CISCO
SECURE

Risk & Compliance als drijvers voor Security Resilience

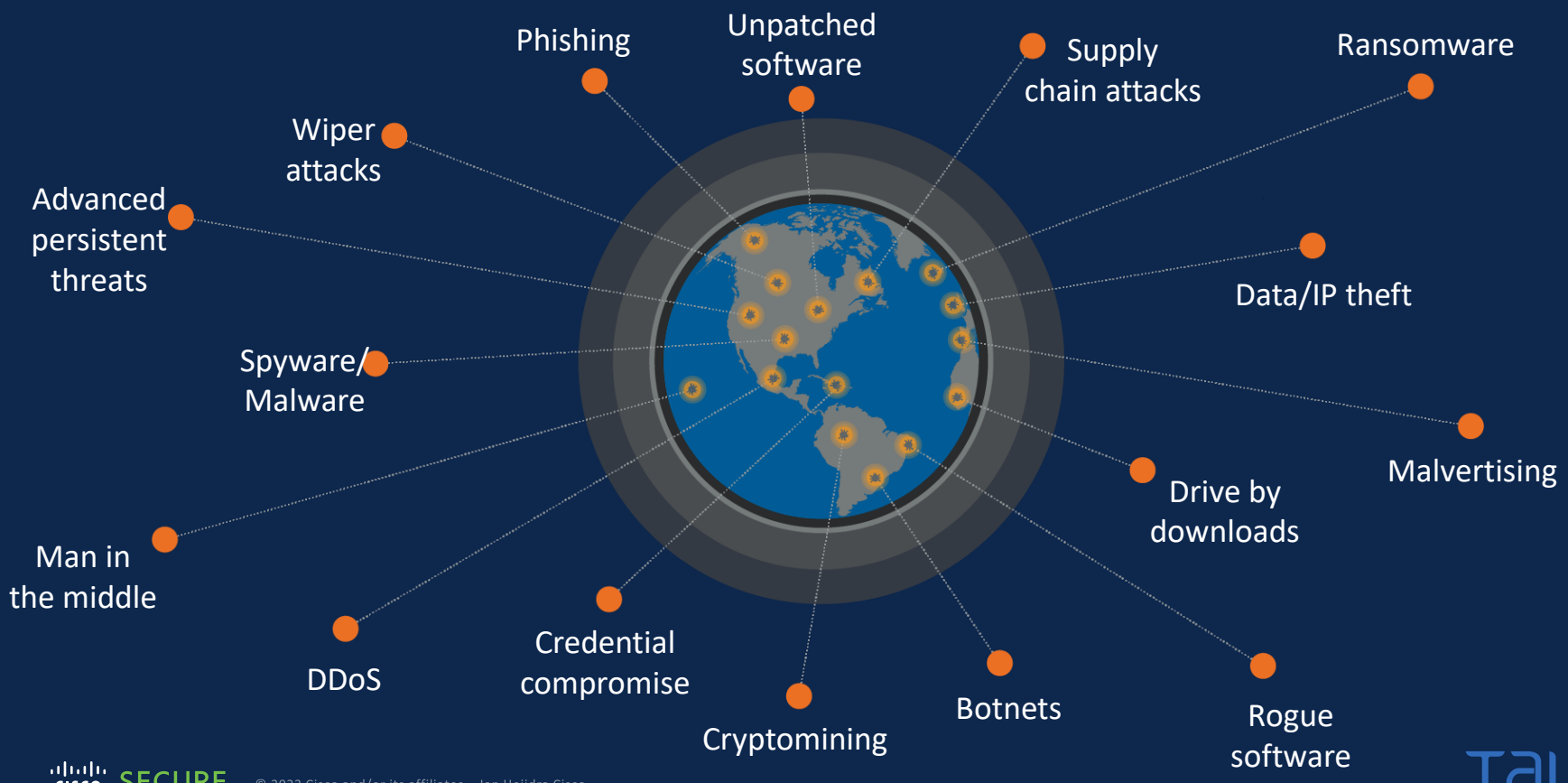
Security anno 2023

Jan Heijdra
Technology Evangelist
November-2022

127.0.0.1
86
36
14
12
1

Jan Heijdra - Technology Evangelist - Cisco Security
jheijdra@cisco.com

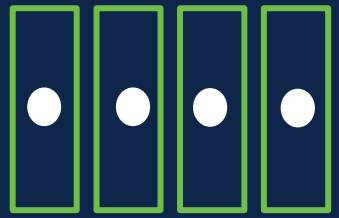
Threat Landscape



TALOS
Cisco Security Research

video

Resilience vraagt een **nieuwe security strategy**



Losse oplossingen

Security Resilience

Prevention	Detectie/response/recovery
Siloed	Connected (mesh/platform)
Alert/threat-centric	Context-gedreven

5 stappen naar weerbaarheid

1. **Zie meer**
   telemetry vanuit ecosystem, actief monitoring en filteren
2. **Voorsorteren op wat komt :** Threat Intelligence
   actionable intelligence en expertise
3. **Acties:** Prioritiseer wat belangrijk is
   risk-based context gedreven analyse, continuous trust assessment
4. **Vul de gaten met een ecosysteem**
   open platform voor users/devices/networks/applications
5. **Elke dag beter:** Optimaliseer effectiviteit & efficiency
   orchestratreer, automatiseer

Data Security (en Privacy) Uitdaging

Vragen die velen niet kunnen beantwoorden:

- Hoeveel data is “kritiek”?
- Wie is de eigenaar van de data ?
- Waar staat de data?
- Wie heeft er toegang tot de data?
- Is de data extern verplaatst?
- Welk percentage bevat identiteitsdata?
- Voldoen we aan de wet?

Beschikbaarheid | Integriteit | Geheimhouding

Security anno 2023

- Weerbaarheid organisaties start bij bewustwording
- Wetgeving (NIS-2/Dora/EU Cyber Resilience Act) naar compliance
- Geopolitieke veranderingen en afhankelijkheden
- Beschikbaarheid security specialisten
- Detectie & Response mogelijkheden
- Risico analyses
- ML/Quantum in handen cybercriminelen?
- Aanhoudende panedemie
- Duurzame IT/Security oplossingen

Cybersecurity: Parliament adopts new law to strengthen EU-wide resilience

Press Releases PLENARY SESSION ITRE 10-11-2022 - 11:50

NIS2: Zorgplicht & Meldplicht

- **Zorgplicht:**
  - Entiteiten moeten passende en evenredige maatregelen nemen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen die zij gebruiken voor hun werkzaamheden of voor het verlenen van hun dienst te beheersen
  - Deze maatregelen omvatten o.a. afhandeling van incidenten, bedrijfscontinuïteit en de beveiliging van toeleveringsketens (supply chain security)

- **Meldplicht**
  - Meldplicht voor significante incidenten bij CSIRT of bevoegde autoriteit (toezichthouder)
  - Getrapte melding: "early warning" binnen 24 uur, melding binnen 72 uur, eindverslag binnen een maand

Tijdlijn NIS2

- Voorlopig politiek akkoord bereikt (28 juni 2022)
- Richtlijn is formeel akkoord na stemming in EP en Raad (verwacht dit najaar)
- Lidstaten hebben 21 maanden om richtlijn te transponeren in nationale wetgeving

Behoefte aan 24/7 monitoring – Detectie en Response

- Veel diensten zijn alleen gefocused op detectie en alerting

- Wanneer er niks met notificaties wordt gedaan is dienst minder bruikbaar

- Behoefte aan 24/7 monitoring op basis vana telemetry correlatie en auto-response mogelijkheden

- Cisco SecureX eerste stap voor Threat Hunting, monitoring en Automatische response acties.
(Conscia Case St. Franciscus op 8 December in Corpus)

- Cisco Managed Detectie en Response services

- Vergroten paraatheid op incidenten en crises

VWS trekt hierin samen met het Cyberteam en het Departementaal Coördinatiecentrum Crisisbeheersing (DCC)VWS op, zodat we, indien nodig, in de nationale crisisstructuur bijeen kunnen komen. Het VWS programma Realisatie Digitale Ondersteuning (RDO) heeft een (open source) digitale kwetsbaarheid analyse tool opgeleverd in juli 2022. Hiermee kunnen digitale zwakheden in IT-systemen en technische omgevingen continu volledig geautomatiseerd worden opgespoord en gerapporteerd. Er is dus altijd een actueel beeld van de digitale kwetsbaarheden die direct, en soms zelfs automatisch, moeten worden opgelost. Hierdoor worden we minder kwetsbaar voor digitale dreigingen. Dit cybersecurity middel is ontstaan en wordt onderhouden om de coronatoepassingen veilig te houden, maar kan in principe in elke organisatie (overheid en non-profit) generiek worden ingezet.

“RDO heeft een digitale kwetsbaarheden analyse tool (KAT) opgeleverd”

Strategische visie van het ministerie van Volksgezondheid, Welzijn en Sport (VWS) op informatievoorziening en de prioriteiten van VWS op het gebied van digitalisering en informatisering voor de jaren 2023-2027

Feiten

Onderzoek laat zien dat…

- Gemiddeld 55 nieuwe software vulnerabilities gepubliceerd per dag in 2021.
- 95% van de IT assets heeft minimal 1 vulnerability.
- Organizaties verhelpen ongeveer 1 in 10 vulnerabilities per maand..

Source: Prioritization to Prediction, Volume 8, The Cyentia Institute & Kenna Security

Is Vulnerability management een eindelooze loop van het vinden en oplossen van issues?

Aantallen vulnerabilities

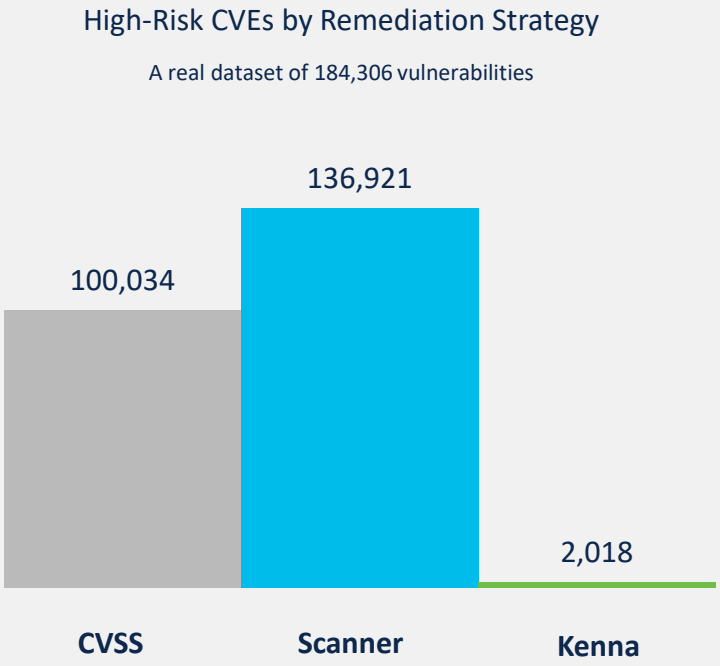
We kunnen niet alles oplossen

Wrijving tussen security en IT

Rapportage op risico niet mogelijk

Controle over je risico’s

Risico’s en hun scores



1.09% of these CVEs are considered high-risk by Kenna

- ✓ 134,903 fewer vulnerabilities to remediate compared to the scanner
- ✓ 98,016 fewer vulnerabilities to remediate compared to CVSS

Missed high-risk vulns

111 CVEs found high by Kenna but not found high by scanner

51 CVEs found high by Kenna but not found high by CVSS

Praten over Risico's ….. Ransomware

1) Email Ransomware Protection

2) Web Ransomware Protection

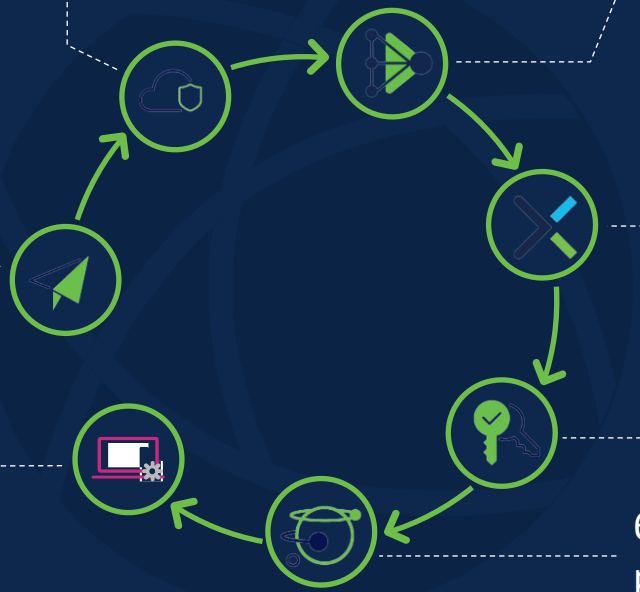
3) Endpoint Ransomware Protection

4) Ransomware investigation and response

5) Access ransomware protection

6) Network ransomware protection

7) Proactively recommend policy and identify threats

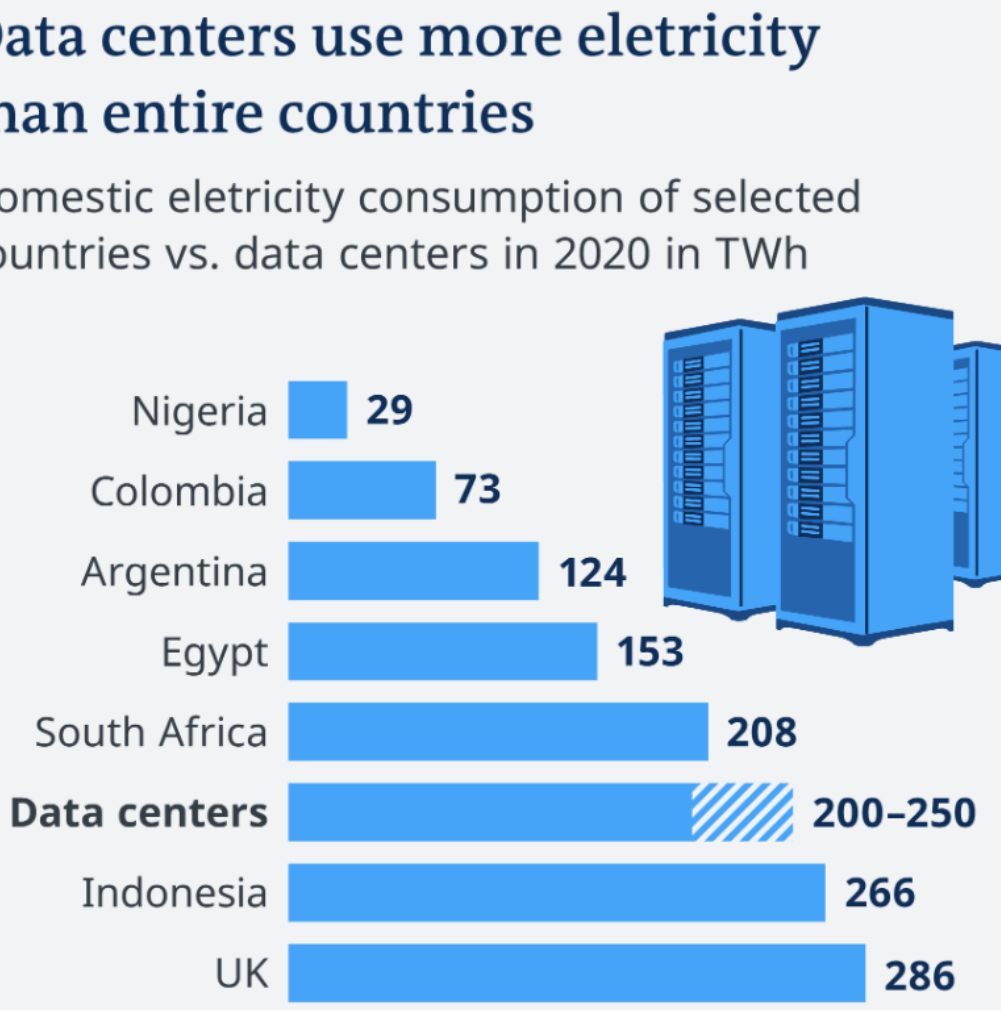


Gezamenlijke risico’s hebben een gezamenlijke aanpak nodig

ICT is not on a path to reduce emissions in line with recommendations from climate science

Source:
https://www.sciencedirect.com/science/article/pii/S2666389921001884

EU Data centers verbuikten 2.7 procent van totale elektriciteitsgebruik in de EU.



We hebben als professionals een plicht om security top of mind te krijgen


cisco
SECURE

Zero Trust?

Verificatie , elke keer opnieuw

Ongeacht wie de gebruiker is
Ongeacht wel apparaat de gebruiker gebruikt
Ongeacht de locatie
Ongeacht de applicaties die men gebruikt

Vertrouw je dit AAPIE?