Hacker, Cracker und die Privatsphäre im Internet

Norbert Jirak ISDS 2018
norbert.jirak@p-k-p.at

Cyber Risk

Wer sind die Player?

- Regierungen & Geheimdienste
  - Kontrollwahn, Überwachung & Unterdrückung von „Andersdenkenden“, ausspionieren von Verhandlungspositionen und Betriebsgeheimnissen, „Cyberwar“
- Kriminelle
  - Erpressung mit Ransomware, Verkauf von Geschäftsgeheimnissen, Kreditkartendaten, gestohlenen Identitäten, etc.
- „Social Media“, Werbebranche und andere Datenkraken
  - Bestimmung des Kaufverhaltens, maßgeschneiderte Angebote für höhere Umsätze

Cyber Risk

- Cyberwar
  - 2010 wurde *Stuxnet* gezielt zur Sabotage iranischer Atomanlagen eingesetzt. Diese Software wurde lt. Edward Snowden von amerikanischen und israelischen Geheimdiensten gemeinsam programmiert, um die iranischen Uranzentrifugen unbrauchbar zu machen.

Digital Trends

Bits before bombs: How Stuxnet crippled Iran's nuclear dreams ...

Cyber Risk

- Cyberwar
  - Diese Art von Schadsoftware kann in modifizierter Form auch gegen jede Art von Infrastruktur, die sog. „SPS“ (Industriesteuerungen) verwenden, eingesetzt werden. Dazu gehören u.a. Kraftwerke, Elektrizitätsverteiler, Verkehrsleitsysteme / Ampelsteuerungen, Wasserwerke, etc.
  - oder auch Raffinerien
  - 2017 wurde eine saudische Raffinerie mit Schadsoftware angegriffen, welche diese buchstäblich in die Luft gejagt hätte, wenn nicht (durch puren Zufall) die Ausführung des Programmes durch einen Fehler unterbrochen worden wäre

Cyber Risk

- Cyberwar

A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.

Cyber Risk

- Cyberwar

  New York Times March 15, 2018

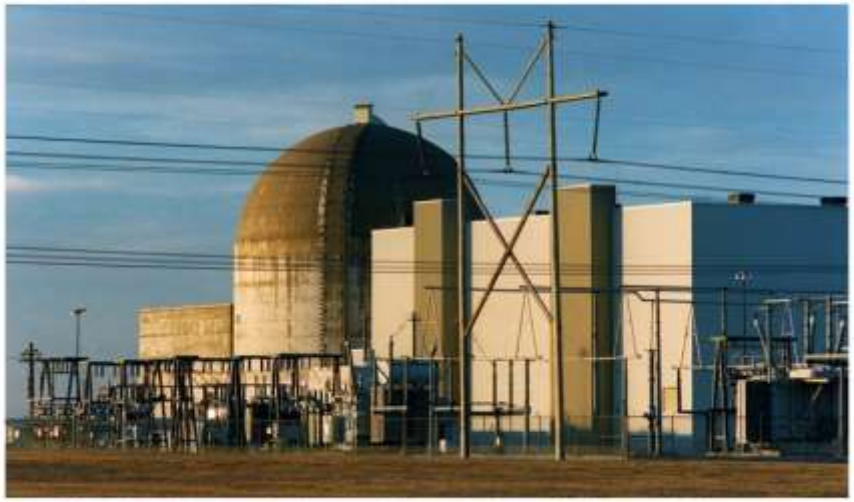
  In August 2017, a petrochemical company with a plant in Saudi Arabia was hit by a new kind of cyberassault. The attack was not designed to simply destroy data or shut down the plant, investigators believe. It was meant to sabotage the firm's operations and trigger an explosion.

  The attack was a dangerous escalation in international hacking, as faceless enemies demonstrated both the drive and the ability to inflict serious physical damage. And United States government officials, their allies and cybersecurity researchers worry that the culprits could replicate it in other countries, since thousands of industrial plants all over the world rely on the same American-engineered computer systems that were compromised

Cyber Risk

- Cyberwar

Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say



The Wolf Creek Nuclear power plant in Kansas in 2000. The corporation that runs the plant was targeted by hackers. David Eulitt/Capital Journal, via Associated Press

Cyber Risk

- Cyberwar

  New York Times July 6, 2017

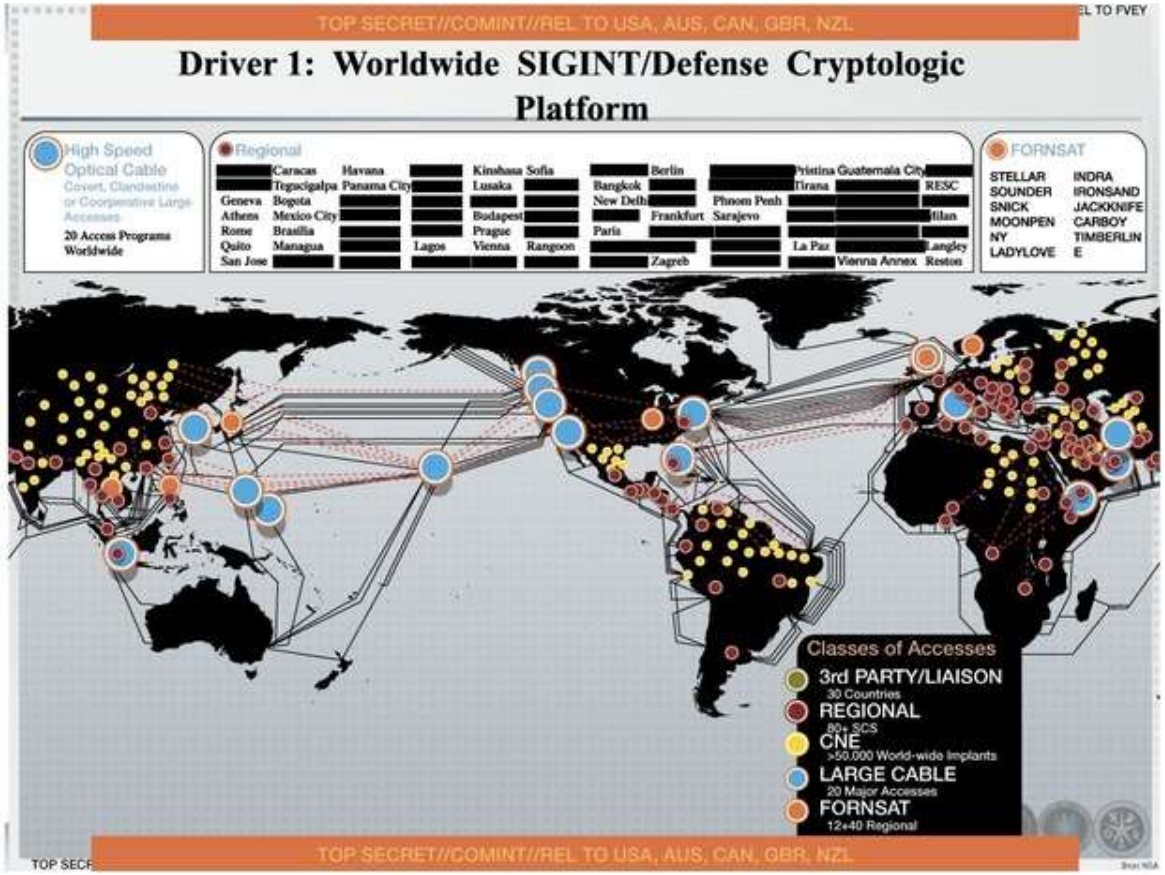
  Since May, hackers have been penetrating the computer networks of companies that operate nuclear power stations and other energy facilities, as well as manufacturing plants in the United States and other countries.

  Among the companies targeted was the Wolf Creek Nuclear Operating Corporation, which runs a nuclear power plant near Burlington, Kansas, according to security consultants and an urgent joint report issued by the Department of Homeland Security and the Federal Bureau of Investigation last week.

  The joint report was obtained by The New York Times and confirmed by security specialists who have been responding to the attacks. It carried an urgent amber warning, the second-highest rating for the sensitivity of the threat.

Cyber Risk

- Spionage



Cyber Risk

- Spionage

  „Five Eyes“

  Zusammenarbeit der Geheimdienste von

  USA, Kanada, Großbritannien, Australien & Neuseeland

Cyber Risk

- Spionage

  Neue Züricher Zeitung 1. März 2018

  „Technisch anspruchsvoll und von langer Hand geplant“ so hat am Donnerstag der deutsche Innenminister, Thomas de Maizière, den Hackerangriff auf das Kommunikationsnetz der Regierung in Berlin charakterisiert. Er sprach von einem ernstzunehmenden Vorfall. Gleichzeitig zeichnete sich ab, dass nicht nur Deutschland im Visier steht

Cyber Risk

- Spionage

  Snowdens Enthüllungen 2013 zeigen, dass die NSA Freund und Feind überwacht

  - Merkls Mobiltelefon und weitere 36 europäische Staats- und Regierungschefs
  - Am 25. August 2013 schrieb der Spiegel, dass die Zentrale der Vereinten Nationen in New York von der NSA abgehört werde.
  - Auch die Internationale Atomenergie-Organisation (IAEO, englisch International Atomic Energy Agency, IAEA), mit Hauptsitz in Wien, wurde von der NSA abgehört

Cyber Risk

- Spionage

Cyber Risk

- Spionage

  Über russische, chinesische etc. Aktivitäten ist weniger bekannt, sie dürften aber den amerikanischen um nichts nachstehen.

Cyber Risk

- Kriminelle

  Ransomware

  Erpresser schleusen Schadsoftware auf den PC des Opfers, die z.B. wie bei “Wannacry” die Festplatte verschlüsselt, und verlangen zw. $ 500.- und $ 1.000.- (meist in Cryptowährungen wie Bitcoin) für den Schlüssel, mit dem die Festplatte wieder entschlüsselt werden kann.

Cyber Risk

- Kriminelle

  Ransomware “Wannacry”

Cyber Risk

- Kriminelle

  Ransomware “Wannacry”

  Microsoft gibt den Regierungen eine Mitschuld für den weltweiten Hackerangriff

  Der Vorwurf: Regierungen behielten entdeckte Sicherheitslücken für sich, um sie für ihre Zwecke zu nutzen, anstatt sie an Softwareunternehmen zu melden.

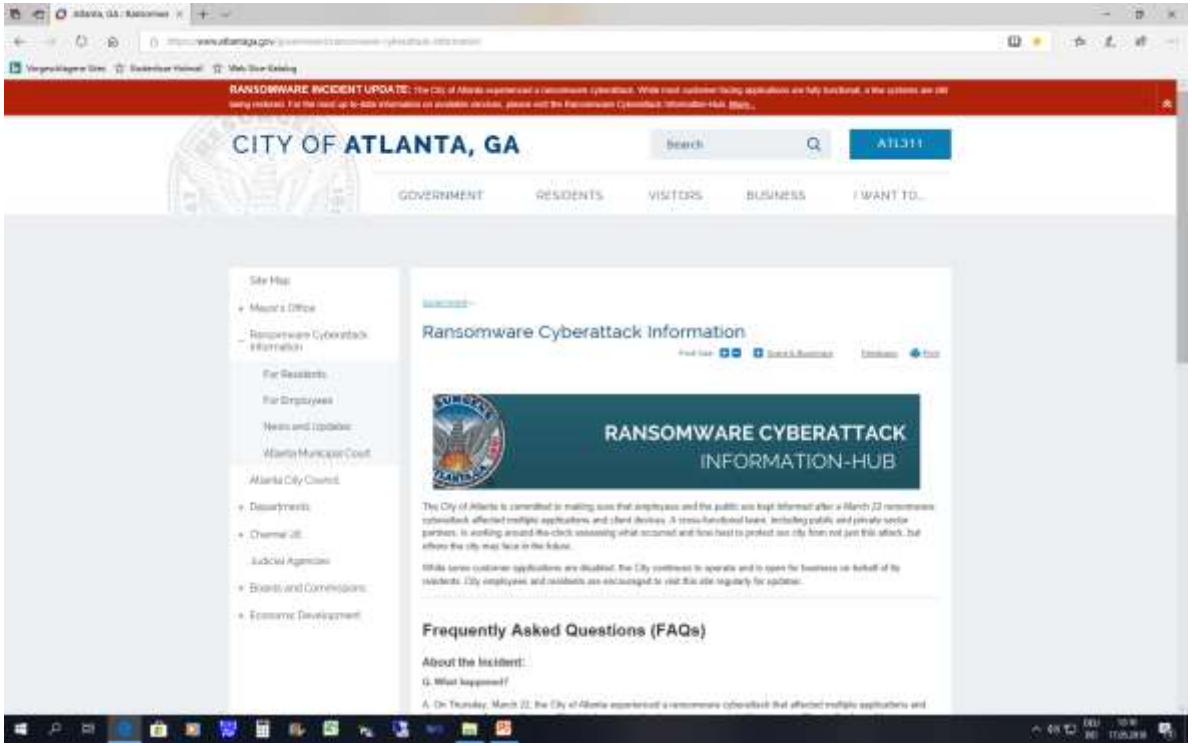
  Die Süddeutsche Zeitung 15. Mai 2017

Cyber Risk

- Kriminelle

  Ransomware “SamSam” beim Angriff auf Atlanta

  https://www.atlantaga.gov/government/ransomware-cyberattack-information



Cyber Risk

- Kriminelle

  “On Thursday, March 22, the City of Atlanta experienced a ransomware cyberattack that affected multiple applications and client devices. As a result, some City data is encrypted and customers are not able to access City applications. Atlanta Information Management (AIM), the City’s technology department, is working to restore service.”

  Wired 23. April 2018:

  “The City of Atlanta spent more than $2.6 million on emergency efforts to respond to a ransomware attack that destabilized municipal operations last month. Attackers, who infected the city's systems with the pernicious SamSam malware, asked for a ransom of roughly $50,000 worth of bitcoin. (The exact value has fluctuated due to bitcoin's volatility.) Atlanta officials haven't said whether they paid the ransom, or even tried, but it seems that they may not have even had the chance; the attackers quickly took the payment portal offline, and left the city to fend for itself. So far, the recovery has been far more costly than the initial demand.”

Cyber Risk

- Kriminelle

  28. März 2018

  A “limited breach” affecting Baltimore’s computer-assisted dispatch system, which is used to support and direct 911 and other emergency calls, was identified Sunday morning, according to Frank Johnson, Baltimore’s chief information officer.

  The disruption was the second cyber attack on a major U.S. city within the past week, coming days after Atlanta was struck by a widespread “ransomware” cyber extortion attack that interrupted bill collection services, downed the airport’s wireless internet and impeded other city services

Cyber Risk

- Kriminelle

  CNBC 11.März 2018

  Equifax hat weitere Details zu den persönlichen Daten und vertraulichen Informationen veröffentlicht, die von Hackern 2017 gestohlen wurden.

  Equifax ist die grösste Wirtschaftsauskunftei der USA, verfügt über Kreditkartendaten, Bonitätsinformationen, Führerscheindaten, Adressen, Passdaten, ….

  “The most common data taken involved names, dates of birth and social security numbers - each between 145.5 million and 146.6 million. Other giant losses included home addresses (99 million), genders (27.3 million) and driver's license numbers (17.6 million).

  However, it's the smaller numbers that may matter the most. The SEC filing confirmed that the intruders compromised key government IDs held at its online dispute portal, including full driver's license info (38,000 people), social security and taxpayer ID cards (12,000) and even passports (3,200). More limited data was also stolen in the main set, including payment card numbers (209,000), tax IDs (97,500) and a driver's license state (27,000)”

Cyber Risk

- Kriminelle

  Kreditkartenbetrug
  Roman Seleznew wurde am 5. Juli 2014 festgenommen,
  auf seinem Laptop wurden die Daten von 1,7 Mio Kreditkarten gefunden
  er war seit 2009 unter Verdacht

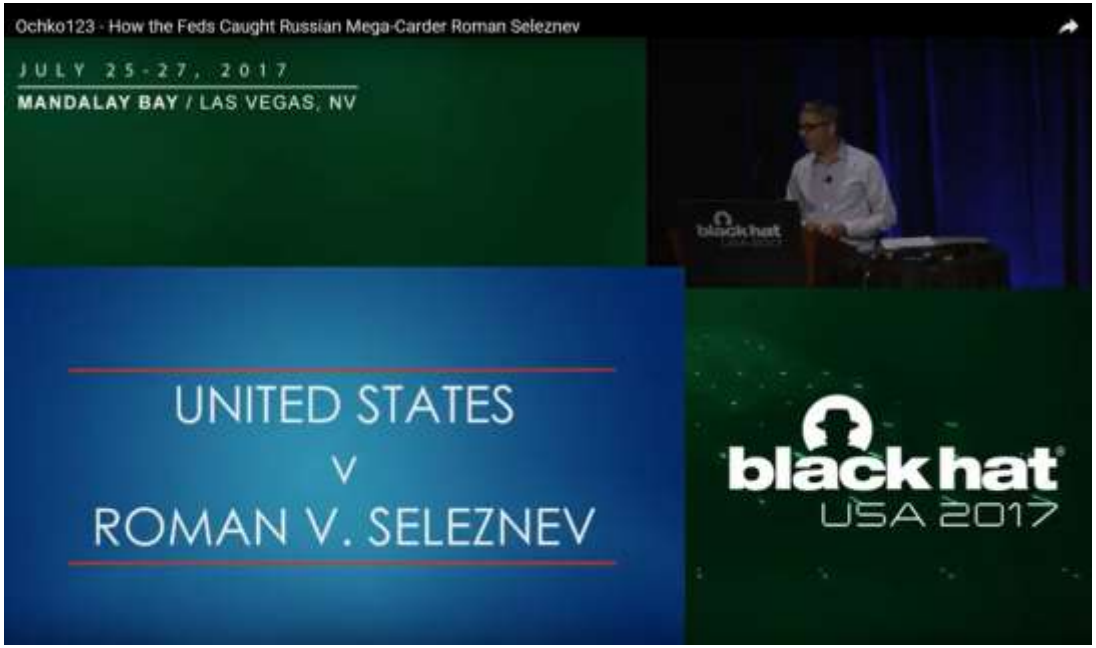
  „Beschaffung“ über maleware auf den POS – Kassen

  FBI hat den Fall 2017 auf der „Black Hat“ in Las Vegas berichtet

Cyber Risk

- Kriminelle

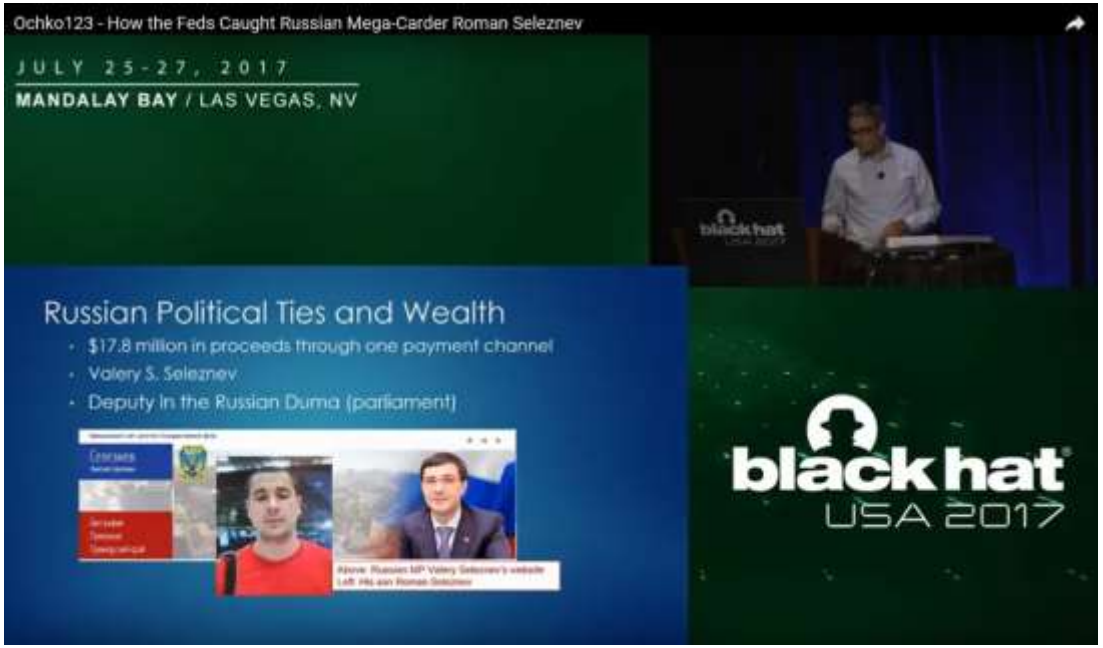
  Kreditkartenbetrug



Cyber Risk

- Kriminelle

  Kreditkartenbetrug



Cyber Risk

- Kriminelle

  Kreditkartenbetrug

Cyber Risk

- Kriminelle

  „botnet“

  mehrere mit Schadsoftware infizierte Computer (das „net of robots“, = „botnet“) arbeiten ferngesteuert, ohne Wissen des Eigentümers

  starten Attacken auf Server (DDos)

  oder verschicken spam-mails

  oder stellen ihre Rechenleistung zum knacken von Passwörtern zur Verfügung

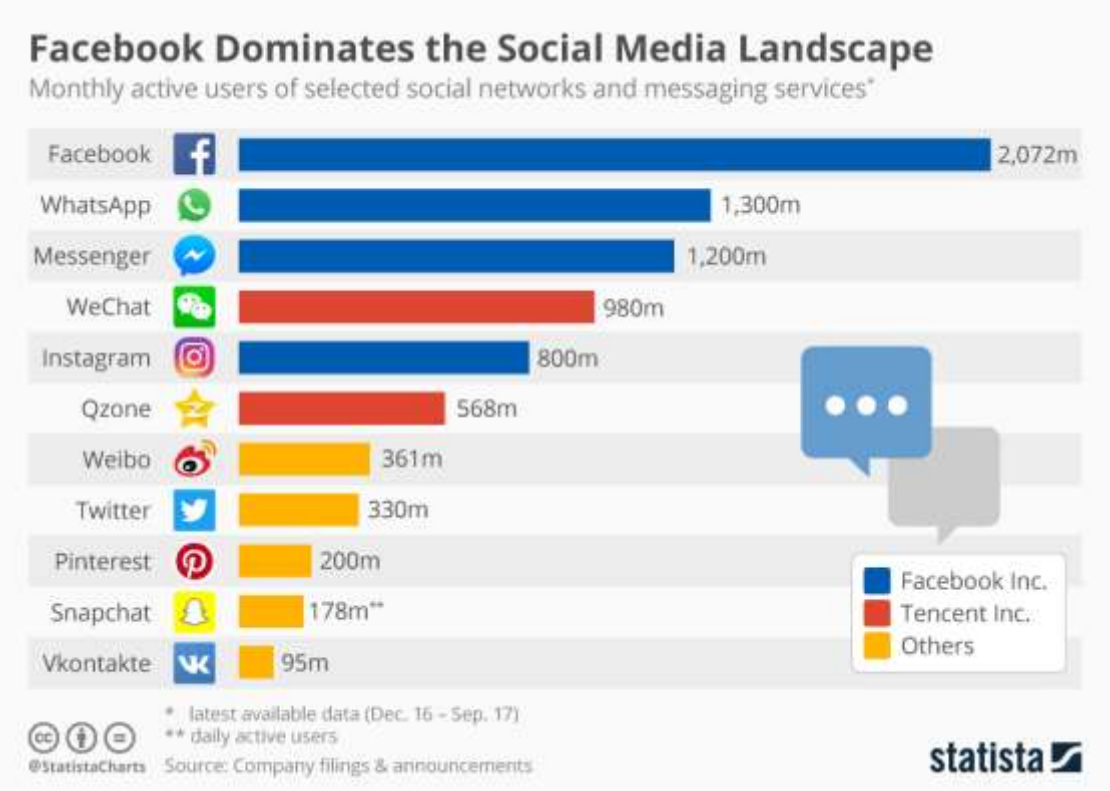
  ……

  Man merkt das i.d.R. nur,

  wenn der Rechner langsamer wird oder der Speicher ausgeht

Cyber Risk

- „Social Media“, Werbebranche und andere Datenkraken



Cyber Risk

- „Social Media“, Werbebranche und andere Datenkraken

  Statista, 26.Jänner 2018:

  „What all of the services mentioned in the chart have in common is their immense attractiveness to advertisers. Not only do they all boast hundreds of millions of users, but they also have the ability to target specific groups based on likes, dislikes and past behavior. That is why social media advertising has grown immensely over the past few years. In the U.S. alone, social media ad revenue is expected to reach $23.8 billion this year, with more growth to come in 2019 and beyond. “

Take Home Message

Ihre Daten sind bares Geld wert

Cyber Risk

- „Social Media“, Werbebranche und andere Datenkraken

Google	(Suchmaschine)
Android	(Betriebsystem)
Chrome	(Browser)
Gmail	(e-mail)
YouTube	(Videoplattform)
Google Maps	
Google News	
Google Ventures	(Beteiligungsgesellschaft)
Uber	(Taxi)
Tune.In	(Streaming / Internet-Radio)

Cyber Risk

- „Social Media“, Werbebranche und andere Datenkraken

Facebook	(social network)
WhatsApp	(social network)
Facebook Messenger	(Instant Messaging)
Instagram	(Instant Messaging)
Onavo	(VPN-Dienst)
Twitter	(Instant Messaging)
Vine	(Videoplattform)
Yahoo	(mail & Suchmaschine)
Tumblr	(Mircoblogging-Dienst)

Cyber Risk

- „Social Media“, Werbebranche und andere Datenkraken

SnapChat	(Instant Messaging)
Pinterest	(social networking)
WeChat	(Instant Messaging) China
Qzone	(social networking) China
Weibo	(Mircoblogging-Dienst) China
Vkontakte	(social networking) Russland

Cyber Risk

- „Social Media“, Werbebranche und andere Datenkraken

Facebook mit Schnüffel-Offensive

Das schlägt dem Fass den Boden aus! Facebook, schon bisher kein Musterbeispiel für Datenschutz, ermuntert iOS-User neuerdings zur Installation von Spionage-Software. Verkauft wird das Ganze als Schutzmaßnahme.

Konkret wurde der Facebook-App in der Rubrik „Entdecken“ der Punkt „Protect“ („schützen“) hinzugefügt. Wer hier klickt, landet im App-Store und kann das VPN-Tool „Onavo Protect“ installieren, das vor den Bedrohungen im Web schützen soll.

Allein: Mit Installation läuft nicht nur der gesamte Datenverkehr über den Onavo-Server. Zusätzlich erlaubt sich die Firma die Analyse aller Daten und Inhalte – Zugriff aufs Handy samt Erfassung des Nutzerverhaltens inklusive. Eigentümer von Onavo ist seit 2013 – Facebook

Februar 2018

Cyber Risk

- „Social Media“, Werbebranche und andere Datenkraken

  Yahoo

  Am 12. Juli 2012 wurde bekannt, dass es Crackern gelungen war, Hunderttausende von Benutzernamen mit ihren Kennwörtern zu ermitteln, da die entsprechende Datenbank weder hinreichend gesichert noch hinreichend verschlüsselt gewesen war. Die Zugangsdaten wurden im Internet veröffentlicht

Cyber Risk

- „Social Media“, Werbebranche und andere Datenkraken

  Google

  im Juni 2017 hat die EU-Kommission gegen den US-Konzern eine Strafe von 2,42 Milliarden Dollar verhängt, weil „Google nachweislich die Ergebnisse ihrer Shopping-Suchmaschine zugunsten der eigenen Anzeigenkunden manipuliert habe“

  Uber

  besitz ein tool namens „God View“ zum tracking von Fahrern und Kunden in Echtzeit

  futurezone: „Uber now collecting location data even after you leave a driver’s car. With the latest update to the app is now tracking your location constantly if you’ve got the app running in the background. Oh, and it’s also asking that you always share your address book. Until now it had only collected your location data if you had the app open.”

Cyber Risk

- „Social Media“, Werbebranche und andere Datenkraken

  Twitter

  3. Mai 2018 Reuters

  Twitter Inc. (TWTR.N) urged its more than 330 million users to change their passwords after a glitch caused some to be stored in readable text on its internal computer system rather than disguised by a process known as “hashing”

Cyber Risk

- Wie funktioniert Datendiebstahl?
  - Schadsoftware wird auf den Rechner geschleust, auf dem die Daten liegen,
  - die Schadsoftware stellt eine Verbindung mit dem Angreifer her
  - Daten werden abgesaugt

Cyber Risk

- Wie kommt die Schadsoftware auf den Rechner ?
  - „social engineering“

    der Angreifer bringt das Opfer (oder einen seiner Mitarbeiter) dazu, ein Programm auszuführen, einen Link anzuklicken etc.
  - phishing

    über (fake) Nachrichten wird das Opfer verführt, Links oder Anhänge anzuklicken und damit die Schadsoftware zu installieren
  - Sicherheitslücken

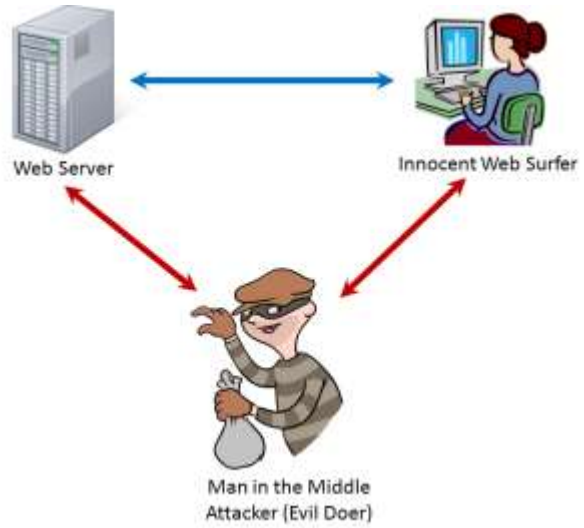
    Fehler im Betriebssystem oder Programmen werden benützt, um einen Rechner unter Kontrolle zu bekommen

Cyber Risk

- Wie bekommt man Zugang zu fremden Konten und Rechnern ?
  - Zugangsdaten ausspähen
  - Zugangsdaten / Passwörter zurücksetzten (lassen)
    - „Passwort vergessen?“
  - Zugangsdaten / Passwörter „erraten“
    - Es gibt Programme, die mittels „Passwortdateien“ und „brute force“ Passwörter knacken, im Internet zum Download

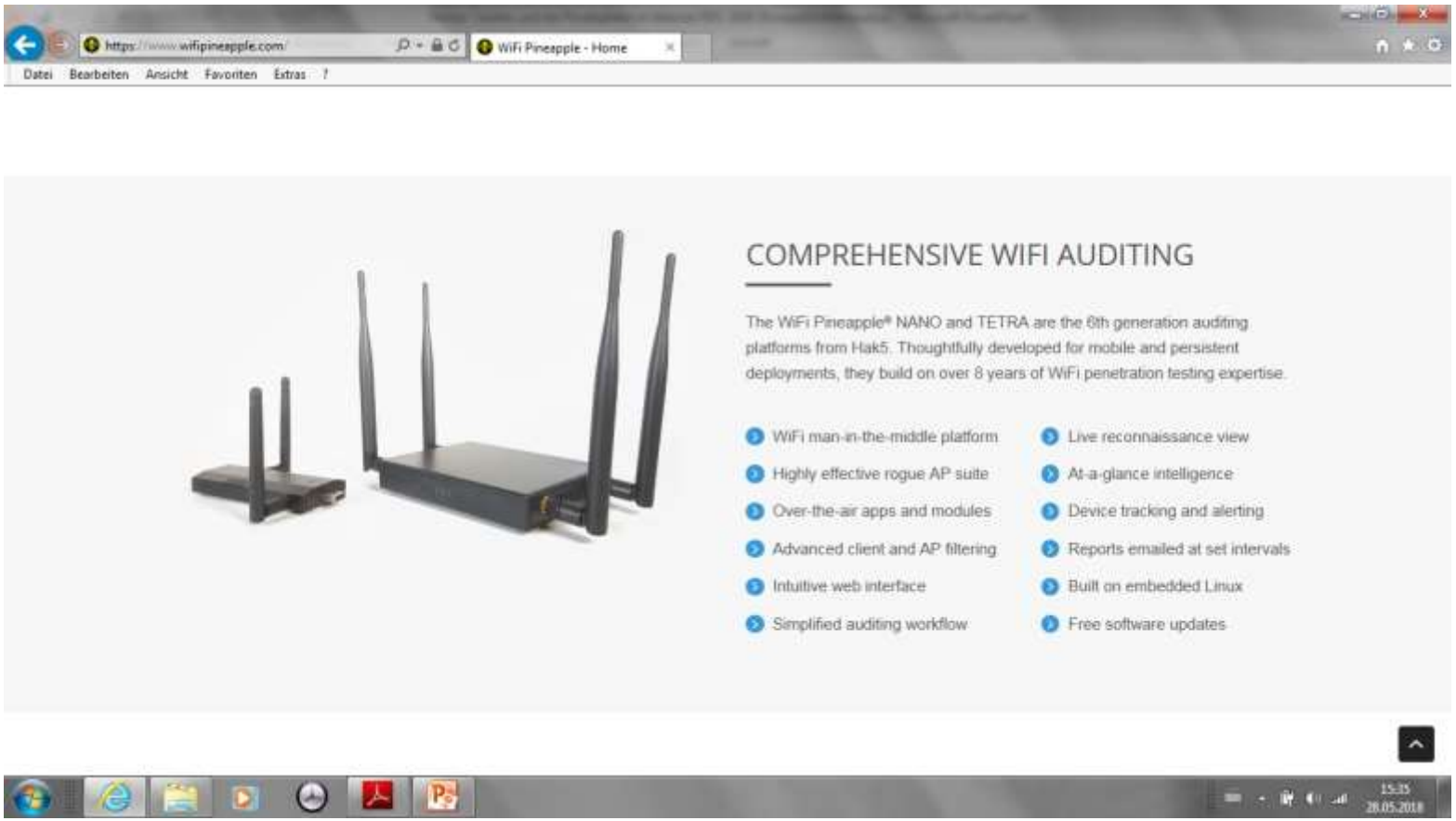
Cyber Risk

- Zugangsdaten / Passwörter ausspähen
  - „man in the middle“



  - besonders leicht bei WLAN zu realisieren

Cyber Risk


https://www.wifipineapple.com/
WiFi Pineapple - Home
Datei Bearbeiten Ansicht Favoriten Extras ?
COMPREHENSIVE WIFI AUDITING
The WiFi Pineapple® NANO and TETRA are the 6th generation auditing platforms from Hak5. Thoughtfully developed for mobile and persistent deployments, they build on over 8 years of WiFi penetration testing expertise.
WiFi man-in-the-middle platform
Highly effective rogue AP suite
Over-the-air apps and modules
Advanced client and AP filtering
Intuitive web interface
Simplified auditing workflow
Live reconnaissance view
At-a-glance intelligence
Device tracking and alerting
Reports emailed at set intervals
Built on embedded Linux
Free software updates

Cyber Risk

- Wie können wir uns schützen?
  - Möglichst wenig Daten preisgeben.
    - Was z.B. Facebook nicht hat, kann dort auch nicht gestohlen werden.
  - Hardware-Firewalls verwenden
    - Blockiert effizient unerlaubte Kommunikation
  - regelmäßig Software Updates durchführen
    - Sicherheitslücken werden oft geschlossen bevor sie davon betroffen sein können

Cyber Risk

- Wie können wir uns schützen?
  - Keine „Default“-Passwörter belassen oder verwenden
    - Bei Konfiguration neuer Geräte (z.B. WIFI-Router) sofort Passwort ändern
  - Starke Passwörter verwenden
    - Möglichst lang, mit Sonderzeichen und Zahlen
  - Passwörter regelmäßig ändern
    - „alte“ Passwörter in Datenbanken sind für Angreifer wertlos

Cyber Risk

- Wie können wir uns schützen?
  - Kryptische oder falsche Antworten auf Sicherheitsfragen
    - z.B. Geburtsort „Erde“, Haustier „Anaconda“, Lieblingsfarbe „Bunt“
    - „Übernahme“ von Konten finden oft über das Zurücksetzten von Passwörtern statt
  - regelmäßig Backups erstellen
    - Backup einspielen statt Lösegeld zahlen (Ransomware)
  - Keine fraglichen Links, Anhänge etc. in emails anklicken
    - Prüfen sie den Absender und dessen e-mail Adresse auf Plausibilität
    - wenn sie (verdächtige) Anhänge unbedingt sehen wollen, dann:
      Anhang mit rechter Maus „Speichern unter“ erst mal abspeichern
      und dann mit dem Virenscanner checken

Cyber Risk

- Wie können wir uns schützen?
  - sensible Daten nur auf https-Seiten eingeben
    - Finger weg, wenn die URL nicht mit https:// beginnt
  - Bildschirmtastatur benützen
    - Keylogger und Funkempfänger sehen nur Maus-Klicks

Cyber Risk

- Wie können wir uns schützen?
  - Freies WLAN nicht für sensible mails, netbanking etc. nützen
    - Wer da „mithört“ können wir nicht wissen
  - In „fremden“ Netzen möglichst VPN verwenden
    - „virtual private network“ ist eine verschlüsselte Punkt-zu-Punkt-Verbindung
  - lesen sie die Nutzungsbedingungen bevor sie zustimmen
    - und überlegen sie, ob sie auch ohne diesen Dienst leben können, wenn sie den Nutzungsbedingungen eigentlich nicht zustimmen wollen

Take Home Message

Sicherheit kostet Geld und Anstrengung

Take Home Message

Sicherheit und Bequemlichkeit schließen sich gegenseitig aus

Danke für ihre Aufmerksamkeit