CYBER SECURITY 2017

- Rückblick
- Learnings
- Ausblick 2018

News aus der
CYBERSECURITY WORLD

powered by
RADAR SERVICES

INHALT

4 Cybercrime Report 2017

6 2017 – Darauf hatten es die Angreifer abgesehen

8 Erstes Quartal

10 Zweites Quartal

12 Drittes Quartal

14 Viertes Quartal

16 2017 – Die Cybercrime-Opfer

18 Fünf Learnings aus 2017

20 2017 – Eine neue Dimension

22 Cybersecurity 2018 – Fünf Top Trends für die IT-Sicherheit

CYBERCRIME REPORT 2017

Ein Rückblick auf das was in 2017 geschah, offenbart die enorme Bandbreite der Online-Verbrechen und IT-Sicherheitslücken. Fazit: ein Monat des Schauderns nach dem anderen.

Sechs Billionen Dollar jährlich – das ist die **Schadensumme** durch Cyber-Crime, mit der der „Official 2017 Annual Cybercrime Report" des US-Analysten „Cybersecurity Ventures" von Mitte Oktober 2017 für das Jahr 2021 rechnet. Das wären **fast zehn Prozent der heutigen globalen Wirtschaftsleistung**. 2015 belief sich seine Prognose noch auf „bloß" drei Billionen Dollar. Irgendwo dazwischen liegt der Betrag, den die unzähligen Cyber-Attacken rund um den Globus im Jahr 2017 an Schaden verursacht haben – die genaue Höhe weiß niemand.

Diese Entwicklung geht Hand in Hand mit dem Anstieg der heute etwa 3,9 Milliarden Internet-Nutzer auf prognostizierte sechs Milliarden im Jahr 2022. Spätestens dann wird Cyber-Crime nicht nur für den größten Vermögenstransfer in der Geschichte stehen, sondern wahrscheinlich auch eine der größten Bedrohungen für die Menschheit selbst darstellen. Denn die meisten Menschen, Unternehmen und Institutionen sind auf diese Art von Verbrechen, durch das heute laut „breachlevelindex.com" **jede Minute gut 3.500 Datensätze gestohlen** werden, weitgehend unvorbereitet. Und das, obwohl die Ausgaben für Cyber-Security, so der Analyst Gartner, auf heuer rund 86,4 Milliarden Dollar weltweit gestiegen sind.
Offenbar nicht genug, denn all diese Sicherheits-Investments haben die nun geschilderten Cyber-Crime-Fälle nicht verhindern können. Und diese sind nur die Spitze des Eisberges.

2017
Darauf hatten es die Angreifer abgesehen

Personenbezogene Daten und vertrauliche Dokumente

- Kontodaten
- Vertraulicher Emailverkehr
- Kreditkartendetails
- Sozialversicherungs- und andere Versichertendaten
- PayPal-Accounts
- Passwörter von Social Media Plattformen
- Personaldaten
- Daten bei Fahrdiensten
- Emailaccount-Daten
- Identity-Betrug
- Whats App Nachrichten
- Fotos und Daten von Privatpersonen bei Klinikaufenthalten
- Chatinhalte, .u.a. aus Dating-Plattformen

Cyber-Erpressungen

- Großunternehmen
- Behörden und Institutionen
- Privatpersonen
- Kleine und mittelständische Firmen

Manipulation

- Router
- WLan-Netze
- Apple PCs
- TV-Geräte
- technisches Spielzeug

Strategisch wertvolle Daten

- Spionage bei staatlichen Institutionen und Unternehmen
- Vertraulicher diplomatischer und geschäftlicher Emailverkehr
- Unternehmenspläne

Chaos

- Fake News
- Online Propaganda
- Online Bombendrohungen
- Veröffentlichungen von vertraulichem Emailverkehr

ERSTES QUARTAL 2017

JANUAR 2017

10.1., Rom – Die italienische Polizei verhaftet nach acht Monaten Ermittlungen die Geschwister Francesca Maria und Giulio Occionero, die von London aus einen international operierenden **Cyber-Spionagering** aufgezogen haben sollen. Unter dessen Zielen: der Präsident der Europäischen Zentralbank, frühere italienische Regierungschefs, sowie ein Mitglied der Papst-Wahlkonklave.

23.1., London – Die britische Lloyds-Bank veröffentlichte, dass **20 Millionen Kundenkonten** in Großbritannien während einer breit angelegten Denial-of-Service-Attacke, der zwischen 11. und 13. Jänner auch Halifax und die Bank of Scotland zum Opfer fielen, gleichzeitig einem Hacker-Angriff ausgesetzt waren. Die Attacke konnte vom Lloyds-IT-Security-Team durch „**Geo-Blocking**" der von den Hackern benutzten Server abgewehrt werden.

31.1., Prag – Der Außenminister der Tschechischen Republik gibt Details über „den größten Sicherheitsskandal der letzten Jahre" in seinem Land bekannt. E-Mail-Accounts von „Dutzenden hochrangigen Diplomaten" seien im Jänner 2017 von Hackern ausgebeutet worden, angeblich auch **klassifizierte Korrespondenzen** mit der Nato und der EU.

FEBRUAR 2017

3.2., Oslo – Die **Hacker-Gruppe APT 29** soll laut dem norwegischen Inlandsgeheimdienstes (PST) die Armee, den Geheimdienst, die Arbeiterpartei, die Behörde für Strahlungssicherheit, das Ministerium selbst und sogar einige Schulen ins Visier genommen haben.

10.2., Rom – Kurz darauf geht das **italienische Außenministerium** ebenfalls mit Details einer Hacking-Attacke an die Öffentlichkeit, der es im Frühjahr 2016 vier Monate lang ausgesetzt war.

24.2., San Francisco – Bei **Cloudflare**, einem großen US-Internet-Dienstleister, der Content Delivery Netzwerke, IT-Security- und DNS-Services anbietet, wird eine massive Sicherheitslücke bekannt. Über Monate hinweg konnten auch verschlüsselt übertragene Daten seiner **sechs Millionen Kunden** entwendet werden. Darunter Positionsdaten und Passwörter von **Uber-Passagieren** und private Chats von Dating-Seiten.

MÄRZ 2017

7.3., wikileaks.org – Die Enthüllungsplattform beginnt mit der Veröffentlichung von 8.761 **Vault-7**-Dokumenten und Files, die bisher umfangreichste Darstellung der **CIA-Cyber-Spionageprogramme**. Vault 7 beschreibt Malware oder Viren wie etwa „Weeping Angel", „Hammer Drill" oder „Brutal Kangaroo", die Handys, Tablets, WhatsApp-Nachrichten oder TV-Geräte ausspionieren und sich in fremden System wie Skype, Wifi-Netzen oder selbst PDFs einnisten.

29.3., Moskau – Sergei Pavlovich, 33, einst eine der bekanntesten Figuren der russischen Cyber-Unterwelt und Autor des Hacker-Buchs „**How to Steal a Million**", gibt nach zehn Jahren Haft der „Moscow Times" ein Interview. Kernaussage: „Es ist leichter, eine Wahl zu hacken als Ebay oder Citibank. Denn Banken, Zahlungssysteme oder große Handelsplattformen können sich qualifizierte IT-Security-Experten leisten. Das heißt aber nicht, dass es russische Hacker nicht trotzdem geschafft haben."

ZWEITES QUARTAL 2017

APRIL 2017

12.4., London – Britische Parlamentarier verdächtigten Hacker, eine **Wahlregister**-Website im Vorfeld des **Brexit-Referendums** manipuliert zu haben.
20.4., Buckinghamshire, Großbritannien - Die InterContinental Hotel Group, eine der größten Hotelgruppen weltweit, gibt Cyberangriffe auf 1.200 involvierte Hotels in den USA bekannt. Ziel waren die Kreditkartendaten der Hotelgäste.
24.4., Tel Aviv – Ein 18-jähriger Schüler wird wegen fingierter **Online-Bombendrohungen**, Cyber-Erpressung und Identity-Betrug gegen rund 2.000 Institutionen weltweit angeklagt.
25.4., London – Der Teenager Adam Mudd wird zu zwei Jahren Haft wegen 1,7 Millionen Cyber-Attacken auf die Systeme von Minecraft, Xbox Live, Microsoft und auf das Spiele-Chat-Tool TeamSpeak verurteilt. Er habe ein weltweites **Hacking-as-a-Service-Geschäft** betrieben und so an die 400.000 Pfund (in Dollar und Bitcoin) verdient.

MAI 2017

5.5., Paris – Kurz vor der französischen Präsidentschaftswahl wird auf der anonymen Website **PasteBin** ein 9GB-Datensatz mit gehackten E-Mails der „En-Marche!"-Bewegung von **Emmanuel Macron** gepostet.
12.5., weltweit – Die Lösegeld-Malware „**WannaCry**" startet den wahrscheinlich bisher **größten Cyber-Angriff der Geschichte**, in dem **über 230.000 Computer mit Windows-Betriebssystem in 150 Ländern gehackt** wurden. Dem Angriff fielen auch etliche internationale Großunternehmen aus allen Branchen zum Opfer.
17.5., Den Haag – Auf einer IT-Sicherheitskonferenz verblüfft der **elf-jährige** Reuben Paul das Experten-Publikum mit einem **Live-Hack** des Bluetooth-Systems eines **Teddybären**. Sein Werkzeug: ein einfacher „Raspberry Pi"-Computer nicht größer als eine Kreditkarte. „Ein Teddybär ist auch nur ein Teil des Internet of Things", so der Knirps.
27.5., Valetta – Die Regierung in Malta verdächtigt das Hacker-Kollektiv „**Fancy Bears**", hinter den massiven Cyber-Attacken gegen sie kurz vor und während ihres **EU-Ratsvorsitzes** in der ersten Hälfte 2017 zu stecken.
30.5., Prag – Ein tschechisches Gericht bewilligt die Auslieferung des russischen Hackers **Yevgeniy Nikulin**, der 2012 in großem Stil Kunden-Passwörter von **LinkedIn, Dropbox** and Formspring gestohlen haben soll.
31.5., Litauen – Eine Hacker-Truppe namens „**Tsar Team**" veröffentlicht 25.000 kompromittierende Fotos und Personaldaten von Patienten einer **Klinik für Schönheitschirurgie** aus mehr als 60 Ländern.

JUNI 2017

24.6., San Jose, Kalifornien – Anthem, die größte **US-Krankenversicherung**, stimmt einer **Vergleichszahlung von 115 Millionen Dollar** zu, die bisher größte Schadensersatz-Zahlung im Zusammenhang mit einem Cyber-Datendiebstahl.
21.6., Washington - Eine Vertreterin des Heimatschutzministeriums sagte vor dem US-Kongress aus, dass **Hacker im Rahmen der US-Präsidentschaftswahl 2016 in 21 US-Bundesstaaten Angriffe** auf das Wahlsystem unternommen hätten.
27.6., weltweit – Ausgehend von der Ukraine machen die Erpressungstrojaner „**Petya**" und „**NotPetya**" zahllose Rechner vor allem in Europa und den USA funktionsunfähig. Betroffen sind etwa die Ruine des Kernkraftwerks Tschernobyl, global tätige Chemie- und Pharmakonzerne, eine der weltweit größten Reedereien und Logistik-Unternehmen. Laut Veröffentlichungen der dänischen Reederei Maersk wird der Schaden durch die Petya-Attacke mit **300 Millionen Dollar** beziffert, FedEx und TNT Express geben jeweils gleich hohe Verlustschätzungen an.

DRITTES QUARTAL 2017

JULI 2017

3.7., Canberra – Der „Guardian Australia" enthüllt, dass Personendaten von australischen **Medicare-Versicherten** im Darknet für **30 Dollar je Datensatz** angeboten werden.

11.7., Moskau – Laut einem Bloomberg-Bericht habe das russische, weltweit tätige IT-Sicherheitsunternehmen **Kaspersky** weitaus enger mit dem russischen Geheimdienst zusammengearbeitet als bisher angenommen. Vor allem in den USA und Großbritannien wird Kasperky in den Folgemonaten mit weiteren **Spionage-Vorwürfen** konfrontiert.

17.7., London – Ein Lloyds-Report bezeichnet Cyber-Crime als eines der größten Risiken der nächsten zehn Jahre und schätzt den möglichen Schaden für die Weltwirtschaft auf bis zu **120 Milliarden Dollar**, in etwa so viel, wie die Katastrophen-Hurrikans Katharina und Sandy verursacht haben.

20.7., Washington – Das US-Justizministerium schließt die beiden Dark-Net-Seiten „**AlphaBay**" und „**Hansa**", zwei der größten illegalen Plattformen für **Drogen** und **Waffen** mit, so Europol, rund 40.000 Anbietern und etwa 200.000 gelisteten Mitgliedern.

AUGUST 2017

15.8., Edinburgh – Das schottische Parlament wird Opfer einer massiven **„Brute-Force"-Cyber-Attacke**, genauso wie wenige Wochen zuvor Abgeordnete des Parlaments in London.

SEPTEMBER 2017

7.9., Atlanta – Das große US-Kreditrating-Unternehmen **Equifax** gibt bekannt, dass Hacker durch einen Dateneinbruch Zugang zu umfangreichen **Sozialversicherungs- und Personaldaten** von potentiell **143 Millionen Amerikanern**, inklusive der Kreditkarten-Nummern von über 200.000 US-Konsumenten sowie auch Daten von 400.000 Briten, erlangt hätten.

18.9., weltweit - Das weltweit milliardenfach im Einsatz befindliche Programm „**CCleaner**" soll eigentlich die Leistung von PCs und Android-Smartphones verbessern. Nun wurde jedoch mitgelieferte Schadsoftware in dem Programm gefunden. Sobald sie aktiv war, habe die Software diverse Informationen über den befallenen Computer gesammelt, verschlüsselt und an einen externen Kommandoserver gesendet. Dieser Vorfall zeigte vielen Sicherheitsverantwortlichen **eine neue Dimension**, mit der Angreifer versuchen, an ihr Ziel zu kommen.

25.9., New York – Eine Cyber-Attacke auf **Deloitte** wird bekannt. Bei dem ausgeklügelten Hack sollen im Oktober und November 2016 vertrauliche E-Mails und interne Unternehmenspläne von etlichen **Blue-Chip-Klienten** entwendet worden sein.

VIERTES QUARTAL 2017

OKTOBER 2017

3.10., Sunnyvale, Kalifornien – Im August 2013 wurde der Internet-Dienst Yahoo Opfer einer der bis dahin umfangreichsten Cyber-Attacken. Anfang Oktober musste das inzwischen von Verizon übernommene Unternehmen zugeben, dass **drei Milliarden Yahoo-Konten** waren – der bisher **größte Daten-Cyber-Diebstahl** der Geschichte.

16.10., Leuven – Der belgische Sicherheitsexperte Mathy Vanhoef publiziert Schwachstellen des Wifi-Sicherheits-Protokolls WPA2, wodurch „**Attacken gegen alle modernen, gesicherten Wifi-Netzwerke möglich**" seien. Laut seinem Bericht sind Betriebsysteme wie Android, Linux, Apple-IOS, Windows, OpenBSD, MediaTec oder Linksys sowie eine Reihe von Geräten betroffen.

31.10., USA und Großbritannien – Hacker haben sich in die Email-Kommunikation zwischen renommierten Kunstgalerien und deren Kunden geschaltet. Sie leiten die Kundenzahlungen auf ihre Konten um.

NOVEMBER 2017

20.11., Hongkong – Während bisher vorwiegend Bitcoin-Börsen Ziel von Hackern waren, geben nun auch die Betreiber der Cryptowährung „**Tether**" in einem „Critical Announcement" bekannt, dass ihnen Tokens im Wert von 31 Millionen Dollar bei einer Cyber-Attacke gestohlen wurden.

21.11., San Francisco – Die Taxi-Plattform **Uber** räumt ein, dass Hacker bereits im Oktober 2016 Namen, E-Mailadressen und Telefonnummern von weltweit rund **50 Millionen Kunden** und etwa **sieben Millionen Vertrags-Fahrern** gestohlen hatten, aber dies über ein Jahr geheim hielt und den Erpressen ein Lösegeld von 100.000 Dollar zahlte. EU-Behörden ebenso wie nationale europäische Datenschutzinstitutionen äußern sich in der Öffentlichkeit empört und beschließen weitere Untersuchungen des Falls.

25.11., Brüssel – East Stratcom, die 2015 gegründete **EU-Taskforce** zum Kampf gegen Online-Progaganda und Fake-News, wird mit einem Jahresbudget von 1,1 Millionen Euro ausgestattet. EU-Parlamentarier kritisieren dieses Budget als viel zu gering.

27.11., Cupertino, Kalifornien – Eine **schwerwiegende Sicherheitslücke** im Apple-Betriebssystem OSX 10.13.1 „**High Sierra**" wird bekannt. Sie ermöglicht einem Angreifer, die vollständige Kontrolle über ein Gerät zu erlangen.

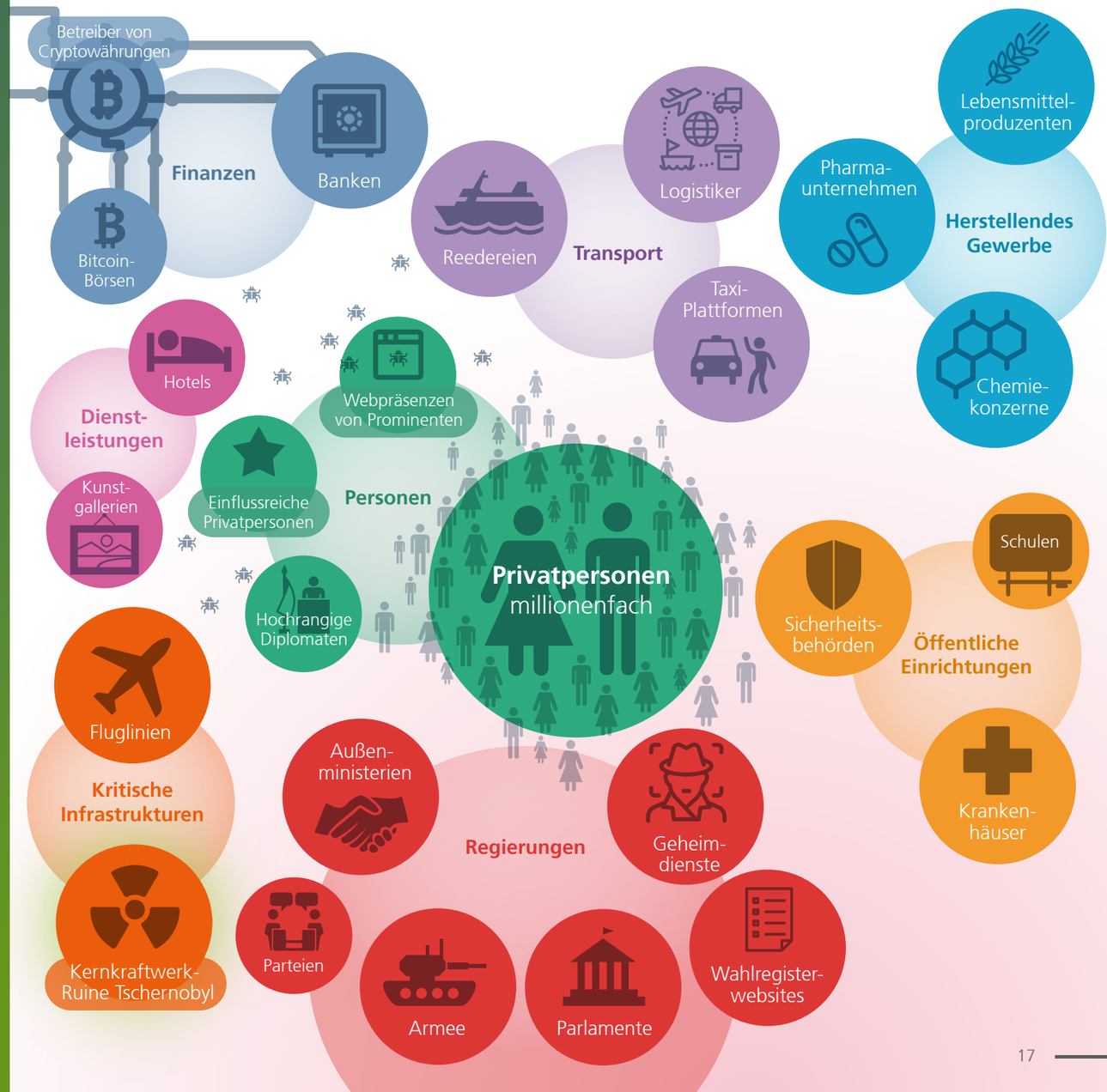
DEZEMBER 2017 (STAND 8.12.)

4.12., San Josef, Kalifornien – Der Online-Zahlungdienst **PayPal** bestätigt einen Cyber-Einbruch bei seiner erst im Juli 2017 gekauften Tochtergesellschaft „TIO Networks", die die digitale Abwicklung von Transaktionen erledigt. **1,6 Millionen PayPal-Kunden** sind betroffen.

7.12., Slowenien – Die Bitcoin-Plattform „**NiceHash**" wird gehackt, 4.736,42 Bitcoins im Wert von momentan gut **70 Millionen Dollar**, gehen verloren. Der Dienst ist momentan nicht verfügbar.

8.12., weltweit - Ein **IoT-Botnetz** greift derzeit **weltweit Modems von Huawei** über einen Wartungsport an. Ähnlich wie vor rund einem Jahr bei Angriffen auf das Netz der Deutsche Telekom könnten Angreifer versuchen, den Wartungsport des Geräts für den Aufbau eines Botnetzes auszunutzen.

2017
Die Cybercrime-Opfer



Fünf Learnings aus 2017

Harald Reisinger, Geschäftsführer von RadarServices, zieht Schlüsse aus dem Cyber Crime-Jahresrückblick 2017:

1. Angriffe: Zu jeder Zeit, an jedem Ort

Die Sicherheitslage war das ganze Jahr 2017 über angespannt. Opfer von Cyberattacken erlitten hohe Finanz- und Imageschäden bis hin zur Existenzbedrohung. Europäische und amerikanische Firmen wurden massiv attackiert. Große und kleine Unternehmen sind gleichermaßen betroffen, keine Branche war ausgenommen. Auch Behörden und öffentliche Institutionen standen sehr oft im Kreuzfeuer.

2. Kontinuierliches und umfassendes IT Security Monitoring wird noch zu wenig eingesetzt

„Detection and Response" im Fachjargon: das zeitnahe Erkennen von IT-Risiken aller Art ist heute die einzige Möglichkeit, eine Organisation dauerhaft vor großen Schäden durch Cyberangriffe zu schützen. Es umfasst das schnelle Schließen von bekannt gewordenen Schwachstellen bis hin zur genauen Beobachtung der Auffälligkeiten bei Systemen und Datenverkehr. Millionenfache Datenentwendung passiert nicht über Nacht. Daher sind die vielen Fälle des massenhaften Datenverlusts in 2017 auf entweder nicht-existentes oder nicht-funktionierendes IT Security Monitoring zurückzuführen.

3. Vertuschen ist keine Option

Opfer von Cyberattacken schrecken - verständlicherweise - vor einer Veröffentlichung eines Vorfalls zurück. Jedoch führt ab einer gewissen Schadensgröße kein Weg daran vorbei, Meldepflichten nachzukommen und/oder proaktiv die betroffenen Kunden oder gar die Öffentlichkeit zu informieren. Allem voran der Vorfall bei Uber zeigte, dass ein falscher Umgang mit Veröffentlichungspflichten zu noch größeren Reputationsschäden, internationalem Aufsehen und Vertrauensverlust führen kann. Ab 2018 verschärft sich diese Lage nochmals: dann drohen im Rahmen der EU-Datenschutzgrundverordnung (EU-DSGVO) Strafen in Millionenhöhe.

4. Öffentliche Stellen für die Cyberabwehr sind da, aber viel zu klein

Die öffentlichen Mühlen mahlen zu langsam. Behörden vieler Länder beklagen Angriffe. Regierungen sind grundsätzlich gewillt, Engagements für mehr Cybersicherheit auszuweiten, aber allem voran in Europa sind sie zu zögerlich in der Bereitstellung von Budgets, dem Aufbau einer europäischen Cybersicherheits-Industrie und der Zusammenarbeit mit dem hiesigen privaten Sektor. Die Lage spitzt sich zu, da bereits in 2017 große außereuropäische Sicherheitsfirmen öffentlich der Staatsspionage bezichtigt wurden.

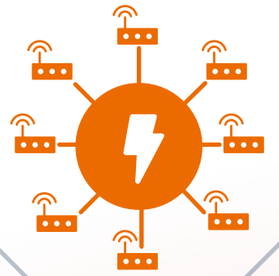
5. Die große Unbekannte: wer sind die Täter?

Wer hinter den Angriffen steht, ist in 98% der Fälle nicht auszumachen. 2017 zeigte, dass schon Elf-Jährige in der Lage sein können, Sicherheitslücken zu finden und auszunutzen. Das andere Extrem stellen die professionell organisierten Hackergruppen dar. Die Öffentlichkeit lernt sie meist unter einem Pseudonym kennen, aber wer dahinter steckt, das weiß keiner. So bleiben die größten Straftaten heute massenweise ungestraft.

2017
Eine neue Dimension

Diese Angriffe bereiten IT-Sicherheitsexperten besonders Kopfschmerzen

Riesige Botnetze durch Zusammenschalten von Routern



Das Wachstum von Hacking-as-a-Service

WannaCry: der bisher größte Cyberangriff der Geschichte

Die Nutzung von vermeintlich harmlosen Programmen für die Schadsoftwareverbreitung

Cybersecurity 2018 Fünf Top Trends für die IT-Sicherheit

Was die Cyber-Security-Experten von RadarServices für das neue Jahr prognostizieren: Christian Polster, Chefstratege und CFO von RadarServices, gibt den Ausblick.

1. IoT als Eldorado für Cyberangreifer

Die Weiterentwicklung des Internet of Things ist nicht aufzuhalten. In wenigen Jahren wird jede Schraube eine IP-Adresse haben. Während das ganz neue Möglichkeiten eröffnet, stellt es immense Herausforderungen an die IT-Sicherheit von Unternehmen und Privatpersonen. Dringend müssen neue Sicherheitskonzepte für das IoT aufgestellt und praxiserprobt werden.

2. Gezielte Angriffe in einer neuen Dimension

Zahlreiche Großunternehmen bieten immer noch zu viel Angriffsfläche. Die IT ist weltweit verteilt, der Überblick über alles ist oft nicht vorhanden. Gleichzeitig wirkt der Druck der EU-Datenschutzgrundverordnung ebenso wie weitere neue und alte Compliancevorschriften. IT-Sicherheitsverantwortliche benötigen in diesem Umfeld vor allem eins, um große Schäden zu verhindern: Transparenz und die richtige Information zur richtigen Zeit.

3. Ransomware gegen den Mittelstand

Weil sich Großunternehmen inzwischen besser gegen Erpresser-Software zu verteidigen wissen, werden sich Ransomware-Attacken in Zukunft zunehmend gegen Klein- und Mittelbetriebe und vernetzte Steuerungs-Geräte richten. Diese potentiellen Opfer müssen sich den angepassten Geschäftsmodellen der Angreifer bewusst werden und sich Experten suchen, die ihre IT effektiv und effizient schützen.

4. Nationale Unsicherheit

Nationale Sicherheit muss neu gedacht werden. Der Schutz von kritischen Infrastrukturen aber auch das Sicherstellen der dauernden Funktionsfähigkeit der öffentlichen Infrastruktur eines Landes bedeuten immense Herausforderungen. Das ist heute Behörden, aber auch Cyberangreifern bewusst.

5. Ohne den Einsatz künstlicher Intelligenz geht es nicht

Durch den Einsatz von machine learning lassen sich viele Schwachstellen, verdächtiges Systemverhalten oder Zero-Day-Attacken schneller aufspüren und bekämpfen. Aber auch die „Gegner“ werden die Möglichkeiten von künstlicher Intelligenz voll ausschöpfen, indem sie alles über neue Verteidigungsstrategien und Schutzmaßnahmen lernen. Kurzum: Wenn sich Unternehmen nicht mit dem Einsatz von KI in der IT-Sicherheit befassen, werden ihre Sicherheitsmaßnahmen in kurzer Zeit obsolet.

RADAR SERVICES

The European Experts
in IT Security Monitoring
and IT Risk Detection

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. Basis dafür ist eine hochmoderne, eigenentwickelte Technologieplattform mit der Kunden ihr Security Operations Center (SOC) aufbauen können oder die in Kombination mit Security-Analyse-experten, bewährten Prozessen und Best Practices als SOC as a Service zur Verfügung steht. Das Ergebnis: Eine besonders effektive und effiziente Verbesserung von IT-Sicherheit und -Risikomanagement, kontinuierliches IT Security Monitoring und ein auf Knopfdruck verfügbarer Überblick über die sicherheitsrelevanten Informationen in der gesamten IT-Landschaft einer Organisation.

Die Headquarters von RadarServices befinden sich in der Cybersecurity World in Wien. An diesem weltweit einzigartigen Ort wird IT-Sicherheit erlebbar. Hier befindet sich das größte Security Operations Center (SOC) Europas. Und hier werden die heutigen und zukünftigen Herausforderungen für IT-Sicherheitsverantwortliche in Unternehmen und der aktuelle Stand von Research und Innovation in der Branche auf 2.000 qm illustriert.

RadarServices
Zieglergasse 6
1070 Wien
Österreich

T: +43 (1) 929 12 71-0
F: +43 (1) 929 12 71-710
E: sales@radarservices.com
www.radarservices.com

RadarServices Deutschland
Taunustor 1
60310 Frankfurt a. M.

T: +49 (69) 2443424 655
E: sales_germany@radarservices.com

ISO 27001 CERTIFIED

PUBLIC