CYBER SECURITY 2017

- → Review
- → Learnings
- → Outlook 2018

News from the
CYBERSECURITY
WORLD

powered by
RADAR
SERVICES

CONTENTS

CYBERCRIME REPORT 2017

A review of the incidents that occurred in 2017 reflects the wide range of online crimes and IT security flaws.

Six trillion dollars a year – that is the **amount of loss** caused by cybercrime expected in the “Official 2017 Annual Cybercrime Report” published in mid-October 2017 by the US analyst “Cybersecurity Ventures” for the year 2021. This would be **almost ten percent of today’s global economic output**. In 2015, it had still predicted losses amounting to “just” three trillion dollars. The amount of loss caused by countless cyberattacks all over the world in 2017 is somewhere between these figures – no one knows the precise amount.

This development is accompanied by an increase in the number of Internet users: from 3.9 trillion today to six trillion expected for 2022. This will be the time when cybercrime will finally not only be synonymous with the biggest transfer of assets in history, but probably also has become one of the worst threats to mankind itself. For most individuals, companies or institutions are largely unprepared for this kind of crime, which, according to “breachlevelindex.com”, is today responsible for the **theft of at least 3,500 data records every minute**. All this despite the fact that the global expenses for cybersecurity have increased this year to some 86.4 billion dollars, according to analyst Gartner.
Still not enough, as it seems, for all these investments in security were not able to prevent the incidents of cybercrime described below. And these are just the tip of the iceberg.

2017 What attackers were looking for

Personal data and confidential documents

- Bank account details
- Confidential emails
- Credit card details
- Social security numbers and other insurance data
- PayPal accounts
- Social media logins
- Personal data
- Data at transportation companies
- Email account data
- Identity theft
- Whats App messages
- Photos and data of hospital patients
- Chat content, e.g. from dating platforms

Ransom money

- Large enterprises
- Authorities and public institutions
- Individuals
- Small and medium-sized companies

Manipulation

- Router
- Wireless networks
- Apple PCs
- TVs
- Toys

Strategically important data

- Espionage at public institutions and companies
- Confidential diplomatic as well as business emails
- Data on corporate strategy

Chaos

- Fake News
- Online propaganda
- Online bomb threat
- Disclosure of confidential emails

FIRST QUARTER 2017

JANUARY 2017

Jan 10, Rome – The Italian police arrested Francesca Maria and Giulio Occionero, who supposedly built up an internationally active **cyber espionage network**. Some of the reported targets: the president of the European Central Bank, former Italian prime ministers and a member of the Pope election committee.

Jan 23, London – The British Lloyds Bank published that it suffered a 48-hour online attack this month as cybercriminals attempted to block access to **20m UK accounts**. Halifax and Bank of Scotland were also bombarded with millions of fake requests, designed to grind the group's systems to a halt.

Jan 31, Prague – The Czech Republic has suffered a damaging security breach after hackers infiltrated the emails of **dozens of its most senior diplomats** in a massive cyber-attack.

FEBRUARY 2017

Feb 3, Oslo – Norway's foreign ministry, army and other institutions have been targeted in a **cyber-attack by "APT 29"**, a group suspected of having links to Russian authorities, according to Norwegian intelligence, which was one of the targets.

Feb 10, Rome – The Guardian newspaper reports that **Italy's foreign ministry** was attacked in 2016 by malware, which compromised email communications and went undetected for months, according to a source close to the department.

Feb 24, San Francisco – **CloudFlare**, a content delivery network and web security provider that helps optimize safety and performance of **over 5.5 Million websites** on the Internet, is warning its customers of the critical bug that could have exposed a range of sensitive information, including passwords, and cookies and tokens used to authenticate users.

MARCH 2017

Mar 7, wikileaks.org – WikiLeaks begins its new series of leaks on the **U.S. Central Intelligence Agency. Code-named "Vault 7"** by WikiLeaks, it is the largest ever publication of confidential documents on the agency.

Mar 29, Moscow – According to Sergei Pavlovich, one of the Russian-speaking world's most notorious hackers, "**it is easier to hack an electoral system than eBay or Citibank**". By the early 2000s he was one of the leading figures in the Russian and Eastern European cyber-underworld. In an interview with the Moscow Times he gave a rare insight into a community that has been accused of carrying out aggressive cyber-activity.

SECOND QUARTER 2017

APRIL 2017

Apr 12, London – A website which allowed Britons to **register to vote** in last year's **European Union referendum** might have been targeted by foreign hackers causing it to crash before the deadline, a committee of British lawmakers said.

Apr 20, Buckinghamshire, UK – Global hotel chain InterContinental Hotels Group Plc (IHG.L) said 1,200 of its franchised hotels in the United States, including Holiday Inn and Crowne Plaza, were victims of a three-month cyber attack that sought to steal customer payment card data.

Apr 24, Tel Aviv – A teenager was indicted for a series of more than 2,000 **bomb threats** and related actions against institutions, airports and police stations in various countries.

Apr 25, London – Teenager Adam Mudd admitted creating malware in 2013 which was used to carry out **1.7 million cyber attacks**. Among the victims were gaming websites including Minecraft and Xbox Live.

MAY 2017

May 5, Paris – A collection of links to torrent files appeared on the anonymous publishing site **PasteBin**. The 9GB trove purports to be an archive of leaked emails from the party of **Emmanuel Macron**, the left-leaning candidate currently favoured to win France's election.

May 12, worldwide – The **WannaCry** ransomware attack was a May 2017 worldwide cyberattack by the WannaCry, a ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin.

May 17, Den Hague – At a cyber safety conference, **11-year-old** prodigy Reuben Paul used a "Raspberry Pi" to hack into audience members' bluetooth devices and download phone numbers. Paul then reportedly used one of the numbers to hack into the **teddy bear**, which connects to the Internet via Bluetooth or WiFi, and used the toy to record a message from the audience.

May 27, Valetta – Malta assumed the **presidency of Europe's Council of Ministers** in January, an important position under which it chairs high-level meetings in Brussels and sets Europe's political agenda. Since then, the Maltese government's IT systems have seen a rise in attacks, according to a source working within its information technology agency.

May 30, Prague – Yevgeniy Nikulin, who was arrested in the Czech capital in October 2016 and is accused by the FBI of massive hacks of US companies, has moved a step closer to being sent to the US as a Czech judge gave tentative approval for an extradition to go ahead.

May 31, Lithuania – Hackers have published more than **25,000 private photos**, including nude pictures, and other personal data from patients of a Lithuanian **cosmetic surgery clinic**.

JUNE 2017

Jun 24, San Jose, California – Anthem, the largest **U.S. health insurance** company, has agreed to settle litigation over hacking in 2015 that compromised about 79 million people's personal information for **$115 million**, which lawyers said would be the **largest settlement** ever for a data breach.

Jun 21, Washington – Hackers targeted **21 U.S. state election systems in the 2016 presidential race** and a small number were breached but there was no evidence any votes were manipulated, a Homeland Security Department official.

Jun 27, worldwide – **Petya/NotPetya**: The world suffered another ransomware nightmare, with pharmaceutical companies, Chernobyl radiation detection systems, the Kiev metro, an airport and banks all affected among many others. Falling victim to the cyber attack is set to cost Maersk, the world's largest container ship and supply vessel operator, up to **$300m in lost revenues.**

THIRD QUARTER 2017

JULY 2017

Jul 3, Canberra – The Australian Federal Police has launched an investigation into the leak of sensitive **Medicare details**, which were allegedly sold by criminals on the "dark web".

Jul 11, Moscow – US Homeland Security is banning the Russian security software maker **Kaspersky Lab**. The DHS Acting Secretary directed all Executive Branch agencies and departments to identify any Kaspersky products being used, make a plan to eliminate their use and begin that discontinuation. Similar warnings were also given in the UK later on.

Jul 17, London – A major global cyber-attack has the potential to trigger **$53 billion** of economic losses, roughly the equivalent to a catastrophic natural disaster like 2012's Superstorm Sandy, according to a scenario described in a research by Lloyd's.

Jul 20, Washington – The US Justice Department announced the seizure of the largest criminal marketplace on the Internet, **AlphaBay**, which operated for over two years on the dark web and was used to sell deadly **illegal drugs**, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, **firearms**, and toxic chemicals throughout the world.

AUGUST 2017

Aug 15, Edinburgh – Scotland's devolved parliament is suffering an ongoing **brute-force cyber attack**, similar to the Parliament in London a couple of weeks ago.

SEPTEMBER 2017

Sep 7, Atlanta – It has been marked as the worst data breach in US history: Attackers stole **half the US population's Social Security numbers** from **Equifax** this spring, the company notified in September. The fallout has been swift, with government agencies looking into the incident, class action lawsuits being filed, and consumers demanding free credit freezes.

Sep 18, worldwide – **CCleaner**, one of PCWorld's recommendations for the best free software for new PCs, might not have been keeping your PC so clean after all. In an in-depth probe a a malicious bit of code injected by hackers was discovered. It could have affected more than 2 million users who downloaded the most recent update. This is **a new dimension** of cyber attacks, IT security experts say.

Sep 25, New York – The Guardian revealed that accountancy firm **Deloitte** has been targeted by a sophisticated hack that compromised the confidential emails and plans of some of its **blue-chip clients**.

FOURTH QUARTER 2017

OCTOBER 2017

Oct 3, Sunnyvale, California – **Yahoo** announced that all **3 billion of its accounts** were hacked in a 2013 data theft, tripling its earlier estimate of the size of the **largest breach in history**, in a disclosure that attorneys said sharply increased the legal exposure of its new owner, Verizon Communications Inc.

Oct 16, Leuven – The security protocol used to protect the vast majority of wifi connections has been broken, potentially exposing wireless internet traffic to malicious eavesdroppers and attacks, according to the researcher who discovered the weakness. Mathy Vanhoef, a security expert at Belgian university KU Leuven, discovered the **weakness in the wireless security protocol WPA2**.

Oct 31, USA and UK – Hackers are stealing large sums of money from art galleries and their clients using a straightforward email deception.

NOVEMBER 2017

Nov 20, Hongkong – Hackers have stolen another $30.9m in cryptocurrency. In a "critical announcement", cryptocurrency startup **Tether** said the funds had been removed from the Tether Treasury wallet on 19 November and sent to an unauthorized bitcoin address.

Nov 21, San Francisco – **Uber** concealed a massive global breach of the personal information of **57 million customers and drivers** in October 2016, failing to notify the individuals and regulators, the company acknowledged. Uber also confirmed it had paid the hackers responsible $100,000 to delete the data and keep the breach quiet. Governments all over Europe announced to look into this case deeper.

Nov 25, Brussels –The EU is stepping up its campaign to counter disinformation and fake news from Russia by spending more than €1m a year on its **specialist anti-propaganda unit** East Stratcom.

Nov 27, Cupertino, California – Anyone using MacOS **High Sierra** was on high alert. A Twitter user revealed a **massive security vulnerability** which allows anyone to log into a system as an administrator without valid login credentials.

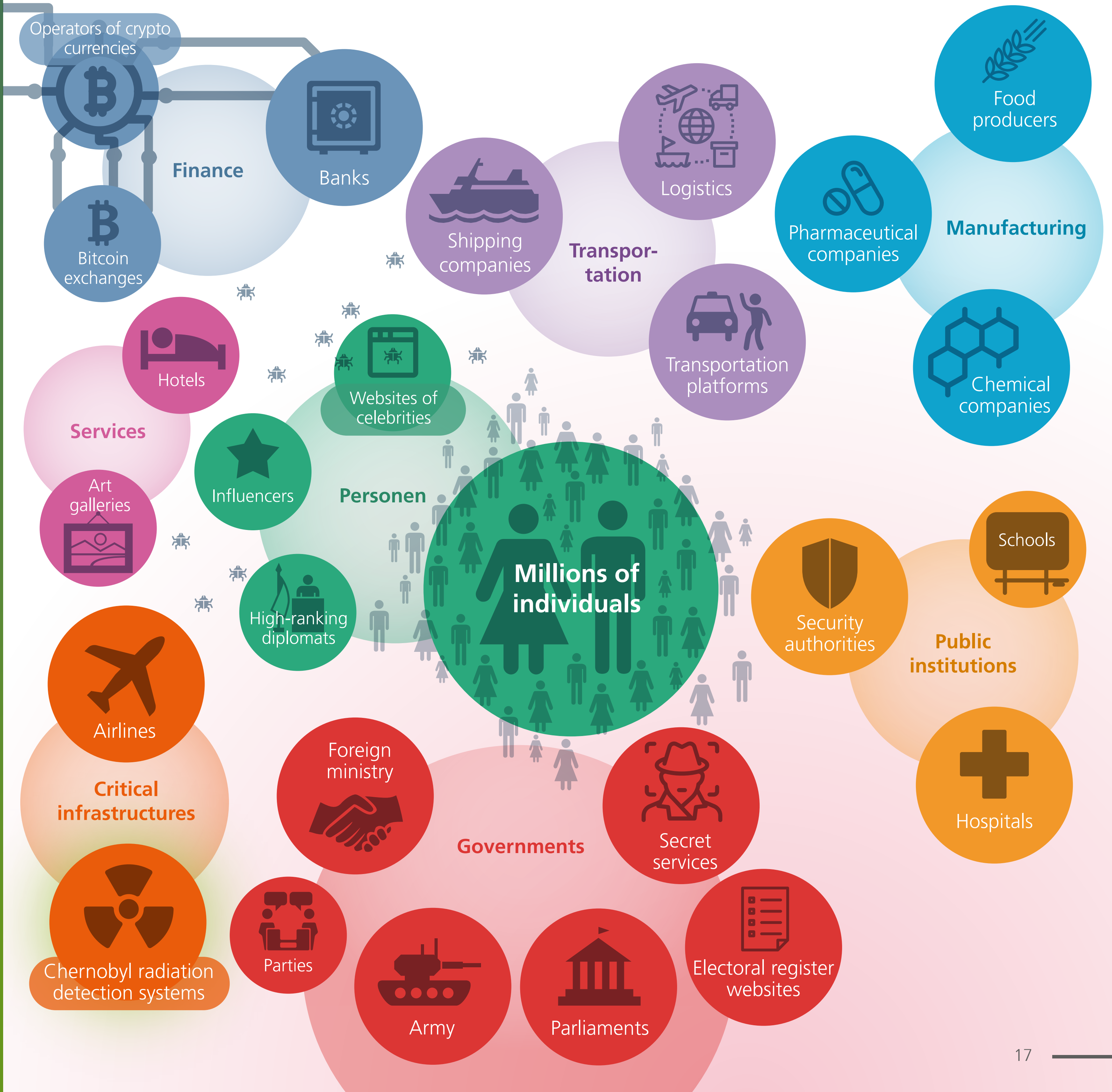
DECEMBER 2017

Dec 4, San José, California – **PayPal** disclosed that the personal information of around **1.6 million users** may have been compromised at its TIO Networks unit, a company it acquired earlier in 2017.

Dec 7, Slovenia – A cryptocurrency mining marketplace, **NiceHash**, said it lost about **$64 million** worth of bitcoin in a hack of its payment system.

Dec 8, worldwide – A **botnet** of 100,000 home broadband routers is lying dormant and could be activated at any time. Security researchers found a new strain of the virulent **IoT malware** Mirai is being used to amass devices.

2017
Cybercrime victims



Finance

Operators of crypto currencies

Banks

Bitcoin exchanges

Transportation

Shipping companies

Logistics

Transportation platforms

Manufacturing

Food producers

Pharmaceutical companies

Chemical companies

Services

Hotels

Art galleries

Personen

Websites of celebrities

Influencers

High-ranking diplomats

Millions of individuals

Public institutions

Security authorities

Schools

Hospitals

Critical infrastructures

Airlines

Chernobyl radiation detection systems

Governments

Foreign ministry

Secret services

Parties

Army

Parliaments

Electoral register websites

Five lessons learnt from 2017

Harald Reisinger, Managing Director of RadarServices, draws conclusions from the annual cybercrime review for 2017:

1. Attacks: at any time, any place

The situation in terms of security was tense all through the year 2017. The victims of cyberattacks suffered high financial and image losses that were even existence-threatening in some cases. European and US companies were massively attacked. Companies big and small were equally affected, no branch of industry escaped unscathed. Even public institutions and authorities found themselves frequently under fire.

2. Continuous and comprehensive IT security monitoring is still underused

Experts call it "Detection and Response": today, the timely detection of all kinds of IT risks is the only way to protect an organisation from major losses caused by cyberattacks. This includes everything from fast remediation of known vulnerabilities to close monitoring of conspicuous incidents in systems and data traffic. The theft of millions of data records does not happen overnight. Therefore, the numerous incidents of massive data loss in 2017 are due to either non-existent or non-functioning IT security monitoring.

3. Keeping losses secret is not an option

It is understandable that victims of cyberattacks are often unwilling to make incidents public. However, if the losses exceed a certain amount, disclosure obligations must inevitably be met and/or the customers concerned – or even the public – must be informed. Especially the Uber incident showed that inappropriate handling of disclosure obligations may result in even bigger reputational damage, attract international attention and lead to lack of trust. With effect from 2018, this situation will be aggravated even further: within the framework of the EU General Data Protection Regulation (EU-GDPR), fines amounting to millions of euros may then be imposed.

4. Public institutions for cyberdefense exist, but are much too small in size

The public mills grind too slowly. In many countries, public authorities have suffered from attacks. Governments are basically willing to expand their commitment to more cybersecurity, but above all in Europe they are too hesitant to make funds available, to establish a European cybersecurity industry and to collaborate with the domestic private sector. The situation is currently escalating, since large non-European security companies were publicly accused of government espionage already in 2017.

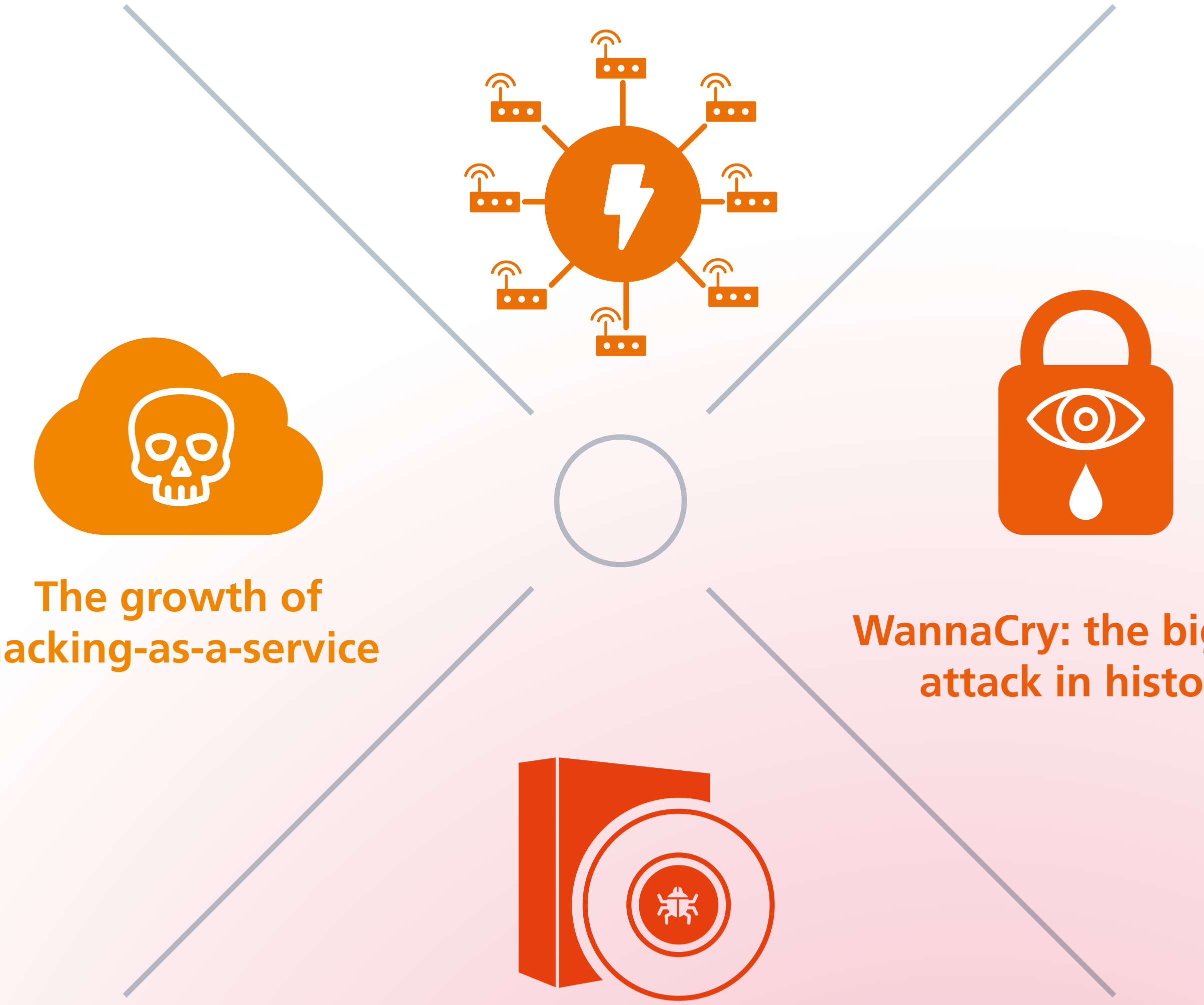
5. The great unknown: who are the attackers?

In 98% of the cases, it cannot be determined who is behind the attacks. In 2017, it was revealed that even eleven-year-olds may be able to find and utilise security gaps. The contrary extreme are professionally organised groups of hackers. They are usually known in public by a pseudonym, but no-one knows who is behind it. Hence, the biggest offences remain unpunished to a large extent.

2017

A new dimension

The attacks which concerned IT security experts most



Huge botnets through connected routers

The growth of hacking-as-a-service

WannaCry: the biggest attack in history

Spreading malware via well-known and supposedly harmless software

Cybersecurity 2018 Five top trends in IT security

What the RadarServices cybersecurity experts predict for the new year: Christian Polster, Chief Strategy Officer and CFO of RadarServices, outlines the future.

1. IoT as an Eldorado for cyber attackers

The further development of the Internet of Things is unstoppable. In a few years from now, every screw and bolt will have its own IP address. While this opens up entirely new possibilities, it also presents tremendous challenges to the IT security of companies and private individuals. New security concepts for the Internet of Things (IoT) must urgently be drawn up and tested in practice.

2. A new dimension of targeted attacks

Many large companies are still much too vulnerable. Their IT is distributed all over the world, yet what is missing is an overview of the whole system. At the same time, they are under pressure from the EU General Data Protection Regulation as well as from additional compliance regulations old and new. What IT security officers need most to prevent major losses is mainly transparency and the right information at the right time.

3. Ransomware against small and medium-sized companies

Because large companies are by now able to defend themselves better against ransomware, such attacks will increasingly be directed towards small and medium-sized companies and networked control devices in the future. These potential victims must become aware of the adjusted business models of these attackers and find experts that are able to protect their IT effectively and efficiently.

4. National insecurity

National security needs rethinking. Protecting critical infrastructure, but also ensuring the permanent functioning of a country's public infrastructure, poses enormous challenges. Public authorities are fully aware of this, but cyber attackers are as well.

5. The use of artificial intelligence is a must

By using machine learning many vulnerabilities, suspicious system behaviour or zero-day attacks can be detected and warded off more quickly. But also the "opponents" are going to exploit the opportunities opened up by artificial intelligence by learning everything there is to know about new defence strategies and protective measures. In brief: if companies fail to address the need for AI in IT security, their security measures will become obsolete in no time.

RADAR SERVICES

The European Experts
in IT Security Monitoring
and IT Risk Detection

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. The cutting-edge, inhouse-developed technology platform is the basis used for building up a client's Security Operations Center (SOC) or it is used in combination with our expert analysts, documented processes and best practices as SOC as a Service. The result: Highly effective and efficient improvement of IT security and IT risk management, continuous IT security monitoring and an overview of security-related information throughout the entire IT landscape of an organization.

The Cybersecurity World is a worldwide unique place. In this building IT security is made to come alive. It is the home of Europe's largest Security Operations Center (SOC). Here today's and tomorrow's challenges for IT security responsibles in companies as well as the current state of research and innovation in this sector are illustrated on 2,000 sqm.

RadarServices
Zieglergasse 6
1070 Vienna
Austria

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

RadarServices Germany
Taunustor 1
60310 Frankfurt a. M.

Phone:	+49 (69) 2443424 655
Email:	sales_germany@radarservices.com

ISO 27001
CERTIFIED

PUBLIC