Emerging threats or old threats?

Tonu Tammer

Head of CERT-EE
Information System Authority

Only Estonia

500M digital signatures

98% digital prescriptions

95% taxes declared online

33% votes cast over internet

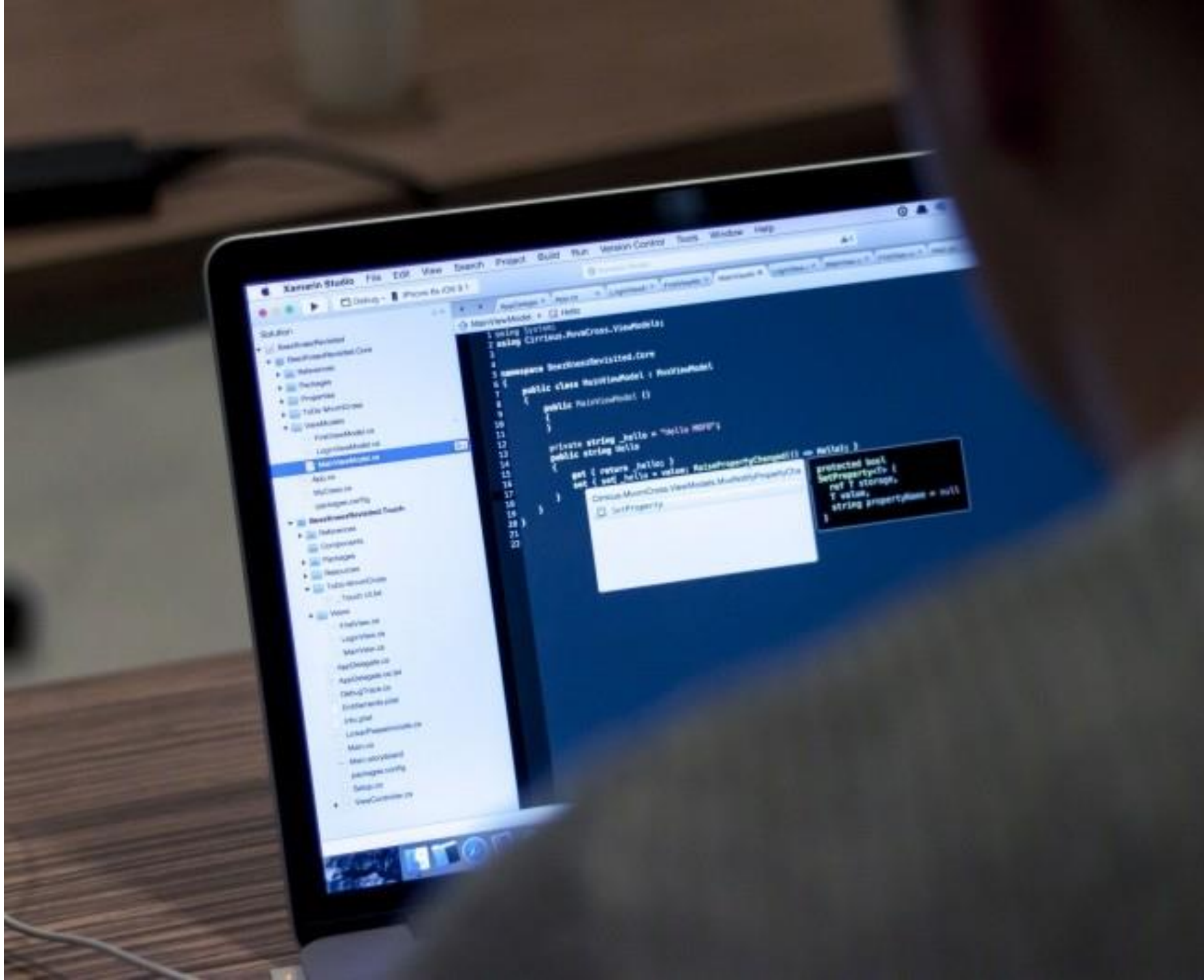
Risks

Supply chain –> new technologies, dependecies, global weaknesses

Platform –> legacy

Workforce –> international competition

Everyday user –> volumes of data, IoT, AI



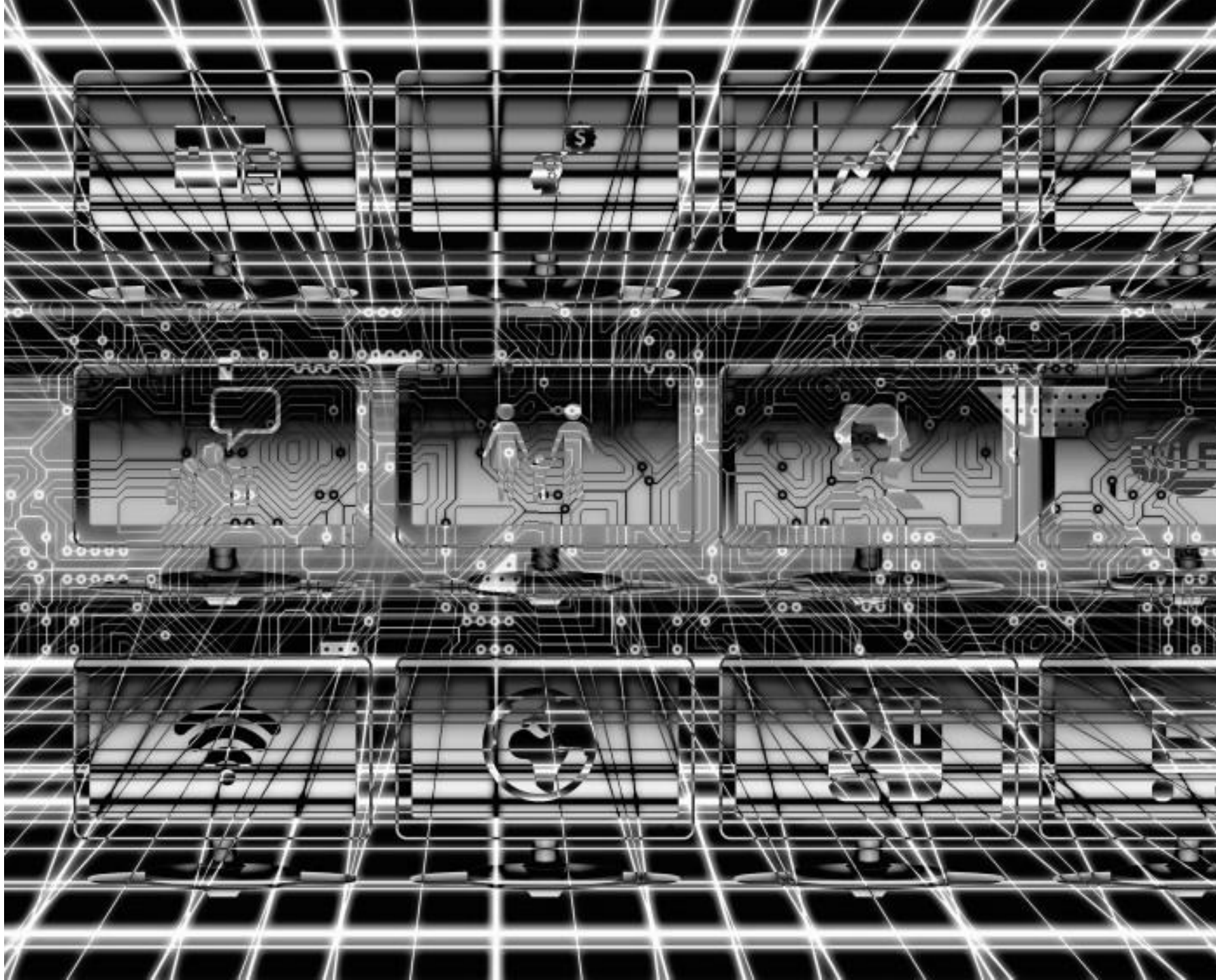
Mantra

PATCH – PATCH
PATCH – PATCH

And then again …

PATCH – PATCH
PATCH – PATCH

But I just did! Or …



Emerging or old?

Few weeks ago –>

- First indications of compromise of IoT of particular vendor
- Variety of SW versions afected
- Latest 8.x (few devices on 8, non latest)
- Popular in Estonia v3.x, v4.x, v5.x
- **V7.2 - PHP2.0 fixed**

PATCH – PATCH – PATCH

Emerging or old?

During summer –>

- First indications of compromise of IoT of particular vendor
- Variety of SW versions afected
- Latest 6.x (few devices on latest)
- Popular in Estonia v4.x, v5.x

PATCH – PATCH – PATCH

Emerging or old?

First question from the community?

- CVE? When fixed?
- Fixed by vendor in March 2018

Reaction: this is old, our devices are running on newer version

Number of devices patched and reconfigured

But...

Emerging or old?

The same targets got hit again despite measures!

Fingerprint of compromise very similar

- Something new?
- Something left behind?

Emerging or old?

The same targets got hit again despite measures!

Fingerprint of compromise very similar

- Something new?
- Something left behind?

Emerging or old?

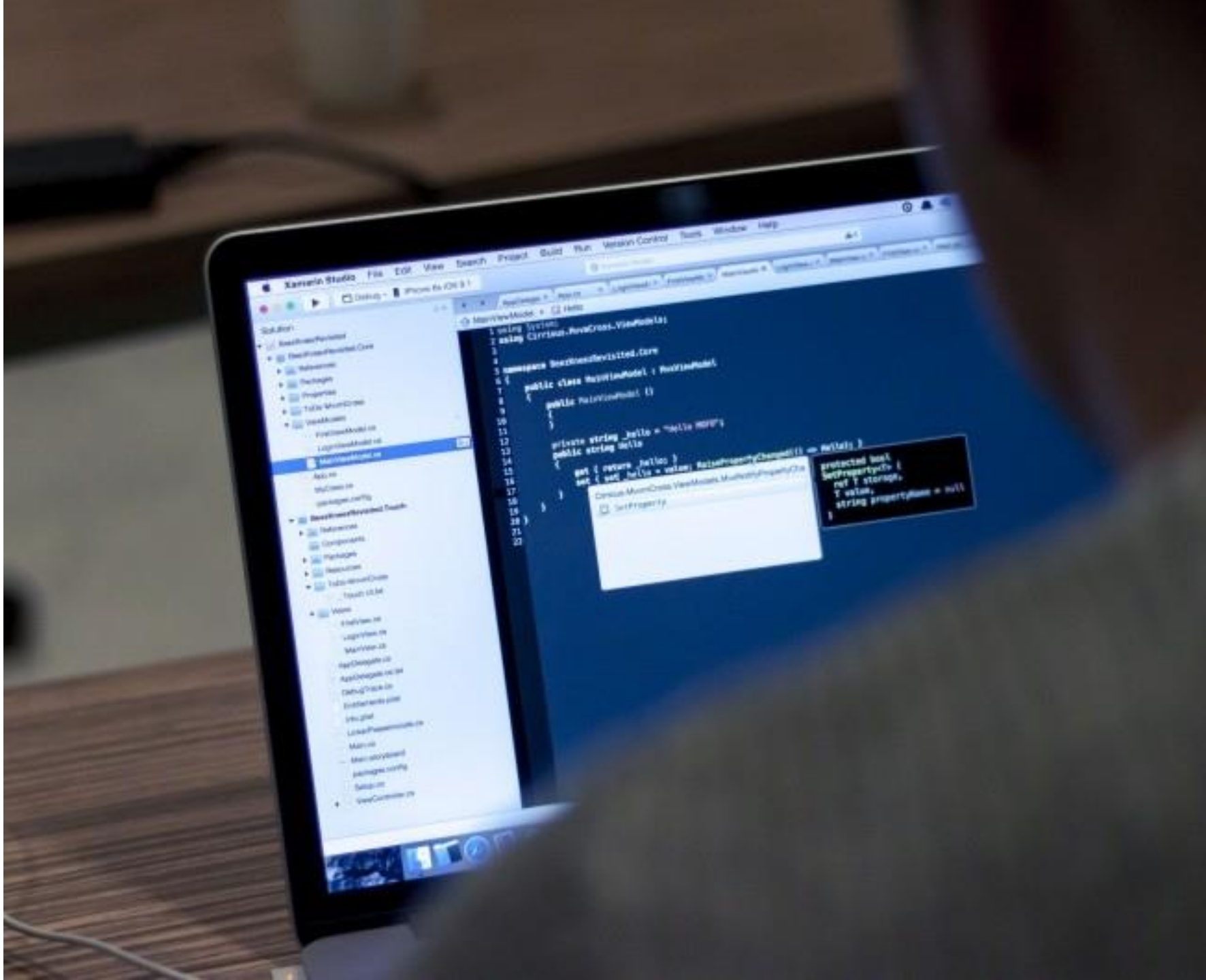
We concluded it is not something left behind! Phew…

- Also no CVE
- Soon update from vendor
- An upgraded version no longer vulnarable

Emerging or old?

First question from community always: what is CVE?

- Which happens first? Bug or CVE?
- Are all bugs reported as CVE?
- Can bugs be exploited without CVE?

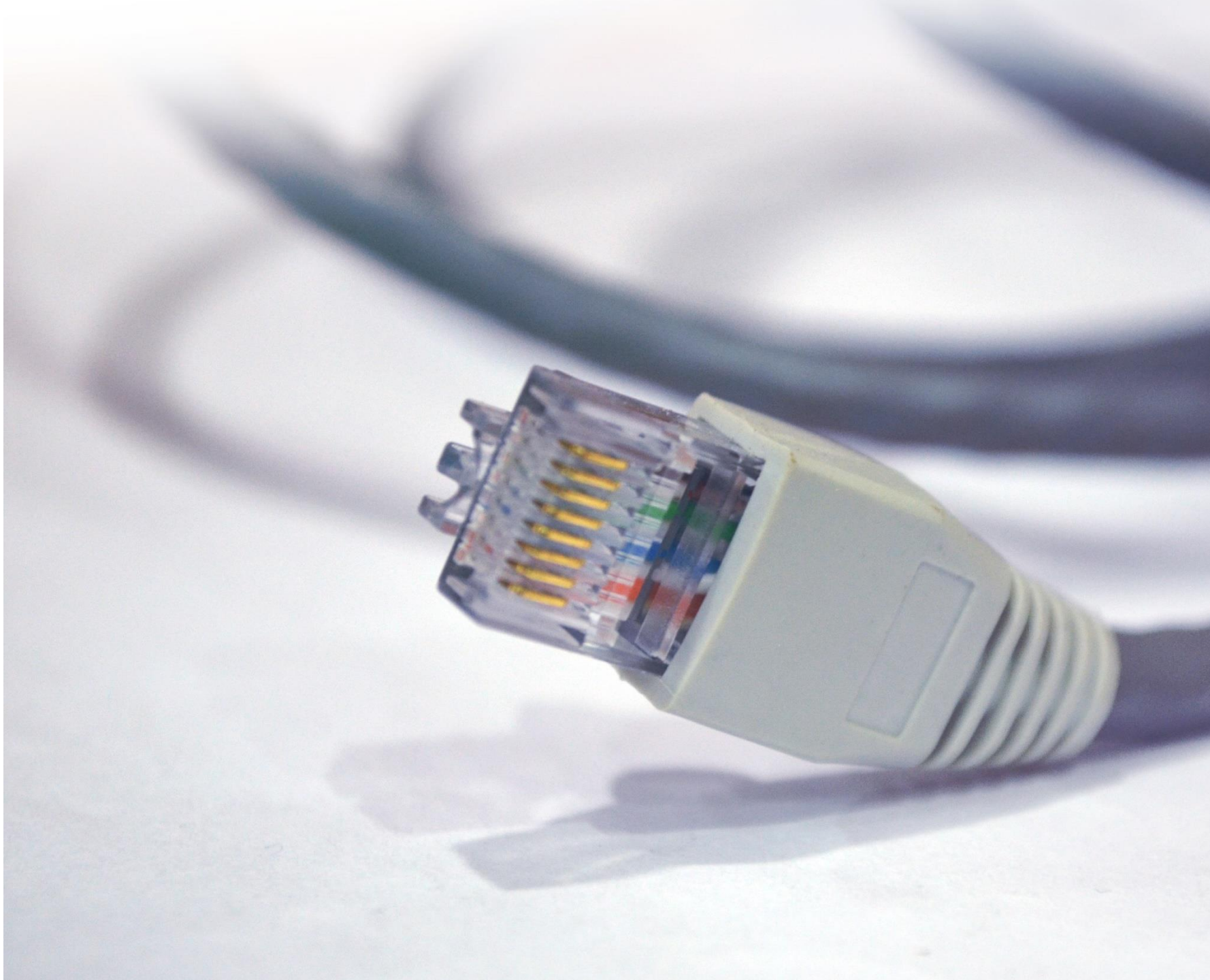


Emerging or old?

Conclusions:

- Some things can be old, some new – if it can be exploited it will be exploited
- Bugs come before CVE!
- There are more bugs than CVE!
- Bugs don’t need CVE to get exploited!

Always upgrade i.e. patch – patch – patch



Thank you!