Netherlands Cyber Security Strategy

Michel van Leeuwen
Head of Cyber Security Policy
Ministry of Security and Justice
Netherlands: small country, big time vulnerable

#1 80% online banking

#2 94% > 1 pc per family

#3 After VS en UK on internet

#4 62% shops on internet (4th in EU)

95% youth uses sociale media
Internet ocean cable connects Europe through Amsterdam IX
Cyberthreat is substantial

- Hacking as much as bicycle theft in NL

- Risk e-fraude is 3.5% -> pickpockets 1.7%
  (politieacademie, 2013)

- 13% van de Nederlanders slachtoffer van cyber crime
  (Veiligheidsmonitor CBS, 2014)
The Netherlands: wake up calls (2011-now)

- Diginotar
- Leaktober
- Dorifel
- Pobelka
- DDOS-attacks
- Hold Security
Door NCSC afgehandelde incidentmeldingen

- Hulpverzoek
- Privaat
- Overheid

Q4-'11 | Q1-'12 | Q2-'12 | Q3-'12 | Q4-'12 | Q1-'13 | Q2-'13 | Q3-'13 | Q4-'13 | Q1-'14
Impact incidentmeldingen overheid

- Malware-infectie: 7%
- Poging tot hacken: 4%
- Websitekwetsbaarheid: 6%
- Onbeschermd/kwetsbaar systeem: 9%
- Phishing: 5%
- Aanvalsdreiging: 17%
- Uitlekken informatie: 7%
- DDoS-aanval: 11%
- Overig: 7%

Impact incidentmeldingen privaat

- Malware-infectie: 7%
- Poging tot hacken: 4%
- Websitekwetsbaarheid: 2%
- Onbeschermd/kwetsbaar systeem: 7%
- Phishing: 5%
- Aanvalsdreiging: 20%
- Uitlekken informatie: 14%
- DDoS-aanval: 7%
- Overig: 4%
Legislative framework

• Law - Security breach notification – in progress
• Law – Computer criminality III – in progress
• Budapest Convention
• EU – Directive Network and Information Security
• Law – Intelligence and Security Services
• Law – code of criminal procedure
• Guideline responsible disclosure

• Laws, directives and regulations on privacy, child abuse, financial sector, telecom ...
National cyber governance framework

NETWORK & INFOSECURITY
- NCSC
- DEFCERT
- Business-CERTs

PROSECUTION
- POLICE
  Public Prosecution Service
- AIVD
- MIVD

INTELLIGENCE

CONFLICT
- MOD
- Military
- NATO
Network & Infosecurity in the Netherlands

Ministry of Security and Justice – policy coordination

Ministry

Authorities

NCSC

Law

Regulation and oversight

Assistance and cooperation

Government and businesses in critical infrastructure
Cyber security beeld: 4 belangrijke trends

- Hyper-connectivity
- Legacy
- Crime & state sponsored
- Privacy
Vision

The Netherlands, together with partners, are committed to create a secure digital domain in which the opportunities of digitalisation are used, threats are confronted and fundamental rights are protected.
Cyber Security: The state of the art in the Netherlands

- Prevention
  - Knowledge
  - Awareness
  - Security measures
  - Training
- Respons
  - Identification/Interests
- Situational Awareness
  - Advising
  - Prosecution
  - Crisis management
- Detection
  - Threat Analysis
National Cyber Security Strategy I - 2011

- **Public Private Partnership**
- **First action programme:**
  1. Setting up CS Council and National CS Centre
  2. Setting up CS Threat Assessment
  3. Increasing the resilience of critical infrastructure
  4. Increasing response capacity on attacks/disruptions
  5. Intensifying investigation and prosecution of cybercrime
  6. Encouraging research and education
National Cyber Security Strategy 2
From awareness to capability
<table>
<thead>
<tr>
<th><strong>NCSS - 2011</strong></th>
<th><strong>NCSSII - 2013</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Private Cooperation</td>
<td>Public Private Participation</td>
</tr>
<tr>
<td>Focus on structures</td>
<td>Focus on networks / strategic coalitions</td>
</tr>
<tr>
<td>Capacity building national oriented</td>
<td>Capacity building national as well as international</td>
</tr>
<tr>
<td>Do what you think is right (intuition)</td>
<td>Balance (as a result of knowledge / experience):</td>
</tr>
<tr>
<td></td>
<td>- Measures throughout cyber chain</td>
</tr>
<tr>
<td></td>
<td>- Threats, assets and controls.</td>
</tr>
<tr>
<td>Defining principles (for example, multistakeholder</td>
<td>Defining a vision: for example on governance</td>
</tr>
<tr>
<td>model, international cooperation)</td>
<td></td>
</tr>
<tr>
<td>General approach</td>
<td>Risk based approach</td>
</tr>
<tr>
<td>Unaware → Aware</td>
<td>Aware → Skilled</td>
</tr>
</tbody>
</table>
Developments

- Broad approach to “space” means triangle of:
  - Security
  - Freedom
  - Economic/social benefits
- A more international approach and increased number of actors
- Need for a comprehensive governance model
National Cyber Security Strategy II
Economic / Social benefits

Government

- NCSS2
  - Transparency
  - (Self) regulation
  - Developing Knowledge

Security

Private parties

Freedom

Citizens
Cyber hygiene and more responsible

Private party

Cyber hygiene and more responsible

Citizen

Accountable and duty of care

Government

Facilitating, direction, steering
The Dutch Approach

Doctrine:
public private cooperation
&
private public participation
Relevant PPP cyber security fora

**Strategic-policy level**
Cyber Security Council
Committee Critical Infrastructure
NCSC Council

**Tactical-operational level**
ISAC’s Liaisons
Incident Response Board

**Operational level**
Operational Incident Response Team forum
International CERT community
NL Cyber security

- Resilient against cyberattacks and able to protect its critical infrastructure
- Fight cybercrime
- Invest in secure ICT products and services taking into consideration the promotion of privacy
- Build coalitions for freedom, security and peace in the digital domain
- Invest in innovation and adequate knowledge levels
Action programme; some successes in 37 actions

- Trusted Network Initiative
- National detection and response network
- Strengthening analysis capabilities
- Strengthening Military Cyber Defence capabilities
- Global conference on cyberspace 2015/GFCE
- Tender for the National Cyber Security Research agenda
- Public-Private taskforce cybersecurity education
- Fusion Cell – Economic Crimes Taskforce
- Engaging ethical hackers
Challenges for a secure Netherlands digital gateway to Europe

- Third Strategy? -> Netherlands Cyber Space Strategy
- The ‘harder’ things:
  - from awareness to responsible behavior
  - e-skills, e-government, e-business
  - measuring effectiveness
  - getting private sector involved financially
  - responsible zero day usage
  - encryption/decryption
  - international standards
  - secure hard- and software
  - international norms
  - internet governance
  - future opportunities/threats – Big Data, Internet of Things