TeleTrusT "IT-Sicherheitsrechtstag 2023"

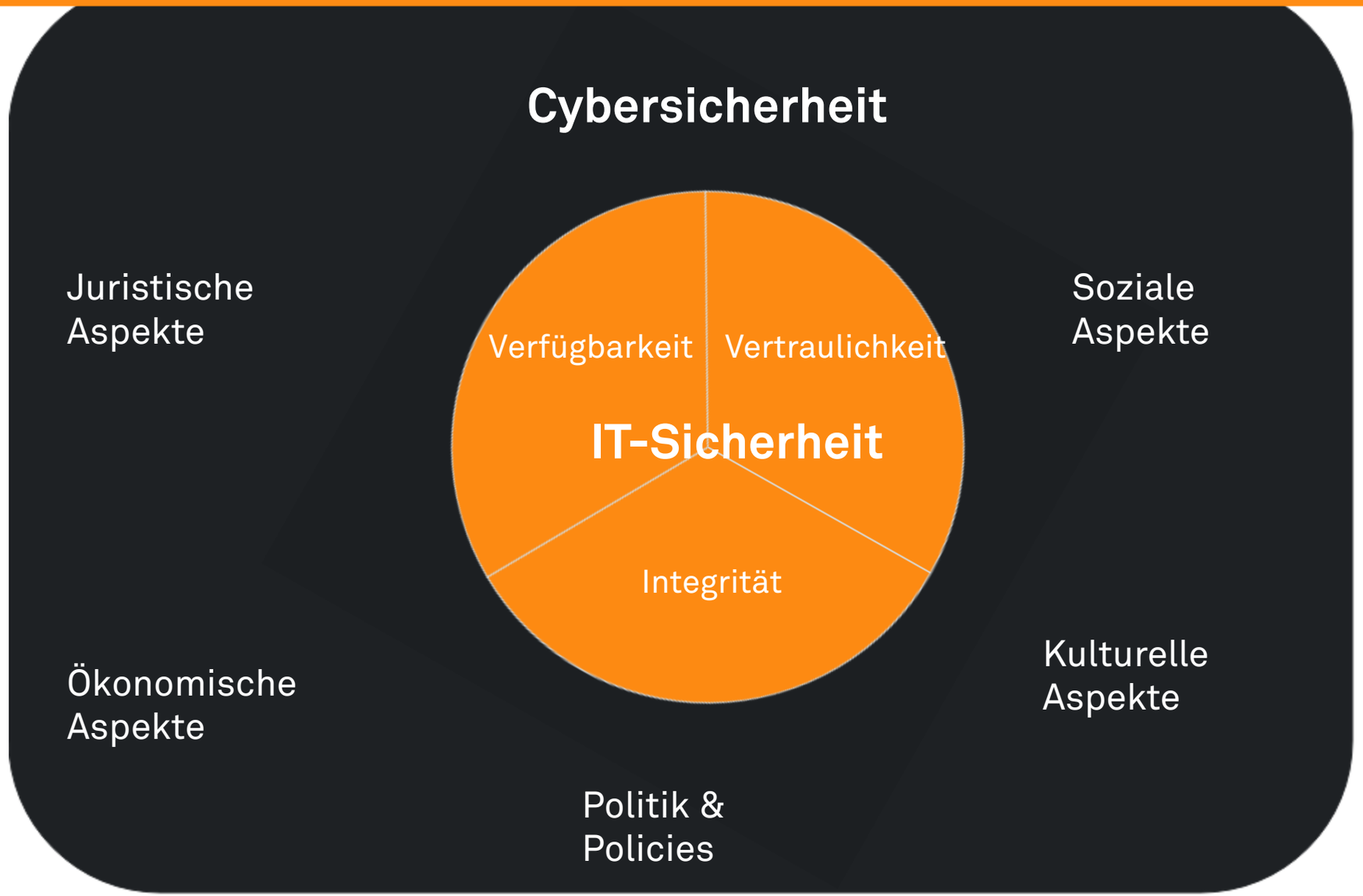
Berlin, 28.09.2023

Cyber Resilience Act und die Verbraucher:innen Beschwerden vorprogrammiert?

Julia Schuetze, Projektleiterin Cybersicherheitspolitik und Resilienz, Stiftung Neue Verantwortung e.V.

1. Überblick – *Definitionen Cybersicherheit und Resilienz*
2. Rückblick – *Prominente Fälle, die Verbraucher:innen betrafen*
3. Einordnung – *Resilienz-fördernde Instrumente im CRA und Bedeutung für Verbraucher:innen*
4. Einschätzung – *Offene Fragen, Punkte zur Diskussion*

Überblick: *Cybersicherheit*



(Cyber-)Resilienzfähigkeiten

- Vorfälle antizipieren
- Vorfällen widerstehen
- Zentrale Prozesse und Infrastrukturen (oder Dienstleistungen) aufrechterhalten können
- Sich von Vorfällen erholen
- Sich anpassen können

(Abgeleitet aus BSI-Standard 200-4, the BCI, ENISA, NIST-SP 800-172, MITRE Working Group)

Rückblick: *2016 SmartThings*

ANN ARBOR—Cybersecurity researchers at the University of Michigan were able to hack into the leading “smart home” automation system and essentially get the PIN code to a home’s front door.

Their “lock-pick malware app” was one of four attacks that the cybersecurity researchers leveled at an experimental set-up of Samsung’s SmartThings, a top-selling Internet of Things platform for consumers. The work is believed to be the first platform-wide study of a real-world connected home system. The researchers didn’t like what they saw.

How is all this possible? The security loopholes the researchers uncovered fall into a few categories. One common problem is that the platform grants its SmartApps too much access to devices and to the messages those devices generate. The researchers call this “over-privilege.”

“The access SmartThings grants by default is at a full device level, rather than any narrower,” Prakash said. “As an analogy, say you give someone permission to change the lightbulb in your office, but the person also ends up getting access to your entire office, including the contents of your filing cabinets.”

“The bottom line is that it’s not easy to secure these systems” Prakash said. “There are multiple layers in the software stack and we found vulnerabilities across them, making fixes difficult.” The researchers told SmartThings about these issues in December 2015 and the company is working on fixes. The researchers rechecked a few weeks ago if a lock’s PIN code could still be snooped and reprogrammed by a potential hacker, and it still could.

In a statement, SmartThings officials say they’re continuing to explore “long-term, automated, defensive capabilities to address these vulnerabilities.” They’re also analyzing old and new apps in an effort to ensure that appropriate authentication is put in place, among other steps.

https://news.umich.edu/hacking-into-homes-smart-home-security-flaws-found-in-popular-system/

Rückblick: *Smart home devices 2015 - 2021*

A principal research scientist at the security firm Sophos, Wisniewski wanted to know whether the average off-the-shelf device had major security vulnerabilities. He wasn't skilled at hacking into physical devices — what insiders call "firmware hacking" — so he figured the project, which he undertook in 2015, would be a fun way to practice, even if he struggled to break in.

A few days later, he had a whole collection of hacked smart devices.

That's because the software Wisniewski found inside was shoddier tha he expected, he said. Rather than up-to-date programs with security problems patched up, the devices were filled with bundles of code haphazardly pulled from the Internet. Some of the code came from projects that programmers had stopped updating, so software bugs festered and hackers could easily exploit them.

https://www.washingtonpost.com/technology/2021/11/18/smart-home-security/

Six years later, things aren't much better, but our adoption of connected home products has exploded. More than 77 percent of households with a WiFi network reported owning at least one smart home device in 2021, compared with 65 percent just one year earlier, according to research firm IDC. But off-brand smart home devices could be riddled with vulnerable software, and shoppers have no way of knowing. Once inside

But there's another element at play here: Software security. Big-name smart device makers have reputations to maintain and a vested interest in securing smart appliances even after they leave the shelves. When a security firm found a bug in Amazon's voice assistant Alexa that could have allowed hackers to access voice recordings from people's homes, Amazon swiftly fixed the problem.

Smaller brands, however, are a toss-up, according to Wisniewski. If the code is up to date when you buy the product, it might not be for long, as many devices don't come with the ability to accept software upgrades remotely. Beyond that, plenty of products are "white label," or slapped

Rückblick: *MERIS – „a botnet of a new kind“*

Named **Mēris**, the Latvian word for "plague," the botnet has been primarily used as part of a DDoS extortion campaign against internet service providers and financial entities across several countries, such as Russia, the UK, the US, and New Zealand.

But instead of focusing on bandwidth attacks, like most Mirai variants, Meris focused on modules specialized in launching volumetric attacks, and, apparently, they found a sweet spot.

In the aftermath of its recent spree of attacks, Meris broke the record for the largest volumetric DDoS attack twice. It did it the first time earlier this summer, in June, when it was behind a large 17.2 million RPS DDoS attack that hit a US financial company, according to Cloudflare, which had the unpleasant task of mitigating this particular attack.

Qrator says that after analyzing the source of most of the attack traffic, most of it led back to devices from MikroTik, a small Latvian company that sells networking gear such as routers, IoT gateways, WiFi access points, switches, and mobile network equipment.

The company said it wasn't able to determine if the attacker found and weaponized a zero-day in MikroTik's software or if they're just living past exploits.

Nonetheless, a zero-day appears to be in play, just by the large number of MikroTik devices that appear to have been enslaved in Mesir's gigantic 250,000-strong mesh.

As far as we have seen, these attacks use the same routers that were compromised in 2018, when MikroTik RouterOS had a vulnerability, that was quickly patched.

Unfortunately, closing the vulnerability does not immediately protect these routers. If somebody got your password in 2018, just and upgrade will not help. You must also change password, re-check your firewall if it does not allow remote access to unknown parties, and look for scripts that you did not create.

We have tried to reach all users of RouterOS about this, but many of them have never been in contact with MikroTik and are not actively monitoring their devices. We are working on other solutions too.

https://therecord.media/meet-meris-the-new-250000-strong-ddos-botnet-terrorizing-the-internet

Rückblick: *Alexa*

Our findings show that certain Amazon/Alexa subdomains were vulnerable to Cross-Origin Resource Sharing (CORS) misconfiguration and Cross Site Scripting. Using the XSS we were able to get the CSRF token and perform actions on the victim's behalf.

These vulnerabilities would have allowed an attacker to:

- *Silently install skills (apps) on a user's Alexa account*
- *Get a list of all installed skills on the user's Alexa account*
- *Silently remove an installed skill*
- *Get the victim's voice history with their Alexa*
- *Get the victim's personal information*

In effect, these exploits could have allowed an attacker to remove/install skills on the targeted victim's Alexa account, access their voice history and acquire personal information through skill interaction when the user invokes the installed skill.

Successful exploitation would have required just one click on an Amazon link that has been specially crafted by the attacker.

https://research.checkpoint.com/2020/amazons-alexa-hacked/

We reported these vulnerabilities to Amazon in June 2020, and Amazon has subsequently fixed the issue.

(Cyber-)Resilienz fördernde Instrumente?

- Konformitätsbewertung (Selbstbewertung bzw Konformitätsbewertung durch Dritte, abhängig von der Produktkategorie)
  - Verpflichtende Cybersicherheitsmaßnahmen
    - Risiko Analyse und Management
    - Security by Design
    - „Software Bill of Materials“
- „Sweeps“
- Meldeprozess/Reaktionsmöglichkeiten
  - Bereitstellung von Sicherheitsunterstützung und Software-Updates zur Behebung identifizierter Schwachstellen
  - Garantien während des Produktlebenszyklus
  - Ggf Widerruf

Bedeutung für den Verbraucher:in

- Vor dem Kauf
  - Genereller Überblick Rechte bei Produkten mit digitalen Elementen – welche Produkte betrifft es und welche nicht?
- Beim Kauf
  - ~~Informationen zur Produktsicherheit und sichere Nutzung~~
  - Wie lange ist das Produkt sicher? Welche Garantien habe ich?
- Nach dem Kauf
  - Wenn das Produkt kaputt ist, kann ich reagieren? Könnte es ein IT-Sicherheitsfehler sein? Wie kann ich das Produkt wieder funktionsfähig bekommen? ~~Muss ich etwas tun, um das Produkt abzusichern?~~
  - Es wurde eine kritische Schwachstellen in meinem Produkt gefunden, laut Medien berichten, was muss ich jetzt tun?
  - An wen kann ich mich wenden?

Beispiel offene Fragen und Punkt, die besonders Verbraucher:innen betreffen: *Reaktionsmöglichkeiten*

- CRA Proposal September 2022 „In case of a security incident, manufacturer must inform consumers within at least 24 hours to prevent possible consequential damage and avert harm. Producers must share technical and background information with affected consumers to raise liability claims.

- ITRE Committee July 2023: „1.7 To avoid any uncertainty when it comes to interpretation, the EESC suggests that the Commission draw up guidelines to guide manufacturers and consumers on the exact rules and procedures that apply in practice, since it appears that a number of products within the scope of the proposal are also subject to other legislation on cybersecurity.

Beispiel offene Fragen und Punkt, die besonders Verbraucher:innen betreffen: *Garantien und Reaktionen*

- ITRE Committee July 2023: „• ITRE Committee July 2023: “The report proposes flexible duration for the expected product lifetime, which should be clearly stated, and obligation that manufacturers provide automatic security updates and to differentiate between security and functionality updates where feasible.”

Beispiel offene Fragen und Punkt, die besonders Verbraucher:innen betreffen: *Welche Produkte*

- ITRE Committee July 2023: „The report expands the list of critical products under class I, to include as well home automation systems and products that enhance private security, such as cameras and smart locks.”

> The proposed CRA divides digital products covered by the regulation into two main categories, based on their level of risk. The first is **default non-critical products**, i.e. hardware and software with a low level of criticality (e.g. hard drives, smart home assistants or connected toys). The second is **critical products** (listed under Annex III), which are further divided into two sub-categories, class I lower risk (e.g. virtual private networks and routers) and class II higher risk (e.g. operating systems for desktops and mobile phones or smart meters) reflecting criticality and intended use.

- In Council, Member States’ representatives (Coreper) reached a common position on 19 July 2023, allowing the Council to enter in negotiations with the European Parliament. Council notably removed the notion of "critical" from products with digital elements and deleted a substantial number of the products listed in the Annex III. Council introduced three categories of products, critical for essential entities as defined by the NIS2, that would fall under mandatory European cybersecurity certification by means of a delegated act.

Beispiel offene Fragen und Punkt, die besonders Verbraucher:innen betreffen: *Welche Produkte*

- In Council, Member States' representatives (Coreper) 19 July 2023

device or remotely by the manufacturer. The processing or storage at a distance is covered only in so far as necessary for a product with digital elements to perform its functions. This could for instance be the case where a hardware device requires access to an application programming interface or a database developed by the manufacturer. For example, many smart home devices are designed to communicate with a cloud service provided by the manufacturer, which enables users to control and monitor the devices at a distance using a mobile application. In such case, the cloud service is therefore in the scope of this Regulation as a remote data processing solution.

Weitere Diskussion und Fragen

Julia Schuetze
Projektleiterin Cybersicherheitspolitik und Resilienz
Stiftung Neue Verantwortung e.V.
Email: jschuetze@stiftung-nv.de
julia@schuetzedigital.com (ab 1. Oktober)
@juschuetze (Twitter)

Stiftung Neue Verantwortung