Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Securing the Internet of Things

through regulation and standardisation

Eelco Vriezekolk

2021-04-28

Today's topics

1. about Agentschap Telecom
2. an example, new product
3. Radio Equipment Directive
4. certification Cyber Security Act
5. discussions and questions

Agentschap Telecom

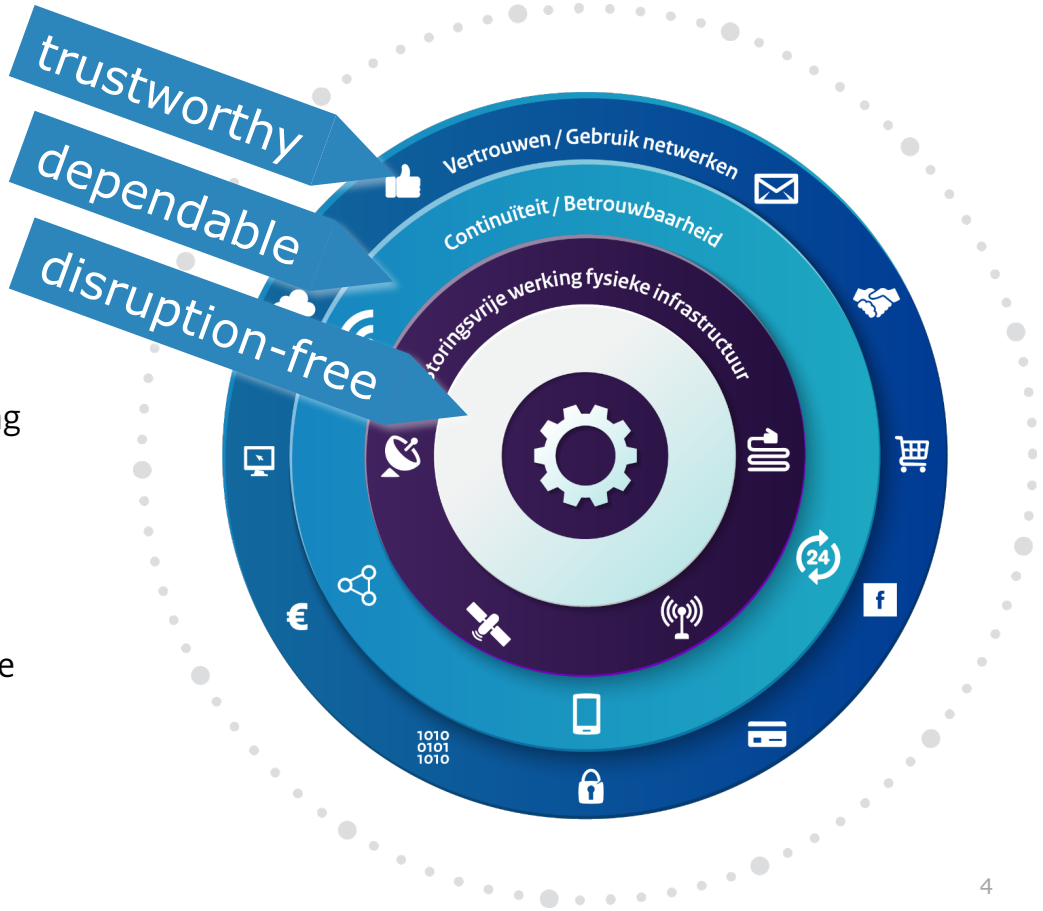
Founded in 1927.

Initially a department within the national telco, but a government service since its privatisation in 1989.

400 employees; headquarters in Groningen, second office in Amersfoort .

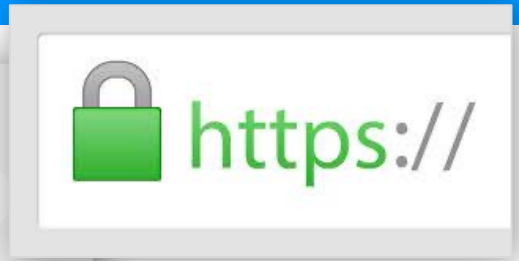
Agentschap Telecom

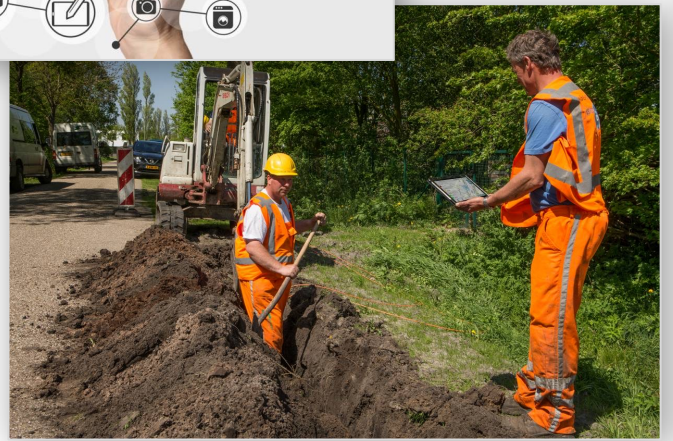
The responsibilities of the Telecom Agency are extensive. For example, we check whether digging and trenching are conducted safely, we check whether scales are weighing correctly and we are involved in cyber security. Relevant work for, for example, inspectors, frequency planners, data analysts and cybersecurity experts. That is what makes working at Agentschap Telecom so diverse and challenging.

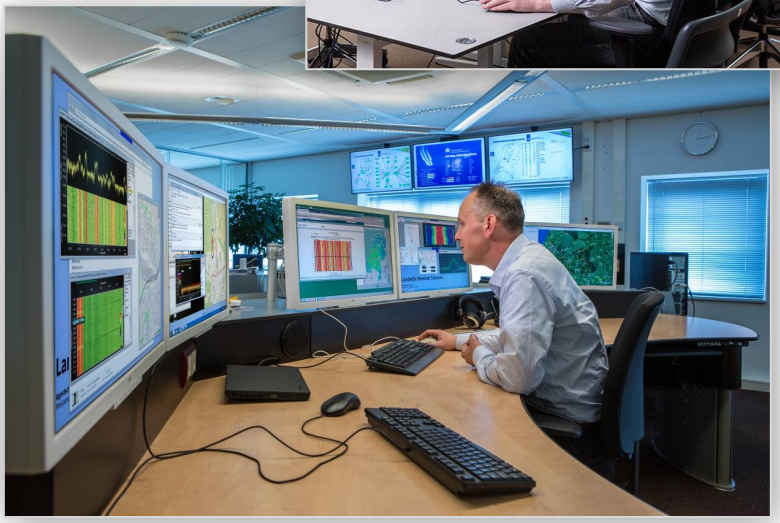



American


TV
IOT


https://





An example

Indoor air purification device

- air quality sensors
- filtering and purification system
- cloud service & app

What legal product requirements?

What is not covered by legislation?

An example

Hazards

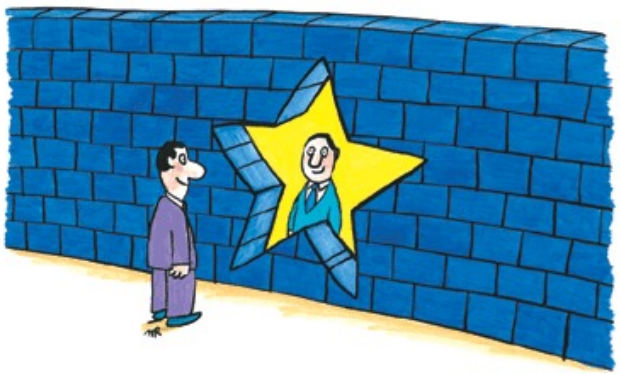
- electrical (shock)
- health (ozone emissions etc.)
- EMC (interference on wireless equipment)
- privacy (home or away?)
- abuse (botnet, DDOS)
- cyber security
- … and perhaps other?

National product regulation

Expensive for manufacturer

- creates complexity
- increases legal uncertainty
- slows product cycles
- hinders innovation
- reduces product availability
- increases consumer prices

European product regulation



European product regulation

Avoids conflicting national requirements.

Harmonised technical requirements:

- free movement of goods
- single European market

European product regulation

Appliances burning gaseous fuels
Cableway installations designed to carry persons
Construction products
Electromagnetic compatibility
Equipment and protective systems in potentially explosive atmospheres
Explosives for civil uses
Lifts
Low voltage equipment
Machinery safety
Measuring instruments
Medical devices: Active implantable
Medical devices: General
Medical devices: In vitro diagnostic
New hot-water boilers fired with liquid or gaseous fluids (efficiency requirements)
Non-automatic weighing instruments
Packaging and packaging waste
Personal protective equipment
Pressure equipment
Radio equipment
Recreational craft
Simple pressure vessels
Toys safety

European product regulation

No prior approval

- Self-certification (when using harmonised standard)
- Second-party certification (harmonised standard / essential requirements)

Market surveillance

European product regulation

Cybersecurity is not currently addressed!

- of the product itself
- of the cloud service

How to solve?

- improve current product directives
- certification of products, services and processes
- create new “horizontal” cybersecurity directive

Radio Equipment Directive

RED reach = “any device that contains a wireless module” (approx)

RED contains dormant clauses, that can be activated
by the European Commission.

- mostly consumer oriented
- early life cycle: when placed on the market
- compulsory
- baseline security (some application may require a higher level)
- covers abuse, fraud, privacy
- high level of enforcement possible
- self-assessment or second-party certification

Radio Equipment Directive

RED reach = “any device that contains a wireless module” (approx)

RED contains dormant
by the European Comi

- mostly consumer o
- early life cycle: wh
- compulsory
- baseline security (s
- covers abuse, frau
- high level of enforc
- self-assessment or second-party certification

3.3.a. Radio equipment interworks with accessories
3.3.b. Radio equipment interworks with other radio equipment
3.3.c. Connected to interfaces of the appropriate type
3.3.d. Not harm the network nor misuse network resources
3.3.e. Protection of personal data and privacy
3.3.f. Protection from fraud
3.3.g. Access to emergency services
3.3.h. Facilitate its use by users with a disability
3.3.i. Only compliant software can be loaded

Radio Equipment Directive

Process:

- European Commission decides on classes of devices, requirements
- Implementation period starts
- Standardisation request (ETSI, CEN/CENELEC)
- Harmonised standard published

Radio Equipment Directive

What about the product life cycle, firmware updates?

- consumer rights regulations
- RED requirements

What about cloud service?

Software development process?

→ Need for additional certification.

Cyber security Certification

Certification of products, services and processes.

Based on *certification schemes*.

Assurance level Basic, Substantial, High.

In NL

- self-certification or third-party certification for Basic
- third-party certification only for Substantial and High
- prior government approval required for High

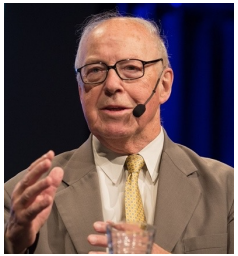
Schemes:

Common Criteria evaluation, IACS,
IOT, Cloud services, 5G, more in the future

Assurance level ≠ Security level

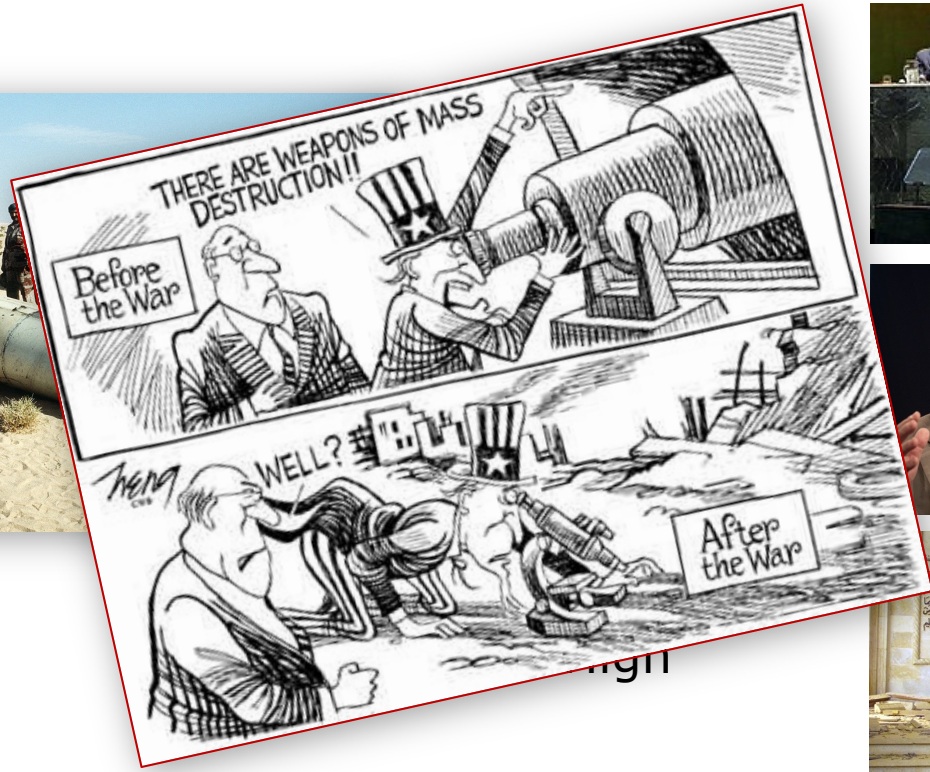
Basic:

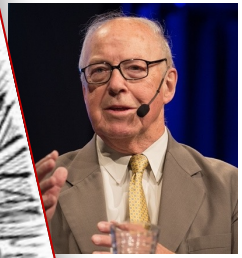
Substantial:



High:

Assurance level ≠ Security level





Cyber security Certification

Certification at higher levels is expensive

Certification is voluntary

- for now
- market pressure through large customer procurement policies
- can be compulsory on a national level

This certification-system is still in its infancy.

Some points of discussion

What is the preferred route to securing the IOT ecosystem?

A: Self-regulation by the market

B: Legislation and regulation by governments

Some points of discussion

Which regulatory approach is preferable?

A: a single mandatory minimum security level (simplicity, low cost, maintainable)

B: different mandatory levels, depending on application domain (complex, etc)

Some points of discussion

Which considerations should have priority with creators/manufacturers?

A: commercial considerations (marketshare, profit)

B: security considerations (public values, end-user interests)

Conclusion

Many cyber threats, but currently little in cyber regulation

New cyber regulation is being drafted (RED and CSA)

RED and CSA cover different areas, are not “silver bullets”

Agentschap Telecom actively involved & responsible for enforcement

One final remark

We are hiring security experts and IT-auditors

https://WerkenVoorNederland.nl

https://agentschaptelecom.nl

Werken bij Agentschap Telecom?

Een dag zonder telecommunicatie. Zou jou dat nog lukken? Grote kans dat je antwoord ‘nee’ is. Want een dag zonder bellen, internetten of bijvoorbeeld muziek en video streamen is ondenkbaar. Gelukkig hebben we in Nederland betrouwbare (tele)communicatienetwerken.

Daarover gaat Agentschap Telecom.