Thorsten Urbanski and Ildiko Bruhns, ESET Deutschland

POSITION PAPER

DIGITAL SOVEREIGNTY is only possible with strong IT security

Digital Security
Progress. Protected.

Nation State autonomy is a prerequisite for the economy, for healthcare and for our society to be able to act and exist. While it sounds simple, it is by no means self-evident in the present day. Above all, repeated failures in the area of IT security ensure that the much-invoked theme of digital sovereignty falls into question.

Ever since the COVID-19 pandemic began, we have known that Europe is in anything but good shape when it comes to digital sovereignty. Inadequate or even completely absent digitalization strategies revealed an enormous need for action early on in the pandemic. It quickly became apparent that companies, institutions and public authorities had become too dependent on digital imports from non-European countries – or countries whose values weren't aligned – instead of relying on their own expertise. The effects are still clearly noticeable: Supply bottlenecks, missing components, and both products and solutions that do not comply with European security standards are among the current challenges placing companies and institutions at risk of faltering. All of this combined endangers Europe's digital sovereignty and could contribute in the long term to its economic strength falling by the wayside.

There is not only a lack of laptops, servers and mobile digital devices for remote work but also a lack of cloud infrastructure and applications. Above all, there is also a lack of mature IT security concepts and technologies in many areas, as the increased and often successful attacks on public authorities, hospitals and governments have shown. It has long been clear that digital sovereignty is not feasible without strong IT security.

IT SECURITY AS A BASIC PREREQUISITE FOR ECONOMIC AND POLITICAL SELF-DETERMINATION

The German Federal Office for Information Security (BSI) therefore recommends that companies invest 20 percent of their IT budget in digital security. What companies actually invest, however, appears to be quite different. According to official estimates, companies currently spend less than 10 percent of their total IT budget on technical security measures. In addition, many companies are dependent upon IT security services from non-European countries,according to a survey by the German digital association Bitkom. Of the 1,100 organizations across all branches of industry with 20 or more employees, 55 percent were affected. Nine out of 10 of the companies surveyed see the need for Germany to invest more money in IT security solutions in order to improve its technological position and come considerably closer to digital sovereignty. Cybersecurity also plays a crucial role for a digitally sovereign Europe. First and foremost, digital sovereignty means creating a secure data infrastructure for Europe with protected cyberspaces for citizens. This can only be achieved based upon the regulations and laws in force in Europe and with participants from within our own ranks. After all, the primary goal of digital sovereignty is to reliably prevent the manipulation, unauthorized access and forwarding of data.

> *"IT security must be at the top of the agenda for EU member states. Efforts to develop a new common policy on network and information security is a step in the right direction. A comprehensive European cybersecurity strategy is also absolutely imperative if we want to protect the digital sovereignty of all EU member states."*
>
> Thorsten Urbanski, Head of the TeleTrusT working group *IT Security made in EU*

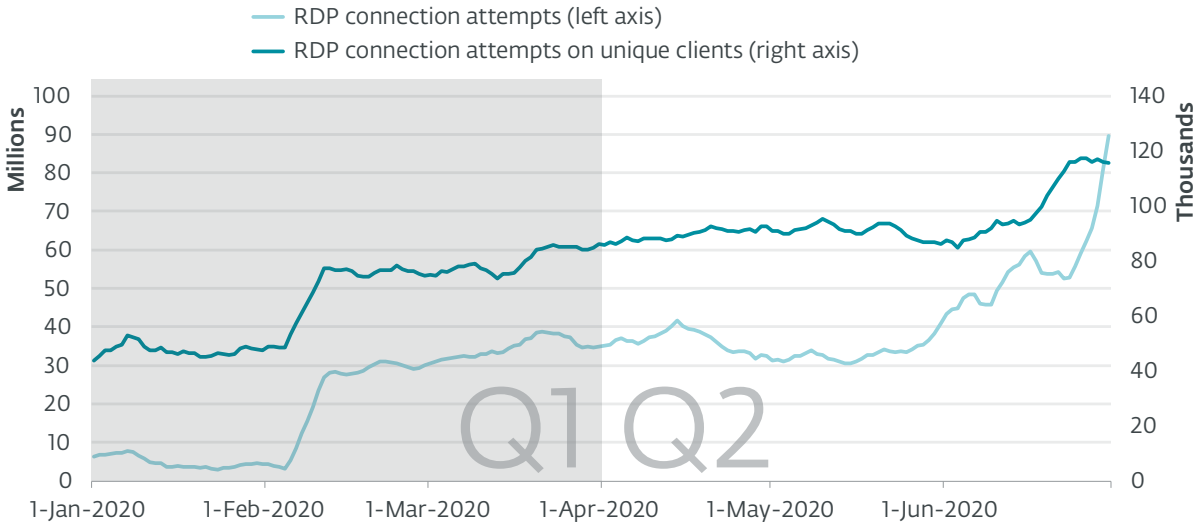
Technology and software from Europe must therefore be clearly positioned along with a reliable IT security concept. This is the only way to drive competitiveness forward, especially with Industry 4.0 in mind, but also for the operation of critical infrastructure (CRITIS). The intensified level of threat clearly demonstrates that there is an immediate need to catch up and take action, particularly in the area of IT security.

TIME IS OF THE ESSENCE

Cybercriminals are increasingly targeting companies, institutions and even governments. *Hacker groups* such as *LuckyMouse*, *Winnti Group* and *Calypso* exploit even the smallest of vulnerabilities. Whether through espionage, supply chain or ransomware attacks, the financial damage is often immense. However, one of the greatest current threats to public organizations clearly emanates from so-called advanced persistent threats (APTs).

For example, the recent *security vulnerabilities in Microsoft Exchange* that came to light made email servers around the world easy prey for cybercriminals. Small companies were targeted just as much as hospitals, large corporations or big players such as the European Banking Authority. Attacks with ransomware are also still among those types of attacks companies and institutions are confronted with; the most recent examples of which are MediaMarkt and Saturn, consumer electronics retailers in Germany and the Netherlands. The ransomware attack on the US IT management software Kaseya VSA also caused a frenzy when criminals demanded a ransom of $70 million.

The relocation people's offices to the four walls of their homes has also opened up numerous backdoors for hackers; for example, the free Remote Desktop Protocol came under constant attack. In December 2020 alone, the European IT security company ESET registered an average of 14.3 million attacks per day in Germany, Austria and Switzerland. This corresponds to 166 attacks a second!



Trends of RDP connection attempts in Q1 2020-Q2 2020, seven-day moving average

Source: ESET Threat Report Q2 2020, p. 22

IT SECURITY MADE IN EUROPE

Attacks like the MS Exchange attack are not isolated incidents. This was demonstrated, for instance, by the security vulnerability found in Citrix software that paralyzed the University Hospital in Düsseldorf in September 2020. Experts assume that the health and government sectors will have to expect further attacks on platforms such as Microsoft SharePoint and Oracle as processes continue to be digitalized. Governments and public authorities must ensure that they become more independent in the area of information security so that they will not be defenseless against such threats in the future.

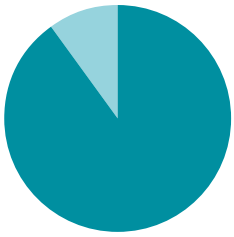
A survey by the European Commission shows just how important this is: According to this survey, 80 percent of Europeans would make their health data available if data protection and security were guaranteed. The cases of these respondents and other examples demonstrate how essential trust in information protection and data security is for advancing digitalization in Europe.

For this reason, the German IT-Sicherheit e.V. (TeleTrusT) has launched the discretionary labeling option "IT Security made in EU" (ITSMIE). This mark of trust enables European creators of IT security solutions to stand out from foreign competitors and demonstrate that their solutions comply with strict European data protection regulations. The seal is not only intended to signify trust but also to bring products and technologies from the EU into focus for business and government.

For example, concerning tenders, public authorities may assume that an outstanding solution with the seal "IT Security made in EU" will meet the highest requirements.

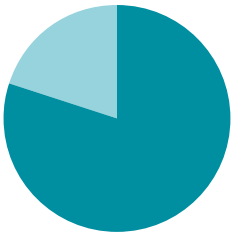
Organizations and users thus ensure that they are able to trust the performance and reliability of the technologies and solutions so labeled with the seal, as well as their unconditional compliance with the law. With this seal, creators with their headquarters in the EU voluntarily commit to ensuring that their security solutions are trustworthy, comply with the most stringent data protection requirements and do not contain any hidden backdoors. The company must undertake to meet the requirements of the EU's General Data Protection Regulation.

What EU citizens expect from digitalization in healthcare



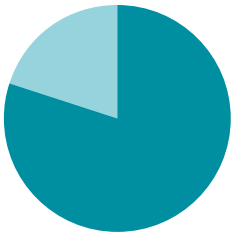
90 %
of Europeans

expect to have access to their own health data, which requires compatible and high-quality health data



80 %
of Europeans

would make their data available if data protection and data security were guaranteed



80 %
of Europeans

would provide an evaluation regarding the quality of medical treatment if such digital possibilities and the corresponding infrastructure for patient-centered healthcare were available

Source: European Commission/DG for Taxation and Customs Union

ASPECTS THAT BUILD TRUST

- The company headquarters must be in the EU.
- The company must offer trustworthy IT security solutions.
- The products on offer must not contain any hidden access (no backdoors).
- The company's IT security research and development must take place in the European Union.
- The company must undertake to comply with the requirements of the EU's General Data Protection Regulation.

ESET: THE EUROPEAN RESPONSE TO CYBERCRIME

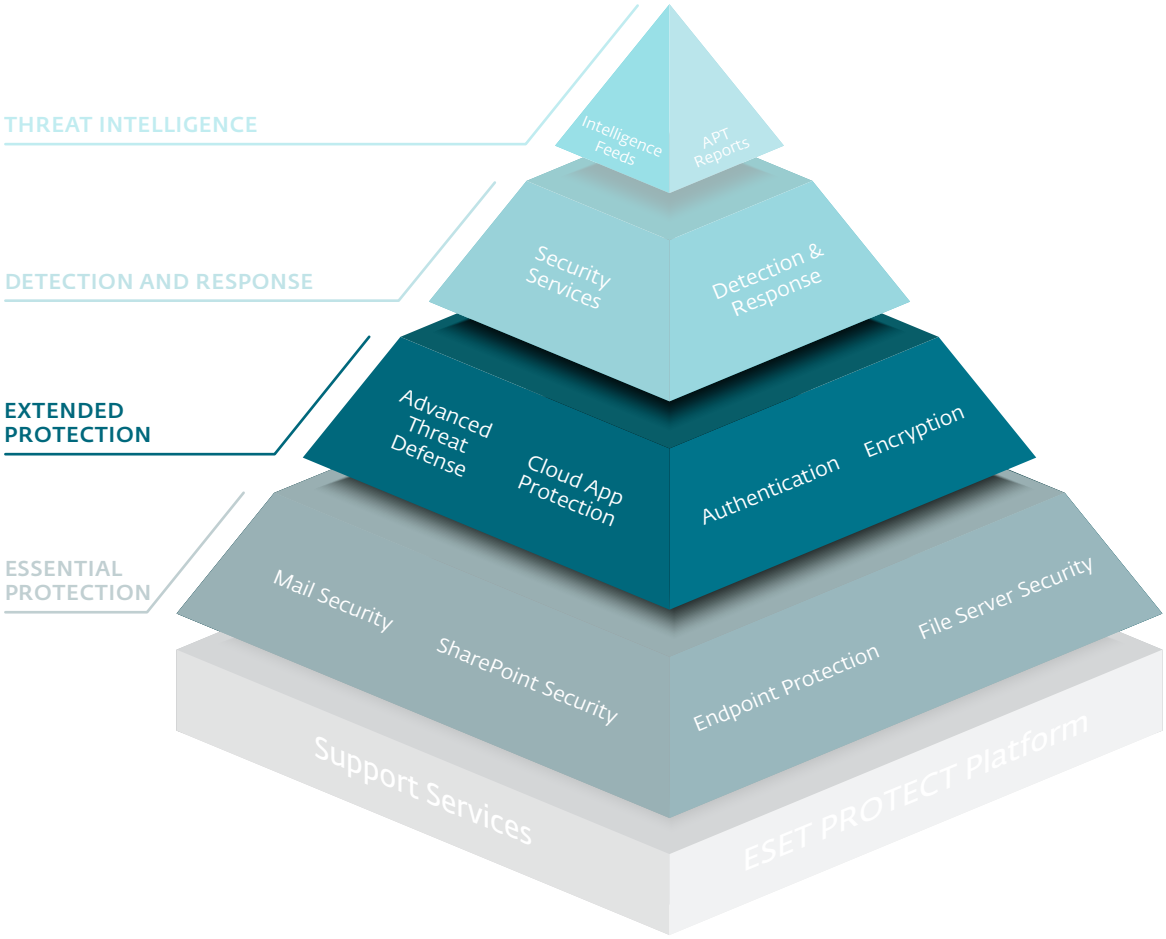
100 companies have already signed up to the initiative. IT security company ESET was one of the first companies to participate. By signing the voluntary declaration of conformity, ESET has confirmed its commitment to EU data protection and trusted IT protection solutions. In addition, the security specialist launched several research collaborations in 2020 and 2021, including with the European Organization for Nuclear Research (CERN), Europol and the French National Agency for the Security of Information Systems (ANSSI). There will also be further exchanges with transnational cybersecurity organizations in the future.

Thinking and acting with foresight is also exactly what organizations desperately need in the fight against cybercriminals. In the case of the Microsoft Exchange attacks, many public authorities and companies would have been spared had they been using endpoint detection and response solutions. This technology continuously searches within a system for security vulnerabilities, suspicious behavior and unusual events.

In order for organizations to identify external attacks, employee misconduct and unwanted applications as quickly as possible, they need to be fully informed about what is happening on their networks. As ESET researchers have determined, organizations are increasingly being targeted by criminals for three main reasons:

- Technical inadequacy due to the COVID-19 pandemic
- Untrained employees unintentionally become security vulnerabilities
- The rise of cybercriminals as professional hacker groups

Zero Trust Security Implementation Stage



The ESET maturity model for the Zero Trust security.

SECURITY FROM A SINGLE SOURCE: ZERO TRUST AS A STRATEGY

There is no doubt that public authorities and companies must rise to the challenge of digitalization. If IT managers want to be proactive, they should adopt a consistent Zero Trust security approach within their organization because conventional protection solutions, consisting of malware and spam filters as well as firewalls, are no longer sufficient to prevent cyberattacks. Professional APT attacks are increasingly circumventing these mechanisms by infiltrating systems stealthily, unnoticed and in multiple stages. For this reason, ESET has also developed a *Zero Trust* approach and adapted it to the requirements of different organization sizes. In the case of Zero Trust, all internal and external devices, processes and people are first classified as potentially dangerous so as not to take any risks. With comprehensive protection to the fullest extent for all devices from inside and out, ESET even goes one step further than what is required by the BSI.

ESET's "Zero Trust Security" approach consists of a three-stage maturity model that builds upon each level. The higher the level, the more secure the protective effect – that is, "more mature. The model starts with the basic-level "Basic Protection Plus," which follows the principle of "Multi-Secured Endpoints." It is suitable for any size organization, regardless of individual protection needs. Thanks to its high degree of flexibility, it can also be easily applied across industries to meet the needs of companies, public authorities or the healthcare sector. This is followed by two Zero Trust levels with further increasing security measures and services.

ESET develops all of the technology in-house and in its own research labs. This also includes multi-factor authentication and data encryption – across all popular operating systems, whether cloud-based or on-premises. As a result, ESET security solutions are uniform and based upon a commitment to Zero Trust Security. This is a great example of what future-proof IT security solutions must look like if they are to become a secure anchor for companies, institutions and public authorities in their digital sovereignty, and thus an investment in Europe's future.

About ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services to deliver comprehensive, multilayered protection against cybersecurity threats for businesses and consumers worldwide.

ESET has long pioneered machine learning and cloud technologies that prevent, detect and respond to malware. ESET is a privately owned company that promotes scientific research and development worldwide.

ESET IN NUMBERS

1bn+
internet users protected

400k+
business customers

200+
countries & territories

13
global R&D centers

SOME OF OUR CUSTOMERS

MITSUBISHI MOTORS Drive your Ambition

protected by ESET since 2017 more than 9,000 endpoints

Allianz Suisse

protected by ESET since 2016 more than 4,000 mailboxes

Canon Canon Marketing Japan Group

protected by ESET since 2016 more than 32,000 endpoints

T

ISP security partner since 2008 2 million customer base

COMMITTED TO THE HIGHEST INDUSTRY STANDARDS

AV comparatives APPROVED Business Security DEC 2021

ESET received the Business Security APPROVED award from AV - Comparatives in the Business Security Test in December 2021.

Leader WINTER 2022

ESET consistently achieves top rankings on the global G2 user review platform and its solutions are appreciated by customers worldwide.

FORRESTER®

ESET solutions are regularly recognized by leading analyst firms, including in "The Forrester Tech Tide(TM): Zero Trust Threat Detection And Response, Q2 2021" as a sample vendor.

Digital Security
Progress. Protected.

welivesecurity™