RADAR
CYBER SECURITY

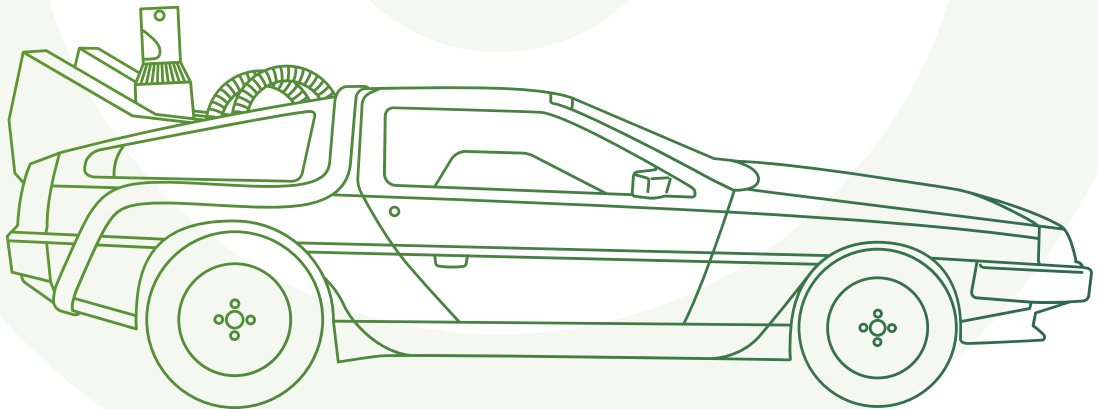
CYBER SECURITY TREND REPORT

A look at 2020

Looking back to move forward.

Technology is involved in every aspect of daily life, thereby having an effect on core areas such as the supply of energy and water, as well as the healthcare and food industries.

There is virtually no part of our life that remains untouched by technology or is not digitally connected. Technology is finding its way into our working and personal lives to an ever-greater extent – at the same time, this technology is becoming increasingly complex and thus more susceptible to attacks and tampering. The larger and more complex the infrastructure, the more vulnerable companies are.



THE EVER-PRESENT THREAT OF CYBER ATTACKS

Cyber attacks and data theft/fraud have been among the top ten risks listed by the World Economic Forum for years, both in terms of the likelihood of them occurring and the extensive, damaging effects they can have. The serious ramifications of cyber attacks mean that they will continue to occupy a fixed place on this list. According to a survey conducted by the German digital association Bitkom, three out of every four companies have fallen victim to acts of sabotage, data theft or espionage, causing a total of 102.9 billion euros of annual damage to the German economy.

THE 26-BILLION-DOLLAR PROBLEM

The FBI recently published figures on the number of business and private emails that have been compromised. The damage here has risen to over 26 billion dollars worldwide since July 2016, more than twice as much as was reported in 2018. Compromising emails is a comparatively simple and effective route for cyber attackers in contrast to trying to hack into a company's infrastructure. Exploiting this communication channel using personalized messages makes it easy to impersonate a trusted employee, customer or partner to then gain access rights to the company's entire infrastructure or to instruct employees to make unlawful transfers or change account details.

New challenges

DANGER IS ALWAYS LURKING

Employees work at home, on the train, at the airport, in the hotel or at the customer's. They are mobile, accessing company networks from anywhere in the world, thereby creating more opportunities for attacks and posing an ever-growing security risk for the entire company. Clear program and policy development, communication, risk assessment, and technology implementation, together with continuous monitoring and evaluation activities must be tailored to address the specific challenges associated with mobile devices.

A CONNECTION UNDER THIS NETWORK NUMBER

Companies with a number of locations must ensure security and minimize risks everywhere – in production halls, offices or branches. If not, vulnerabilities in smaller branches may result in a very unpleasant surprise. At the same time, access to the Internet as well as company and production networks must be ensured at all times. According to Gartner, any disruption or downtime costs the company an average of 4,900 euros every minute. Time is money, even more so when services and products cannot be provided and millions of euros in revenue are lost.

AWAY IN THE CLOUDS

Greater volumes of data also need more power, which is why an increasing number of applications are migrating from the company's internal data center to the cloud. Protecting the cloud environment along the data it contains, as well as the actual process of transferring itself, must be given particular attention. By the same token, the use of public cloud services must be taken into account, including the risks of potential downtime, such as was the case with the Google cloud in March last year.

FROM ALI G TO 5G

5G offers a whole host of attractive possibilities, from faster data transmission speeds to improved reliability, and will lead to a flood of new connected devices and, by extension, even more personal data. There will be no limits to the information-gathering bonanza triggered by everything from e-health apps to smart cars and smart cities. These private, personal data must be properly protected against misuse and theft.

Focus on:

Cyber security is an integral part of corporate governance. After all, instead of merely providing support and ensuring that systems run smoothly, security plays a much greater role in actually promoting the business. Cyber security has a direct impact on a company's reputation, share price, turnover, brand value, business relationships with customers and partners, and product launches.

It is very difficult to identify the technical heart of a company today. Is it the IT security team, the data center or the email server? Is it the source codes, patents, customer data or the applications in the cloud? Each new technology adds an additional layer of complexity to the issue of security for companies, which is why new approaches to cyber security are needed to be able to remain competitive and harness the potential for value creation latent in digitalization in an efficient way.

Radar Cyber Security Outlook 2020

WHAT CYBERSECURITY PROFESSIONALS NEED TO KNOW:

1 HEALTH CHECK-UP

Part of a company's digital health report should include update and patch cycles, as well as regular data backups. Installing and properly configuring applications, IoT devices and protocols is also needed here.

Patch cycles need to be implemented swiftly and reliably – from distribution to deployment. This is the only way to ensure that any potential vulnerabilities can be quickly eliminated. Security must be guaranteed for the entire lifetime of a network or device, and cyber security measures must be updated on an ongoing basis.

2 ON YOUR MARKS, GET SET, GO!

Mechanisms to protect data must be in place – the faster they kick in, the better. However, a large number of hacker attacks becoming known this year were only detected after an average of six months. In extreme cases, some were only uncovered years later. The EU's GDPR states that data protection violations must be reported within 72 hours, otherwise penalties may be imposed. Notwithstanding the legal requirements, vulnerabilities in company and production systems must be promptly detected to ensure that the company is protected against malicious acts, tampering and theft – not days or weeks later. Making use of security modules can play a major role here in substantially shortening this reaction time as well as reducing the effort required to remedy the incident.

3

WHAT'S THE MAGIC WORD? DATA!

Information and data are very valuable to companies, and at the same time are responsibilities that need to be protected. It has been more than a year since the EU's GDPR came into force, during which time more than 89,000 violations of data security were recorded, according to the International Association of Privacy Professionals (IAPP). According to the GDPR Enforcement Tracker, www.enforcement-tracker.com, penalties of more than 350 million euros have been imposed throughout Europe under the GDPR. In Germany, the total amount of fines imposed under the GDPR amounts to around EUR 24.6 million; in Austria, the figure is around EUR 18.1 million. The actual number of incidents that go undetected and unreported can only be estimated. The importance of protecting data will only grow in view of the rising level of networking, even in critical areas.

4

GENERAL IT UNCERTAINTY

Knowledge is power, including when it comes to stocktaking and monitoring a company's services, processes, hardware and software. IT security can be improved by tracking down previously unknown assets, as having an overview of devices located in the company's network is absolutely essential for ensuring that compliance policies are followed. This also includes reporting stolen or faulty devices.

5

NO ACCESS FOR UNAUTHORIZED PERSONS

Monitoring access does not just involve securing buildings, rooms and physical IT resources. It also includes restricting connections to computer networks, system files, and data, thereby regulating who can see or use what in the company's network. After all, there is no need for every employee to have access to all areas, devices and servers. Suitable authorizations, rights, alerts and audits control access or entry to buildings and sensitive areas.

6

WELL, WHO ARE YOU?

Not only is it necessary to check logins and data traffic when they come from or are transmitted to external sources, but this also needs to be monitored within the company. When it comes to basic security matters, it is imperative for passwords to be changed regularly and for standard passwords to be changed, especially for IoT devices. These security guidelines must be enforced everywhere in the company without exception. If it turns out that these guidelines are not being followed, corrective action must be taken immediately. Additional security can be ensured by means of two-factor authentication, with this second step making it much more difficult for attackers to hack into accounts. Text message notifications, apps, biometric data such as face recognition, and security keys are used for authentication purposes.

7

CLEAR RULES

Cyber security can also be improved by automatically monitoring the status of systems and networks thanks to use cases, taking relevant values and indicators as benchmarks. This improves security and makes it easier to detect anomalies swiftly, thereby helping to avert truly malicious and critical attacks and risks. Use cases can be further developed to detect and lock down attack vectors at an early stage. They are an integral part of any successful security concept, ensuring that every implemented security module and tool, and every developed use case, is usable and valuable.

8

SECURITY PARADIGM SHIFT

Companies forming part of the critical infrastructure need to move away from availability towards a comprehensive approach to security. Such companies include providers and operators in the fields of energy, information technology and telecommunications, traffic and transport, healthcare, water, food, financial services, and insurance. Further legislation will extend these requirements to the defense industry, cultural and media companies, and waste management. What this means is that, in addition to complying with the GDPR, companies must adhere to the Network and Information System Security Act (NIS) or, in Germany, the IT Security Act 2.0. These oblige companies to implement comprehensive security measures and to demonstrate their effectiveness. In the case of German companies responsible for critical infrastructure (KRITIS companies), this also means deploying state-of-the-art systems specifically designed to detect attacks.

9

MORE DEVICES, MORE PROBLEMS

The sheer number of devices and applications, including a growing number of IoT devices, poses many risks, meaning it is of paramount importance to secure connections to data centers and cloud storage. With so many devices, there is always the question of what to do with them. Keep them or throw them away? Devices that are no longer needed and that may contain confidential data, such as printers and photocopiers, should be disposed of properly and securely.

10

MINI DEVICES AND BIG DATA

IoT devices have led to a change in processes and redesigned services. The Internet of Nano Things (IoNT) will provide even deeper insights into production and company areas, while at the same time contributing to the deluge of data in the coming years. The devices differ considerably from IoT in size, with an extremely refined and sophisticated design and manufacturing process. They measure and monitor temperatures, humidity, water quality or exhaust gas values. Nanosensors are increasingly finding their way into smart homes, smart cars, the healthcare sector and farming, in addition to highly sensitive production facilities. Both the devices that also collect critical or personal data and their digital connection to the network must be closely monitored and protected by companies.

Cyber security checklist

WHAT NOW FOR CYBER SECURITY?

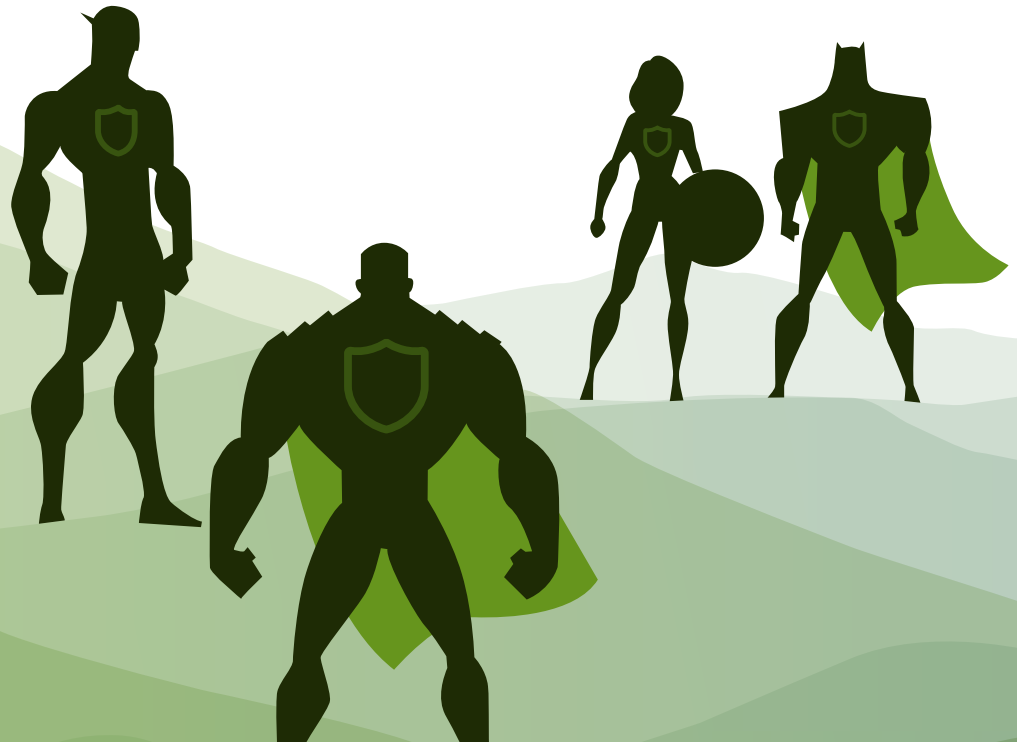
An end-to-end security approach is needed to protect people and companies from ever greater and more extensive threats. Any area in the company can become a potential gateway for cyber attacks. Global networking and Industry 4.0 mean that a comprehensive approach is needed to protect IT and OT from cyber attacks, as this is the only way for companies to be able to create a resilient IT and OT infrastructure and minimize the risk of operational standstills.

PROCEED WITH CARE

According to Statistics Austria, one in ten companies has not taken any precautions to protect themselves against IT security incidents. A TÜV survey in Germany revealed that one in eight companies has been the target of a systematic cyber attack in the last twelve months.

The risks facing companies remain very high. The number and types of threats are changing constantly and require the use of early detection systems, including in the area of critical infrastructure. The NIS Act and the new IT Security Act 2.0 are now focusing on critical infrastructure companies following the data protection requirements of the GDPR. They must protect their systems comprehensively, using attack detection systems, and with the right modules and tools in accordance with the latest technological standards. This includes modules such as Log Data Analytics, also known as SIEM, Network Behavior Analytics, or NBA, and Vulnerability Management and Compliance, or VMC. Cyber security measures must be constantly updated, and tools and methods must be constantly developed and refined.

Cyber security is a marathon, not a sprint.



PULLING TOGETHER

Cyber security is something that concerns everyone, which is why every department in the company needs to be aware of this. Attackers often play on the ignorance and good faith of employees, meaning that it is very important for every company to make their own employees aware of security-related issues. The importance and responsibility of security aspects must also be anchored in management, if for no other reason than because of liability under the GDPR. IT security modules, data protection and security awareness go hand in hand.

SIZE DOES NOT MATTER

When it comes to cyber security, there is no such thing as small or uninteresting targets. Many medium-sized companies are regularly targeted by attackers as well-known drivers of innovation, technology and business. The damage caused has devastating repercussions both for large enterprises as well as medium-sized ones. Many medium-sized companies in particular do not invest at all in IT security or, if they do, only to a limited extent. Any downtime can quickly spiral into insolvency for such companies. Investing in cyber security and the right detection modules at an early stage can therefore prove to be a worthwhile undertaking to prevent attacks in a very short space of time.

AN OVERVIEW TO SEE EVERYTHING

Companies are often under the misconception that many different solutions also translate into more security. A survey by the IT research and analyst firm ESG shows that 55 percent of companies have more than 25 different cyber security products in use. Having more security tools does not automatically increase security, often having the opposite effect instead. This is because having so many tools generates a lot of data and a high workload for the

handful of security experts normally working in companies. The result is that there is not enough time to make optimum use of these tools, as all these different solutions produce findings and data that must be inspected, evaluated and have conspicuous features identified. An overview such as the Risk & Security Cockpit, which uses machine learning to correlate, evaluate and bundle all events, improves the efficiency of the work and reduces threats and risks for companies. Use cases also make it easier to identify risks at an early stage. On top of this, experts from Radar Cyber Security's Cyber Defense Center add important information and instructions to the data.

CONTINGENCY PLAN

The right cyber security tools make all the difference when it comes to ensuring long-term security. A strategy for reacting to critical security incidents is needed in addition to the long-term security approach and security concept.

The emergency plan contains measures to be taken and instructions for action to limit or avert damage. Incidents in which emergency plans are used include power failures, technical faults, fire, burglary, vandalism, hacker attacks, criminal acts, personnel shortage or operating errors. This includes technical instructions, responsibilities, alarm chains, lists of measures, communication regulations, contact information or measures to rapidly procure spare parts. The emergency plan always includes both technical and organizational information, enabling companies to react swiftly and appropriately to such extraordinary, critical events. Using firefighting and forensic interventions, Radar Cyber Security assists customers with recommendations for remedial action.

CYBER THREAT HUNTING AND ORCHESTRATION

From reaction and early detection to the next steps

When it comes to cyber security, it has long since ceased to be sufficient to merely react to attacks. In addition to early detection, Radar Cyber Security is also focusing more on proactive Cyber Threat Hunting, the search for threats and malicious activity, using machine learning. Instead of just reacting to warnings and violations, the aim is to contain dangers and minimize risks at an early stage. However, Cyber Threat Hunting is no substitute for IT or OT security monitoring modules, instead serving as a complement to them in early detection.

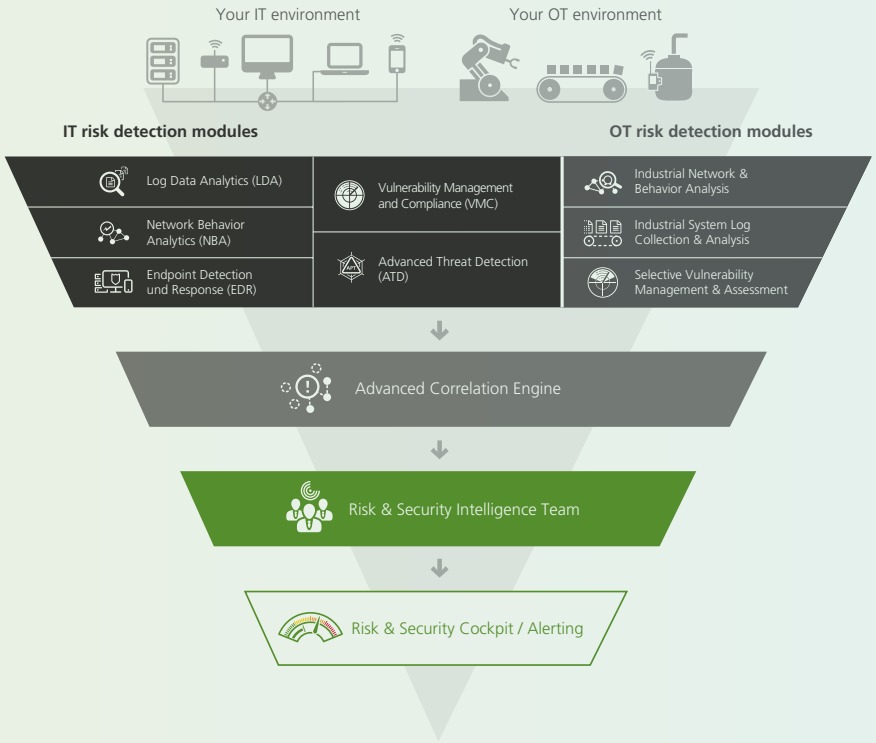
RAIN

Radar Analytics Interface

With RAIN, the Radar Analytics Interface, company security teams and CDC experts gain an even deeper insight into all system data, being able to visualize these so as to make optimum use of them. Comprehensive drill-down and correlation functionalities enable the most complex queries to be executed – supported by an illustration of the relationships between the various elements. As soon as certain malware behavior patterns are detected, experts can create new rules, a process that makes RAIN even smarter and more effective in detecting threats and enables security efforts and risk remediation to be coordinated in the best way possible.

Cyber security: build or buy?

Radar Managed Services vs. Radar Platform



IT AND OT SECURITY AS MANAGED SERVICES

As a cyber security service provider, Radar Cyber Security offers integrated IT and OT security monitoring as a standard service. Customers are always up-to-date as regards to their IT and OT risks including real-time alerts thanks to the Radar Risk & Security Cockpit. Hardware and the latest technologies are in use for customers. Highly trained experts are available around the clock. Managed services also improve processes and IT infrastructure.

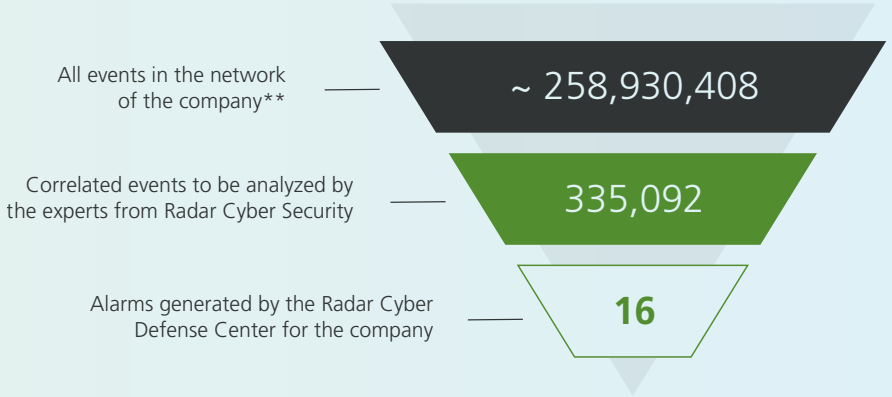
- → Lower costs: operating and maintenance
- → Integrated all-in-one solution
- → Established analysis processes
- → Threat Intelligence continuously updated
- → Radar Risk & Security Cockpit with overview of IT risks including real-time alerting
- → No other human resources: experts for a dedicated CDC
- → Flexibility and scalability
- → Experience from a professional provider

ESTABLISHMENT OF A DEDICATED CDC WITH THE RADAR PLATFORM

The Radar Platform gives you next-generation cyber security detection technology for your own Cyber Defense Center (CDC). It is a unique all-in package to set up an efficient and effective Cyber Defense Center or Security Operations Center (SOC).

- → Total package comprising hardware and software – equipment included as an option
- → Support during all phases: planning and implementation through to integration and continuous improvement such as security system and workflows
- → Adapted to customer needs: latest updates, integrated threat intelligence and continuous improvements
- → Empowerment: service and/or sales

Managed Security Services with NBA & LDA*



*available: On Premise, Cloud, Virtual
**Values refer to the monthly average of one customer (> 10,000 employees) in 2019

RADAR CYBER SECURITY | Safeguard your digital journey.

Radar Cyber Security is Europe's leading technology company in the field of Detection & Response. In focus: The early detection of IT and OT security risks for corporations and public authorities offered as a Solution or a Managed Service. The cutting-edge, inhouse-developed technology plat-form is the basis used for building up a client's Cyber Defense Center (CDC) or it is used in combination with our expert analysts, document-ed processes and best practices as CDC as a Service. The result: Highly effective and efficient im-provement of IT security and IT risk management, continuous IT and OT security monitoring and an overview of security-related information throughout the entire IT and OT landscape of an organization.

Radar Cyber Security HQ
Zieglergasse 6
1070 Vienna
Austria

Phone: +43 (1) 929 12 71-0
Fax: +43 (1) 929 12 71-710
Email: sales@radarcs.com
Web: www.radarcs.com

Radar Cyber Security Deutschland
Taunustor 1
60310 Frankfurt am Main
Germany

Phone: +49 (69) 2443424 655
Fax: +49 (69) 2443424 150
Email: sales_germany@radarcs.com
Web: www.radarcs.com/de

Radar Cyber Security Schweiz/Liechtenstein
Schaanerstrasse 1
9490 Vaduz
Liechtenstein

Phone: +423 237 90 90
Fax: +423 237 74 99
Email: sales_switzerland@radarcs.com
Web: www.radarcs.com/ch

R_CYBER_2019_EN_1