?
3. Wat doet de **CISO**?
4. Wat zijn **risico's en dreigingen**?
5. Wat zijn de nieuwste **ontwikkelingen**?
6. Hoe **digitaal weerbaar** zijn wij?
7. Wat is de **verantwoordelijkheid** van de gemeenteraad?



Gemeente
Geertruidenberg

Wat is digitale weerbaarheid?

*“Het vermogen van de gemeente om zich te **beschermen tegen digitale dreigingen en aanvallen**, en om **snel** te **herstellen** na een incident. Dit omvat zowel technische als organisatorische maatregelen op **informatiebeveiliging**”.*

Gemeente Geertruidenberg

Wat is informatiebeveiliging?

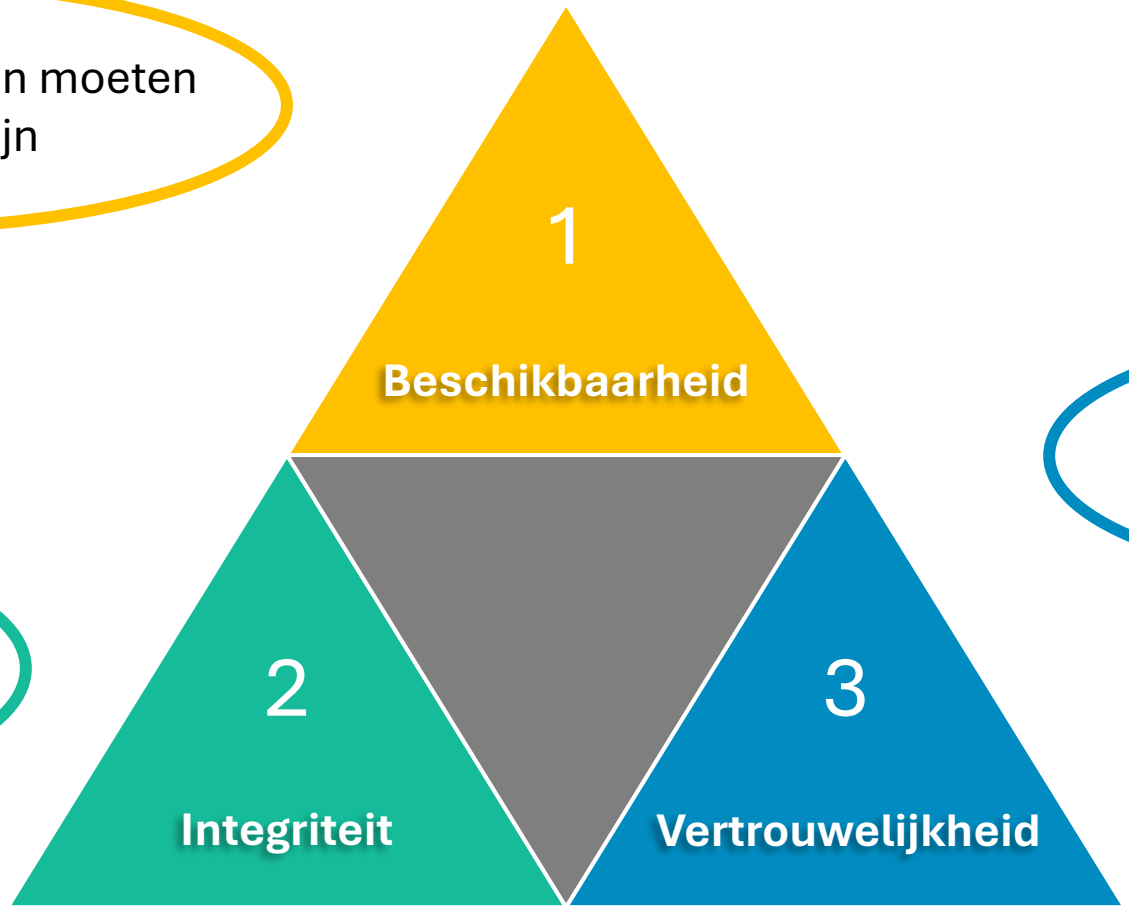
*“Informatiebeveiliging is het geheel van maatregelen en procedures dat bedoeld is om de **beschikbaarheid**, **integriteit** en **vertrouwelijkheid** van informatie te waarborgen.”*

Gemeente Geertruidenberg

Wat is informatiebeveiliging?

Informatie en systemen moeten beschikbaar zijn

- Storingen
- Aanvallen
- Herstellen



Alleen toegankelijk voor bevoegde personen

- Geen toegang voor onbevoegden

Informatie moet juist en volledig zijn

- Niet ongeautoriseerd wijzigen, verwijderen of beschadigen.

Gemeente Geertruidenberg

Wat doet de CISO?

Wat doet een Chief Information Security Officer (CISO)?

1. Ontwikkelt en implementeert **beleid** op **informatiebeveiliging**
2. Identificeert **beveiligingsrisico's** en adviseert welke maatregelen te nemen
3. Zorgt ervoor dat de organisatie aan **wet- en regelgeving** voldoet
4. Helpt bij het oplossen van **beveiligingsincidenten**
5. Verhoogt **bewustwording** op informatiebeveiliging



De CISO is een **onafhankelijke adviseur** die gevraagd en ongevraagd advies geeft.

Gemeente Geertruidenberg

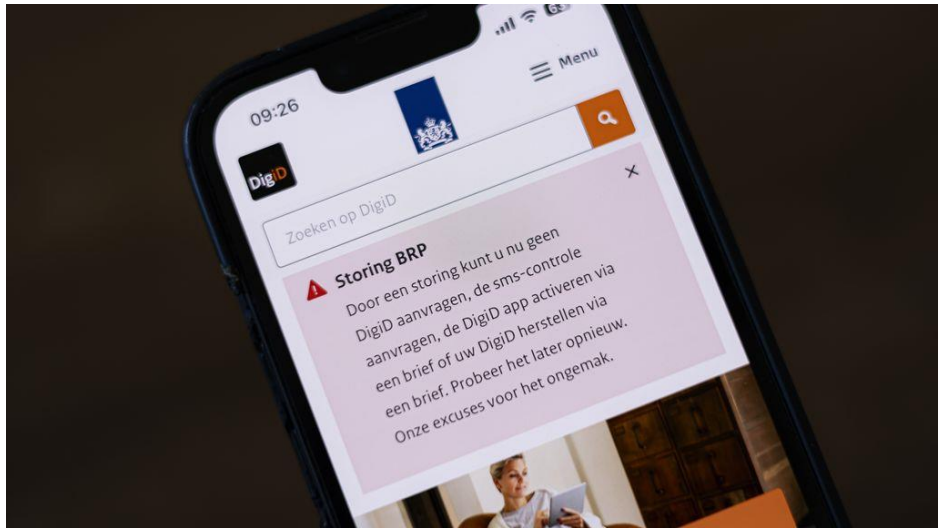
Wat zijn de risico’s en dreigingen?



NOS Nieuws • 19 juli 2024

Wereldwijd problemen door computerstoring: onder meer luchthavens en ziekenhuizen getroffen

8,5 miljoen computers getroffen door een fout in testsoftware van bedrijf CrowdStrike.



NOS Nieuws • 28 augustus 2024

Systemen bij overheidsdiensten plat door storing bij ministerie van Defensie

Gemeente Geertruidenberg

Wat zijn de risico’s en dreigingen?



NOS Nieuws • 7 oktober 2021

Industrieconcern VDL Groep getroffen door digitale aanval – miljoenen euro’s aan schade

Alle 105 bedrijven onder VDL groep zijn getroffen. Na 1 maand zijn alle bedrijfsactiviteiten weer volledig actief.



NOS Nieuws • 19 april 2023

Cybercriminelen eisen meer dan miljoen euro van KNVB na ransomware-aanval

Cybercriminelen dreigingen paspoorten en contracten van Oranje-spelers te publiceren.

Gemeente Geertruidenberg

Wat zijn de risico’s en dreigingen?



RTL Nieuws • 9 november 2021

Criminelen eisen 50 miljoen dollar van MediaMarkt na ransomware-aanval



NOS Nieuws • 13 mei 2017

Parkeerbedrijf Q-park getroffen door cyberaanval

Gemeente Geertruidenberg

Wat zijn de risico's en dreigingen?



NOS Nieuws – 5 februari 2020

Hackers Universiteit Maastricht zaten maanden in netwerk

De universiteit betaalt 200.000 euro aan losgeld.



RTL Nieuws - 17 februari 2021

Cyberaanval op Universiteit Amsterdam en Hogeschool van Amsterdam

Hackers hadden toegang tot wachtwoorden van studenten en medewerkers.

Gemeente Geertruidenberg

Wat zijn de risico’s en dreigingen?



RTL Nieuws - 13 september 2020

Veiligheidsregio in Gelderland getroffen door gijzelsoftware

De interne systemen zijn beperkt beschikbaar en e-mail werkt niet. De informatie voor brandweeruitrukken is wel toegankelijk, alsook de meldingssystemen P2000 en C2000.



VRT Nieuws – 12 december 2022

Cyberaanval op gemeente Antwerpen, hackergroep dreigt om privégegevens publiek te maken

Meer dan 500 gigabyte aan data gestolen. Kosten kunnen oplopen tot 70 miljoen euro.

Gemeente Geertruidenberg

Wat zijn de risico's en dreigingen?



NU.nl – 28 maart 2017

Systemen Tweede Kamer getroffen door ransomware

Details van de infectie zijn niet openbaar. Er is aangifte gedaan en er loopt een (forensisch) onderzoek.



RTV Utrecht - 27 maart 2017

Gemeente Blaricum, Eemnes en Laren doelwit van cyberaanval

Gemeenten zijn genoodzaakt alle computers los te koppelen van het internet.

Gemeente Geertruidenberg

Wat zijn de risico’s en dreigingen?



RTV Oost – 17 december 2020

Hof van Twente getroffen door ransomware-aanval, veel persoonlijke informatie van inwoners weg

Het herstel van de systemen kostte meer dan 4 miljoen euro.



NU.nl – 22 augustus 2022

Honderdduizenden bestanden Gelderse gemeenten aangeboden op dark web

130 gigabyte aan gestolen gegevens.
Ruim 730.000 bestanden met gevoelige persoonsgegevens en vertrouwelijke informatie.



RTL nieuws – 21 april 2022

Vijf gemeenten getroffen door hack bij leverancier

Gemeente Geertruidenberg

Wat zijn de risico’s en dreigingen?



INFORMATIE
BEVEILIGINGS
DIENST

Actueel dreigingsbeeld

INFORMATIE BEVEILIGINGS DIENST



Meer ransomware, destructievere gevolgen



Steeds meer en ernstiger kwetsbaarheden in software



Gevaren in ketens uit het zicht

Grootste risico's voor gemeenten

INFORMATIE BEVEILIGINGS DIENST



Uitval van dienstverlening en bedrijfsvoering



Vertrouwelijke informatie in verkeerd handen



Fouten in de dienstverlening

Gevolgen voor gemeenten

INFORMATIE BEVEILIGINGS DIENST



Hoge herstelkosten
Reputatieschade
Minder vertrouwen in de overheid

1. Informatiebeveiliging wordt vaak gezien als (onnodige) **kostenpost**
2. **Preventiekosten** zijn **laag** vergeleken met incidentenkosten
3. Incidenten kosten **tonnen of miljoenen euro's**
4. **Grote impact** op medewerkers
5. **Herstel** duurt **weken tot maanden**
6. **Verlies** van **vertrouwen** bij inwoners
7. **Reputatieschade** voor organisatie en bestuurders

Succesfactor nummer 1

INFORMATIE BEVEILIGINGS DIENST



Bewustwording is topprioriteit!

1. Bijna alle digitale aanvallen beginnen met phishing
2. Medewerkers vormen de eerste bescherming tegen aanvallen
3. Regelmatige bewustwording zorgt ervoor dat deze bescherming op niveau blijft
4. Bewustwording zorgt ervoor dat iedereen, medewerkers en leidinggevenden, zijn verantwoordelijkheid neemt

Weerbaarheid vergroten:
6 succesfactoren

INFORMATIE BEVEILIGINGS DIENST



Wat zijn de nieuwe ontwikkelingen?



BIO2 | Baseline Informatiebeveiliging Overheid

Gemeente Geertruidenberg

Wat is de NIS2-richtlijn?

***N**etwork and **I**nformation **S**ecurity*

1. **Versterken digitale weerbaarheid** van essentiële sectoren
2. **Hogere beveiligingseisen** voor bedrijven en overheden
3. Snellere en effectievere **respons op incidenten**



Gemeente Geertruidenberg

Waarom de NIS2-richtlijn?

Toenemende digitale dreigingen



Cyberaanval kost Maersk 255 miljoen euro

rtl nieuws



Gijzeling VDL raakt ook Philips en ASML; indirect slachtoffer van hack toeleverancier AD

Cyberaanval kost Antwerpen bijna 100 miljoen euro



Gigantische kosten en nog altijd niet opgelost: zes maanden na een cyberaanval worstelt de stad Antwerpen nog met de gevolgen ervan.

De Standaard

Voor wie is de NIS2-richtlijn?

Wet beveiliging netwerk- en informatiesystemen



- Vitale aanbieders
- Rijksoverheid
- Digitale dienstverleners

Cyberbeveiligingswet



- Digitale aanbieders
- Post- en koeriersdiensten
- Afvalstoffenbeheer
- Levensmiddelen
- Chemische stoffen
- Energie
- Transport
- Bankwezen
- Infrastructuur financiële markt
- Gezondheidszorg
- Digitale infrastructuur
- Afvalwater
- **Overheidsdiensten**
- Ruimtevaart
- Beheer van ICT diensten

Gemeente Geertruidenberg

Wat zegt de NIS2-richtlijn?

Cyberbeveiligingswet

Toezichthouder Rijksinspectie Digitale Infrastructuur

Zorgplicht



Risicobeheer

Risicoanalyse



Incidentbeheer

Incidentenbehandeling

Meldplicht



Bedrijfscontinuïteit

Crisisbeheer



Leveranciersbeheer

Contractbeheer

Toeleveringsketen



Cyberhygiëne

Bewustwording & opleiding

Toegangsbeleid

Authenticatie

Netwerkbeveiliging

Cryptografie & encryptie

Wat zijn de gevolgen van de NIS2?



1. Ambtelijke leiding

- **Hoofdelijk aansprakelijk** voor cyberbeveiliging
- **Verplichte kennis**, vaardigheden en opleiding op gebied van informatiebeveiliging
- **Inzicht in risico's** en genomen security-maatregelen

2. Organisatie

- **Meldplicht** van beveiligingsincidenten *aan de IBD*
- **Zorgplicht** op gebied van informatiebeveiliging, oftewel het voldoen aan de BIO.
- **Toezichthouder** *Rijksinspectie Digitale Infrastructuur*.

3. Niet naleving

- **Boetes** (max. 10 miljoen of 2% jaaromzet)
- **Schorsing** van leden van de ambtelijke leiding

Gemeente Geertruidenberg

Wat is zijn de nieuwe ontwikkelingen?

BIO2 | Baseline Informatiebeveiliging Overheid

Gemeente Geertruidenberg

Wat is de BIO?

BIO | Baseline Informatiebeveiliging Overheid

De Baseline Informatiebeveiliging Overheid (BIO) is een **set van maatregelen voor informatiebeveiliging** die specifiek zijn ontwikkeld voor overheidsorganisaties in Nederland.

Gemeente Geertruidenberg

Wat is de BIO?

BIO | Baseline Informatiebeveiliging Overheid

- Versterkt beveiliging
- Verplicht
- Controle en verantwoording

ENSIA | Eenduidige Normatiek Single Information Audit

Gemeente Geertruidenberg

Hoe digitaal weerbaar is de gemeente?

ENSIA

BIO



BIO2

Gemeente Geertruidenberg

Hoe digitaal weerbaar is de gemeente?

ENSIA | Eenduidige Normatiek Single Information Audit

DigiD: voldaan aan alle normen

Suwinet: niet voldaan

Gemeente Geertruidenberg

Hoe digitaal weerbaar is de gemeente?

BIO

Gemeente Geertruidenberg



Hoe digitaal weerbaar is de gemeente?



BIO2

Gemeente Geertruidenberg

5 **Geoptimaliseerd** — Uitingen ten aanzien van de prestaties maken integraal deel uit van de bedrijfsstrategie

4 **Voorspelbaar** — De kwaliteit van de processen wordt gemeten zodat het kan worden bijgestuurd

3 **Vastgesteld** — De werkzaamheden worden organisatiebreed volgens een vastgestelde wijze uitgevoerd

2 **Beheerst** — De werkzaamheden binnen de processen worden beheerst (herhaalbaar) uitgevoerd

1 **Informeel** — De organisatie pakt zaken ongestructureerd op. Het handelen is hiermee niet voorspelbaar en gebeurt reactief.

De verantwoordelijkheid van de gemeenteraad

1. **Controleren** van het College van B&W op het goed **uitvoeren** van het **informatiebeveiligingsbeleid**.
2. Het **goedkeuren** van **budgetten** voor **informatiebeveiliging** die door het college van B&W worden voorgesteld.
3. Het **goedkeuren** van **jaarverslagen** van het college van B&W, waarin informatiebeveiliging is opgenomen.
4. **Advies en richting geven** aan het **informatiebeveiligingsbeleid** door bijvoorbeeld **moties of wijzigingen** voor te stellen.

Gemeente Geertruidenberg

Max Aarts
CISO
m.aarts@geertruidenberg.nl



Gemeente
Geertruidenberg