

[illegible]



National Cyber Crime Centre

National vision & strategy for fighting cyber crime

Vision

Vision for the Danish cyber crime activities

To bring Denmark to the leading edge in terms of the collaboration between society and police, in order to prevent and solve cyber crime

Safeguarding

Integrity

Innovation

Focused

Strategic

Strong

With the victim
in focus

Public Private
Partnership

Strengthening of
the entire police

Quality and
competency

Research based
innovation

Future organizing



Challenges

- International borderless crime
- Moving constantly changing target – require transformation agility
- Anonymized services (Tor) and hidden internet (Silk Road)
- Virtual currencies (bitcoin)
- Shift from IPv4 to IPv6 (4.000.000.000 (4 bill.) to 340.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000..)
- Cloud services (different local national legislation)
- Slow reaction or different national priorities by national authorities
- Outdated legislation

CaaS – Crime as a Service

Table 1. Prices for zero-day vulnerabilities.

Adobe Reader	\$5,000–\$30,000
Mac OS X	\$20,000–\$50,000
Android	\$30,000–\$60,000
Flash or Java Browser Plug-ins	\$40,000–\$100,000
Microsoft Word	\$50,000–\$100,000
Windows	\$60,000–\$120,000
Firefox or Safari	\$60,000–\$150,000
Chrome or Internet Explorer	\$80,000–\$200,000
iOS	\$100,000–\$250,000



France Email Database 1 million Available

France Email Database 1 million

PRICE LOWERED!

\$495.49

[Add to cart](#)

[View](#)

USA DOCTOR EMAIL DATABASE



USA Doctor email Database (0.7 Million)

PRICE LOWERED!

\$114.34 tax incl.

~~\$127.65 tax incl.~~

(price reduced by 10 %)

Quantity :

Availability: 999 items in stock

[Add to cart](#)

[Add to my wishlist](#)

PayPal

Click here to pay

Cases

- Sexual abuse of children
- Drug trading on Silk Road (Tor and Bitcoin)
- Scareware/Ransomware/cryptolocker
- Ddos as an extortion / hacktivism feature
- Hacking of customer databases (Password/UserID/Google)
- Hacking Danish Police mainframe systems
- Hacktivism in general (targeting our politicians)
- Multiple variants over the theme, fraud..

Future

NC3 - National Cyber Crime Center

- The above mentioned activities
- National data-intelligence platform for investigation
- Preparing for *Intelligence lead policing*
- Improved prevention capabilities
- Enhanced PPP private-public-partnership
- Strengthening of cross organisational cooperation
- EC3 – Interpol – PET – Center for Cyber Security



Protection and threats

Security and awareness are the only solutions to prevent this!!

- ✓ ISO standards are great – watch out for the potential “sleeping pill”
 - ❖ Be aware that the ISO standard is very much a paper exercise
 - ❖ Make sure it does not park real risks under a “formal risk assessment”
 - ❖ Example – a non critical webserver, does not get the proper attention

- ✓ Awareness and its potential inefficiency
 - ❖ Leave it not to users skills and attention to safeguard your data
 - ❖ Only if there are no digital means to safeguard, awareness is the single most efficient

- ✓ If it’s too good to be true, it often is
 - ❖ Fraud is everywhere out there, so be vigilant and sceptical
 - ❖ Be aware of threats and harrassment

Protection and threats

✓ Do not forget that this is a **digital discipline** – not a paper exercise!



Remove/eliminate **all your high-risk** vulnerabilities
– and measure it monthly!



Collect all **your logs and analyze** them with security intelligence
– real time!



Protect your **data perimeter and endpoints**
– understand and measure it!



Monitor **your traffic in and out**
– via IDS/IPS and logging or DLP solutions if necessary!



Respond to alerts generated
– hire a couple of experts!

Contact



Kim Aarenstrup

Director

National Danish Police,
Cyber Crime Centre

Polititorvet 14

1780 København V

E-mail: kaa006@politi.dk