Triple C
Cyber Crime Control

16 april 2019

NIVE OPLEIDINGEN

E11EVEN

Agenda

- Inleiding
- Triple C: Cyber Crime Control (CCC)
  - CYBER
    - Hoe ziet het digitale landschap er uit?
    - Internet of things
    - Darkweb
    - Quantum computing
  - CRIME
    - 11 voorbeelden van cybercriminaliteit
  - CONTROL
    - Wanneer ben ik in control?
    - Interactieve enquête
    - De werk- en denkwijze van een hacker
    - Controls
- Vragen stellen aan een ethical hacker

Inleiding (1/2)

Theunis Kloosterman

1973, Wommels

Heerenveen

E11EVEN B.V.

- Registeraccountant (RUG)
- IT-auditor (VU)
- Gerechtelijk deskundige (Leiden)

Frysk Jeugd Orkest

- Vz stichtingsbestuur

Kevin Morssink

1991, Zutphen

Heerenveen

E11EVEN B.V.

- Ethical hacker
- ICT-security consultant
- Forensic IT-specialist
- Software ontwikkelaar

CodeIgniter Security Team

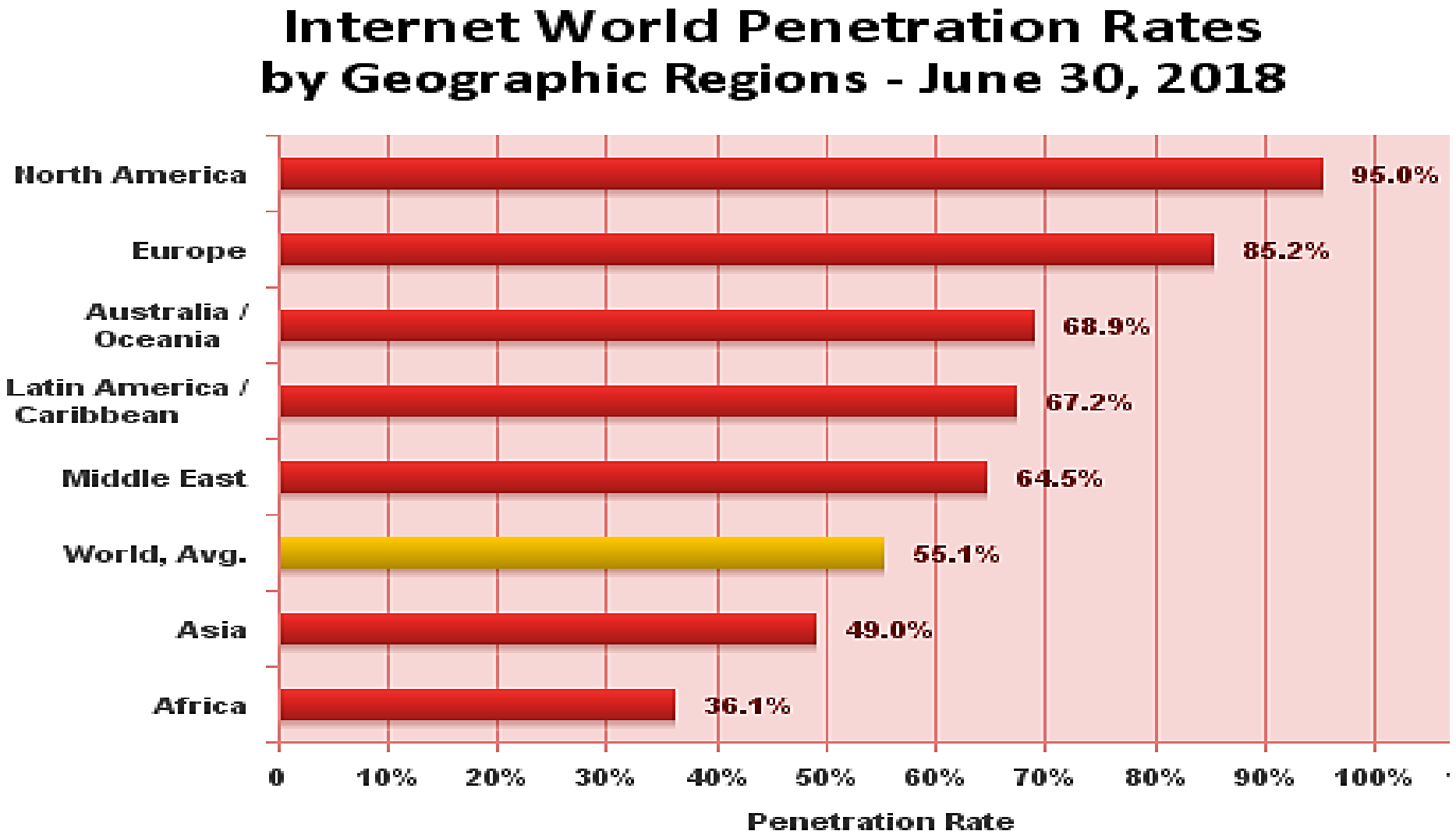
Inleiding (2/2)

- Waarheidsvinding
  - Forensic accounting
  - Forensic technology
  - Deskundigen onderzoek
- Software as a service
  - Secure dataplatform APO11O™
- Hacking on demand
  - Ethical hacking
  - ICT-security scans
  - Penetratietesten
  - Advisering over beleid en gedrag

Cyber: Hoe ziet het digitale landschap er uit?

- 4,2 miljard internetgebruikers wereldwijd
- 55,1% van de wereldpopulatie
- Internetdichtheid in Nederland 98%
- Stijging bandbreedte
- Steeds meer apparaten online bereikbaar
- Ontwikkelingen rekenkracht computers
- Steeds afhankelijker van ICT

Cyber: Hoe ziet het digitale landschap er uit?



Cyber: Internet of Things (IoT)

- De meerderheid van internetgebruikers zijn semi-intelligente apparaten die autonome beslissingen kunnen nemen
- Door mensen bediende apparaten in de minderheid
- Particulieren en bedrijven

Cyber: Darkweb

Cyber: Quantum computing

- Hoelang zijn de huidige encryptiestandaarden nog veilig?
- Kwantumalgoritme van Shor (1994)
- NSA investeert 79,7 miljoen USD in project "Penetrating Hard Targets" om een kwantumcomputer te ontwikkelen om encryptie te ontsleutelen (2014)
- Bekendste vorm van encryptie in dagelijks gebruik HTTPS (TLS/SSL)

Crime

- 11 voorbeelden van actuele berichten

Control: Wanneer ben ik in control?

- Organisatorische maatregelen
- Technische maatregelen

Control: Interactieve enquête

https://e11even.nl/nive

Control: De denkwijze van een hacker

- Om je te wapenen en je te beschermen is inzicht nodig in de werkwijze van de vijand
- Veelvoorkomende design flaw is **security through obscurity**: “Security through obscurity would be burying your money under a tree. The only thing that makes it safe is no one knows it's there.”

Control: De werkwijze van een hacker

- Verkennen
  - Identificeren *(mens en machine)*
  - Prioriteren *(zwakste schakels)*
- Scannen
  - Crawlen / indexeren
  - Passief
    - *Fingerprinting*
    - *Inspecting*
    - *Sniffing*
    - *Open bronnen*
  - Actief
    - *Injecteren*
    - *Brute-forcing*
    - *Exploiting*
    - *Fuzzing*
- Analyseren en relateren
  - *WHOIS registers*
  - *Databases met historische gegevens*
  - *Databases met bekende kwetsbaarheden (CVE, exploits)*
- Testen
- Rapporteren *(OWASP, CVSS)*

Control: Controls

- Organisatorisch
  - Creëer beveiligingsbewustzijn
  - Formuleer informatiebeveiligingsbeleid
    - Heldere, duidelijke regels en afspraken
    - Compliant met wet – en regelgeving
  - Identificeer en inventariseer ICT-systemen waar verwerking van data plaatsvindt
  - Bepaal het eigenaarschap van de data, ICT-systemen en de verwerking van de data
  - Voer een risicoanalyse uit ten aanzien van vertrouwelijkheid en beschikbaarheid van data en ICT-systemen. Weet ~~of~~ waar je kwetsbaar bent
  - Creëer een positieve organisatiecultuur waarin afspraken worden nagekomen en regels worden nageleefd
    - Voorbeeldgedrag van leidinggevenden
    - De ICT-afdeling is geen aap op een rots
    - Aanspreken op gedrag
    - Bespreken van gedrag
    - Belonen en sanctioneren van gedrag
  - Maak ICT-security onderdeel van het geldende control framework
    - Vertrouwelijkheid van gegevens
    - Beschikbaarheid van gegevens
    - Integriteit van gegevens
  - Zorg voor toereikende fysieke beveiliging

Control: Controls

- Duidelijke interne en externe communicatie over afspraken, eigenaarschap en verantwoordelijkheden ten aanzien van ICT-security is essentieel voor het 'in control' zijn. Dit wil met ICT-projecten nog wel eens anders lopen ...

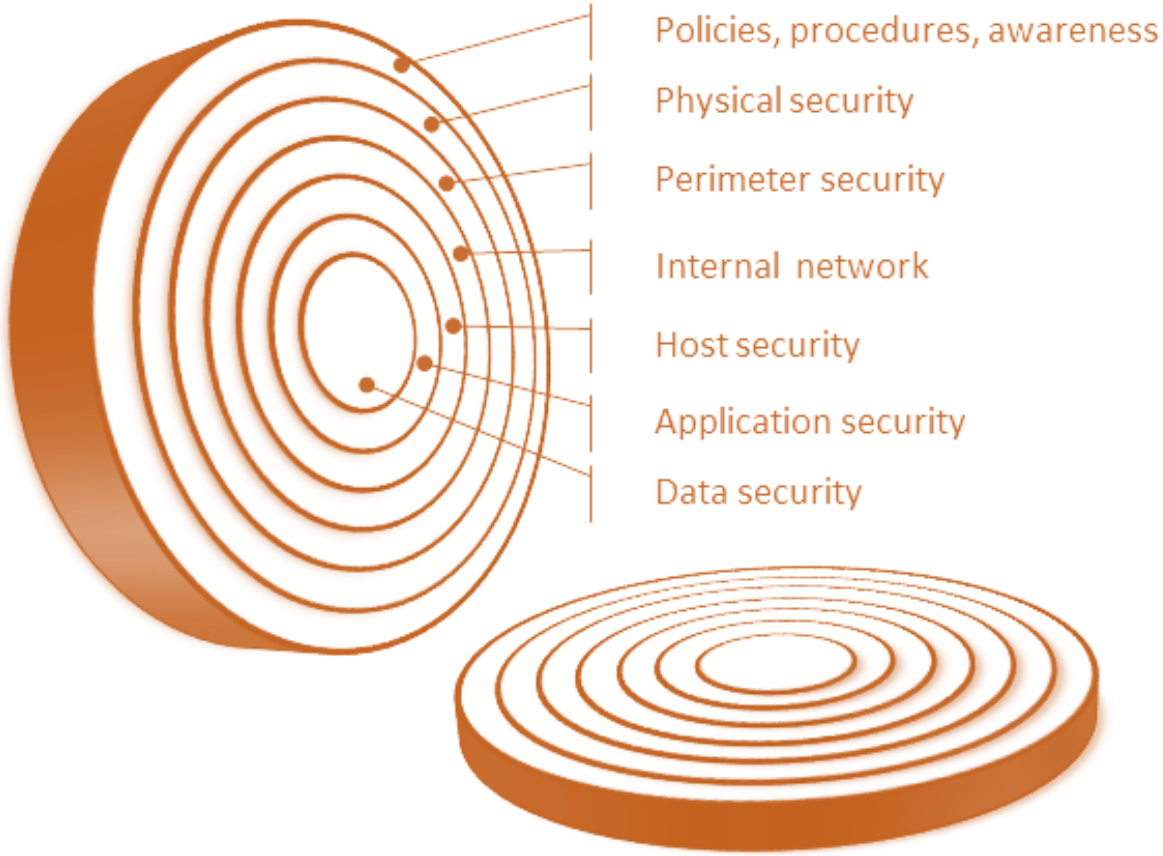
Control: Controls

- Gedrag van de mens is de zwakke schakel

Control: Controls

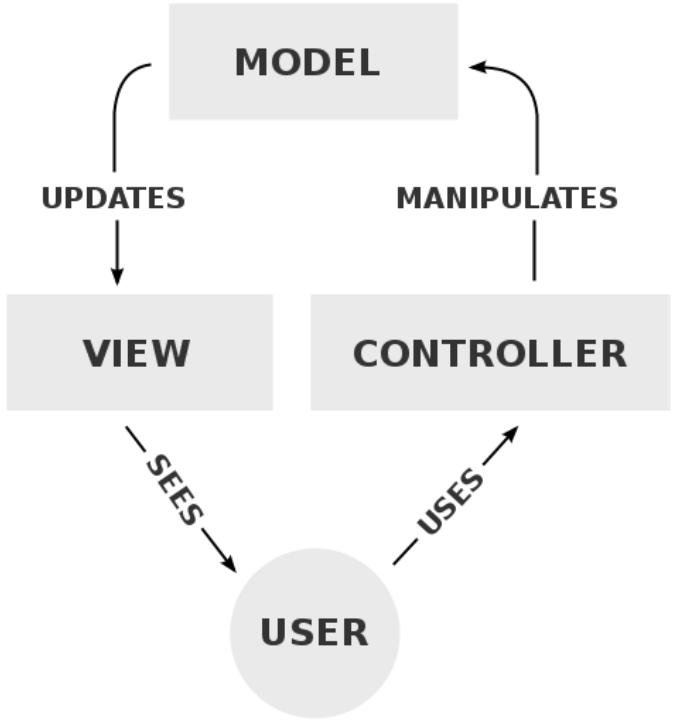
- Technisch
  - Layered security versterken
  - Back-up recovery procedures instellen, testen en naleven
  - Updates tijdig doorvoeren
  - Monitoren en loggen
  - Honey pots inzetten
  - Periodiek de beveiliging laten testen
  - Spreek de taal en stel de juiste vragen
    - Layered security
    - Frameworks en standaarden
    - White- en blacklisting

Control: Controls



Control: Controls

- Frameworks en standaarden
  - Vereist hergebruik van functionaliteiten
  - Internationale community
  - Documentatie
- Design patterns
  - **Model-view-controller-model (MVC)**
  - Model-view-adapter (MVA)
  - Model-view-presenter (MVP)
  - Model-view-viewmodel (MVVM)
  - Presentation-abstraction-control (PAC)



Control: Controls

- Whitelist, accepteer niets behalve …
- Blacklist, accepteer alles behalve …

Tips

hackingondemand.com

Vragen stellen aan een ethical hacker

hackingondemand.com

NIVE OPLEIDINGEN

E11EVEN