Cybersecurity in post-covid times

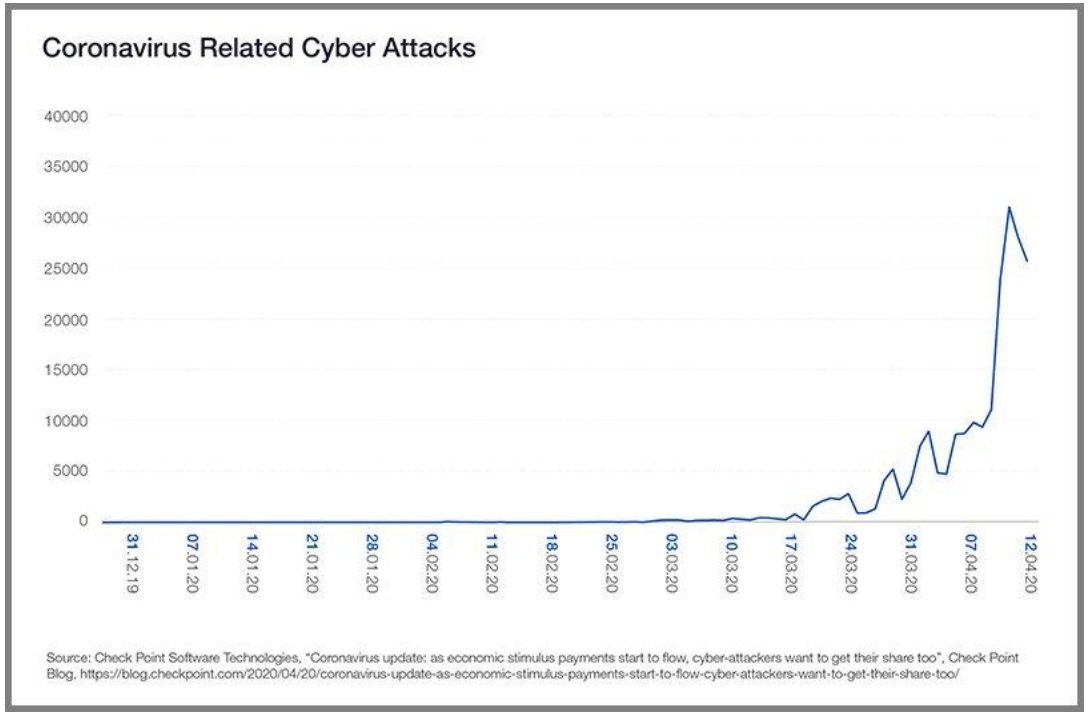
Ljubljana, October, 2021

Miloš Krunić
Cyber Security Manager

A1 Telekom Austria Group

Pandemic of … cyber attacks

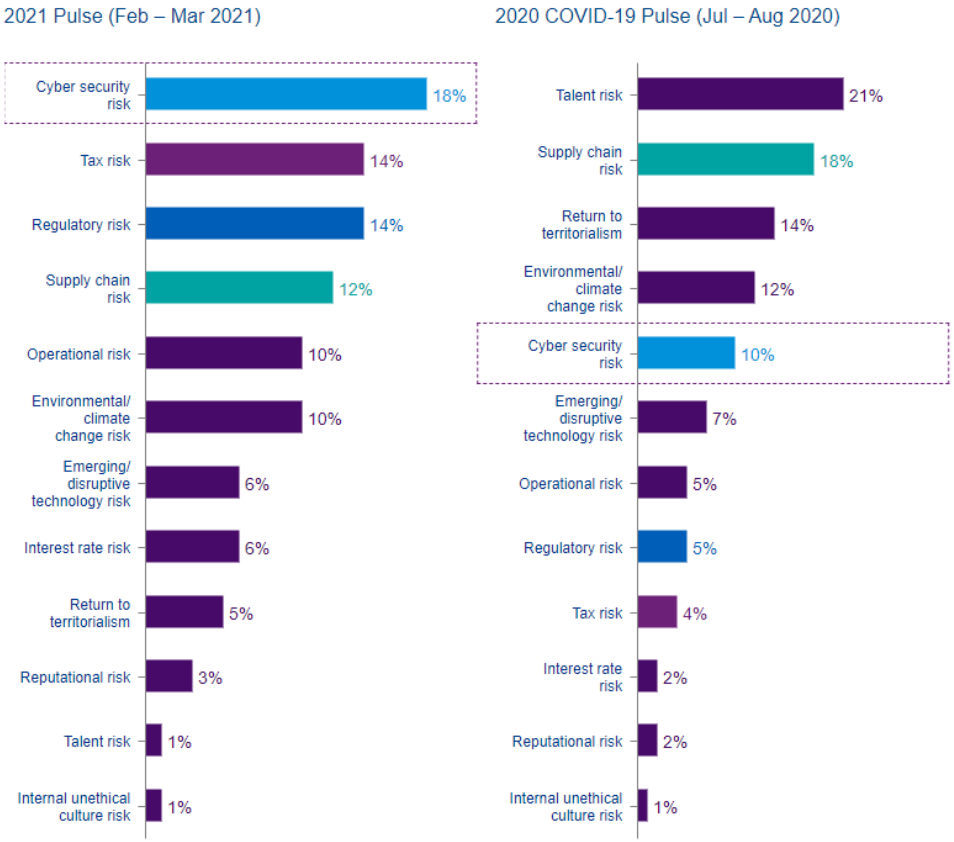
- Working from home has become a new normal.
- Not only more attacks, also larger targets.
- COVID accelerated digital transformation.
- With automation new threats arise.



No. 1 threat

- KPMG‘s 2021 Outlook Pulse Survey about CEOs 3-year outlook: cyber security risk is **no. 1 threat to companies‘ growth**.

- CEOs plan to spend more on digital technologies than last year, with **52 percent prioritizing data security measures**.



Source: KPMG 2021 CEO Outlook Pulse

A bit of statistics..

- By the end of 2021, cybercrime is expected to cost the world $6 trillion. By 2025, this figure will climb to $10.5 trillion.

- 61% of cybersecurity professionals believe that their cybersecurity team is understaffed. Moreover, the cybersecurity skills gap will remain a huge challenge, creating **3.5 million unfilled jobs** in 2021.

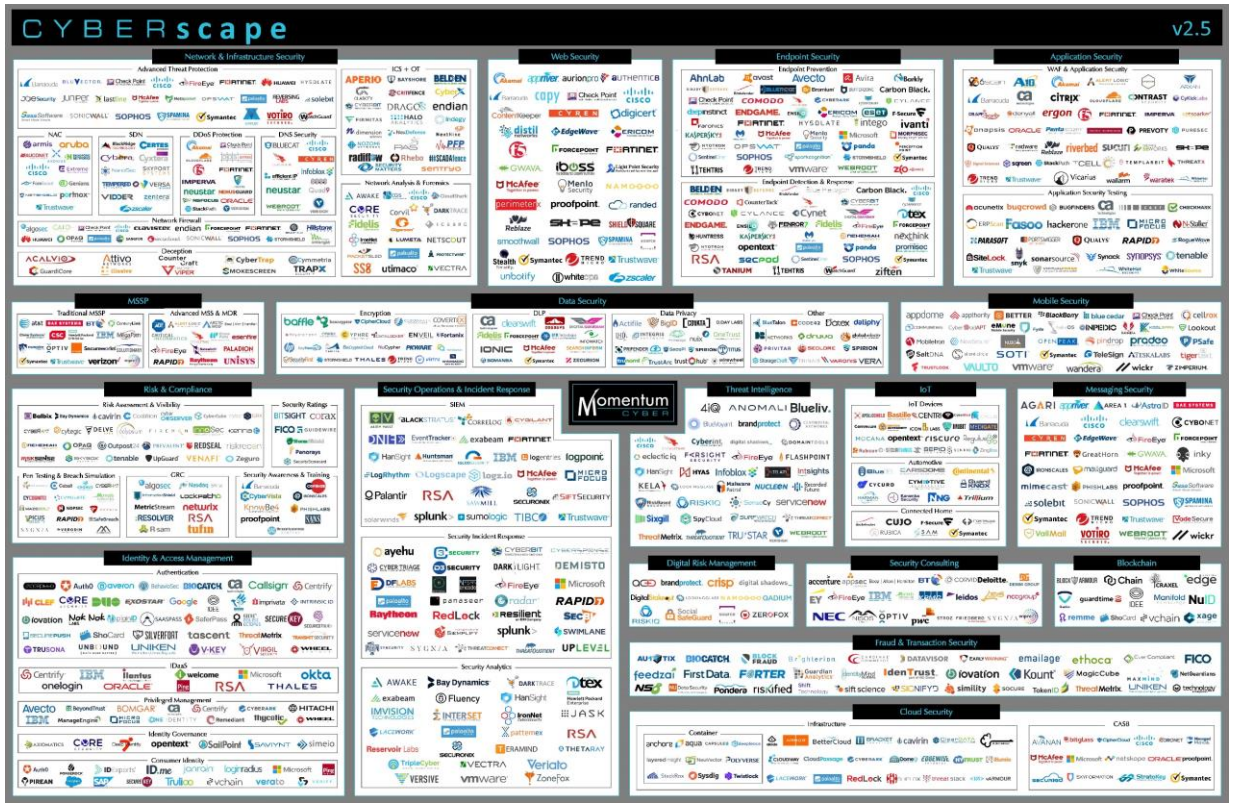
- Since the start of the pandemic, there has been a 300% increase in reported cybercrimes in the USA.

- In 2021:

- 85% of breaches involved a human element
- 61% were due to stolen or compromised user credentials
- Social engineering was observed in over 35% of incidents

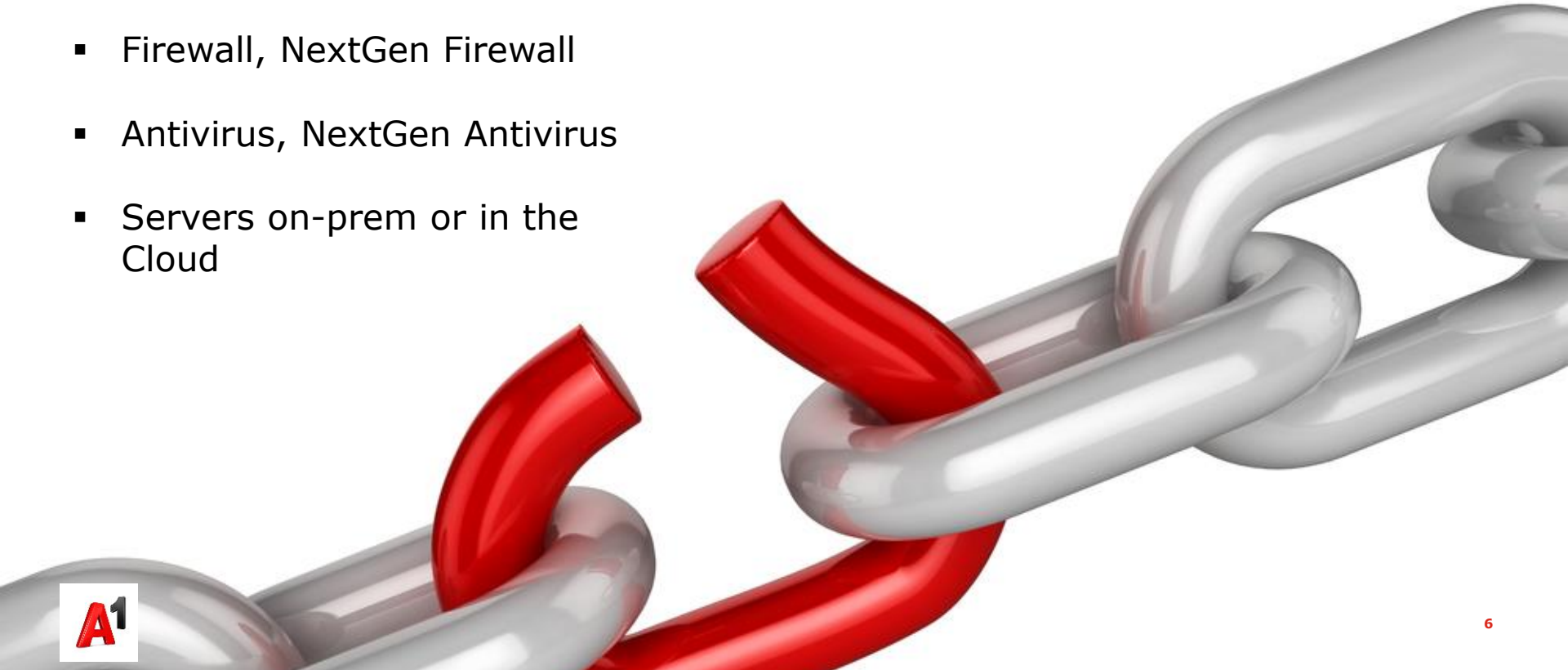
Source: packetlabs.net

Now what? Even more products & vendors?



The usual environment in a Slovenian mid-sized company

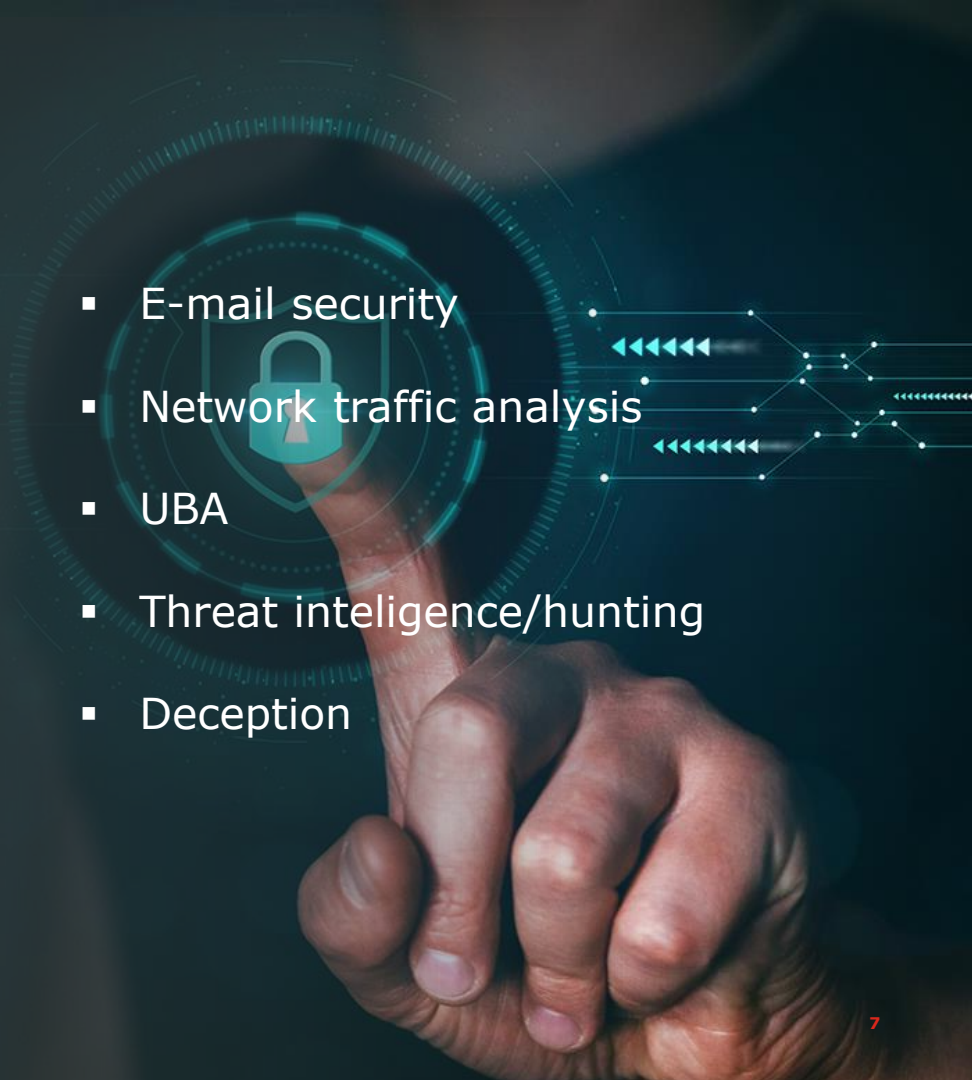
- Firewall, NextGen Firewall
- Antivirus, NextGen Antivirus
- Servers on-prem or in the Cloud



CyberSec needs nowadays

- NG Firewall, NG Antivirus, MFA
- SOC
- SIEM
- XDR
- Penetration Testing

- E-mail security
- Network traffic analysis
- UBA
- Threat inteligence/hunting
- Deception



MFA (Multi Factor Authentication)

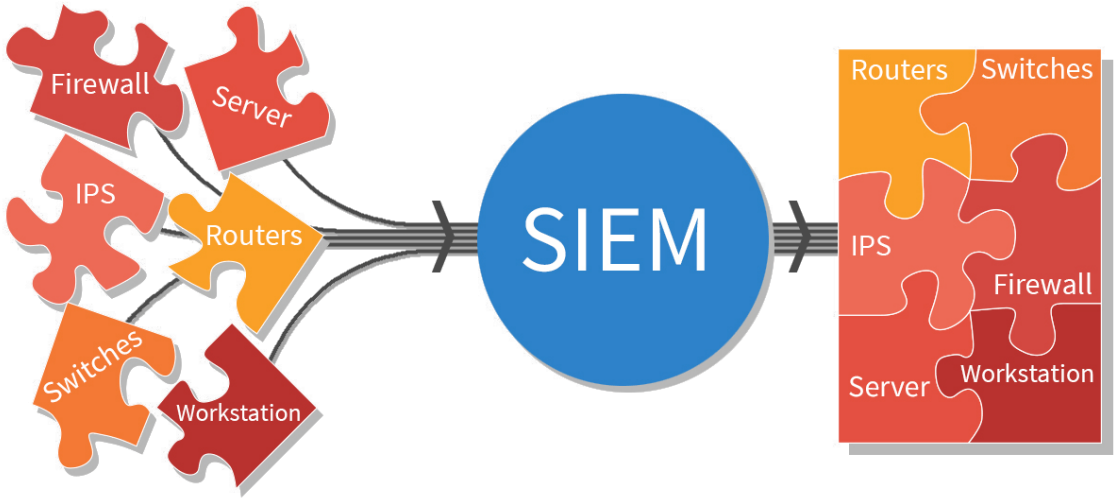
- Something the user has
- Something the user knows
- Something the user is
- Somewhere the user is

A Security Operation Center (SOC)

- **Prevention**
- **Detection & Defense**
  - Real-time alarm messages
  - Processing by security analysts
  - The Risk & Security Cockpit
- **Reporting**
  - Individual reports and statistics

Security information and event management (SIEM)

- Data collection
- Policies
- Data consolidation and correlation
- Notifications



XDR (**extended detection and response**)

- Detection and response
- Reducing false positives
- Faster & more accurate triage
- Centralized configuration
- Comprehensive analytics

Penetration Testing / Vulnerability Assessment

- Identify and Prioritize Security Risks
- Intelligently Manage Vulnerabilities
- Leverage a Proactive Security Approach
- Verify Existing Security Programs Are Working and Discover Your Security Strengths
- Increase Confidence in Your Security Strategy
- Meet Regulatory Requirments

Phishing Attack

email

E-mail security

- Anti Phishing (Spear Phishing)
- Anti Malware & Ransomware
- Email Policy

Network traffic analysis

- Credential theft
- Lateral movement
- Data exfiltratrion
- Risky connections

UBA (User behavior analytics)

Detection of

- insider threats
- targeted attacks
- financial fraud

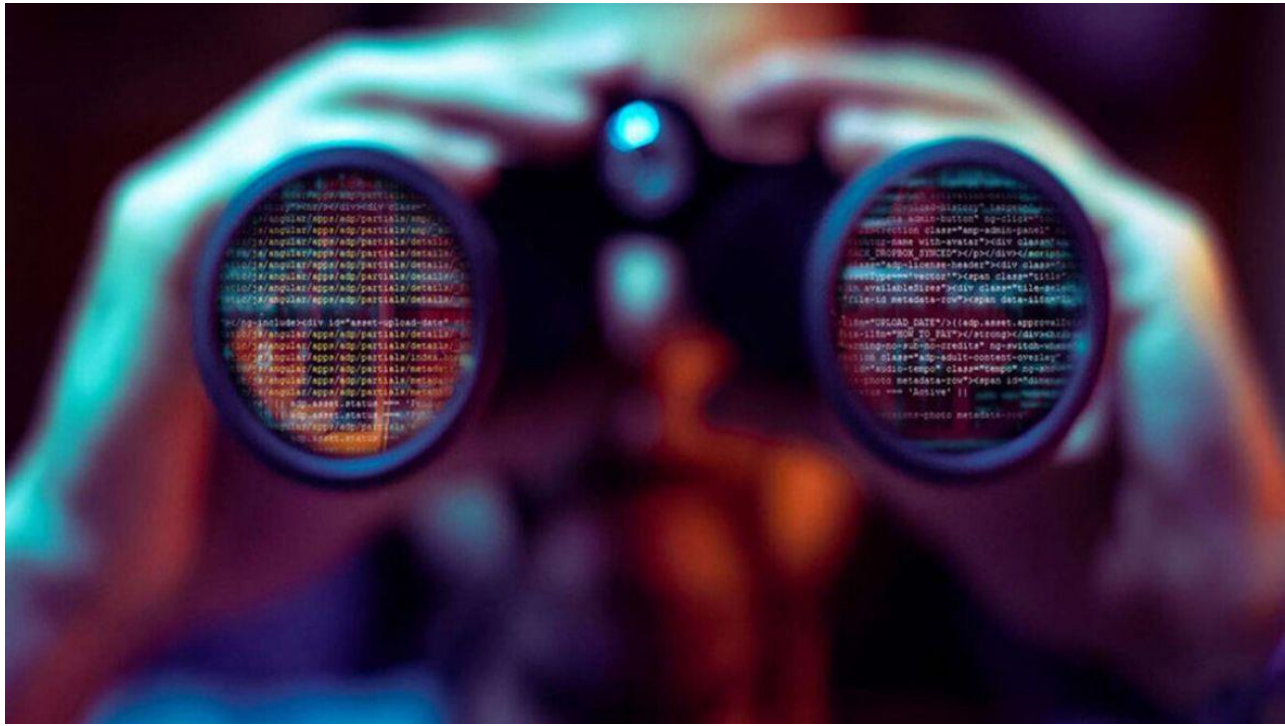
Threat inteligence

Keep organizations informed of risks:

- advanced persistent threats
- zero-day threats and exploits

Threat hunting

- The Trigger
- Investigation
- Resolution



Deception (Honeypots)

- Early Post-Breach Detection
- Reduced False Positives and Risk
- Scale and Automate at Will
- From Legacy to IoT

Black or white?

Build your **own defence**

- Need qualified people that are hard to get (what business am I in?)
- Constant training and improvements
- Investment in equipment and solutions
- Have full control over the detection and defence set up

100% CSaaS

- Focus on supporting core business
- Use (shared) highly-skilled specialists
- Always up to date with latest discoveries
- Loss of control

How can I **improve** my defence and **optimize** security operations at the same time?

A1 – selected security achievements

What makes us special in Cyber Security?

Our security experts have been awarded multiple prices at the most prestigious industry competitions such as the **Austrian (ACSC)** and the **European Cyber Security Challenge (ECSC):**

- 2015 first place (ECSC)
- 2019 third place (ECSC)
- 2020 first and second place (ACSC)

As of September 2020, A1 Digital Germany is official partner of the cyber security alliance **„Allianz für Cyber-Sicherheit"** of the Federal Office for Information Security („Bundesamts für Sicherheit in der Informationstechnik).

A1 Digital is certified as „Qualified body" (under the **authority of the Austrian Federal Ministry of Interior**) to render audits and consulting services in the area of cyber security for critical infrastructure.

Our experts are certified according to §§ 55ff of the Federal Security Police Act („Sicherheitspolizeigesetz").