GUARDIAN 360°

Wentzo

Informatiebeveiliging, het is meer dan alleen maar IT

Jeff Scipio | Partner Director Guardian360 | j.scipio@guardian360.nl | +31 6 22 25 74 74

De realiteit …

27 oktober 2022

NCSC (Nationaal Cybersecurity Centrum) overspoeld door cyberincidenten. Het aantal meldingen van cyberincidenten is in vijf jaar verdrievoudigd. Vorig jaar ontving Nationaal Cybersecurity Centrum (NCSC) ruim tweeduizend meldingen. Ook worden aanvallen heviger. Bedrijven betalen miljoenen losgeld om van hackers af te zijn. Dit meldt het AD.

7 oktober 2022

Door een hack op IT-bedrijf ID-ware zijn persoons- en pasgegevens van tal van Nederlandse (overheids)organisaties gelekt. De Volkskrant schrijft dat onder meer gegevens van de ministeries van Justitie en Veiligheid, Defensie, Financiën en Binnenlandse Zaken, de Politieacademie, Prorail, TNO en Alliander zijn gelekt. Ook een grote hoeveelheid data van ID-ware zelf is gestolen en online gezet.

30 september 2022

Microsoft bevestigt dat cybercriminelen twee zero-day kwetsbaarheden misbruiken voor aanvallen op Microsoft Exchange Server 2013, 2016 en 2019. De kwetsbaarheden stellen cybercriminelen in staat om remote code execution-aanvallen uit te voeren.

Zien we door de bomen het bos nog wel?

Wat komt er op ons af?

Oude vertrouwde virussen

Malware

Ransomware

Afpersing door datalek

Keten aanvallen

Wie zijn de boosdoeners?

Online criminelen

Activisten

Georganiseerde bendes

Landelijke actoren

Iedereen is wel een doelwit voor iemand, je zou er moedeloos van worden!

GUARDIAN 360°

Wentzo

100% beveiliging bestaat niet, 'in control' zijn wel!

Informatiebeveiliging in relatie tot risicobeheersing

"Heilige drie-eenheid" binnen informatiebeveiliging:
- Mensen
- Processen
- Techniek

Guardian360 voegt een andere drie-eenheid toe:
- Preventie
- Detectie
- Herstel

" Everything on black is not a risk management strategy, Hoskins."

GUARDIAN 360°

Wentzo

Guardian360 diensten

- Continu preventieve scanning en monitoring van:
  - IP-adressen (Intern en extern)
  - Websites en webapplicaties
  - IOT & Scada devices
- Detectie door Hacker Alert
- Compliance module (processen), o.a.:
  - ISO27001
  - NEN7510
  - GDPR/ AVG
  - OWASP (Open Web Application Security)

Dashboard
Relations
Issues
Integration

Dashboard

HACKER ALERTS	CRITICAL RISKS	HIGH RISKS	MEDIUM RISKS	LOW RISKS	INFORMATIONAL RISKS
0	340	1064	9495	2901	3692

ISO 27001:2013	ISO 27001:2017	GDPR/AVG	NEN 7510:2017	ISO 27017:2015	OWASP
8	8	7	8	8	7

NCSC	PCI DSS	BIC	NOREA	BIO	SAMBO ICT
7	8	8	7	8	7

DIGID 2.0	DIGID 1.0
7	7

TOTAL SCAN OBJECTS	TOTAL IP ADDRESSES	TOTAL WEBSITES
1184	83614	231

RISK LEVEL DISTRIBUTION

HOE ZIEN WIJ SECURITY?

1. Is niet een eenmalig iets maar een continue proces

2. Is niet alleen voor de IT manager belangrijk. Ook het MT moet er iets van vinden (beleid, budget enz.)

3. Is de basis voor een goede bedrijfsvoering. Borgen van de continuïteit (beschermen van de belangrijkste assets)

4. Is van belang om aan te kunnen tonen dat het bedrijf 'In Control' is

5. Rapportage moet door het MT te lezen en te begrijpen zijn (zij moeten immers het security beleid maken en hebben daar budget voor!)

Informatiebeleid; zorg ervoor dat de Security Officer en de Privacy Officer/ FG (Functionaris Gegevensbescherming) dezelfde 'bladzijde lezen'

Informatiebeveiliging is niet uitsluitend een IT aangelegenheid

- Voorzie de Security Officer van een overzicht:
  - Met IT kwetsbaarheden
  - Met oplossingen zodat deze snel opgelost kunnen worden

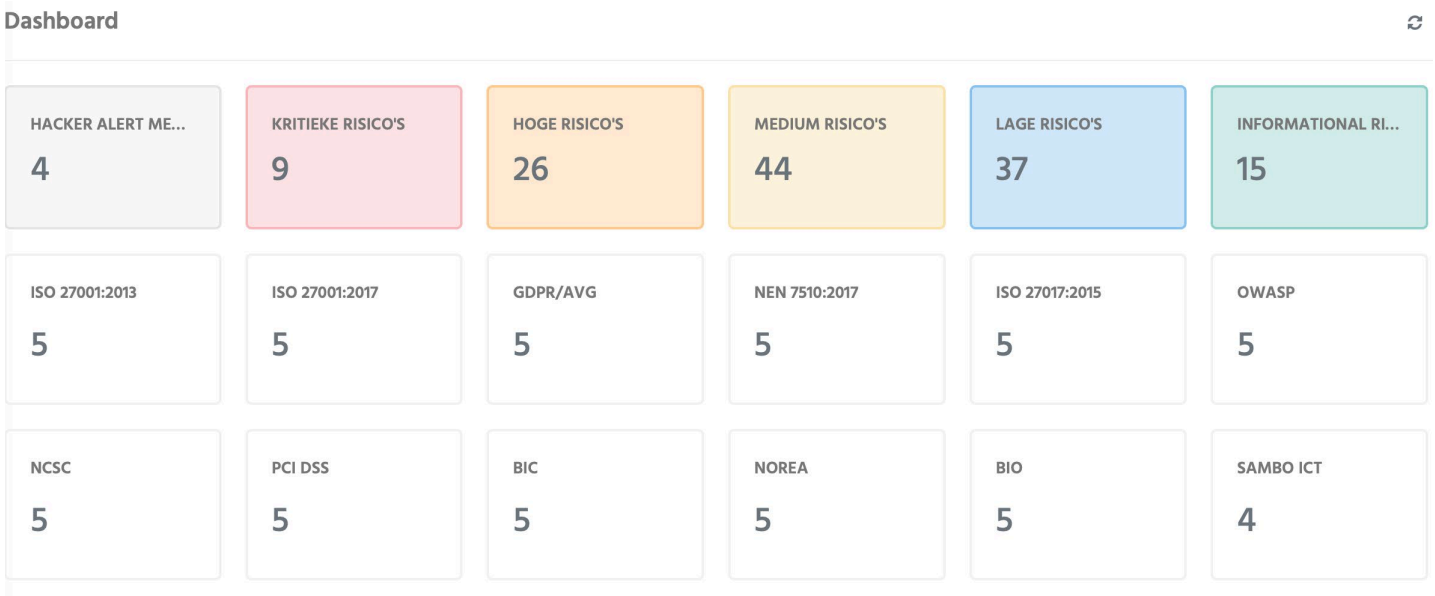
- Voorzie de Privacy Officer / FG van een overzicht:
  - Per gevonden kwetsbaarheid gerelateerd aan afwijking van normeringen
  - Met oplossingen zodat hij samen met de Security Officer de juiste mitigerende maatregelen kan nemen

IT vulnerability management; maak afwijkingen van normeringen inzichtelijk

	BIC	Baseline Informatiebeveiliging Corporaties	5	116

Non-Conformiteit	Referentie	Paragraaf	Beschrijving	Issues
Inputvalidatie	G360-001	14.2.1, 14.2.5	Inputvalidatie wordt uitgevoerd om ervoor te zorgen dat alleen correct gevormde gegevens de werkstroom binnengaan in een informatiesysteem, waardoor wordt voorkomen dat onjuist geformuleerde gegevens in de database blijven en een storing in verschillende stroomafwaartse componenten veroorzaken. Gegevens van alle potentieel niet-vertrouwde bronnen moeten worden onderworpen aan inputvalidatie, waaronder niet alleen webklanten op het internet, maar ook feeds via extranetten, leveranciers, partners, leveranciers of toezichthouders, die elk afzonderlijk kunnen worden gecompromitteerd en misvormd kunnen worden gegevens. Bron: https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Input_Validation_Cheat_Sheet.md	19
Software Misconfiguratie	G360-002	12.5.1, 14.2.2, 14.2.3	Goede beveiliging vereist dat een veilige configuratie wordt gedefinieerd en geïmplementeerd voor de toepassing, frameworks, applicatieserver, webserver, databaseserver en platform. Veilige instellingen moeten worden gedefinieerd, geïmplementeerd en onderhouden, omdat standaardinstellingen vaak onveilig zijn. Bron: https://www.owasp.org/index.php/Top_10_2013-Top_10	42
Systeeminformatie Publicering	G360-003	9.4.1	Veel webapplicaties beschermen gevoelige gegevens, zoals softwareversies, (gevoelige) configuratiebestanden en verificatiegegevens, niet correct. Aanvallers kunnen die informatie misbruiken voor hun kwaadwillige doel. Bron: https://www.owasp.org/index.php/Top_10_2013-Top_10	15
Netwerk Misconfiguratie	G360-006	13.1.1, 13.2.1, 13.2.2, 13.2.3	Netwerk Misconfiguratie wordt gedefinieerd als de beveiligingszwakte die wordt veroorzaakt door een toepassing die geen maatregelen neemt om het netwerkverkeer te beschermen met oplossingen zoals TLS. Bron: https://www.leansecurity.com.au/insufficient-transport-layer-protection	33
Zwakke Wachtwoorden	G360-007	9.2.4, 9.3.1	Aanvallers hebben toegang tot honderden miljoenen geldige gebruikersnaam- en wachtwoordcombinaties voor inbelvervulling, standaard beheerdersaccountlijsten, geautomatiseerde brute force en woordenboekaanvaltools. Implementeer deze niet met standaard referenties, met name voor beheerders. Aanvallers kunnen zwakke referenties detecteren en deze gebruiken met behulp van geautomatiseerde	7

Inzichtelijk maken welke gevaren (kwetsbaarheden) er zijn



GUARDIAN 360°

Wentzo

Inzichtelijk maken van zwakke wachtwoorden

Zwakke Wachtwoorden

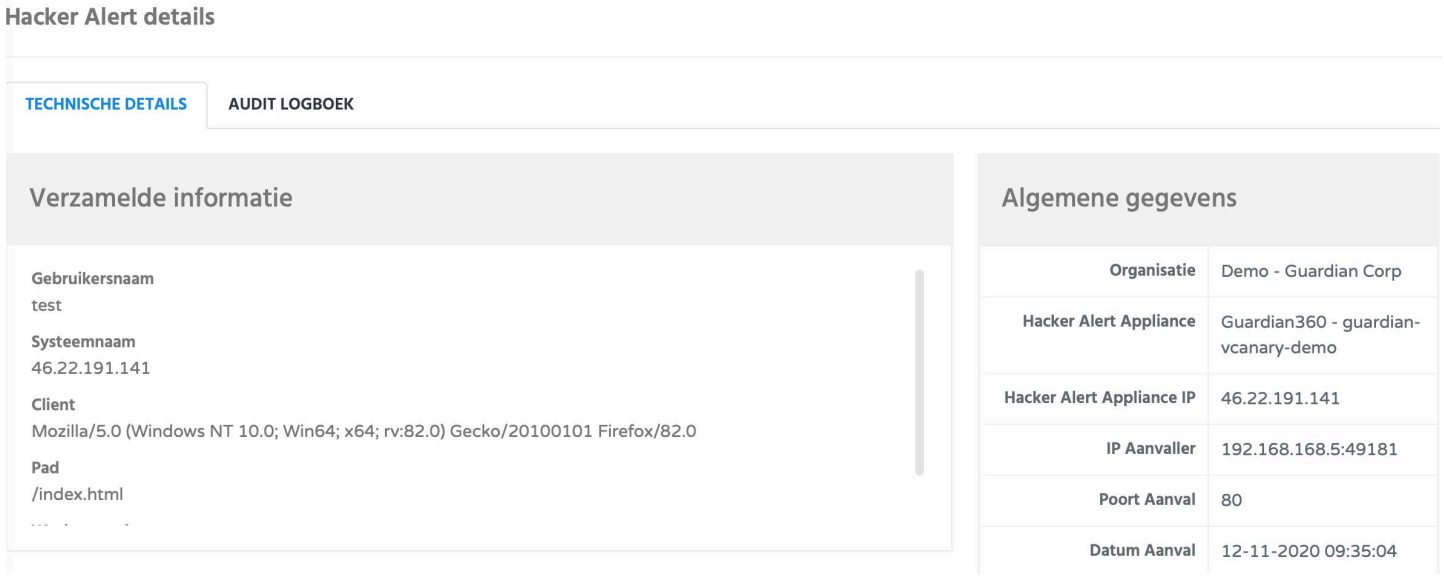
Aanvallers hebben toegang tot honderden miljoenen geldige gebruikersnaam- en wachtwoordcombinaties voor inbelvervulling, standaard beheerdersaccountlijsten, geautomatiseerde brute force en woordenboekaanvaltools. Implementeer deze niet met standaard referenties, met name voor beheerders. Aanvallers kunnen zwakke referenties detecteren en deze gebruiken met behulp van geautomatiseerde hulpmiddelen met wachtwoordlijsten en woordenboekaanvallen.

ISO 27001:2013	9.2.4, 9.3.1
ISO 27001:2017	9.2.4, 9.3.1
GDPR/AVG	32(1B), 5(1F, 2)
NEN 7510:2017	9.2.4, 9.3.1
ISO 27017:2015	9.2.4, 9.3.1
OWASP	OTG-AUTHN-002, OTG-CONFIG-001
NCSC	B.02, U/PW.05
PCI DSS	8.4, 8.5

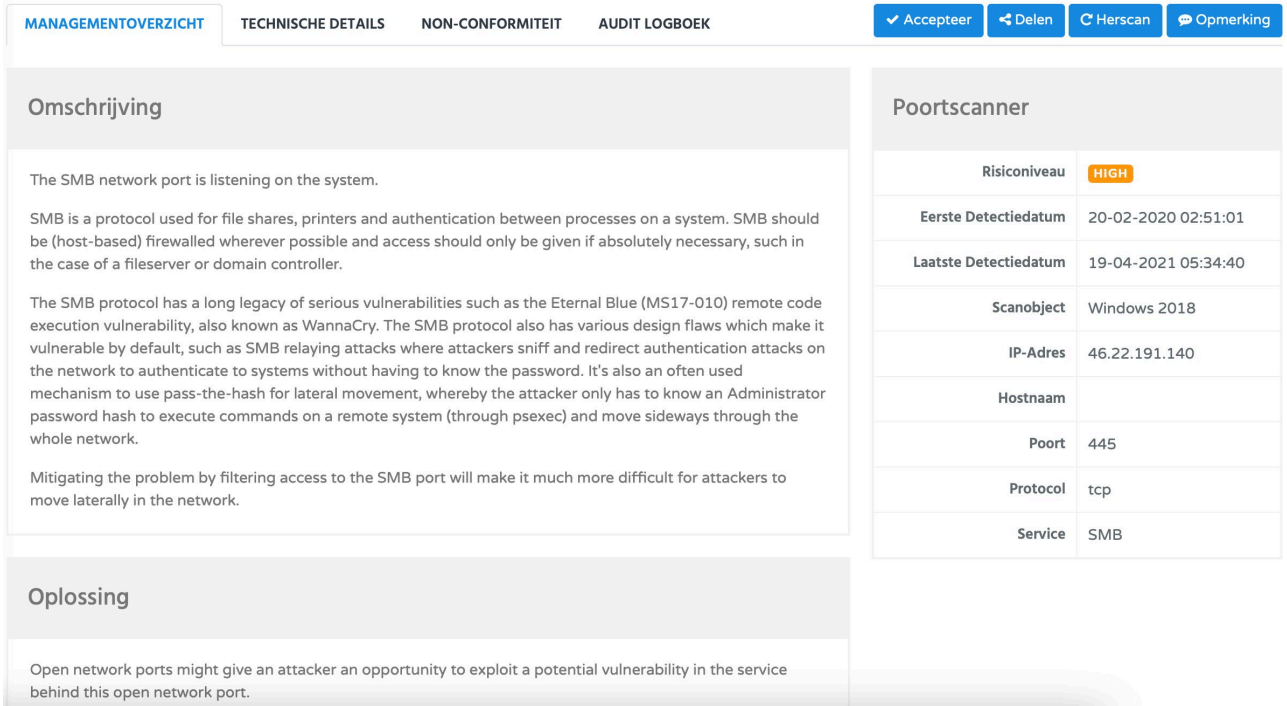
Wachtwoordscanner

Risiconiveau	CRITICAL
Eerste Detectiedatum	22-07-2020 10:03:16
Laatste Detectiedatum	19-04-2021 08:20:20
Scanobject	OWASP Broken Web Apps
IP-Adres	46.22.191.139
Hostnaam	
Poort	445
Protocol	tcp
Service	SMB

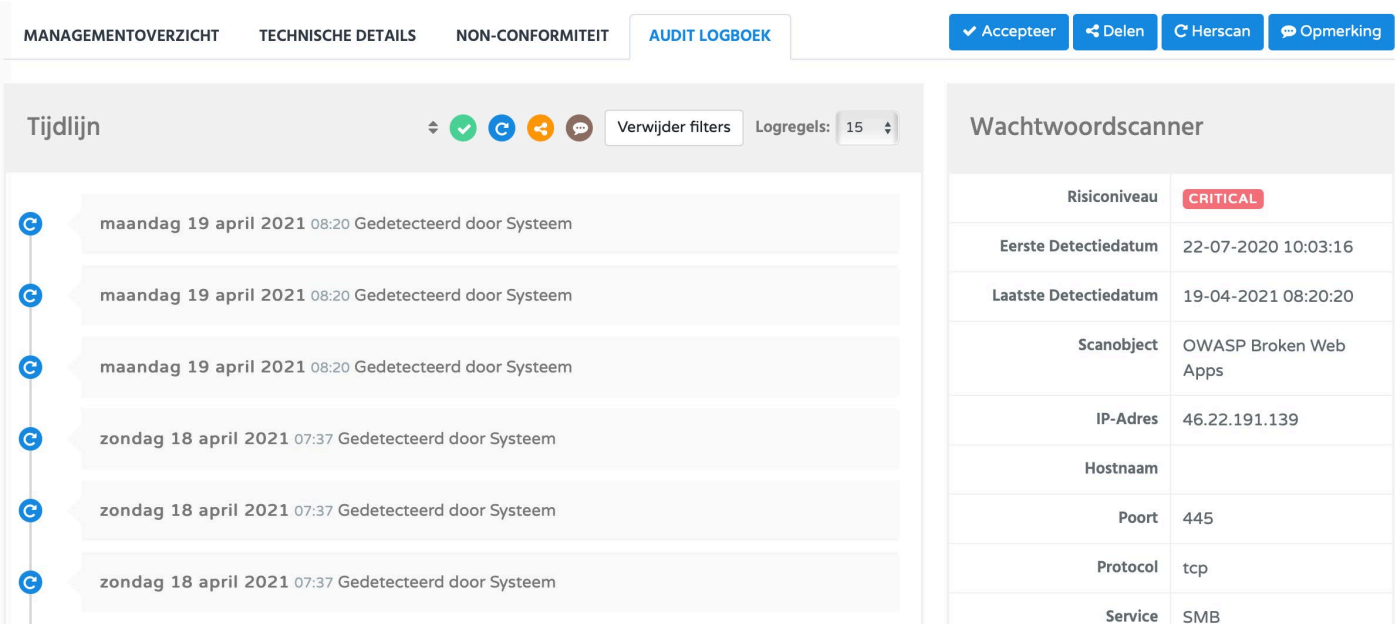
Waarschuwen wanneer een hack dreigt plaats te vinden



IT kwetsbaarheden management; maak kwetsbaarheden inzichtelijk



IT kwetsbaarheden management; maak audit trails inzichtelijk



IT kwetsbaarheden management zorgt ervoor dat u 'in control' bent

Zwakke Wachtwoorden

Aanvallers hebben toegang tot honderden miljoenen geldige gebruikersnaam- en wachtwoordcombinaties voor inbelvervulling, standaard beheerdersaccountlijsten, geautomatiseerde brute force en woordenboekaanvaltools. Implementeer deze niet met standaard referenties, met name voor beheerders. Aanvallers kunnen zwakke referenties detecteren en deze gebruiken met behulp van geautomatiseerde hulpmiddelen met wachtwoordlijsten en woordenboekaanvallen.

ISO 27001:2013	9.2.4, 9.3.1
ISO 27001:2017	9.2.4, 9.3.1
GDPR/AVG	32(1B), 5(1F, 2)
NEN 7510:2017	9.2.4, 9.3.1
ISO 27017:2015	9.2.4, 9.3.1
OWASP	OTG-AUTHN-002, OTG-CONFIG-001
NCSC	B.02, U/PW.05
PCI DSS	8.4, 8.5

Wachtwoordscanner

Risiconiveau	CRITICAL
Eerste Detectiedatum	22-07-2020 10:03:16
Laatste Detectiedatum	19-04-2021 08:20:20
Scanobject	OWASP Broken Web Apps
IP-Adres	46.22.191.139
Hostnaam	
Poort	445
Protocol	tcp
Service	SMB

Hoe nu verder?

1. Vraag aan je huidige IT leverancier of zij het volgende inzichtelijk willen maken?
    1. Een overzicht van de gevonden IT kwetsbaarheden
    2. Hoe zij hackers proberen te detecteren
    3. Hoe zij afwijkingen van de Normeringen/ Compliancy constateren en weergeven

2. Cyber veiligheid hoeft niet en duur en ingewikkeld te zijn.
    1. Investeer in een platform welke betaalbaar is welke eenvoudig te lezen informatie levert

3. Kies voor een Nederlands ISO gecertificeerd cyber security bedrijf waarbij de data in NL blijft en welke de afwijkingen van normeringen/ compliancy in kaart brengt

Ter overdenking

1. Zelf ben je verantwoordelijk om je IT leverancier te controleren

2. IT leverancier is NIET verantwoordelijk voor jullie Informatiebeveiligingsbeleid

3. Zelf ben je verantwoordelijk over hoe er met data omgesprongen wordt

4. **Informatiebeveiliging; ervoor zorgen en kunnen aantonen**

dat je 'In Control' bent.

Guardian360 is 100% Nederlands

- Gevestigd in Nederland
- 100% NL Security SaaS ontwikkelaar
- Nederlands en Europees recht
- Cloudapplicatie die draait op eigen servers in Nederlandse datacentra
- ISO en NEN gecertificeerd
- Opgericht in 2015

Contact:

- Jeff Scipio, Partner Director
- 06 22 25 74 74 j.scipio@guardian360.nl

GUARDIAN 360°