VOLKSHUISVESTING IS TOPSPORT

AEDES CORPORATIEDAG 18 APRIL 2024

vereniging van woningcorporaties

aedes

WHAT THE HACK

LAURENTIUS
Samen voor een thuis

Woonforte

Lieven de Key

WTH – even voorstellen

- Leen Spaans – Woonforte / CorpoNet
- Alex Meester – Lieven de Key / De Vernieuwde Stad
- Anouk van der Zanden – Laurentius

Verbindingsgroep Informatiebeveiliging
Aedes Community Informatiebeveiliging en Privacy

WTH – wie zijn jullie?

- Hoe groot is je organisatie:
  - Onder 10.000 VHE
  - Tussen 10.000 en 20.000 VHE
  - Meer dan 20.000 VHE
- In welke categorie valt je functie:
  - Operationeel
  - Tactisch
  - Strategisch
- Ben je al eens betrokken geweest bij een digitale aanval?
  - Ja
  - Nee
- Wie heeft er een Continuïteitsplan of Incident Respons Plan?

WTH – hoe gaat het nu met…

- Corporatie in Breda
- Ruim 8.000 VHE
- 100 medewerkers
- 1 kantoor
- Maart 2022: Digitale aanval 8 woco’s

WTH – hoe gaat het nu met…

- Huidige situatie: december 2023 laatste punten afgerond
  - Impact op de organisatie
  - Impact op ICT-omgeving

- Grootste uitdagingen
  - Leveranciers en Cloud
  - Printen
  - Koppelingen met Online ERP (DE Online)
  - 1 applicatie niet in Saas

WTH – hoe gaat het nu met…

- Security
  - Security Scan/pentest door Northwave
    - Volwassenheidscheck
    - Pentest
    - Configuratie inventarisatie Microsoft 365
  - Samen Digitaal Veilig
    - Awareness medewerkers
    - Organisatiescan
    - Leverancierssscan
  - BIC 4.0

- Cyberverzekering: **Ja** of **Nee**?

Informatie-beveiliging

Cyber Security

Alex Meester

“security perspectieven”

soms is het goed om focus aan te brengen

Lieven de Key

Fundament

- Altijd al aanwezig, veranderende rol
- Zorgvuldig omgaan met gegevens van huurders
- Vergaande digitalisering* en veilig digitaal werken
- ***Zelf*** verantwoordelijk voor de veiligheid ***én*** die van onze huurders.

Het fundament hiervoor is een informatiebeveiligingsbeleid en een cyber securitybeleid waarmee we veilig en 'in control' zijn, verantwoording af kunnen leggen en het mogelijk maken om op verantwoorde wijze digitaal en innovatief te kunnen werken.

** Visie Digitalisering DT 22 maart 2022*

"Balans tussen mens, organisatie en techniek"

Samenhang

Twee termen die dóór elkaar of mét elkaar worden gebruikt. Beide raken het beschermen van de *informatievoorziening*, gaan over risico's én de maatregelen om deze te beheersen.

kan ik er over beschikken, ervan uitgaan dat het klopt en kan niet 'iedereen' er bij

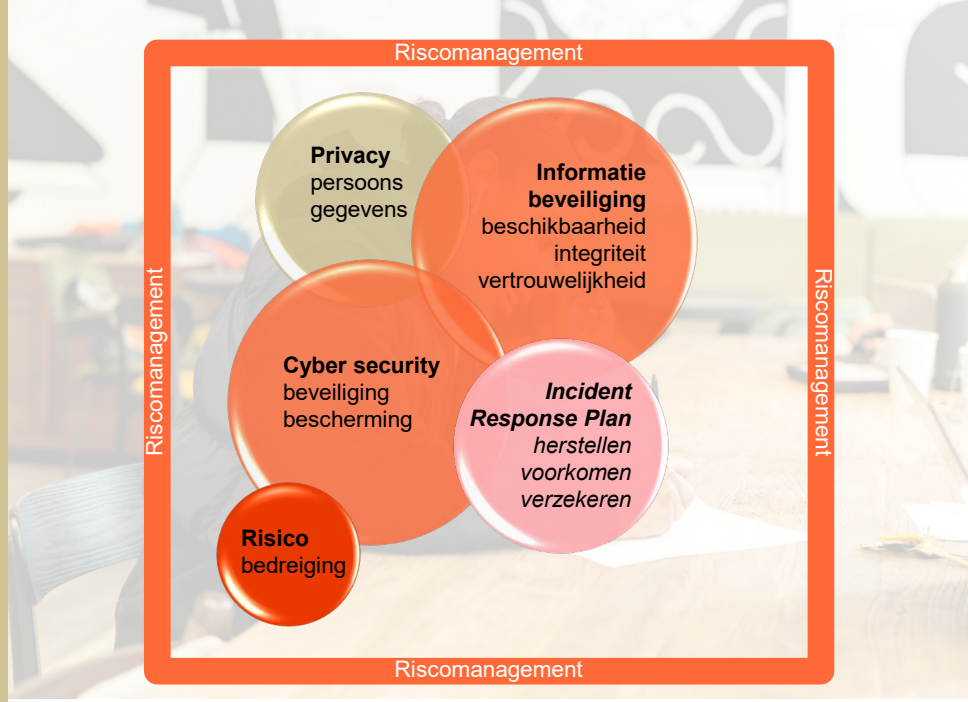
Informatiebeveiliging gaat meer over alles wat we doen om beschikbaarheid, integriteit en vertrouwelijkheid van de *Informatievoorziening* te garanderen.

is onze informatievoorziening goed beschermd tegen ongewenste toegang

Cyber security gaat meer over het beveiligen en beschermen van de *Informatievoorziening*.

Privacy heeft invloed op maatregelen voor IB en CS.
Risico bedreigingen hebben direct invloed op CS.

Een **Incident Response Plan** helpt bij een snelle en gestructureerde aanpak bij cyber incidenten.



"Bewust omgaan met risico's"

Informatiebeveiliging
.. uitgangspunten

- BIC → Baseline Informatiebeveiliging voor (woning)Corporaties.
- Strategie- en beleidsdocumenten Lieven de Key voor zover van toepassing.
- De verantwoordelijkheid voor IB ligt bij het (lijn)management, met de directie als eindverantwoordelijke.
- Risicomanagement vormt de basis voor de maatregelen → Three Lines of Defense
- Wet- en regelgeving, o.a. AVG, WOB, Wet Computercriminaliteit II

“Informatiebeveiliging is van ons allemaal”

*op zoek naar een goede balans tussen mens, organisatie en techniek in samenhang met **Cyber Security** én **Privacy**.*

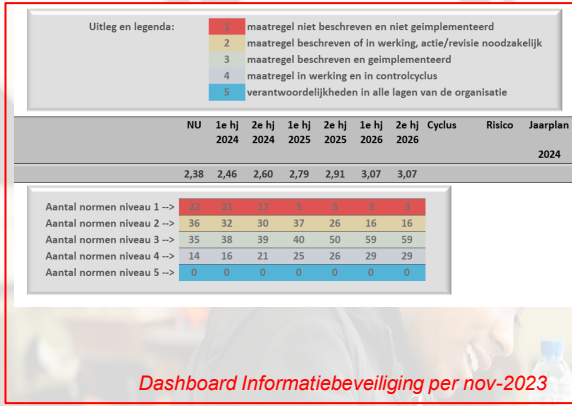
Publicaties

Corponet https://corponet.nl/
BIC 3.0:2019
ICT visie document
Informatiebeveiligingsbeleid 2024-2026: dv-2024-11
Visie Digitalisering DT 22 maart 2022

Informatiebeveiliging
.. wat doen we al

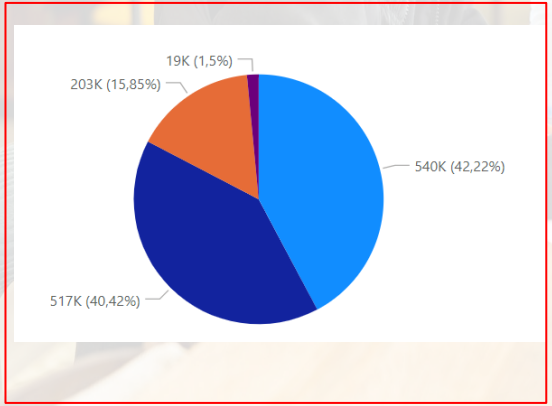
- Voorkomen dataverlies en beperken schade bij incidenten met Veeam
- Toegangsbeperking met autorisatie
  HRM functies gekoppeld aan rollen (RBAC) → balans
- Data minimalisatie met AVG scanner (Data Quality Company)
  Fileserver versus DMS
- Beschermen van data met Azure Record Management en Information Protection *
  Labels (notificaties) en delen in plaats van dupliceren
- Voorlichting, workshops en traingen *
  bewustwording → verplicht, herhalen en toetsen, óók onboarding

** in samenhang met Privacy en data-eigenaarschap*
→ kernteam Privacy, kerngebruikers, data- en proceseigenaren



Dashboard Informatiebeveiliging per nov-2023

7. Veilig Personeel
8. beheer van bedrijfsmiddelen
9. Toegangsbeveiliging
10. Cryptografie
11. Fysieke beveiliging en beveiliging van de omgeving
12. Beveiliging bedrijfsvoering
13 Communicatiebeveiliging
14. Acquisitie, ontwikkeling en onderhoud Informatiesystemen
15. Leveranciersrelaties
16. Beheer van informatiebeveiligingsincidenten
17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
18. Naleving

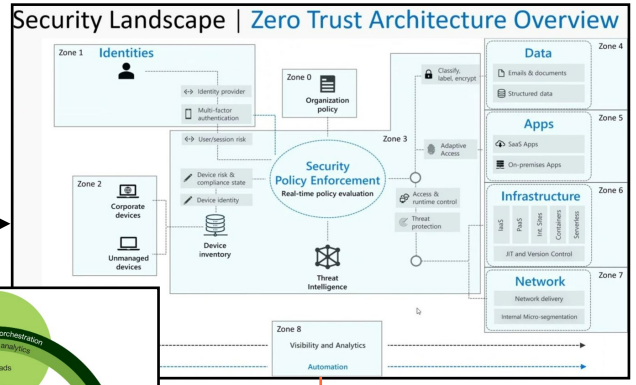


Een 24-uurs blik
- 26 geblokkeerde aanvallen uit Japan, Rusland en Italie; 181 poort scans
- 128 malicious URL's
- 40% van gescande data bevat een AVG issue, maar klopt dat wel?
- 463 van 475 devices fully managed by Trend

"De organisatie aan zet – mét ICT"
controleren, rapporteren, verwerken

Cyber Security
.. uitgangspunten

- Zero Trust Model → Microsoft
  never trust, always verify
- Model Zero Trust eXtended → Forrester
  data centraal
- Meerdere niveaus van beveiliging
- Combinatie van producten én leveranciers
- Standaardisatie in systemen én koppelingen
- Need to Know principe
- Periodieke scan én assessment

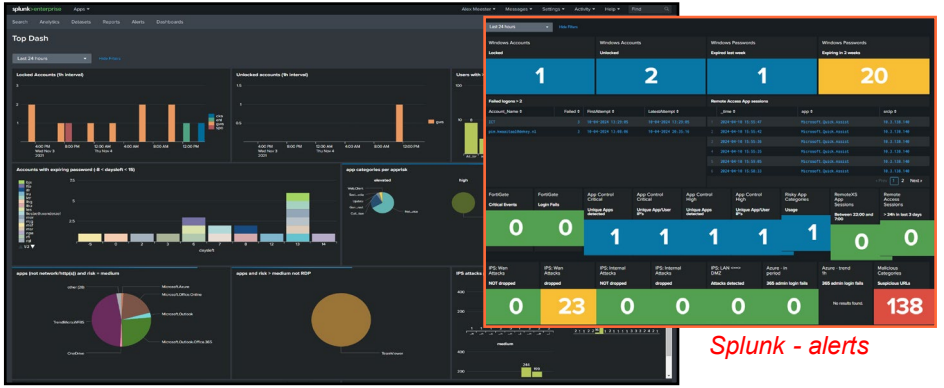


“Security baseline en risicoanalyse”
de basis voor de prioritering van de jaarplannen

Publicaties
Zero Trust Security – An enterprise guide by Jason Garbis, Jerry W. Chapman
Microsoft’s Zero Trust Model (https://www.microsoft.com/en-us/security/business/zero-trust)
Visie Digitalisering tbv DT 22 maart 2022
Cyber securitybeleid 2024-2025: dv-2024-11

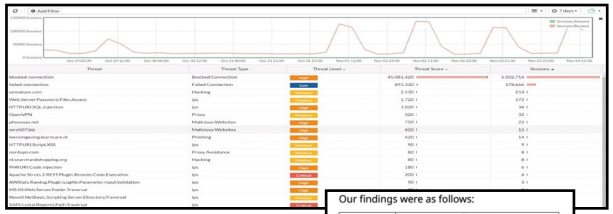
Cyber Security
.. wat doen we al

- Blijf up to date én **up to speed**
  aanpassen en ontwikkelen, maar blijf in control
- Beschermen met Trend Micro (incl. XDR), Defender én Fortigate security
  patronen en gedrag
- Monitoren met Apex Security – NSM/SOC, Splunk,Fortinet analyzer, Defender en Purview
  opvolging Defender en Purview
- Pentesten met Hack Defense
- Cyber Security Assessment (CSAT)
- Encryptie data(verkeer)
- IT-calamiteitenplan en verzekering *



Splunk - alerts

Network Secutiry Monintor - Splunk

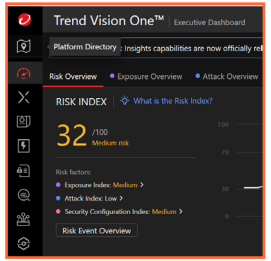


Detectie en blokkering

Our findings were as follows:

Risk	Amount			
	Previous	Resolved	New	Total
CRITICAL	-	-	-	-
HIGH	2	-	-	2
MEDIUM	27	-	-	27
LOW	21	-	-	21
Total	50	-	-	50

Pentest



Threat Monitor

** samenwerking, expertise én inzicht*
→ Met andere corporaties, maar ook daarbuiten.
→ Directie en management betrekken bij risico-bewustzijn én Incident Response Plan
→ ook samenhang met Privacy – DPIA is een belangrijke succesfactor

"Cyber security, de professionals aan zet"
zorg dat je zelf snapt waar het over gaat zodat je weet wat je kunt verwachten en moet doen wanneer het misgaat

Jouw rol in het geheel

- Heb jij data die je niet hoort te hebben?
  opschonen met de DQC AVG scanner, jij beslist
  → 40% data bevat AVG issue
- Heb jij scherp wie overal bij kan?
  Toegangsbeveiliging is niet alleen een verantwoordelijkheid van ICT
  → ken je organisatie, help elkaar (o.a. facturen)
- Weet jij hoe je medewerkers hun data opslaan?
  Outlook is géén archief
  → data in de juiste systemen
- Hoe houd je je medewerkers scherp?
  Trainen, toetsen en coachen
  → stay on board, dus ook herhalen

“Jouw security focus”

Een zelflerende security oplossing, durf je het aan?

Vragen?

De uitdaging is niet om Informatiebeveiliging, Privacy óf Cyber Security te organiseren, maar het in samenhang mét elkaar aan te pakken.

Lieven de Key

WTH – Woonforte

- Corporatie in Alphen aan den Rijn
- Ruim 11.500 VHE
- 120 medewerkers
- 1 kantoor
- Samenwerking in A+

WTH – Woonforte

- (Nog) meer bewustwording na hack 8 corporaties
- Informatiebeveiliging gebaseerd op BIC (3.0)
- Cyberverzekering - afweging
- ICT Calamiteitenplan (BCP)
- Awareness campagne 2024
  - Phishing
  - Mystery guest en caller
- Cyberoefening (geeft input voor BCP)

WTH – CorpoNet

- Via SIG Security: BIC 4.0 (downloaden via www.corponet.nl)
- Aanvulling BBB
- Kennisdeling via SIG Security
- CorpoNet participeert in Verbindingsgroep
- SIG Privacy start weer in 2024
- Werk samen : deel kennis!!

What the Hack

Vragen?

VOLKSHUISVESTING IS TOPSPORT
AEDES CORPORATIEDAG 18 APRIL 2024

vereniging van woningcorporaties
aedes

EINDE

BEDANKT VOOR UW AANDACHT