STUDIE / STUDY

Cyberattacken und IT-Sicherheit in 2025

Cyber-attacks and IT security in 2025

Die Expertenbefragung 2018 zu den Zukunftstrends und -herausforderungen der IT-Sicherheit.

The expert survey of 2018 concerning future trends and challenges in IT security.

Powered by

RADAR SERVICES

FLO

CYBERSECURITY ALLIANCE

Wie sicher ist die IT von morgen?

How secure is tomorrow's IT?

Die Frage „Wie sicher ist die IT von heute“ scheint vor dem Hintergrund immer wieder berichteter Vorfälle und Angriffe nicht leicht beantwortbar zu sein. Noch brisanter ist also die Frage, wie es um die IT-Sicherheit in 2025 gestellt ist.

The question “How secure is today’s IT?” does not seem to be answered easily based on the constantly reported incidents and attacks. Even more controversial is the question how IT security will be set up in 2025.

Die Einzigen, die das einschätzen können, sind heutige Branchenexperten. Sie wurden in dieser Studie zu den digitalen Bedrohungen, die auf uns in den nächsten Jahren zukommen werden, sowie zur Weiterentwicklung der IT-Sicherheit, befragt.

The only ones capable of assessing this are today’s industry experts. They were interviewed in the course of this study with regards to digital threats that are awaiting us in the next couple of years as well as further developments in IT security.

Über die Experten und die Methode.

About the experts and the method.

Befragt wurden für diese Studie ausschliesslich ausgewiesene IT-Sicherheitsexperten.

In the course of this study exclusively designated IT security experts were interviewed.

Insgesamt nahmen 105 Experten teil. Die Befragung wurde im zweiten Quartal 2018 durchgeführt. Die Herkunft der Experten umfasste 25 Länder in Europa und Asien. Sie arbeiten für Unternehmen in der Grösse zwischen 50 und 120.000 Mitarbeitern. Es handelt sich um eine rein qualitativ durchgeführte Studie. Die Antworten wurden schriftlich und anonymisiert abgegeben. Sie wurden einer typologischen Analyse unterzogen.

In total 105 experts participated. The survey was conducted in the second quarter of 2018. Experts from 25 countries in Europe and Asia took part in the survey. They work for companies employing between 50 and 120,000 people. It is an exclusively qualitatively conducted study. The answers were submitted anonymously and in writing. They were subject to a typological analysis.

Wie gut sind Unternehmen auf die Zukunft vorbereitet?

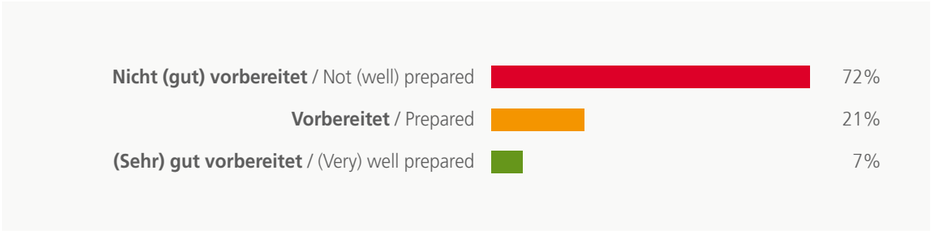
How well prepared are companies for the future?

Sicherheitsexperten schlagen Alarm

Unternehmen sind bei Weitem **nicht ausreichend auf die Zukunft vorbereitet**! Das **sagen 72% der Befragten**. Auf einer Skala von 0 (nicht vorbereitet) bis 10 (sehr gut vorbereitet) geben sie damit ein erschreckendes Bild ab.

IT security experts are concerned

Companies are by far **not sufficiently prepared for the future**! **72% of the interviewees share this opinion**. They evaluated on a scale from 0 (not prepared) to 10 (very well prepared).



Welche Sicherheitsrisiken für Cyberattacken werden von Unternehmen heute unterschätzt?

Which security loopholes are frequently neglected by companies today?

55%

sehen die Nutzer als am meisten unterschätztes Sicherheitsrisiko

55% name users as the most neglected security risk

Ein besonders entscheidender Ausgangspunkt für Gefahren für die IT-Sicherheit sind die Nutzer, ihr Sicherheitsbewusstsein und -Know-how. Ganze 55% der Befragten gaben diese Meinung ab.

Users, their behaviour with regard to IT security, their awareness as well as security know-how are a major issue. 55% of the experts point to that.

16% bemängeln die Sicherheit von IoT-Geräten im Umlauf

16% criticize the security of current IoT devices

Verbundene Geräte bereichern unseren Alltag. Sei es in den Produktionsstätten von Unternehmen (Operational Technology) oder als smarte Geräte für daheim. Sie sind heute jedoch wenig abgesichert. Das machte sich beim Anlagenausfall aufgrund der WannaCry-Attacke oder auch beim Mirai Bot bemerkbar.

Connected devices are part of our daily lives. It is impossible to imagine a production plant without Operational Technology (OT) or a household without smart devices. But from today's perspective, they are quite unsafe. Cyber-attacks like WannaCry or the Mirai Bot are examples which have proven this.

12% beklagen unklare Verantwortlichkeiten und Prozesse

12% miss clear responsibilities and processes

Wer ist für was zuständig und welche Prozesse gibt es, die sicherstellen, dass Sicherheitsmassnahmen von A bis Z strukturiert geplant sind und in der Praxis ablaufen? Wenige Ressourcen, fehlende Zeit und Aufmerksamkeit für die IT-Sicherheit – das lässt die beste Strategie einer Organisation scheitern.

Who is responsible for what and which processes are established to make sure that security measures are in place and they work well in the daily business? Few resources and little time as well as hardly any awareness for IT security – these factors make it difficult for a strategy to be successful in an organization.

Wie wird sich die Anzahl der Cyberattacken bis 2025 entwickeln?

Will we see a rise in cyber-attacks until 2025?

Der Durchschnitt über alle Antworten hinweg liegt bei einer jährlichen Wachstumsrate von 300%. 24% der Befragten halten eine jährliche Wachstumsrate von Cyberattacken zwischen 500% und 1.000% für wahrscheinlich, weitere 7% noch darüber.
Knapp 30% halten einen Anstieg zwischen 100% und 500% pro Jahr für realistisch. Mit einem Rückgang oder eine Seitwärtsbewegung über die kommenden Jahre rechnet keiner der Experten.

The average of all responses: 300% growth of cyber-attacks a year. 24% of the interviewees expect an increase in cyber-attacks between 500% and 1,000%, 7% even above 1,000%. Almost 30% expect a growth rate between 100% and 500%. None of the experts foresee a decline or a sideways trend towards 2025.

300%+ **PRO JAHR**

Wachstum (Durchschnitt über alle Antworten hinweg)
growth p.y. (average of responses)

500%+
Wachstum p.a. prognostizieren 31% der Befragten
growth p.y. anticipated by 31% of interviewees

0%
der Interviewten erwarten keinen Anstieg
of interviewees expect no increase

Cyberattacken der Zukunft: IoT und kritische Infrastrukturen im Mittelpunkt

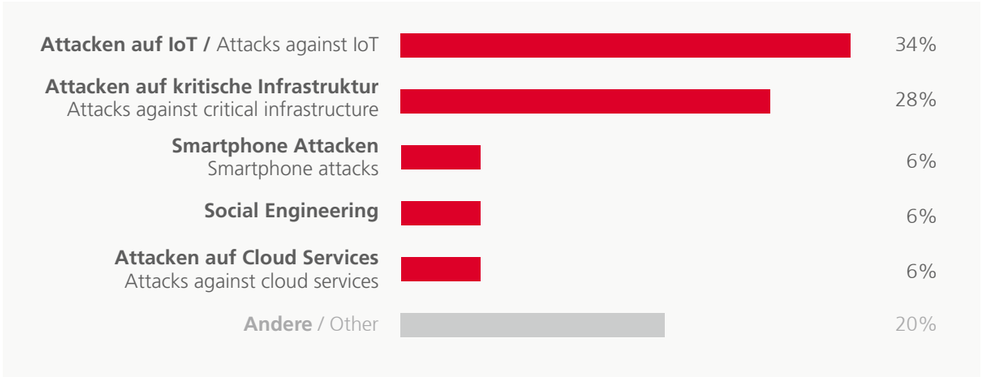
Cyber-attacks of the future: IoT and critical infrastructure in the focus

Das sehen Experten als grösstes Problem: Cyberattacken der Zukunft konzentrieren sich auf das Internet of Things (IoT) und allem voran auf die Operational Technology (OT), also die Steuerung von Produktionsanlagen. Auch Attacken auf die hochentwickelten Systeme von Autos werden im Fokus sein. Zudem: sämtliche (zukünftig) „intelligenten Gegenstände“, die den Alltag der Menschen unterstützen.

This will be a major problem in the eyes of the experts: In the future cyber-attacks will concentrate on the Internet of Things (IoT) and in particular on the Operational Technology (OT) in production plants. Attacks on the advanced systems of cars are expected to be in the spotlight as well. Overall (future) “intelligent things” that support our daily lives will be under attack.

Eine grosse Gefahr stellen laut Experten zukünftig grossflächige Blackouts dar.

Broad blackouts are a major concern for experts as well.



IT-Sicherheitstechnologien von morgen – wie schnell entwickelt sich AI weiter?

Tomorrow's IT security technologies – how quickly is AI evolving?

Experten sagen: IT-Sicherheitstechnologien müssen „intelligent" werden und sehen Artificial Intelligence (AI) / Machine Learning als die entscheidenden Zukunftstrends.

Experts state that IT security technologies have to become more "intelligent" and expect Artificial Intelligence (AI) / Machine Learning to be the major future trends.

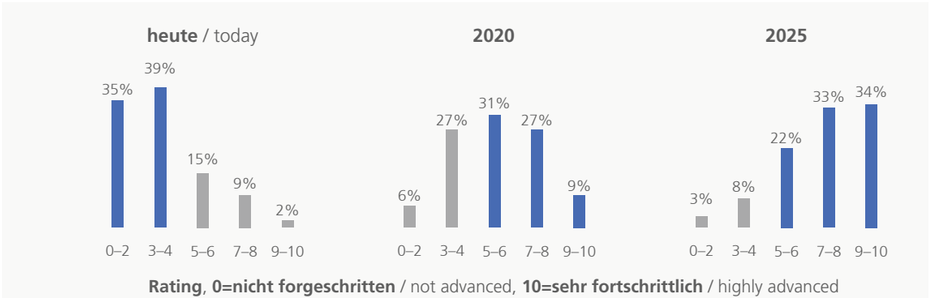
Schon seit 1999 besteht theoretische Forschung zu AI. Die ersten Meilensteine beim tatsächlichen, praktischen Einsatz von intelligenten Systemen wurden aufgrund der immens langen Rechenzeit und den dafür notwendigen, hochleistungsfähigen Prozessoren jedoch erst vor Kurzem erreicht.

Theoretical research on AI exists since 1999. The first milestone for the practical usage of intelligent systems was achieved only recently due to the immensely long computing times and therefore compatible, high-performance processors.

Derzeit sehen 70% der Experten Machine Learning noch in den Kinderschuhen. Bereits in knappen zwei Jahren soll jedoch einiges passiert sein: dann sehen 67% gute oder sogar sehr gute Fortschritte beim Einsatz von Machine Learning im Bereich IT-Sicherheit.
Weitere fünf Jahre danach sind 89% der Experten von einer sehr grossen Einsatzfähigkeit überzeugt. Einigen Entwicklungsspielraum wird es aber auch in 2025 noch geben – denn immerhin noch 11% der Experten bezweifeln auch für 2025 einen grossen Fortschritt.

Currently, 70% of the experts see machine learning still in the early stages. But things will change over time: 67% expect a good or very good progress towards 2020. In 5 years time, 89% are convinced of well and very well-advanced machine learning capabilities. But there is still room for further development: 11% are not yet convinced that machine learning will be well-advanced by 2025.

Einsatzbereitschaft von AI für die IT-Sicherheit / Operational readiness of AI for IT security

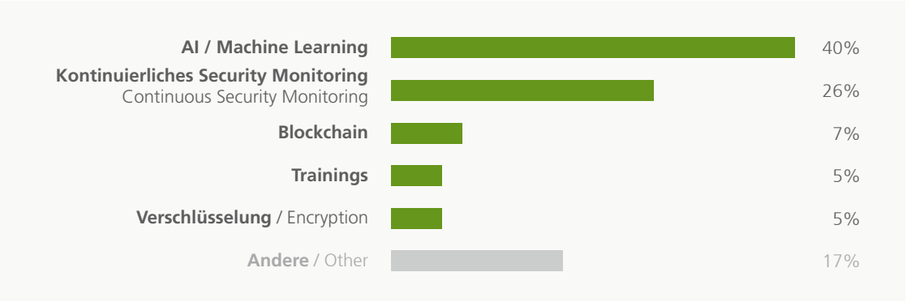


Anregungen für eine zukunftsgerichtete Ressourcenallokation

Suggestions for a future-oriented resource allocation

AI und Machine Learning werden als die entscheidenden Fähigkeiten für zukünftig effektive IT-Sicherheitstechnologien gesehen. Das kontinuierliche IT Security Monitoring in verschiedenen Ausprägungsformen – angefangen von einem Security Information & Event Management (SIEM) bis hin zu einem vollumfänglichen Cyber Defence Centre – nimmt Platz zwei unter den Expertenantworten ein. Aber auch Blockchain ist ein Thema für die Experten. Awareness-Trainings und Verschlüsselung befinden sich auf den beiden letzten Plätzen unter den fünf meistgenannten Antworten.

AI and machine learning are decisive features for effective IT security technologies in the future. Continuous IT security monitoring – ranging from a Security Information & Event Management (SIEM) to a comprehensive Cyber Defence Centre – is named as the second major trend. Blockchain is also a topic for the security experts. Awareness trainings and encryption also belong to the five most frequently given answers.

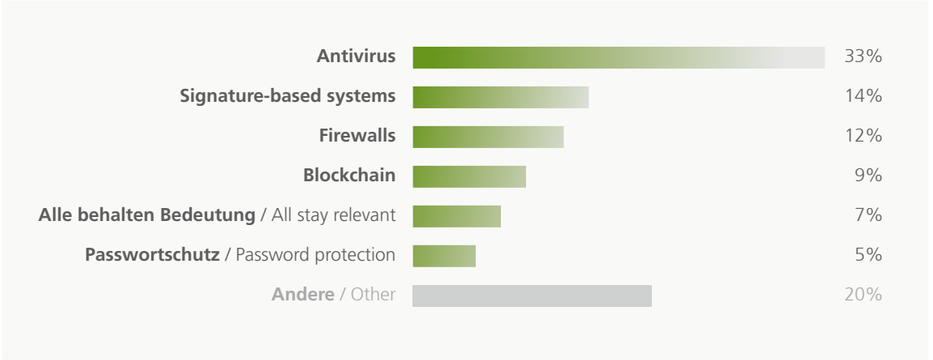


Welche IT-Sicherheitstechnologien werden an Bedeutung verlieren?

Which IT security technologies will have lost importance until 2025?

33% der Experten nennen bei dieser Frage den Virenscanner. Darüber hinaus führen 14% der Befragten signaturbasierte Technologien und 12% Firewalls an. Blockchain wird ebenfalls genannt. Vor dem Hintergrund der Nennung von Blockchain auch bei der vorherigen Frage zum Thema Ressourcenallokation zeigt dies ein geteiltes Bild über ihre Bedeutung für die IT-Sicherheit.

33% of the experts mention anti-virus software. Furthermore, 14% of the interviewees rank signature based technologies and 12% firewalls. Blockchain is named as well although also mentioned in the previous question about resource allocation towards 2025. This indicates a mixed picture when it comes to the significance of blockchain for IT security.



RADAR
SERVICES
Publishing

Verfasser der Studie: Dr. Isabell Claus; Claudia Panozzo, MA

Über RadarServices Publishing
RadarServices Publishing veröffentlicht Artikel, Berichte, Studien und Zeitschriften rund um das Thema IT-Sicherheit. Unser Ziel ist es, Einblick in die Erfahrung von Branchenexperten zu geben und Knowhow zum Thema IT-Sicherheit durch universitäres und nicht-universitäres Research an Unternehmen, öffentliche Institutionen und andere Organisationen weiterzugeben. Wir beziehen Co-Autoren aus Akademia und Wirtschaft aktiv ein um das Wissen über aktuelle Entwicklungen im Bereich IT-Sicherheit in der Öffentlichkeit und im Speziellen bei Führungskräften in Unternehmen sowie in der Politik zu fördern. RadarServices Publishing ist Teil von RadarServices.

Über diese Veröffentlichung
Diese Veröffentlichung beinhaltet ausschliesslich generelle Informationen. RadarServices und/oder dessen verbundene Gesellschaften erbringen mit dieser Veröffentlichung keine fachliche Beratungsleistung. Diese Veröffentlichung ersetzt auch keine derartige Beratungsleistung und sollte auch nicht als Grundlage für Geschäfts- oder Investitionsentscheidungen/-handlungen verwendet werden. Weder RadarServices noch dessen verbundene Gesellschaften haften für Verluste, die eine Person im Verlassen auf diese Veröffentlichung erleidet.

Authors of the study: Dr. Isabell Claus; Claudia Panozzo, MA

About RadarServices Publishing
RadarServices Publishing is publishing articles, reports, studies and journals with regards to the subject matter of IT security. Our goal is to provide an insight into the experiences of industry experts as well as to pass on knowhow regarding IT security through academic and non-academic research to companies, public institutions and other organizations. We are actively including co-authors from academia and the economy in order to promote knowhow about current developments in the field of IT security in the public and especially for corporate executives as well as in politics. RadarServices Publishing is part of RadarServices.

About this publication
This publication exclusively contains general information. RadarServices and/or its related companies do not render technical consulting services with this publication. This publication does not substitute consulting services and should not be regarded as a basis for business or investment decisions/negotiations. Neither RadarServices nor its related companies are liable for losses that incurred due to persons relying on information provided in this publication.

RadarServices ist Europas führendes Technologieunternehmen im Bereich Detection & Response. Im Mittelpunkt steht die zeitnahe Erkennung von Risiken für die Sicherheit der IT von Unternehmen und Behörden als Solution oder als Managed Service.

RadarServices is Europe's leading technology company in the field of Detection & Response. In focus: The early detection of IT security risks for corporations and public authorities offered as a Solution or a Managed Service.

FL1 bietet die Dienstleistungen von RadarServices aus Liechtenstein heraus an. Als erster konvergenter Full-Service-Provider Liechtensteins ergänzt FL1 damit sein Portfolio um Managed Security Services der nächsten Generation.

FL1 is RadarServices' strategic partner for Switzerland and Liechtenstein to provide the Next Generation Managed Security Services in these countries.

Die GENESIS Swiss Team AG ist als Vertriebspartner der FL1 Ansprechpartner für das Portfolio von RadarServices. Unsere Kernkompetenzen im Bereich IT Security liegen im Berechtigungsmanagement, Privileged Access- wie auch SIEM & Log Management. Zu all diesen Bereichen bieten wir zusammen mit FL1/RadarServices eine Managed Security Lösung an.

GENESIS Swiss Team AG
Bernstrasse 34
3072 Ostermundigen

Phone: +41 31 560 35 35
Email: info@genesis.swiss
www.genesis.swiss