GOLDENE ZEITEN

A GOLDEN AGE

FÜR HACKER?

FOR HACKERS?

GOLDENE ZEITEN waren schon immer gleichbedeutend mit großem Reichtum, endlos sprudelnden Geldquellen und einem sorgenfreien Leben. Leben wir in goldenen Zeiten? Viele Unternehmen freuen sich über volle Auftragsbücher, aber Hacker erleben ebenso gerade goldene Zeiten. Der fortschreitendenden Vernetzung und IoT sei Dank. Die Digitalisierung lässt Cyberattacken immer größer, zahlreicher und gefährlicher werden. Wie können die goldenen Zeiten für Cyberkriminelle beendet werden? Wieviel Angriffsfläche bieten Unternehmen und gibt es Strategien die digitalen Raubzüge zu stoppen?

GOLDEN AGES have always been synonymous with great wealth, inexhaustible sources of money and carefree times. Are we living in a golden age? Many companies are enjoying full order books, yet hackers are also experiencing a golden age at the moment. Thanks to the ever-increasing degree of interconnectedness and the IoT. Digitisation is enabling cyber attacks to grow ever larger, more numerous and more dangerous. How can a stop be put to the golden age for cyber criminals? How vulnerable are companies and are there strategies in place to stop the digital raids?

Die Anfänge des Hackings gehen bis 1982 zurück: Die Gruppierung „414s“ waren in mehrere Computersysteme in Amerika eingedrungen. Fahrt nahm das „Geschäftsmodell Hacking“ aber so richtig seit Mitte 2000 auf und wächst seither exponentiell weiter. Anonymous, die Shadow Brokers, Lazarous Gruppe, Fin7, APT28, Snake oder Angriffe wie WannaCry, Carbanak, Moonlight Maze – diese Namen haben internationale Bekanntheit erlangt. Innerhalb weniger Tage können Unternehmen heute vor Schäden in Millionenhöhe stehen – bei WannaCry wurde seitens eines betroffenen Unternehmens von 300 Millionen US Dollar berichtet, bei Carbanak war von einer Milliarde US Dollar Gesamtschaden für die betroffenen Banken die Rede. Das „Gold“, also die finanziellen Benefits aus diesen Angriffen, landen in unbekannten Händen.

Auf einer Zeitachse befinden wir uns demnach schon in einem fortgeschrittenen Stadium der „goldenen Zeiten“. Es gibt aber ein weiteres Problem: Wir bieten durch die starke Digitalisierung in allen Lebensbereichen immer neue Möglichkeiten für Hacker. Ist da ein Ende der goldenen Zeiten in Sicht? Vielmehr das Gegenteil – Reichtum und sprudelnde Geldquellen locken an, machen Angriffe immer vielfältiger, komplexer und größer. Dass das so ist,

Hacking itself dates back to 1982: The “414s” were a group of hackers who had broken into several computer systems in America. The “business model” of hacking really began to gain traction, however, from mid-2000 and has been growing exponentially ever since. Anonymous, the Shadow Brokers, Lazarus Group, Fin7, APT28, Snake or attacks such as WannaCry, Carbanak, Moonlight Maze – these names have achieved international infamy. Within just a few days, companies today can face millions of dollars in damages – in the case of WannaCry, an affected company reported damages of USD 300 million, while, in the case of Carbanak, damages totalling USD 1 billion were purported to have been incurred by the affected banks. The “gold”, i.e. the financial benefits from these attacks, end up in unknown hands.

On a time line, we are therefore already at an advanced stage in the “golden age”. There is, however, an additional problem: we continue to offer new possibilities for hackers thanks to the high degree of digitisation in all areas of life. Is there an end in sight to the golden age? Quite the opposite – wealth and inexhaustible sources of money are enticing, leading to attacks that are increasingly diverse, complex and comprehensive. This fact has also been confirmed

Wie wird sich die Anzahl der Cyberattacken bis 2025 entwickeln? / Will we see a rise in cyber-attacks until 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

Source: RadarServices Expert Survey (2018)

Wie gut sind Unternehmen auf die Zukunft vorbereitet? / How well prepared are companies for the future?

Source: RadarServices Expert Survey (2018)

Radar Global Risk Score – die Berechnung / calculation

In die Berechnung des Radar Global Risk Scores wird der Incident Score, der Vulnerability Score und der Throughput Score einbezogen.

- Der **Throughput Score** misst, ob in der IT-Sicherheitsabteilung einer Organisation mehr oder weniger neue Incidents bekannt werden als in der gleichen Zeitperiode geschlossen wurden.
- Der **Incident Score** gibt den Durchschnitt der gewichteten Risk Scores aller offenen Incidents (z.B. erkannt durch Logmanagement oder Netzwerkstromanalyse) an. Ausgenommen sind hier Incidents die durch die Schwachstellenanalyse erkannt werden.
- Der **Vulnerability Score** gibt den gewichteten Durchschnitt aller offenen Incidents an, die bei der kontinuierlichen Schwachstellenanalyse erkannt wurden.

The Radar Global Risk Score is calculated using the Incident Score, the Vulnerability Score and the Throughput Score.

The **Throughput Score** measures whether a greater or smaller number of new incidents in the IT security department of an organisation are known than were closed during the same period of time.

The **Incident Score** gives the average of the weighted risk scores of all open incidents (for example, detected by log management or network flow analysis). This does not include incidents that are detected by the vulnerability analysis.

The **Vulnerability Score** indicates the weighted average of all open incidents detected during a continuous vulnerability analysis.

wurde unter anderem kürzlich durch eine Studie des Weltwirtschaftsforums bestätigt: Cybersicherheitsrisiken nehmen stetig zu, sowohl in der Wahrscheinlichkeit als auch in ihrem Störpotenzial, sagen die Experten. Auch das Allianz Risk Barometer gibt die Sichtweise wieder: Bei den 10 wichtigsten globalen Geschäftsrisiken 2018 landen Cybervorfälle wie Cyberkriminalität, Systemausfall und die Verletzung der Datenschutzrechte auf Platz zwei.

Fragt man IT-Sicherheitsexperten, so geschehen in einer aktuellen Zukunftsstudie von RadarServices, wird der Trend in Zahlen nachvollziehbar: Im Durchschnitt steigt die Anzahl der Cyberattacken um 300% jährlich. 72% der Experten sagen auch, dass Unternehmen heute noch nicht ausreichend auf die zukünftigen Herausforderungen vorbereitet sind.

Zur aktuellen Sicherheitslage in Europas Wirtschaft und Behördenlandschaft gibt der Radar Global Risk Score einen Überblick. Er wird täglich für jeden Kunden von RadarServices berechnet, beruht damit auf tatsächlichen Zahlen. Faktoren wie die Anzahl neu erkannter Schwachstellen, unautorisierter Zugriffe und anderer Sicherheitsprobleme fließen ein. Da die Kunden des Unternehmens aus nahezu allen Branchen und verschiedenen Ländern kommen, kann der anonymisierte Risk Score als umfassendes Lagebild verstanden werden. Warum so ein Risk Score wichtig ist? Er schafft Transparenz und Vergleichbarkeit. Nur wenn man genau weiß, welche Bedrohungen aktuell bestehen, kann man gezielt

recently, among other things, by a study of the World Economic Forum: cyber security risks are steadily growing, both in terms of likelihood and potential for disruption, according to experts. The Allianz Risk Barometer also reflects this view: of the top 10 global business risks in 2018, cyber-related incidents such as cyber crime, system failure, and privacy violations rank second.

If you ask IT security experts, as happened in a recent RadarServices Future Study, the trend is presented clearly in numbers: on average, the number of cyber attacks is expected to increase by 300 percent annually. 72 percent of experts also say that companies today are not yet adequately prepared for future challenges.

The Radar Global Risk Score provides an overview of the current security situation in Europe’s economy and government landscape. It is calculated every day for each customer of RadarServices, therefore ensuring it is based on real figures. Factors such as the number of newly discovered vulnerabilities, unauthorised accesses and other security issues are included here. As the company’s customers come from almost every sector and from different countries, the anonymised risk score can be understood as a comprehensive picture of the current situation. Why is such a risk score important? It creates transparency and comparability. Only if you know exactly what threats currently exist can you take targeted countermeasures. And the success of the measures

gegensteuern. Und der Erfolg der Maßnahmen und getätigten Investitionen wird dann sichtbar, wenn man sie mit Peers vergleichen kann.

Ganz konkret kann sich der Risikowert zwischen 0 (kein Risiko) und 10 (sehr hohes Risiko) bewegen. Dass die Risikolage in der Praxis durchgehend angespannt ist, erkennt man daran, dass weder ein Land, noch eine Branche einen durchschnittlichen Risk Score von kleiner als fünf hat. Die Trendlinien zeigen über alle Länder und Branchen hinweg eine eindeutige Richtung: nach oben. Seit eineinhalb Jahren weisen die Risk Scores von Industrieunternehmen, Banken und Versicherungen den größten Anstieg auf. Die Trendlinie für Behörden hat währenddessen zwar einen geringen Anstieg, liegt aber von Anfang an auf einem besonders hohen Niveau. Beispielhaft für die Länder Deutschland, Österreich und die Schweiz wird der Risk Score für Unternehmen mit über und unter 500 Mitarbeitern ausgewiesen. Dabei zeigt sich das Risiko für deutsche Großunternehmen als besonders hoch und steigend. Auffällig ist auch der hohe Risikoanstieg bei großen Schweizer Unternehmen. Die Risikoentwicklung österreichischer Unternehmen liegt auf einem konstant hohen Niveau.

Und die Zukunft? Wachsende Sorge bereiten den in der Zukunftsstudie von RadarServices befragten IT-Sicherheitsexperten allem voran Angriffe auf die IoT, speziell die IIoT (Industrial IoT), und gezielte Cyberattacken auf kritische Infrastrukturen, die nicht nur Geld kosten sondern potenziell auch Menschenleben.

Dazu passt auch die mehrfache Ermahnung seitens EU-Gesetzeshütern, dass die Sicherheit schon bei der Entwicklung und der Umsetzung von neuen Systemen, Anwendungen und Geräten mitgedacht werden muss. So steht es zum Beispiel in der EU-DSGVO als auch im aktuellen Threat Landscape Report der ENISA. Wie weit ist hier die Praxis in Zeiten von IoT fortgeschritten? Unterschiedlich.

Zum Schluss noch eine erschreckende Zahl in puncto Sicherheit der modernen Arbeitswelt: Den Schätzungen von Lloyd's of London zufolge könnte ein dreitägiger Ausfall mehrerer großer Cloudanbieter allein in den USA bis zu 19 Milliarden US Dollar betragen. Wer heute noch denkt, dass es ihn nicht treffen kann, könnte spätestens bei Angriffen auf einen Cloudanbieter feststellen, dass mittlerweile alles mit allem vernetzt ist und auch er die Folgen hautnah zu spüren bekommt.

and investments made becomes visible when compared to peers.

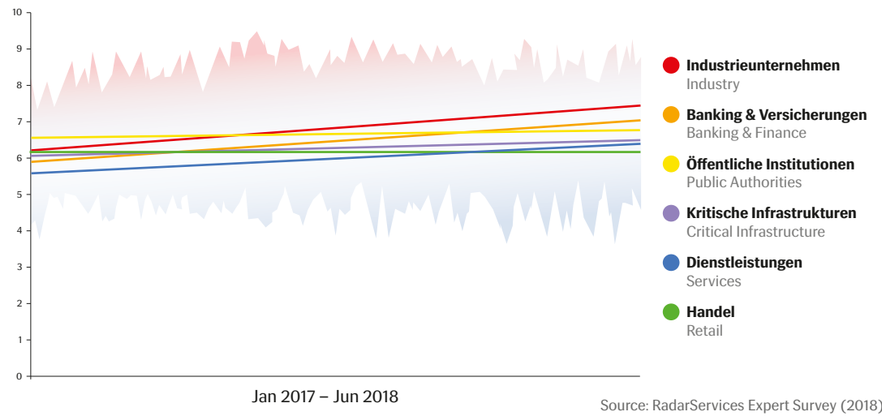
Specifically, the risk value can range between 0 (no risk) and 10 (very high risk). The fact that the risk situation is consistently fraught in practice can be recognised by the fact that neither a country nor an industry has an average risk score of less than five. The trend lines show a clear direction across all countries and sectors: upwards. The risk scores of industrial companies, banks and insurance companies have been experiencing the biggest increase for one and a half years. The trend line for public authorities has meanwhile increased only slightly, yet it was at a very high level from the very beginning. As an example for the countries of Germany, Austria and Switzerland, the risk score for companies with more and less than 500 employees is shown. The risk for large German companies is particularly high and rising. Another striking feature is the high risk increase among large Swiss companies. The risk development of Austrian companies is at a consistently high level.

And the future? Growing concern is expressed in particular by the IT security experts interviewed in the RadarServices Future Study in respect of attacks on the IoT, especially the IIoT (Industrial IoT), and targeted cyber attacks on critical infrastructure that not only cost money but potentially also human lives.

This is also in line with the repeated warnings made by EU law enforcement officials that security must be taken into account when developing and implementing new systems, applications and devices. This is the case, for example, in the EU GDPR and in the current Threat Landscape Report of ENISA. How far has practice progressed in the era of IoT? It varies.

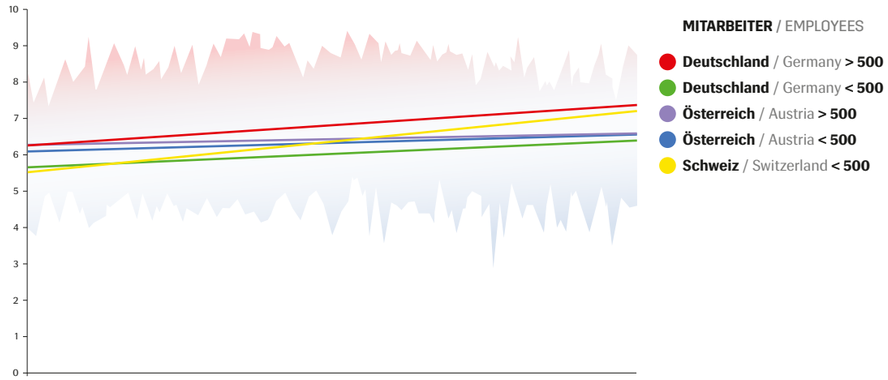
Finally, a frightening number regarding security of the modern working world: according to estimates by Lloyd's of London, a three-day outage of several large cloud providers in the US alone could cost as much as USD 19 billion. If companies still think today that they are immune to this, they will be jolted, in the course of attacks on a cloud provider, into realising that everything is now networked with everything, and they will also experience the consequences first-hand.

Radar Global Risk Score Trend nach Branche (alle Länder)
Radar Global Risk Score trend by industry (all countries)



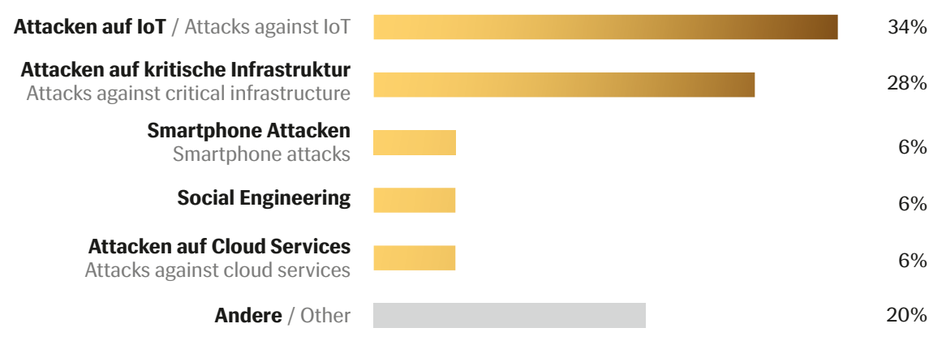
Source: RadarServices Expert Survey (2018)

Radar Global Risk Score Trend nach Land und Firmengröße
Radar Global Risk Score trends by country and company size



Source: RadarServices Expert Survey (2018)

Expertenbefragung zu den IT Security Trends: IoT und kritische Infrastrukturen im Mittelpunkt der Cyberattacken
Expert survey regarding future IT security trends: IoT and critical infrastructure in the focus of cyber attacks



Source: RadarServices Expert Survey (2018)