gasunie
crossing borders in energy

Cyber security in an organization-transcending way

EASEE-gas meeting

March 19, 2015

Paul Bloemen
ICT Security Manager Gasunie
Chair Dutch Energy ISAC

What to talk about

- Why is cyber security important, and even interesting?
- Who cares about cyber security, and who should care?
- Is there a war on cyber, are we winning it?
- Is there anything that we can do together on cyber security? Who is we?
- What happens in the Netherlands on cyber security? And in Europe?

Cyber security

Definition

- The guarantee on availability, integrity and confidentiality of the information supply
- Foremost: malicious intent, but also mistakes, potential sloppiness
- Risk based approach

Actors, components of cyber security measures

- Organization
- People
- Technique

In this order of importance

Threats and measures

Types of threats

- Hacker attacks
- Malware
- Digital espionage
- Internal attacks
- Outage of cyber provisions

Types of cyber security measures

- Prevention
- Detection
- Response

Detection and response become more and more important

Web of measures: defence in depth

- Different targets, like: networks, servers, workplaces, people
- Organization, People, Technique
- Prevention, Detection, Response

No measure in itself is perfect, the web of measures delivers

View on cyber security within the organization

Scope

- The own processes and systems

Importance

- To mitigate the risks on information supply of the organization as a whole
- For the vital processes: most measures are reasonably to well implemented
- Increasing need for certifying the cyber security process and policy
  - For instance: ISO 27001 and ISO 27002

Scope, again

- The measures of the organization, decided by the organization
- Based on de security policy of that organization

View on cyber security within the community

Starting point for every organization

- Cyber security is quite well organized within the own organization
- Initial fear: what have others to do with cyber security of my organization?

Changing world

- Increasing interdependencies of vital processes and systems between organizations:
  - Interfaces as part of supply chains between processes and systems
  - Outsourced services and systems
- Increasing vulnerabilities of the vital systems: connections to the outer world
- Increasing malicious actions by professional cyber crime and states:
  - Money, information, disruption
- Governmental or European requirements on cyber security, by law:
  - The Dutch Gaswet, European privacy regulations

Cyber security will not be owned anymore by the individual organizations

Desired attitude

- Interest of the organizations: self-regulation
- Interest of the community: robustness, resilience of the vital systems
- Bundling of own interest and common interest
  - Could be done: **everybody wants robust, resilient vital systems**

Initiatives in the Netherlands (1)

Starting point

- Public Private Partnership
  - Cooperation between Government, Business, Science

Organizations

- Cyber Security Counsel
- National Cyber Security Center

Documents

- National Cyber Security Strategy
  - An optimum between Freedom, Security and Social Growth
  - A cooperation between Government, Business, Citizens
- Yearly Cyber Security Vision of the Netherlands:
  - Cooperation of government and private parties
  - Content: Interests, Threat actors, Threat means, Vulnerabilities, Measures, Manifestations

Initiatives in the Netherlands (2)

National Cyber Security Center (NCSC)

- Computer Emergency Response Team for central government and vital sectors
- Security advisories service on cyber threats
- Support of "Information Sharing and Analysis Centers" (ISAC's) for several vital sectors, like:
  - Finance, Telecom, Energy, Water, Nuclear, Airport, Multinationals
- Cyber alert service
- ICT Response Board

Benefits

- Public and Private sector:
  - Learn and know about each other
  - Are able to cooperate when necessary

ISAC's in the Netherlands

Information Sharing and Analysis Center

- Unity of sector
- Unity of common interest, like possession of a vital infrastructure

Mission

- Sharing of information about cyber incidents, best practices, own experiences
- Trust is of the utmost importance: it takes time

Organizations don't compete on cyber security

Figures at the end of 2014

- 12 ISAC's, 156 organizations, about 200 – 250 members

Organization

- No membership fee: investment in time and information
- Chairman from the business
- Secretary from NCSC
- Meetings 5 – 7 times a year
- Sometimes work groups to sort out issues

Initiatives in Europe

High level interest in cyber security

- Interdependencies of processes are rather on a European scale than a national issue, like:
  - Finance, Energy, Telecom
- Effects of cyber security incidents can be disastrous
- Cyber security incidents don't stop at the border of countries

Existing initiatives

- European FI-ISAC

Emerging initiatives

- European Energy-ISAC, starts with electricity
- Network of Information Security (NIS) Platform, connecting 200 members all over Europe

European directives, national laws

- Privacy
- Maybe much more to come

Conclusions

Important topics for the near future

- Shared responsibilities for flawless operation within the supply chain
- Information sharing about cyber threats, incidents, best practices
- Accountability on cyber security on a national and European level

What to do

- Pro-active posture on developments
- Active participation on cyber security related activities with government and organizations in the sector

The Netherlands poses a good example of what can be achieved together

Questions: p.a.bloemen@home.nl