8 nov
InAudit
1

Cybersecurity: moet

ROBBERT KRAMER

Cybersecurity: moet

8 nov
InAudit
2

- Wat is Cybersecurity
  - Verschijningsvormen
  - In perspectief
  - Wettelijke kader
- Maatregelen
  - SANS
  - NCSC
  - NIST
- Samenwerken
  - In de sector/regio/Keten
  - Traffic Light Protocol
  - Responsible Disclosure

Wat is Cybersecurity

8 nov
InAudit
3

CyberCrime

- Malware
- Computerinbraak
- Websiteaanvallen
- Botnets
- Denial of Service (DoS)
- Social engineering
- E-mail-gerelateerde verschijningsvormen

Wat is Cybersecurity

- Kwetsbaar
  - Vulnerability staat centraal. Hacker heeft “sleutel” en is op zoek naar een deur waar deze op past.
- Doelwit
  - Doelwit staat central. Hacker zoekt de “sleutel” om binnen te komen (deur te openen).

8 nov
InAudit
5

Wat is Cybersecurity

Wet gegevensverwerking en meldplicht cybersecurity (Wgmc)

Cybersecuritywet

Cybercrime omvat elke strafbare gedraging waarbij voor de uitvoering het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is

computercriminaliteit

Cybersecurity

8 nov
InAudit
6

Moet

Maatregelen (Sans/CIS)

8 nov
InAudit
7

CIS Controls™

V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Maatregelen (NCSC)

https://www.ncsc.nl/actueel/whitepapers/handreiking-cybercrime.html

Enkele hoofdstukken

- Incidentenopvolging
- Onderzoeken van incidenten
- Aangifte doen

Maatregelen (NIST)

- Identify
- Protect
- Detect
- Respond
- Recover

Cybersecurity

8 nov
InAudit
10

Kan

Samenwerken

8 nov
InAudit
11

- Samenwerken in de sector
- Samenwerken in de regio
- Samenwerken in de keten

Samenwerken

- Information Sharing and Analysis Centre
- TLP:RED = Not for disclosure, restricted to participants only. Information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
- TLP:AMBER = Limited disclosure, restricted to participants' organizations. Recipients may only share information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
- TLP:GREEN = Limited disclosure, restricted to the community. Sources may use Information may not be released outside of the community.
- TLP:WHITE = Disclosure is not limited. Information may be distributed without restriction.

Responsible Disclosure

Coordinated Vulnerability Disclosure

Met dit beleid geven bedrijven aan open te staan voor meldingen van kwetsbaarheden van buitenaf, beschrijven ze de randvoorwaarden en geven ze beloftes. Voor melders schiep dit duidelijkheid en creëerde een enigszins veilige omgeving om onderzoek te doen en kwetsbaarheden te melden, zonder direct een strafbaar feit te plegen.

Cybersecurity

8 nov
InAudit
14

Wil

Cybersecurity

8 nov
InAudit
15

Moet + Kan + Wil

DNB organiseert 19 december een workshop cybersecurity voor bestuurders en compliance officers van betaalinstellingen en elektronischgeldinstellingen

Cybersecurity

Moet want bestaat
Kan gestructureerd
Wil je samen doen

DNB organiseert 12 februari een seminar over informatiebeveiliging en cybersecurity voor alle onder toezicht staande instellingen.