

Van IT-dienstverlening naar aantoonbare cyberweerbaarheid

Nieuwe inzichten door BNS hybrIT en HostYou

NIS2 • GDPR • ISO/IEC 27001:2022

Technologie. Organisatie. Aantoonbaarheid.



Cybersecurity is veranderd

VROEGER



Firewall



Antivirus



Back-up



“De IT-partner regelt het”



VANDAAG



Continue monitoring



Identiteit & toegang



Keten- en kwetsbaarheidsrisico's



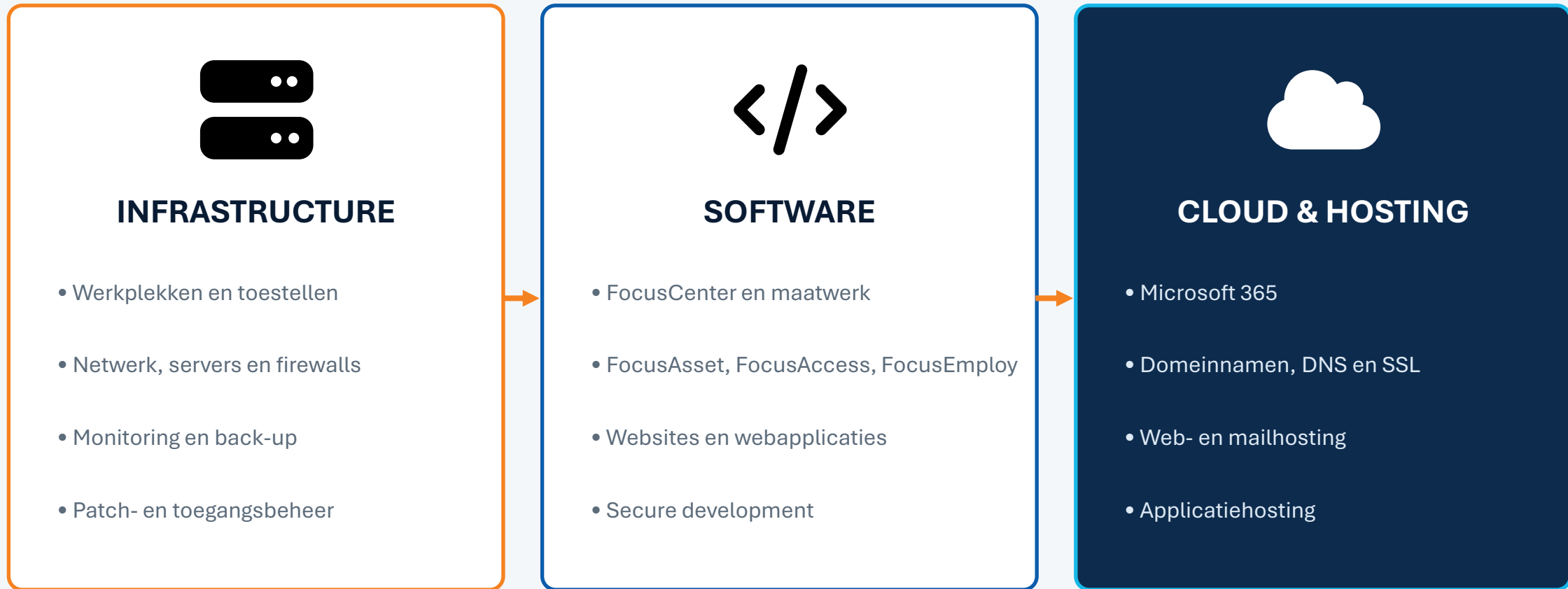
Incidentdetectie & herstel



Managementverantwoordelijkheid

Niet alleen beveiligen. Ook beheersen, opvolgen en aantonen.

Eén digitaal landschap, drie verbonden pijlers

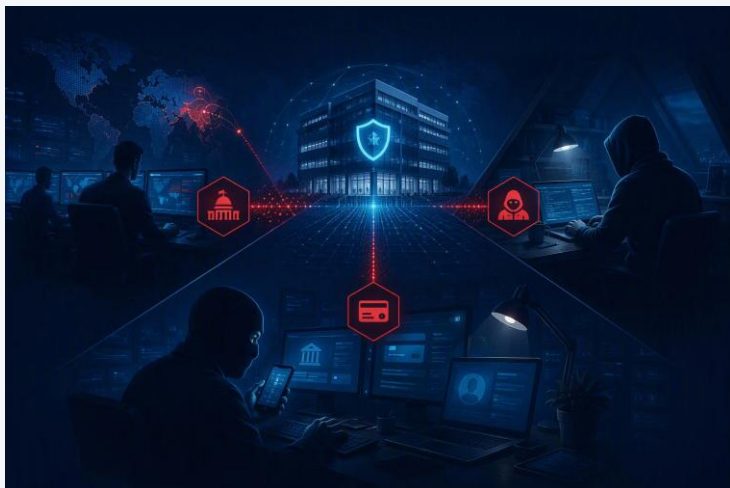


Gedeelde fundering: security • continuïteit • compliance

BAD NEWS

You will be hacked

Wie zit achter hacks en attacks?



Staatelijke actoren

Professionele groeperingen, vaak vanuit het buitenland, gijzelen onze systemen met ransomware. Losgeld en afpersing met gestolen data zijn hun verdienmodel.



De scriptkiddie

Een eenling op zijn zolderkamer die ons wil hacken voor de status. Geen geldmotief, wel uitval en reputatieschade als het hem lukt.



Identiteitsfraudeurs

Fraudeurs gebruiken phishing en gestolen identiteiten om betalingen om te leiden en geld van onze bankrekeningen weg te halen.

Drie heel verschillende daders, dezelfde impact op continuïteit, systemen en gegevens.

Recente incidenten

1. Bol – datalek bij logistieke partner (5 aug. 2026) vrtnws Nieuws Sport Live Ketnet Zoeken WinWin > Consument Webwinkel Bol waarschuwt klanten voor datalek bij partnerbedrijf wo 5 aug. 2026 18u38 2 min  De webwinkel Bol waarschuwt klanten voor een datalek bij logistieke partner Ceva Logistics, waarbij mogelijk klantgegevens zijn ingekeken of gekopieerd.	2. ING – datalek via Ceva Logistics (1 sep. 2026) De Standaard Nieuws Opinie Inspiratie Podcasts Ook ING-klanten getroffen door datalek bij Ceva Logistics 1 september 2026 3 min. leestijd  ING waarschuwt dat er gegevens van deelnemers aan het ING Punten-programma zijn gestolen door een datalek bij logistieke partner Ceva Logistics.	3. Fortinet – 270 Belgische bedrijven getroffen (22 jun. 2026) vrtnws Nieuws Sport Live Ketnet Zoeken Belgique > Économie Russische hackers treffen 270 Belgische bedrijven via lek bij cybersecuritygigant Fortinet ma 22 jun. 2026 4 min  Bij een grootschalige Russische cyberaanval zijn minstens 270 Belgische bedrijven en organisaties getroffen via een lek bij Fortinet. Bij ruim 100 bedrijven liggen de inloggegevens nog steeds online.	4. Proximus – datalek via partner (23 sep. 2026) MarketScreener Koersen Nieuws Analyses Bedrijfsprofiel Proximus meldt datalek door medewerker zakelijke partner 23 sep. 2026 om 18:18 ABM FN  Proximus meldt een beveiligingsincident waarbij een medewerker van een partner op grote schaal de klantendatabase heeft geraadpleegd. Het gaat om naam, adres, e-mail, geboortedatum en telefoonnummer.
5. Proximus – netwerkstoring Waals-Brabant (22 sep. 2026) geoblackout Storingen Providers Over ons Panne bij Proximus in Waals-Brabant op 22 september 2026: daling zet door Beëindigd om 20:15 van 17:15 tot 20:15 regionale storing  Op 22 september 2026 kampt Proximus met een panne in Waals-Brabant. De storing duurde zo'n drie uur en trof vooral vast internet, nauwelijks tv of mobiel.	6. De Bijenkorf – mogelijk datalek (1 sep. 2026) datalekt.nl Cyberincidenten Nieuws Achtergrond Over ons Home > Cyberincidenten > 2026 Bijenkorf waarschuwt klanten voor mogelijk datalek 1 sep. 2026  Een cyberaanval op logistiek dienstverlener CEVA Logistics heeft geleid tot een mogelijk datalek bij webwinkels Bol en de Bijenkorf. De precieze omvang is nog niet bekend.	7. Ajax – datalek via Ceva Logistics (3 sep. 2026) datalekt.nl Cyberincidenten Nieuws Achtergrond Over ons Home > Cyberincidenten > 2026 CEVA-datalek treft ook Ajax 3 sep. 2026  Een hack bij logistiekbedrijf CEVA Logistics heeft geleid tot het mogelijk uitlekken van klantgegevens bij onder meer Ajax, Ace & Tate, Bol, ING en de Bijenkorf.	8. Drukland – datalek (27 sep. 2026) datalekt.nl Cyberincidenten Nieuws Achtergrond Over ons Home > Cyberincidenten > 2026 Online drukkerij Drukland meldt datalek met gehashte wachtwoorden 27 sep. 2026  Online drukkerij Drukland, onderdeel van Simian, is getroffen door een datalek waarbij e-mailadressen en gehashte wachtwoorden van Nederlandse en Belgische klanten zijn buitgemaakt.
9. FysioRoadMap – ransomware (28 sep. 2026) ccinfo.nl NIEUWS CYBERAANVALLEN DREIGINGEN OVER ONS Home > Cyberaanvallen 2026 > september FysioRoadMap getroffen door Nova ransomware aanval 28 september 2026  FysioRoadMap is op 28 september 2026 getroffen door een ransomware-aanval van de Nova groep. Het bedrijf onderzoekt de impact en neemt maatregelen.	10. Volumex Lease – ransomware (15 sep. 2026) ccinfo.nl NIEUWS CYBERAANVALLEN DREIGINGEN OVER ONS Home > Cyberaanvallen 2026 > september Volumex Lease slachtoffer van Radar ransomware 15 september 2026  Volumex Lease is op 15 september 2026 slachtoffer geworden van een ransomware-aanval door de Radar-groep.	11. Venlogistics – ransomware (15 sep. 2026) ccinfo.nl NIEUWS CYBERAANVALLEN DREIGINGEN OVER ONS Home > Cyberaanvallen 2026 > september Venlogistics slachtoffer van ransomwareaanval 15 september 2026  Venlogistics is op 15 september 2026 getroffen door een ransomware-aanval. De impact en mogelijke datalekken worden onderzocht.	12. CAS Exhibition Partners – ransomware (15 sep. 2026) ccinfo.nl NIEUWS CYBERAANVALLEN DREIGINGEN OVER ONS Ransomwareaanval op CAS Exhibition Partners 15 september 2026  CAS Exhibition Partners is op 15 september 2026 doelwit geworden van een ransomware-aanval. Het bedrijf onderzoekt de gevolgen.

Recente incidenten



The screenshot shows a dark web forum post from 'RedStone' on 'DarkWeb Informer.com'. The post title is '[EU] TWIZZIT - 1.53M Members, 178K Groups, 5.5K Organisations (BE/FR/NL) - 1.4GB' and it was posted on Tuesday, September 22, 2026 at 04:47 AM. The user 'RedStone' has a profile picture of a red devil and a 'MEMBER' badge. The post content features the Twizzit logo and text stating: 'Hi [redacted] Community, Today, the full database of **TWIZZIT**, the club management platform for +5,500 organisations across Europe is available for purchase! Sports federations, youth movements, choirs and nonprofits in Belgium, France and the Netherlands. 17+ years of data. Unique members: 1,532,886 Total rows: 4,048,767 Group memberships: 3,375,550'. A large blue speech bubble is overlaid on the right side of the screenshot.

De onbevoegde partij heeft toegang gekregen tot gegevens die niet via een Twizzit-account toegankelijk hadden mogen zijn. Uit ons onderzoek bleek dat er ook persoonlijke gegevens zijn gekopieerd.

EIGENAAR TWIZZIT, ISH

Recente incidenten



Gemeentehuis van Machelen. Inzet: burgemeester Jean-Pierre De Groef. © Marc Baert, Inzet: Marc Baert

Valse e-mail van 'de brandweer' legt dienstverlening van Machelen plat: "Normaal geen persoonsgegevens gelekt"



Jan Guldentops • 1e

Trainer/onderzoeker/consultant/spreker met e...

[Mijn website bezoeken](#)

4 d •



Voorzorgsprincipe

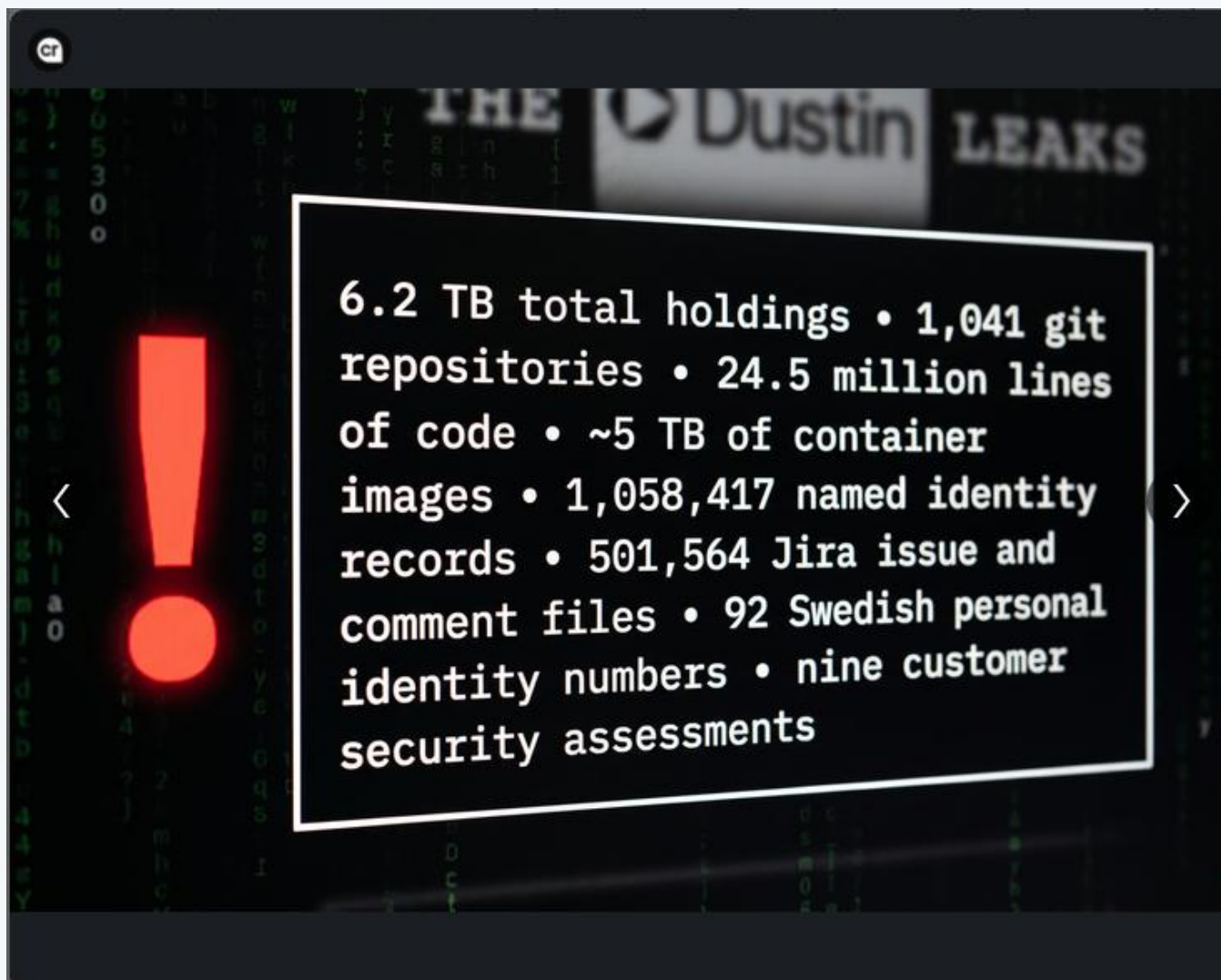
Voor de zoveelste keer blijken er persoonsgegevens gestolen te zijn bij een organisatie, in dit geval de gemeente Machelen.

Opvallend is dat de burgemeester tien dagen geleden nog een statement maakte waarin hij de risico's minimaliseerde en stelde dat "er weinig kans is dat er data gelekt is." Niet dus.

Het is bijna een kroniek van een aangekondigde dood dat hier later op teruggekomen zal worden en er juist wel data buitgemaakt is. Data die ondertussen al tien dagen gebruikt kan worden om andere criminele ongein mee uit te halen.

Het is een crisiscommunicatie playbook dat keer op keer opnieuw gebruikt wordt. Minimaliseer het risico, zeg dat de kans klein is dat data gelekt is om dan stap voor stap, als stukjes salami, de echte toedracht toe te geven. De lijst van organisaties die hierin voorgingen is lang, de datalekken zijn enorm en vooral de schade is groot voor de echte slachtoffers: de burgers van wiens gegevens op straat liggen.

Recente incidenten



THE Dustin LEAKS

6.2 TB total holdings • 1,041 git repositories • 24.5 million lines of code • ~5 TB of container images • 1,058,417 named identity records • 501,564 Jira issue and comment files • 92 Swedish personal identity numbers • nine customer security assessments



Jan Guldentops  • 1e

Trainer/onderzoeker/consultant/spreker met e...

[Mijn website bezoeken](#)

2 w • 



Hackers van [Dustin](#) delen hun buit met de wereld.

De digitale inbrekers Fulcrumsec vertelt zelf dat ze met 6.2 TB aan data weg zijn met allerlei lekkers voor hackers van interne broncode, > 1.000.000 persoonsgegevens, 500K Jira tickets en 9 security audits van klanten.

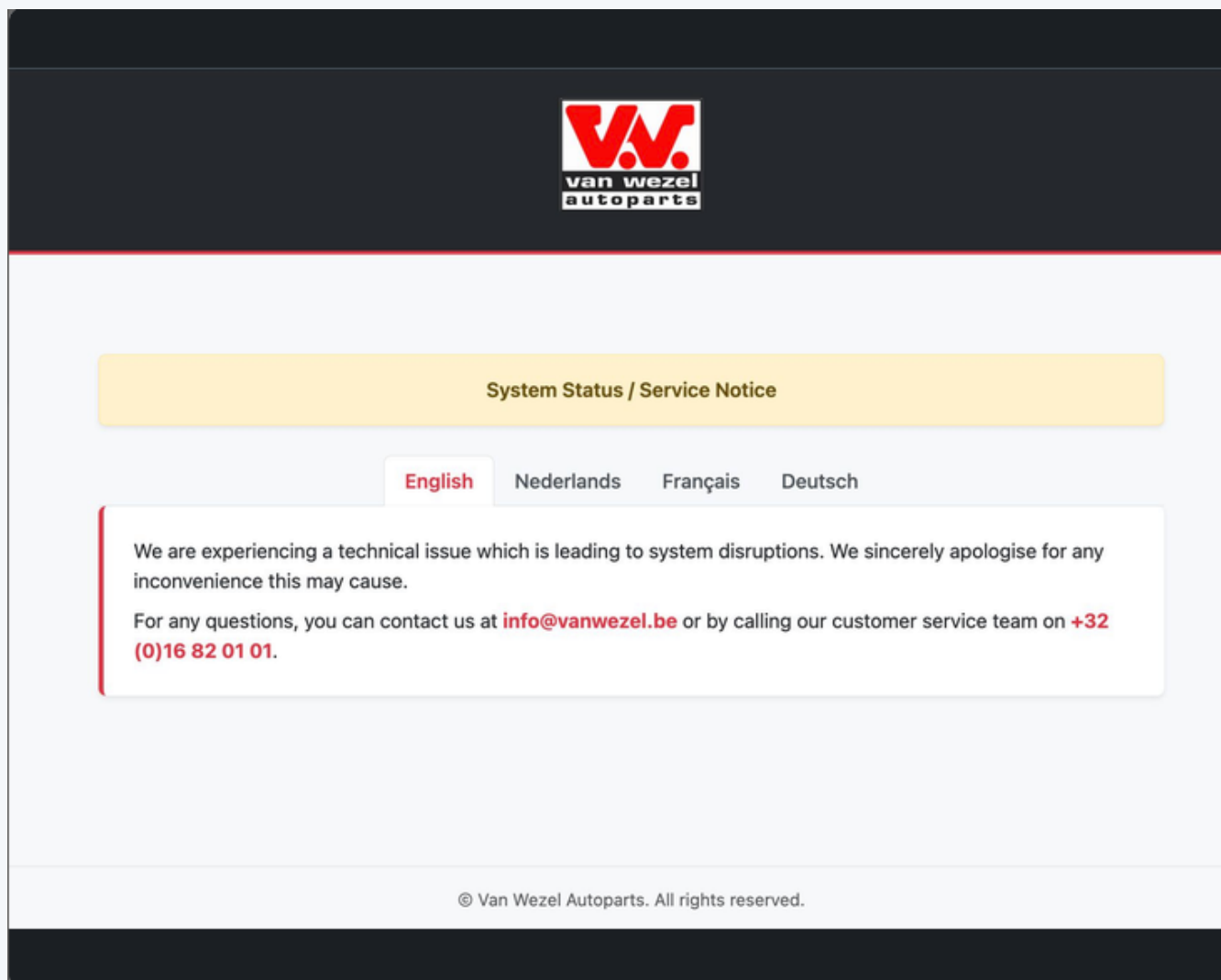
Ondanks het stilzwijgen van Dustin de afgelopen week, wist iedereen die de laatste jaren databreaches en vooral de reacties van de getroffen bedrijven volgt dat er stront aan de knikker was en is.

Meer dan een week heeft het bedrijf in naam van het "forensisch onderzoek" en "we zijn niet zeker dat er data gelekt is" met minimale crisiscommunicatie proberen de onwetendheid vol te houden.

Het is een beetje de kat van Schrödinger die gekruist wordt met de communicatiestrategie van Donald Trump. Zolang de hackers de gestolen data niet publiekelijk voor de wereld tonen, kan je blijven ontkennen dat er iets ernstigs gebeurd is ook al weet je zelf eigenlijk beter.

Hoe langer je ontkent neemt het risico en de schade naar je klanten, organisatie of individuen, exponentieel toe.

Recente incidenten



The screenshot shows the Van Wezel Autoparts website. At the top is the company logo. Below it is a yellow banner with the text "System Status / Service Notice". Underneath the banner are four tabs: "English" (selected), "Nederlands", "Français", and "Deutsch". The main content area contains a message in English: "We are experiencing a technical issue which is leading to system disruptions. We sincerely apologise for any inconvenience this may cause. For any questions, you can contact us at info@vanwezel.be or by calling our customer service team on +32 (0)16 82 01 01." At the bottom of the page, there is a copyright notice: "© Van Wezel Autoparts. All rights reserved."



Jan Guldentops • 1e

Trainer/onderzoeker/consultant/spreker met e...

[Mijn website bezoeken](#)

3 w • Bewerkt •



Je weet dat cyberaanvallen op ondernemingen echt mainstream worden als het op Radio 2 komt en in [Het Laatste Nieuws](#) verschijnt.

Dit gebeurde met autobedrijf [Van Wezel Autoparts](#) uit Tienen. Van Wezel is een groothandel, geen kleine speler met een omzet van 150 miljoen euro per jaar en bijna 250 werknemers. Wat er precies gebeurd is blijft onduidelijk. Het bedrijf is spaarzaam met informatie en heeft volgens HLN een communicatiebureau ingeschakeld voor de crisiscommunicatie.

Ik begrijp die reflex, maar ik vind het altijd een gemiste kans om met andere organisaties te delen wat er misgaat. We kunnen nu enkel afgaan op wat publiek zichtbaar is. Als we naar de internetinfrastructuur van het bedrijf kijken, staat er louter een korte melding op de website over een technisch probleem dat leidt tot systeemverstoringen, met excuses voor het ongemak.

Jammer dat er nog niet openlijk gecommuniceerd wordt over de oorzaak. Meer openheid helpt ons als cybersecurityverdedigers net om ons werk beter te doen. Tegelijk geeft het mij de gelegenheid om zelf op verkenning te gaan en te analyseren.

Recente incidenten

Hetzelfde incident kan tegelijk
continuïteit, systemen én
persoonsgegevens raken.

© Van Wezel Autoparts. All rights reserved.

Als we naar de internetinfrastructuur van het bedrijf kijken, staat er louter een korte melding op de website over een technisch probleem dat leidt tot systeemverstoringen, met excuses voor het ongemak.

Jammer dat er nog niet openlijk gecommuniceerd wordt over de oorzaak. Meer openheid helpt ons als cybersecurityverdedigers net om ons werk beter te doen. Tegelijk geeft het mij de gelegenheid om zelf op verkenning te gaan en te analyseren.

Van drie 'kaders' naar één beheersbaar beveiligingsprogramma

Vergelijking tussen ISO/IEC 27001:2022 controls,
NIS2 artikel 21 en GDPR artikel 32

Van theorie tot praktijk



Een incident volgt geen juridisch kader

Hetzelfde incident kan tegelijk continuïteit, systemen én persoonsgegevens raken.

Bedrijfsimpact

Stilstand en omzetverlies
Herstel en crisisbeheersing
Afhankelijkheid van leveranciers

Cyberimpact

Beschikbaarheid en integriteit
Kwetsbaarheden en aanvalspaden
Melding en toezicht

Privacy-impact

Datalek risico voor betrokkenen
Vertrouwelijkheid van gegevens
Mogelijke melding aan GBA

**De uitdaging is niet “welk kader kies ik?”,
maar “hoe zorg en bewijs ik dat mijn risico’s beheerst zijn?”**

Voor wie geldt welk kader?

De scope verschilt. De operationele maatregelen overlappen sterk.

ISO 27001

KEUZE / CONTRACT

Elke organisatie kan een ISMS invoeren en laten certificeren. De scope wordt door de organisatie bepaald en door de certificatie afgebakend.

NIS2

SECTOR + OMVANG + UITZONDERINGEN

In België geldt NIS2 voor essentiële en belangrijke entiteiten binnen de wettelijk bepaalde sectoren en diensten. Sommige categorieën kunnen ongeacht omvang vallen.

GDPR

VERWERKING PERSOONSGEGEVENS

Artikel 32 geldt voor verwerkingsverantwoordelijken en verwerkers die persoonsgegevens verwerken, ongeacht sector of certificatie.

Toeleveringsketen: ook buiten de directe NIS2-scope kunnen klanten en leveranciers aantoonbare beveiliging verlangen.

Drie kaders, drie verschillende rollen

Wetgeving bepaalt verplichtingen. ISO 27001 organiseert het managementsysteem.

1

ISO/IEC 27001:2022

HOE BESTUREN?

ISMS, risico's, beleid, audits en continue verbetering

2

NIS2 artikel 21

WAT VOOR CYBERWEERBAARHEID?

Technische, operationele en organisatorische risicobeheersmaatregelen

3

GDPR artikel 32

WAT VOOR PERSOONSGEGEVENS?

Passende beveiliging afgestemd op risico's voor betrokkenen



GDPR artikel 32. Beveiliging van de verwerking

GDPR-wetgeving (AVG)
25 mei 2018 (EU)
30 juli 2018 (Belgische wet)

GDPR artikel 32. Beveiliging van de verwerking

GDPR-wetgeving (AVG)

VERWERKERSOVEREENKOMST

30 juli 2018 (Belgische wet)

GDPR artikel 32. Beveiliging van de verwerking

Verwerkersovereenkomst:

De hoofdovereenkomst

Bijlage 1 – Doel, soort, categorie, duur van de verwerking

Bijlage 2 – Technische en organisatorische beveiligingsmaatregelen

Bijlage 3 – Toegestane subverwerkers

Bijlage 4 – Datalekken procedure (optioneel)

GDPR artikel 32. Beveiliging van de verwerking

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, **treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen** om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

a) de pseudonimisering en versleuteling van persoonsgegevens;

b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

GDPR artikel 32. Beveiliging van de verwerking

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, **treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen** om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

a) de pseudonimisering en **versleuteling van persoonsgegevens**;

b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

GDPR artikel 32. Beveiliging van de verwerking

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, **treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen** om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

Versleuteling (encryption): SSL/TLS-certificaat, DMARC, ZTNA, SSH (voor data onderweg – data in transit)
database encryptie, schijf encryptie, immutable backup (voor data in rust – data at rest)

b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

GDPR artikel 32. Beveiliging van de verwerking

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, **treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen** om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

Versleuteling (encryption): SSL/TLS-certificaat, DMARC, ZTNA, SSH (voor data onderweg – data in transit)
database encryptie, schijf encryptie, immutable backup (voor data in rust – data at rest)

b) het vermogen om op permanente basis de **vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht** van de verwerkingssystemen en diensten te garanderen;

c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

GDPR artikel 32. Beveiliging van de verwerking

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, **treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen** om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

Versleuteling (encryption):	SSL/TLS-certificaat, DMARC, STARTTLS, ZTNA, SSH (voor data onderweg – data in transit) database encryptie, schijf encryptie, encrypted backup (voor data in rust – data at rest)
Vertrouwelijkheid:	toegangsbeheer (least privilege), MFA, SPF, DKIM, encryptie
Integriteit:	wijzigingsbeheer, logging en auditing, inputvalidatie, AV, anti-malware, EDR
Beschikbaarheid:	backup policy, remote backup, immutable backup
Veerkracht:	patchmanagement, incident response plan, DDoS protection
tijdig te herstellen;	

d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

GDPR artikel 32. Beveiliging van de verwerking

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, **treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen** om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

Versleuteling (encryption):	SSL/TLS-certificaat, DMARC, STARTTLS, ZTNA, SSH (voor data onderweg – data in transit) database encryptie, schijf encryptie, encrypted backup (voor data in rust – data at rest)
-----------------------------	---

Vertrouwelijkheid:	toegangsbeheer (least privilege), MFA, SPF, DKIM, encryptie
Integriteit:	wijzigingsbeheer, logging en auditing, inputvalidatie, AV, anti-malware, EDR (meer)...

c) het vermogen om bij een fysiek of technisch incident de **beschikbaarheid** van en de **toegang** tot de persoonsgegevens tijdig te **herstellen**;

d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

GDPR artikel 32. Beveiliging van de verwerking

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, **treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen** om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

Versleuteling (encryption):	SSL/TLS-certificaat, DMARC, STARTTLS, ZTNA, SSH (voor data onderweg – data in transit) database encryptie, schijf encryptie, encrypted backup (voor data in rust – data at rest)		
Vertrouwelijkheid:	toegangsbeheer (least privilege), MFA, SPF, DKIM, encryptie		
Integriteit:	wijzigingsbeheer, logging en auditing, inputvalidatie, AV, anti-malware, EDR (meer)...		
Bedrijfscontinuïteit, back-ups en disaster recovery:			
Technisch: backup beleid, immutable backups, redundantie inbouwen, failover			
Organisatorisch: disaster recovery plan, bepaal RTO en RPO, restore tests, incidentbeheer, meldplicht			
d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.			

GDPR artikel 32. Beveiliging van de verwerking

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, **treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen** om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

Versleuteling (encryption):	SSL/TLS-certificaat, DMARC, STARTTLS, ZTNA, SSH (voor data onderweg – data in transit) database encryptie, schijf encryptie, encrypted backup (voor data in rust – data at rest)		
Vertrouwelijkheid:	toegangsbeheer (least privilege), MFA, SPF, DKIM, encryptie		
Integriteit:	wijzigingsbeheer, logging en auditing, inputvalidatie, AV, anti-malware, EDR (meer)...		
Bedrijfscontinuïteit, back-ups en disaster recovery:			
Technisch:	backup beleid, immutable backups, redundantie inbouwen, failover		(meer)...
d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.			

GDPR artikel 32. Beveiliging van de verwerking

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, **treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen** om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

Versleuteling (encryption):	SSL/TLS-certificaat, DMARC, STARTTLS, ZTNA, SSH (voor data onderweg – data in transit) database encryptie, schijf encryptie, encrypted backup (voor data in rust – data at rest)		
Vertrouwelijkheid:	toegangsbeheer (least privilege), MFA, SPF, DKIM, encryptie		
Integriteit:	wijzigingsbeheer, logging en auditing, inputvalidatie, AV, anti-malware, EDR		(meer)...
Bedrijfscontinuïteit, back-ups en disaster recovery:			
Technisch:	backup beleid, immutable backups, redundantie inbouwen, failover		(meer)...
Regelmatig controleren en evalueren van al het bovenstaande.			
Technisch: pentest, kwetsbaarheden scans, testen backups			
Organisatorisch: privacy & security audit, toegangsrechten review, phishing simulaties			
Leveranciers en verwerkers controleren			
Aantoonbaarheid van deze controles en evaluaties = bewijskracht			

GDPR artikel 32. Beveiliging van de verwerking

GDPR-wetgeving (AVG)
25 mei 2018 (EU)
30 juli 2018 (Belgische wet)

Drie kaders, drie verschillende rollen

Wetgeving bepaalt verplichtingen. ISO 27001 organiseert het managementsysteem.

1

ISO/IEC 27001:2022

HOE BESTUREN?

ISMS, risico's, beleid, audits en continue verbetering

2

NIS2 artikel 21

WAT VOOR CYBERWEERBAARHEID?

Technische, operationele en organisatorische risicobeheersmaatregelen

3

GDPR artikel 32

WAT VOOR PERSOONSGEGEVENS?

Passende beveiliging afgestemd op risico's voor betrokkenen



De overlap tussen kaders is groot: risico's beheersen en kunnen aantonen

Dezelfde basiscontroles leveren bewijs voor meerdere verplichtingen.



Risicoanalyse

scope, dreigingen, impact



Toegangsbeheer

rollen, MFA, levenscyclus



Cryptografie

gegevens en
communicatie



Incidentbeheer

detecteren, escaleren,
leren



Continuïteit

back-up, herstel, crisis



Leveranciers

due diligence en afspraken



Monitoring

logging en opvolging



Verbetering

testen, audits en reviews

Eén control library • meerdere mappings • één bewijsarchief

Waar de drie kaders elkaar versterken

Sterk = rechtstreeks en breed ondersteund • Partieel = aanvullende invulling nodig • Beperkt = niet de primaire focus

Beheersdomein	ISO 27001	NIS2 art. 21	GDPR art. 32
Governance, scope en rollen	Sterk	Partieel	Partieel
Risicoanalyse en securitybeleid	Sterk	Sterk	Sterk
Incident handling	Sterk	Sterk	Partieel
Business continuity en crisisbeheer	Sterk	Sterk	Partieel
Supply-chain security	Sterk	Sterk	Partieel
Veilige ontwikkeling en kwetsbaarheden	Sterk	Sterk	Partieel

Van momentopname naar continue monitoring



Zichtbaarheid is de eerste verdedigingslaag

- 1 Scan** Kwetsbaarheden en configuratiefouten zichtbaar maken
- 2 Beoordeel** Technische signalen vertalen naar bedrijfsrisico
- 3 Herstel** Prioriteiten uitvoeren en eigenaarschap vastleggen
- 4 Volg op** Rapporteren, hertesten en continu verbeteren

FocusMonitor

FocusScan Internal

Managed security

Het organisatorische huishouden op orde



FocusAsset

Wat hebben we?

- Bedrijfsmiddelen
- Hardware & software
- Eigenaarschap
- Levenscyclus



FocusAccess

Wie mag waaraan?

- Rollen en rechten
- Applicatiematrix
- Periodieke review
- Toegang intrekken



FocusEmploy

Wie doet wat?

- HR, IT en Facility
- In- en uitdienst
- Goedkeuringen
- Controle op voltooiing

Het organisatorische huishouden op orde



Technische beveiliging houdt aanvallers buiten.

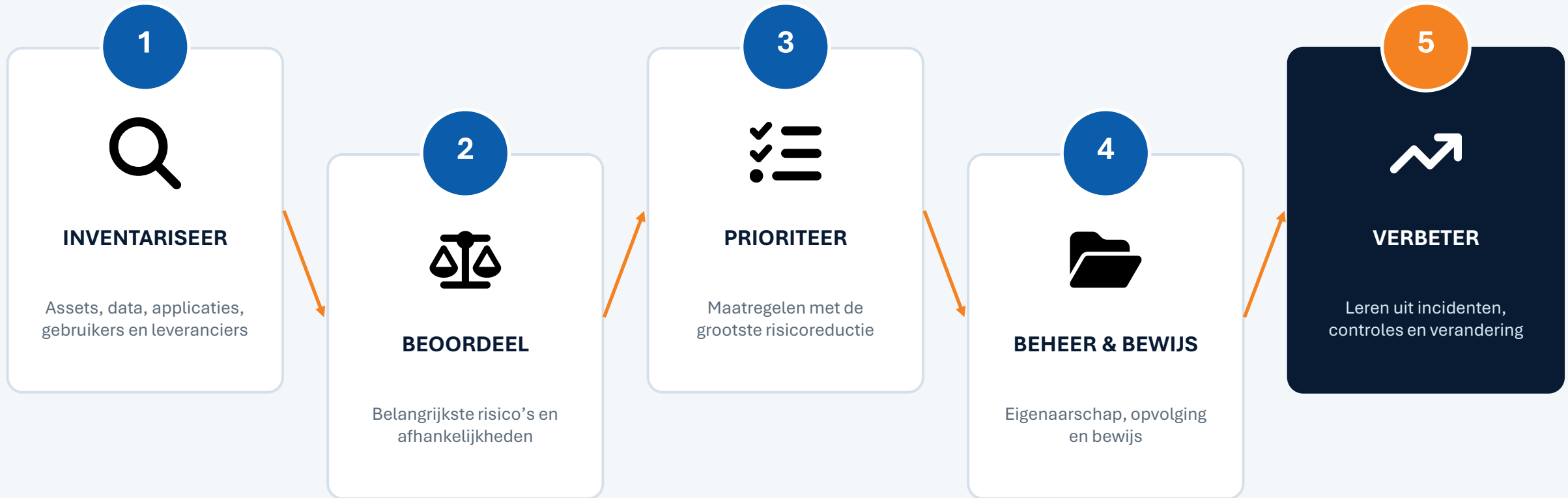
Organisatorische beveiliging voorkomt open deuren.

- Levenscyclus

- Toegang intrekken

- Controle op voltooiing

Een haalbaar groeipad



Start met zichtbaarheid, eigenaarschap en de grootste risico's.

Van verwachting naar concrete dienstverlening

THEMA	ORGANISATORISCH	TECHNISCH	BNS / HOSTYOU
Assets	Eigenaarschap & register	Discovery & scanning	FocusAsset • FocusScan • FocusMonitor
Toegang	Rollen & review	MFA & least privilege	FocusAccess • FocusCenter RBAC
Medewerkers	In- en uitdienstproces, Training	Accounts blokkeren	FocusEmploy • FocusLearn • Phished.io
Kwetsbaarheden	Prioriteiten & opvolging	Scanning & patching	FocusScan • FocusPatch • FocusServices • AVsensor • eMailSensor
Continuïteit	Ontdubbeling, herstelprocedures	High availability, backup & monitoring	HA Servers, storage, network, firewalls • FocusBackup
Websites	Onderhoudsafspraken	Updates, WAF & SSL	HostYou domains & SSL • Managed WordPress • Managed Drupal
Softwareketen	Componenten opvolgen	Software Composition Analysis & SBOM	GitLab/Hub • Aikido • Secure Development by Design (PHP/dotNET)
Incidenten	Escalatie & registratie	Logging & detectie	FocusMonitor • FocusNow Servicedesk

BNS en HostYou ondersteunen uitvoering en aantoonbaarheid. De verantwoordelijkheid blijft bij de organisatie.

BESCHERMEN. BEHEERSEN. AANTONEN.



BESCHERMEN

Technische en organisatorische maatregelen



BEHEERSEN

Eigenaarschap, processen en opvolging



AANTONEN

Registers, rapporten, controles en certificatie

Kies uw volgende stap

FocusScan

Welke kwetsbaarheden vragen aandacht?

FocusCenter

Hoe beheren we assets, toegang en medewerkers?

FocusServices

Security roadmap. Wat pakken we eerst aan?

BNS hybrIT + HostYou - Growing your business. Securing your future.

Bedankt
voor uw aandacht.

Met BNS hybrIT en HostYou aan uw zijde bent u klaar
voor de uitdagingen van morgen.

35
& 25

JAAR

BNS & HOSTYOU

60 JAAR GEDEELDE PASSIE



25
Jaar



35
Jaar