Security in the new digital world: the Internet of Things

Maarten Bodlaender

Outline

- Introducing myself
- This is Nokia

- IoT megatrends

- Impact of new European cybersecurity legislation
  - NIS2 – ISO 27001
  - CRA – SBOM and patching

- Case: securing a large IoT device accordingly

Introducing myself: Maarten Bodlaender

- PhD. in Computer science - inventor on 95 patents
- Executive MBA - career in business development
- Dutch Patent attorney - protecting with law
- CISM-certified CISO – protecting with security controls

- Previously worked at Philips & Genexis
- Last week started at Nokia as Senior Legal Counsel IoT licensing

- I like time with family, (board)games, badminton, golf, sailing, travelling and following the news

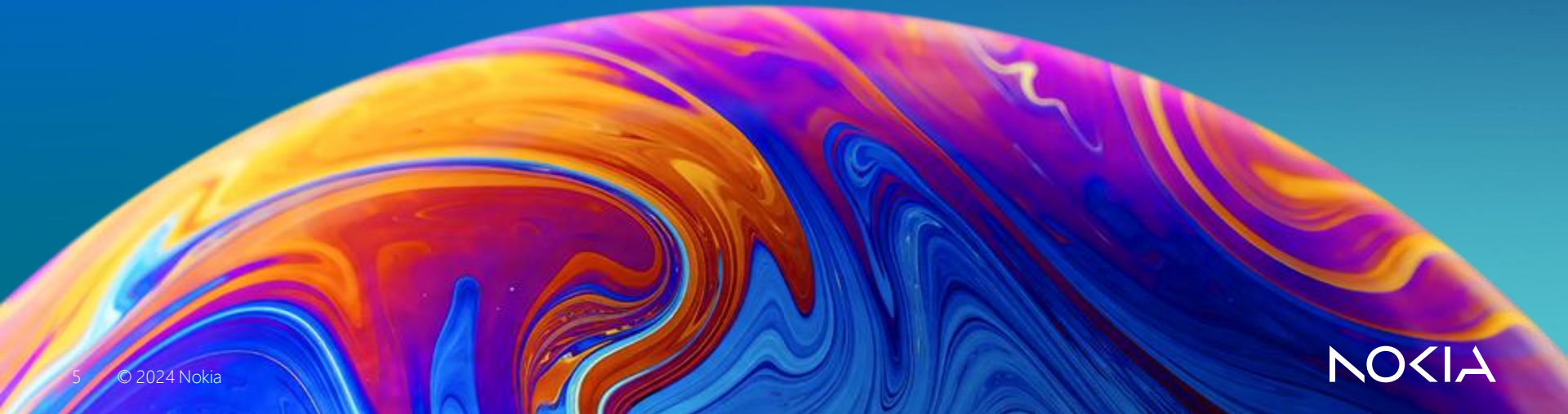
This is

NOKIA

At Nokia, we create technology that helps the world act together

When the world's people, machines and devices are in sync with each other, we can realize the full potential of digital:

- Sustainable business growth
- Productivity in industry
- Inclusive digital access



The technology we lead in: Networks that sense, think and act

Making high performance connectivity more consumable and sustainable

A transformation in how networks are deployed

Opening up networks for innovation and collaboration, securely

A transformation in how networks are applied

Realizing the potential of digital to create a more sustainable, productive and accessible world

Environment

Minimizing our industry's footprint

Industrial digitalization

Enabling sustainable growth

Bridging the digital divide

Providing inclusive access and digital skills

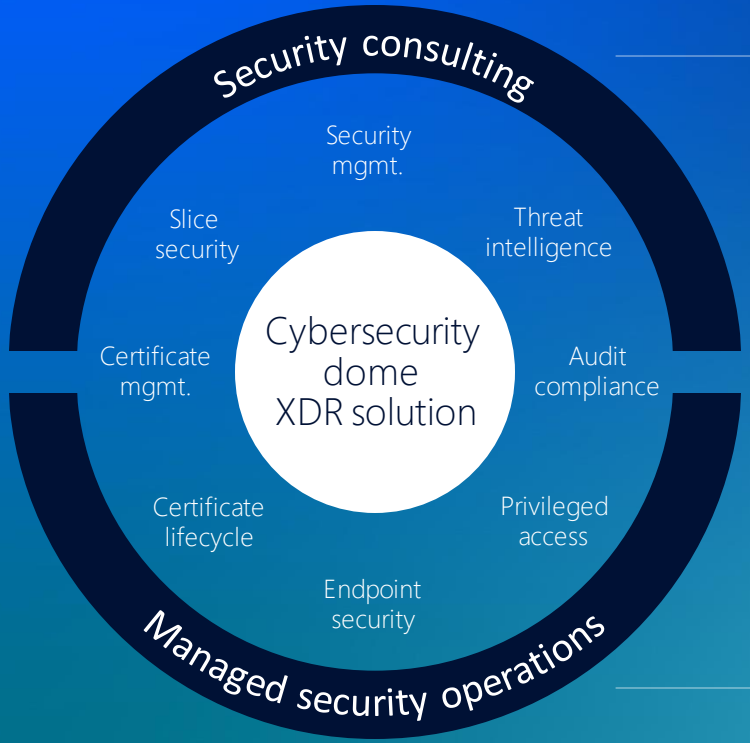
Security and privacy

Protecting the world's critical assets

Responsible business

Driving systemic change

Strengthen security operations



E2E 5G security
across radio, transport, core, slices, cloud & apps

Threat intelligence lab
driving thought leadership & research

AI/ML algorithms
proactively detecting and remediating threats with a rich library of 5G security IPRs

Plug-and-play cyber playbooks
for security automation and orchestration with 5G specific context

Outline

- Let me introduce myself: Maarten Bodlaender
- This is Nokia
- IoT megatrends
- Impact of new European cybersecurity legislation
  - NIS2 – ISO 27001
  - CRA – SBOM and patching
- Case: securing a large IoT device accordingly

In this presentation, the Internet of Things consists of:

Connected devices that can sense, think and act, but are not (easily) manageable by IT

Consumer devices

- Kept in (secure) home, managed by laymen (consumers)
- Low cost

=> Short lifecycles *possible*

- Limited risk beyond botnets

Industrial sensors & actuators

- Often installed in unprotected, remote areas, staff is remote
- Low-cost devices, but 'truck rolls'

=> Long lifecycles

- Often part of system with safety risk

Heavily regulated devices

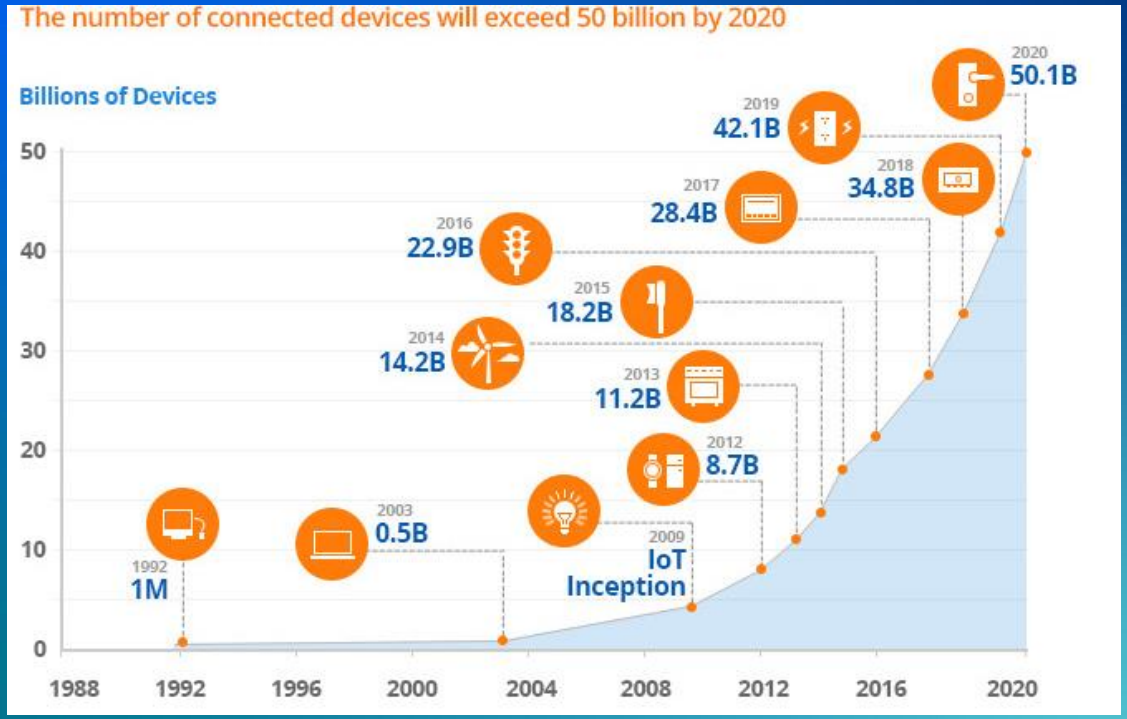
- Kept in protected area, managed by on-site, professional staff
- Expensive capital equipment

=> Long lifecycles

- Typically have safety risk

The Internet of Things is our new normal

The digital society emerged in just 15 years – and security needs to catch up

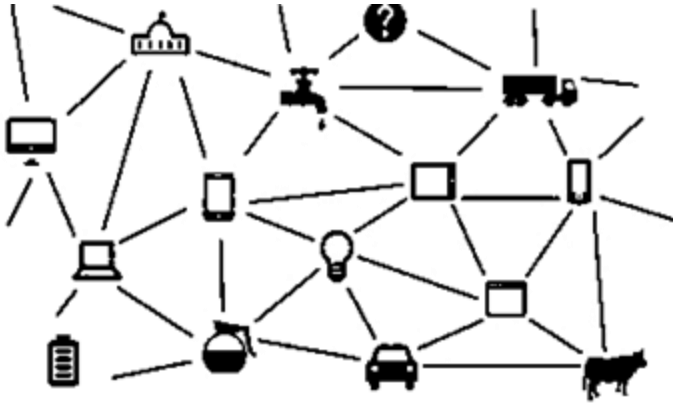


Are the foundations of our security architecture still adequate?

- IT Governance, Credential management, …
- Access control, policies, trust networks
- Security primitives
  (key exchange, encryption)
- Execution platforms
  (Windows, Android, Cloud, Linux, …)
- Hardware

Megatrends that security architectures were never designed for

The Internet of Things



- Everything is now connected
- Information is *everywhere* and *fake*
- Low-cost devices need to be highly secure

Dark cloud computing

- Security *providers under attack*
- *Huge data collections* to be protected
- Who has *control*?

- And the network is coming alive like never before - AI

In the Internet of Things, even simple devices must maintain water-tight security

- Philips Hue shows both the promises and risks of the Internet of Things:
  - in no-time 50+ apps to set atmospheres, and in no-time the first (innocent) hack

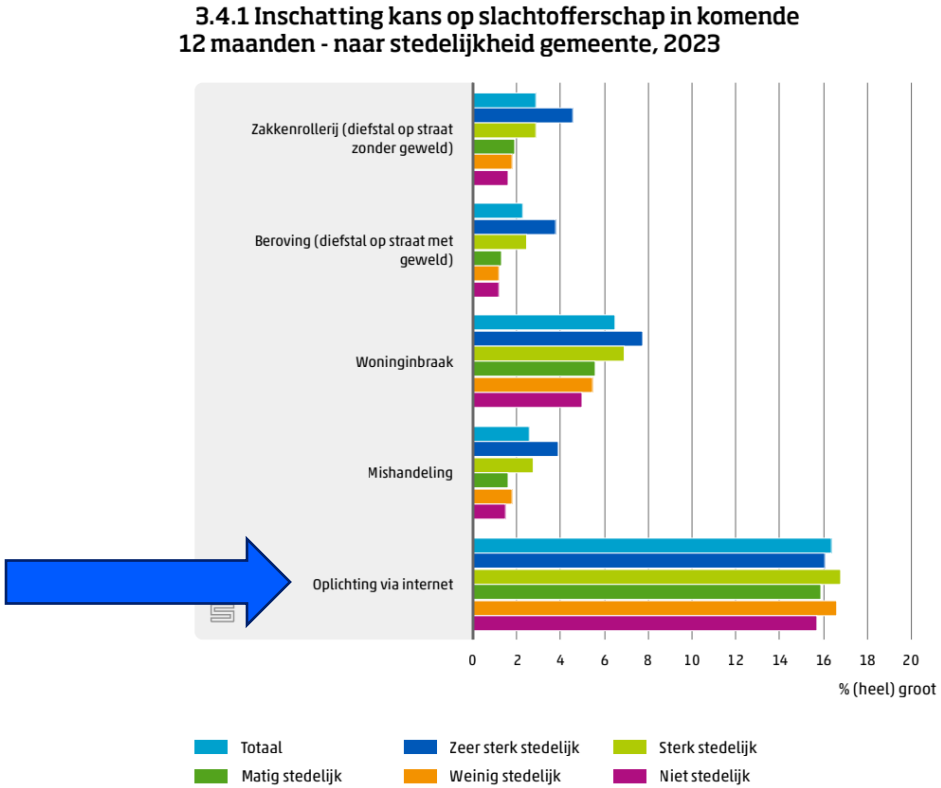
- Security is a service – e.g. Windows XP received security patches for 13 years
  - How does that fit in the business model of selling LED lights (20 year lifetime)?

Not innocent: security weaknesses in the Internet of Things are severely punished

- Example: WANNACRY attack: 19.000 hospital appointments cancelled in the UK

Security providers themselves are under attack

Cybercrime is now the most common crime



(CBS veiligheidsmonitor 2023)

Hacks in the new Digital World lead to (data) loss on a massive scale – shifting the risk profile

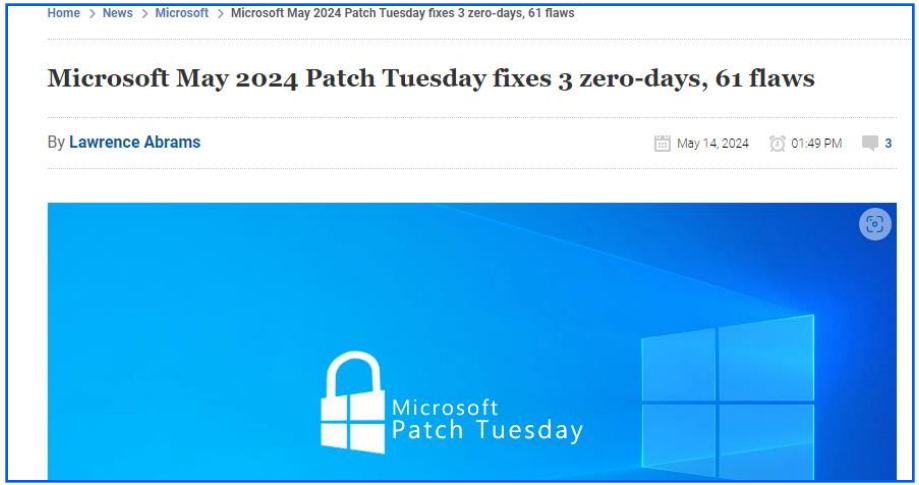
- 22 million U.S. federal employees – with over 5 million fingerprints
- 78 million medically insured at Anthem
- 30 million Ashley Madison accounts – leading to a few suicides
- $1 billion Carbanak bank hacking campaign
- 560 million Ticketmaster customers - 'they' know that you went to see Black Pink …

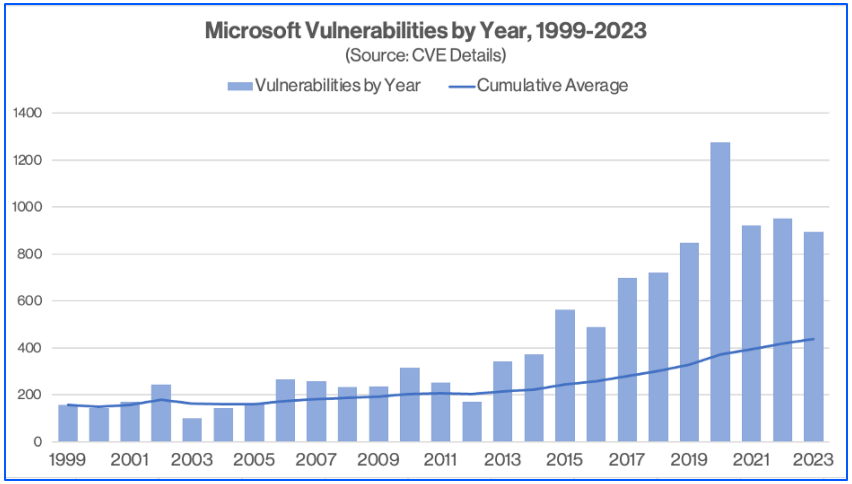
- Think that is bad? How about hacking the Delta-works controls? Or

+

Microsoft releases critical “zero-day” patches every month

For 25+ years, MS Windows has *never* been without open vulnerabilities





Think they will get it right next month? Think other vendors are better? What does this mean for the IoT we depend on?

Outline

- Let me introduce myself: Maarten Bodlaender
- This is Nokia
- IoT megatrends
- Impact of new European cybersecurity legislation
  - NIS2 – ISO 27001
  - CRA – SBOM and patching
- Case: securing a large IoT device accordingly

European Cybersecurity Legislation

- Europe is actively developing new regulations on cybersecurity
  - Cybersecurity chapter of the Radio Equipment Directive
  - Cybersecurity Act
  - Network and Information Security 2 (NIS2)
  - And now the Cyber Resilience Act (CRA)

- Especially NIS2 and CRA are expected to have a significant influence on industry
  - let's take a look at NIS2 first

NIS2 regulates so called “critical infrastructure” sectors

Organizations in these sectors need to implement the NIS2 security requirements

ENERGY

HEALTH

FOOD

WASTE WATER

TRANSPORT

DRINKING WATER

MANUFACTURING

WASTE MANAGEMENT

BANKING

DIGITAL INFRASTRUCTURE

POSTAL & COURIER

PUBLIC ADMINISTRATION

FINANCIAL MARKET INFRASTRUCTURE

DIGITAL SERVICE PROVIDERS

PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR SERVICES

SPACE

RESEARCH

ICT SERVICE MANAGEMENT

CHEMICALS

The impact of NIS2 on digital infrastructure

- The NIS2 directive will be* transposed into national law by October 2024
  - **Operators** classify as **essential** entities under Annex I "Sectors of High Criticality" - 8 Digital Infrastructure – **Providers of public electronic communications networks**
  - **Device vendors** classify as **important** entities under Annex II "Other Critical Sectors“ - 5b **Manufacture of computer, electronic and optical products**

- NIS2 lays down cybersecurity risk-management measures and reporting obligations for entities of a type referred to in Annex I or II
  - requirements on risk management, incident response, vulnerability handling, supply chain security, notification obligations, audits & more.
  - Enforcement through binding instructions, order to cease conduct, fines up to 10M or 2% of global turnover, management held personally responsible & more.

Essential and important entities need to take proportionate technical, operational and organisational measures to manage cyber security risks

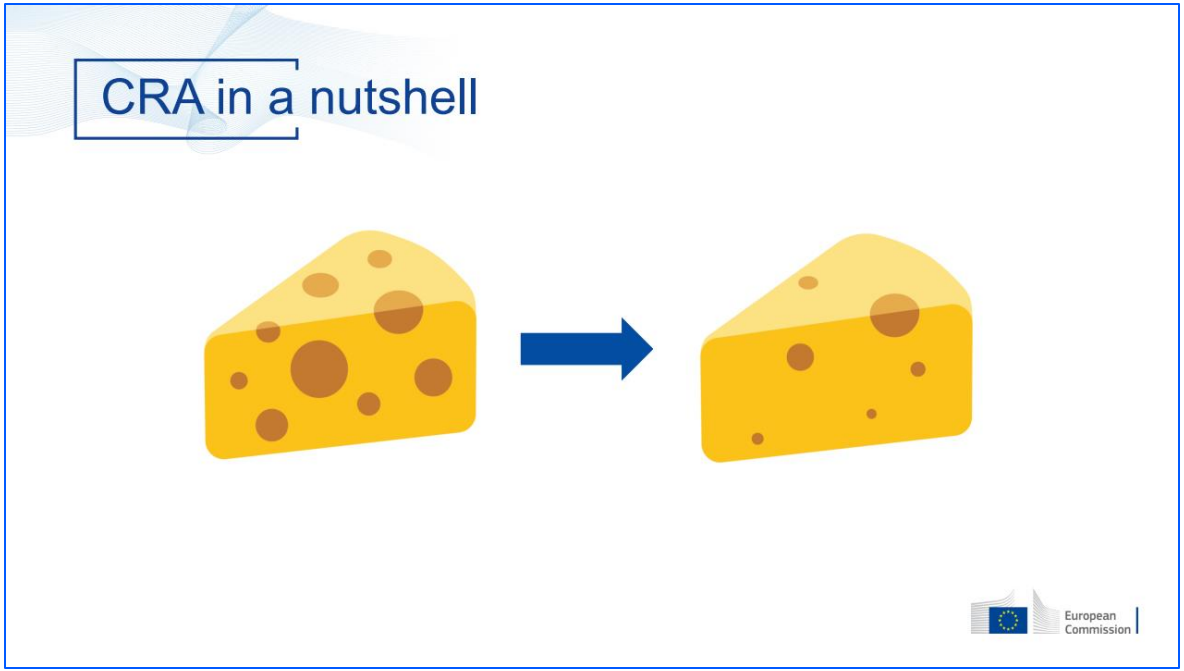
- The measures shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems, and include at least:
  - (a) policies on risk analysis and information system security;
  - (b) incident handling;
  - (c) business continuity, such as backup management and disaster recovery, and crisis management;
  - (d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
  - (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
  - (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
  - (g) basic cyber hygiene practices and cybersecurity training;
  - (h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;
  - (i) human resources security, access control policies and asset management;
  - (j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Cybersecurity risk-management measures and reporting obligations

- Member States shall ensure that the management bodies of essential and important entities
  - approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article
  - are required to follow training, and
  - shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

Now let’s look at the CRA

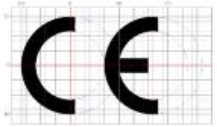
I really loved this slide



Obligations of manufacturers

Assessment of the risks associated with a product

(1) Product-related essential requirements (Annex I, Section 1)
(2) Vulnerability handling essential requirements (Annex 1, Section 2)
(3) Technical file, including information and instructions for use (Annex II + V)



Conformity assessment, CE marking, EU Declaration of Conformity (Annex IV)

Continued compliance with **vulnerability handling** essential requirements throughout the product life time (Annex I, Section 2)

Design and development phase

Maintenance phase
(5 years or across product lifetime, whichever is shorter)

Obligation to report to ENISA within 24 hours:

(1) exploited vulnerabilities
(2) incidents having an impact on the security of the product

Reporting obligations to continue

European Commission

Vulnerability handling requirements

- **Identify and document dependencies** and vulnerabilities, including **SBOM**
- No known vulnerabilities and **address vulnerabilities** without delay
- **Test the security** of the digital product
- Publically **disclose information** about fixed vulnerabilities
- **Coordinated vulnerability disclosure** policy
- Facilitate the **sharing of information** about potential vulnerabilities
- Mechanisms allowing the **secure updating**
- Patches are delivered **without delay**, **free of charge** and with **advisory messages**

European Commission

What is an SBOM?

Under the CRA, companies will need to make their SBOM's available

Software Bill of Material: SBOM

- List of all components in software, their version & associated risks

Example: Like a cake recipe listing all ingredients (and how old they are)

- The SBOM makes it *visible* if there are outdated, risky software components
  - *Patch it, or risk mandatory recall of dangerous products*

Scope

Products with digital elements:

- ✚ **Hardware products** and components placed on the market separately, such as laptops, smart appliances, mobile phones, network equipment or CPUs
- ✚ **Software products** and components placed on the market separately, such as operating systems, word processing, games or mobile apps
- ⓘ The definition of **"products with digital elements"** also includes **remote data processing solutions.**

Not covered:

- ✖ **Non-commercial projects, including open source** in so far as a project is not part of a commercial activity
- ✖ **Services, in particular cloud/Software-as-a-Service** – *covered by NIS2*

Outright exclusions:

- ✖ **Certain products sufficiently regulated on cybersecurity** (cars, medical devices, *in vitro*, certified aeronautical equipment) under the new and old approach

European Commission

The XZ Utils attack on Linux

sneakily backdoor all Linux release tarballs, but not the source code

- "JiaT75" joins XZ Utils project, gains trust over two years
- Fake accounts pressure sole primary maintainer to give trust
- JiaT75 adds malicious code to versions 5.6.0 and 5.6.1
- Backdoor adds remote code execution via SSH to tarballs
- No one knows who "JiaT75" is
- These attacks can happen to all (small) Open-Source projects
  - CRA exclusion means…

In conclusion, NIS2 and the CRA will help mature the security of products in the EU

- Under NIS2, critical infrastructure operators & suppliers are faced with new cyber security obligations
  - Risk management, incident response, recovery, etc. – basically organizations need to implement an ISO27001 Information Security Management System*
- The CRA is not limited in scope to critical infrastructure, and requires patching over the full economic lifecycle, as well as risk management for products & 24-hour notification oblifations
  - My recommendation: add your products to the ISO27001 scope
- Due to all the auditing and public SBOM's, non-compliance will be easily detected and can be (heavily) fined
- Organizations need to ensure their suppliers also comply – challenging with non-EU suppliers & open-source!

*Beyond the scope of today's presentation

Outline

- Let me introduce myself: Maarten Bodlaender
- This is Nokia
- IoT megatrends
- Impact of new European cybersecurity legislation on organizations:
  - NIS2 – ISO 27001
  - CRA – SBOM and patching
- Case: securing a large IoT device accordingly

The impact of cyber security on heavily regulated industries (example: healthcare)

Key characteristics of a heavily regulated industry

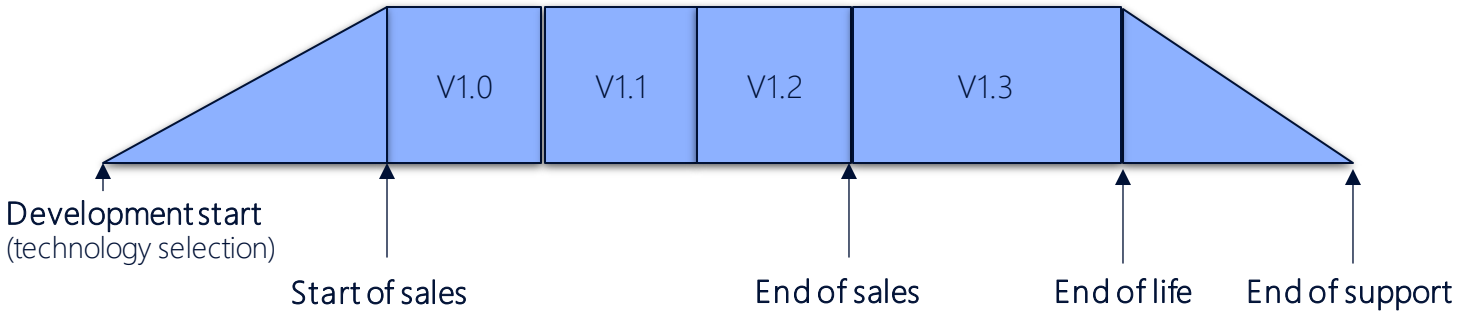
- Heavy & regulated development => slow
- Safety impact => heavy burden of proof
- High cost => long product lifecycles

Key characteristics of a heavily regulated industry

- Heavy & regulated development => slow
- Safety impact => heavy burden of proof
- High cost => long product lifecycles
- Effect: developing a new system can easily take 7+ years

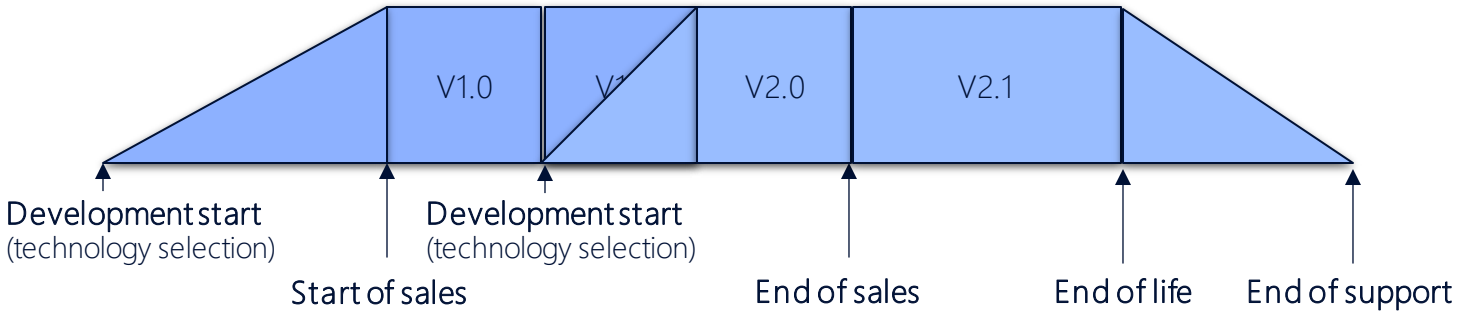
EP Cockpit: the entire room working as one medical system

The full lifecycle of a healthcare product can be 20 years or more



- Issue: the lifecycle of many IT components in the product is much shorter => legacy
- How to align the healthcare & IT lifecycles?

How this is handled today: mid-life technology refresh projects



- Replace all deprecated components, re-program incompatible software, test safety

=> A costly affair. And what if a new attack suddenly breaks the system?

We need to patch vulnerable software to close vulnerabilities

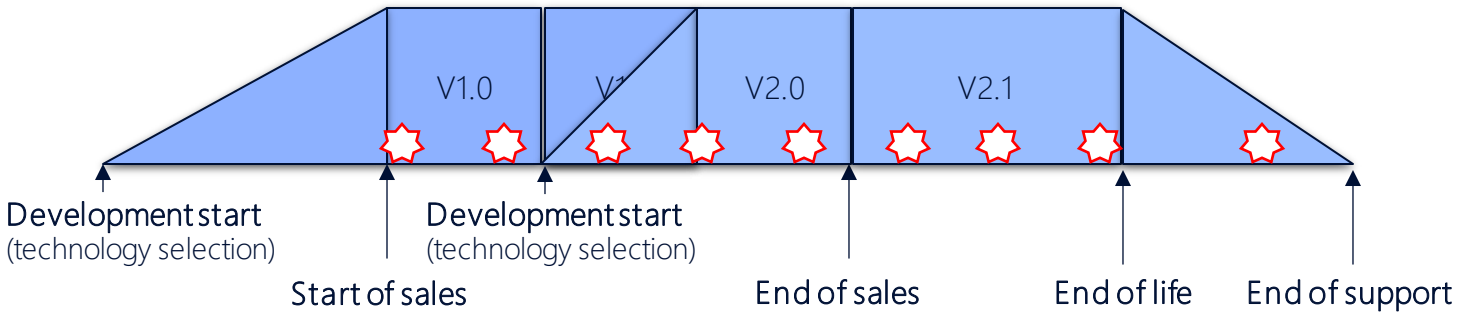
- But … *"patches closed down more power plants than all hackers combined"*
- A patch changes the behavior of the system
- So … is the patch safe for the patient?

⇒ Burden of proof for each patch

⇒ Time consuming testing on each patch

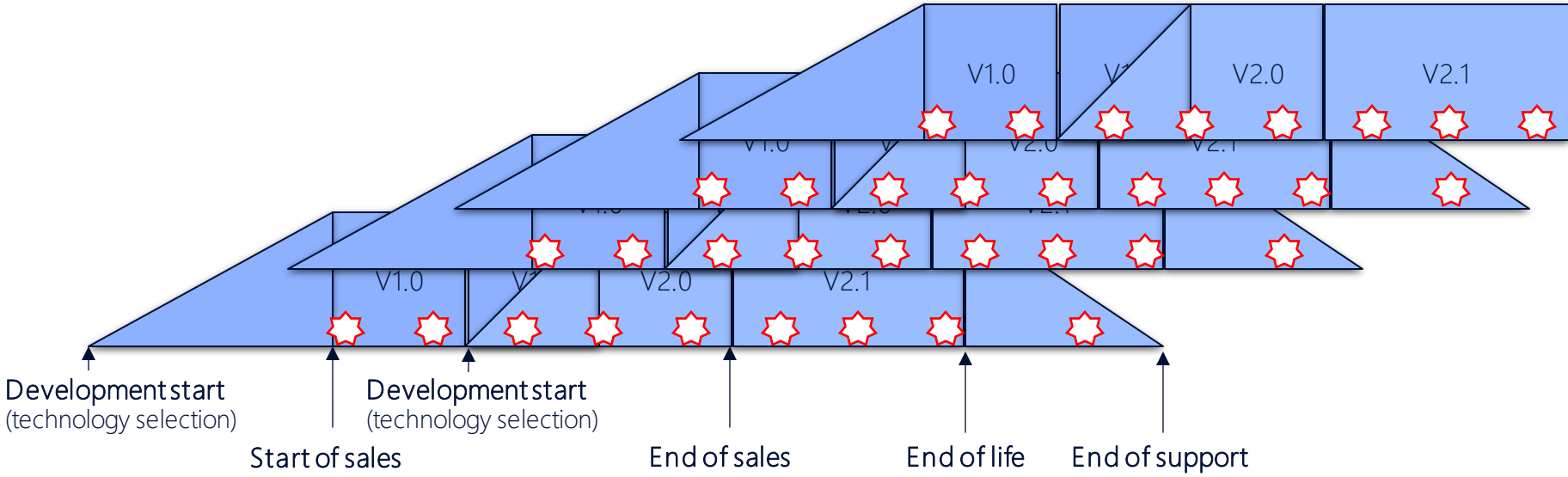
⇒ Rolling out patches in a large system takes 6+ hours (during which no patients can be helped)

Regular patches, supplemented by a technology update



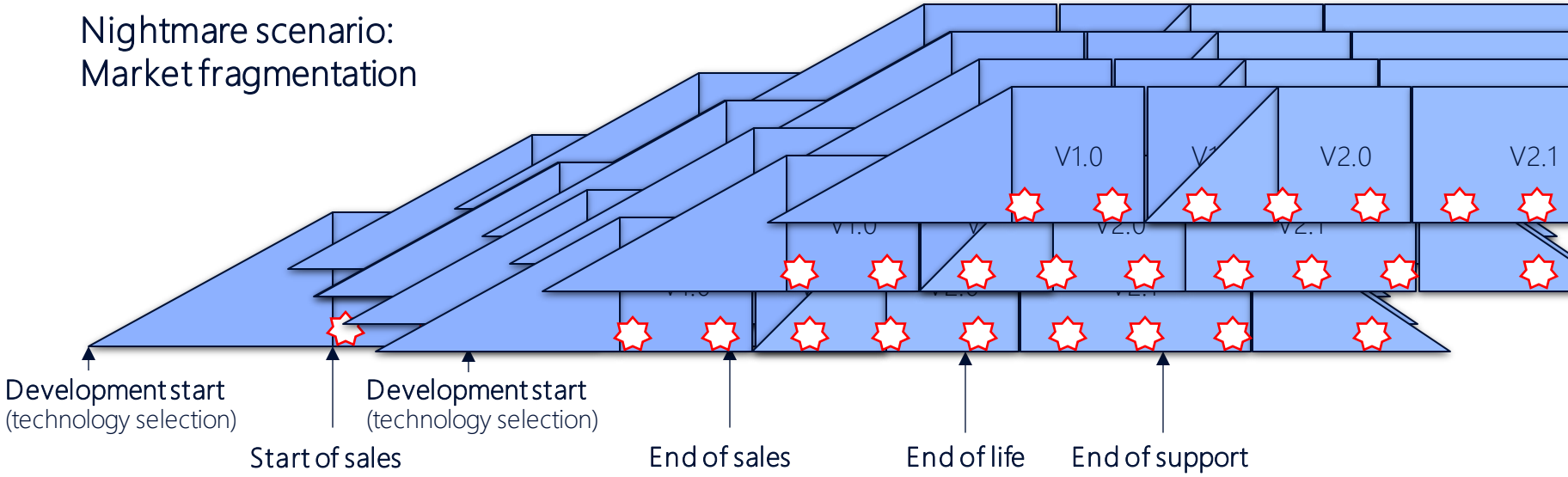
- Even if the patch is provided by supplier, still need to proof the system still works ok
- May still require adapting application software due to patch

Unfortunately, product versions and generations overlap



- There is a significant cost to maintaining the security of long life-cycle products
- While in healthcare, these costs are traditionally incorporated in normal maintenance fees, other industries for which patching obligations are new may need to adapt their business models

The harmonized NIS2 and CRA prevent a nightmare scenario



If
- Each country sets different standards that requires different solutions, and
- Each customer requires incorporation of different technical security solutions, and
- Continuous patching and safety validation is required

Costs would explode and become unbearable for healthcare providers

Concluding

- Networks that can sense, think and act are coming alive with intelligence like never before. They are the fabric of our connected future.
- But hacks in the new digital world can lead to loss on a massive scale - shifting the risk profile.
- To manage these risks, we need to strengthen security operations for the Internet of Things.
- EU laws now require risk management, and patching the Software-Bill-Of-Material over the full lifecycle.
- This poses a heavy burnen on (regulated) industries.
- And the Open Source community needs to figure out how to handle growing cyber risks of open source.
- As long as OS suppliers cannot deliver intrinsically secure components, we are building our digital society on a weak fundament…

(here's room for some university breakthroughs!)


NOKIA

Copyright and confidentiality