Greenbone
Sustainable Resilience

Cyber Security Strategie für KMU

10. IT-Businesstalk in Salzburg

DI(FH) Martin Herfurt
Professional Services

11.04.2019

Vorstellung

Greenbone Networks GmbH

- Professionelles Schwachstellen Management
- Deutscher Hersteller (HQ Osnabrück)
- Produkt seit 2008 am Markt
- Entstanden in Zusammenarbeit mit BSI
- Etwa 50 MitarbeiterInnen (Tendenz steigend)
- Basierend auf OpenVAS
  - >90% der Entwicklung bei Greenbone

DI(FH) Martin Herfurt

- Absolvent der FH Salzburg (TKS 1997)
- Ehem. Mitarbeiter von Salzburg Research
- Mitbegründer der trifinite.group
  - Bluetooth Security
- Geschäftsführer der toothR new media GmbH
- Ehem. Security Auditor bei n.runs AG
- Greenbone Professional Services Consultant
- Seit 20 Jahren in der IT-Sicherheit

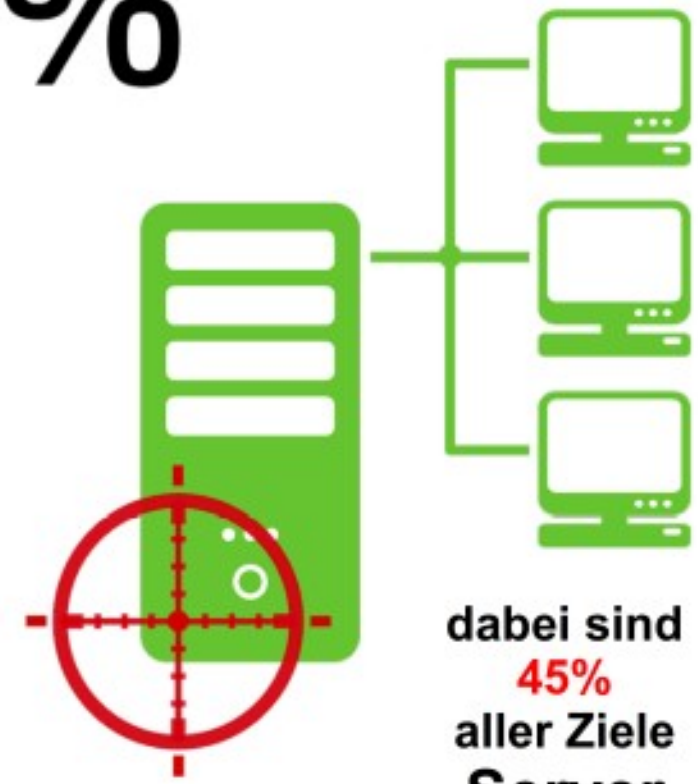
Statistik

Motivation und Angriffsziele

[$ € +] > 70%

mehr als 70% der Angriffe haben ein finanzielles Motiv
oder – steigend – Wirtschaftsspionage als Grund

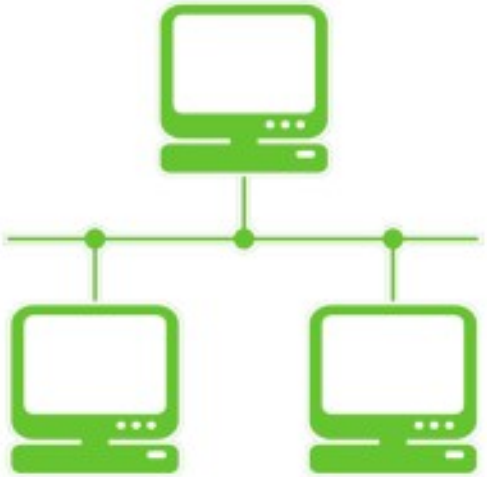
um mit Hacking und Malware zu attackieren



dabei sind 45% aller Ziele Server

Statistik

Wie viele IT-Sicherheitsvorfälle gab es bei Ihnen im letzten Jahr?



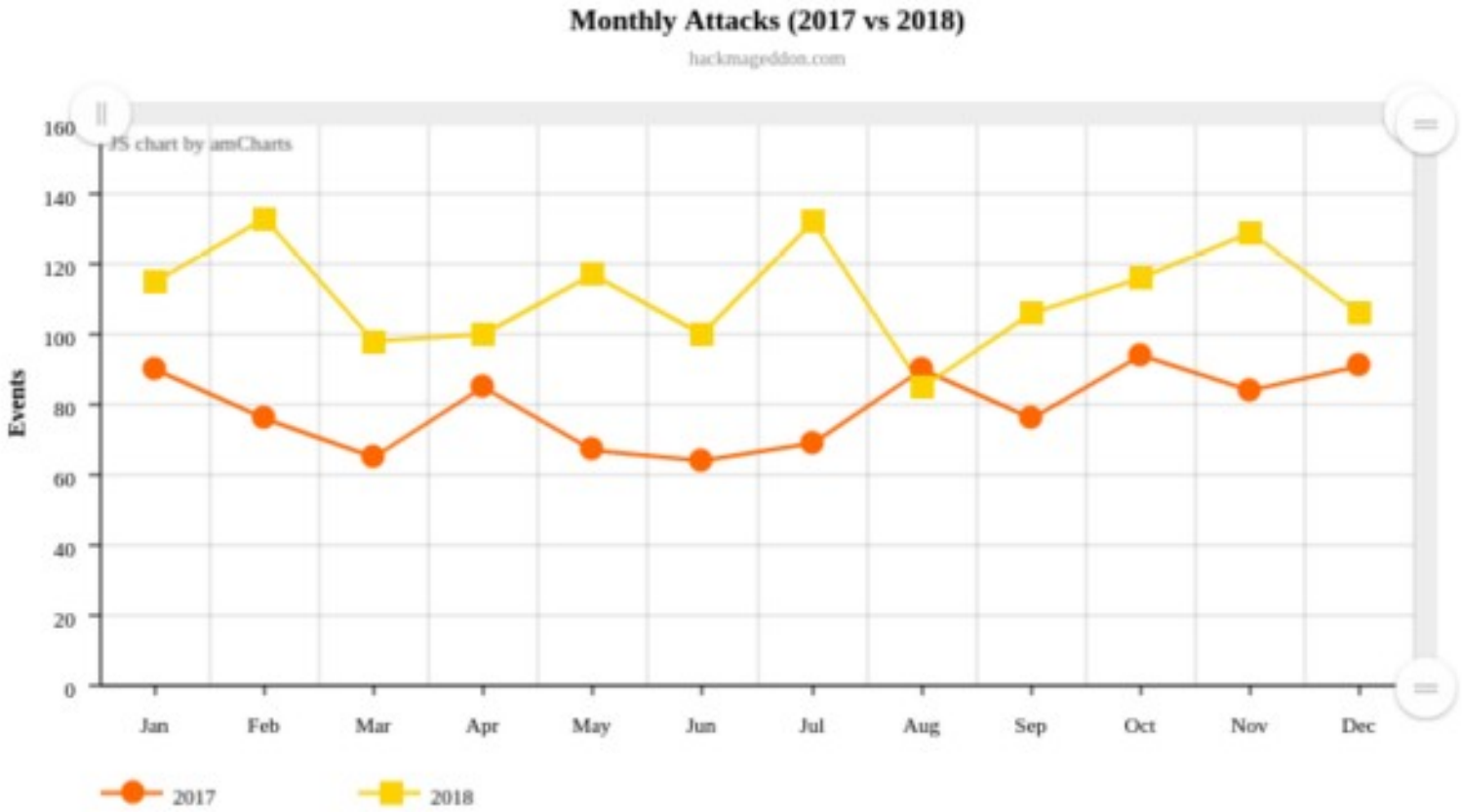
aller Angriffe kommen von Außen

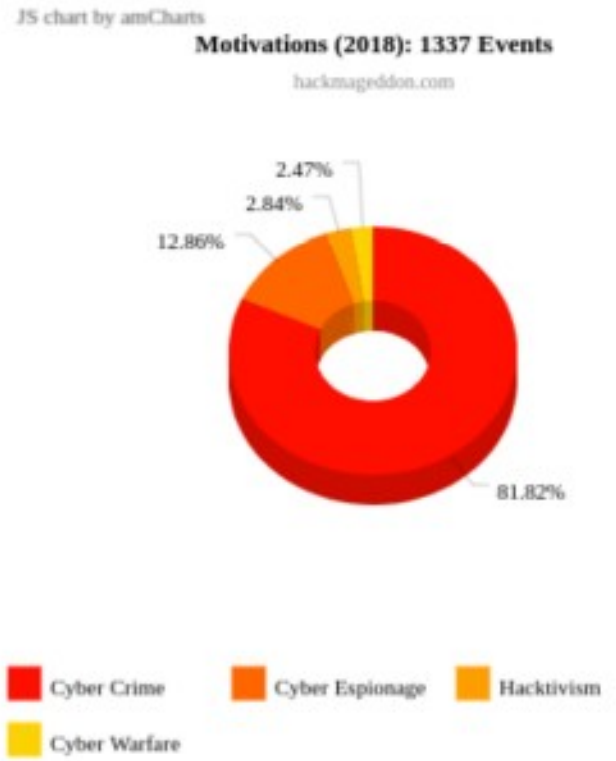
- **24% ... ist uns bekannt**
- **21 % ... keine (von denen wir wüssten!)**
- **die restlichen 55% wussten von Vorfällen**

Angriffe von Innen sind aber deutlich teurer

Statistik

Entwicklung IT-Angriffe im Vergleich 2017/2018





Woran denken Sie beim Stichwort: Großbritannien?

Cyber Essentials

- Seit 2014
- Britisches Äquivalent zum BSI Grundschutz (von 2006)
- Einfach umzusetzen
- Sehr grundlegend (auf den ersten Blick)
- Fünf einfache Spielregeln
- https://www.cyberessentials.ncsc.gov.uk/advice/

National Cyber Security Centre
a part of GCHQ

Cyber Essentials

1. Firewall für die Verbindung zum Internet verwenden

- Unternehmens-Firewalls
- Host Firewalls
- Verringerung der Angriffsoberfläche

2. Die sichersten Einstellungen für Geräte und Software wählen

- Standard-Einstellungen sind oft nicht sicher
- Nicht benötigte Funktionalitäten deaktivieren
- Passwortsicherheit
  - Keine Standard-Passwörter verwenden
  - Unterschiedliche Passwörter verwenden
  - Passwortkomplexität
- 2nd-Factor Anmeldeverfahren
  - Für besonders wichtige Benutzer-Konten
  - Hardware-Token (Security Key)
  - Smartphone-App

Cyber Essentials

3. Kontrollieren wer Zugriff auf Daten und Dienste hat

- Möglichen Schaden minimieren
- Least-Privilege Ansatz
- Administrative Accounts nicht für alltägliche Tätigkeiten verwenden
  - Missbrauchspotential einschränken
- Software nur aus vertrauten Quellen
  - Speziell bei Mobile Apps

Cyber Essentials

4. Schützen vor Viren und Malware

- Malware = Schadsoftware = Virus
  - Von zwielichtigen Websites
  - E-Mail-Anhänge
  - Fremden Datenträgern (z.B. USB-Sticks)
- Neuer Trend: CryptoCurrency-Malware löst Verschlüsselungs-Malware (Ransomware) ab
- Gegenmaßnahmen
  - Anti-Malware Scanner
  - Application Whitelisting
  - Sandbox Umgebungen (z.B. für E-Mail Anhänge)

Cyber Essentials

5. Geräte und Software auf aktuellem Stand halten

- Betriebssysteme und Anwendungen aktuell halten
  - Windows 10 (2018: 255 Vulns – 118 >= CVSS 5.0)
  - Apple macOS X (2018: 108 Vulns – 73 >= CVSS 5.0)
  - Linux Kernel (2018: 175 Vulns – 72 >= CVSS 5.0)
  - Android (2018: 611 Vulns – 407 >= CVSS 5.0)
  - Apple iOS (2018: 154 Vulns – 106 >= CVSS 5.0)
  - Wordpress (2018: 17 Vulns – 13 >= CVSS 5.0)
- Maßnahme
  - Patch-Management
  - Schwachstellen-Management

Werbeeinschaltung

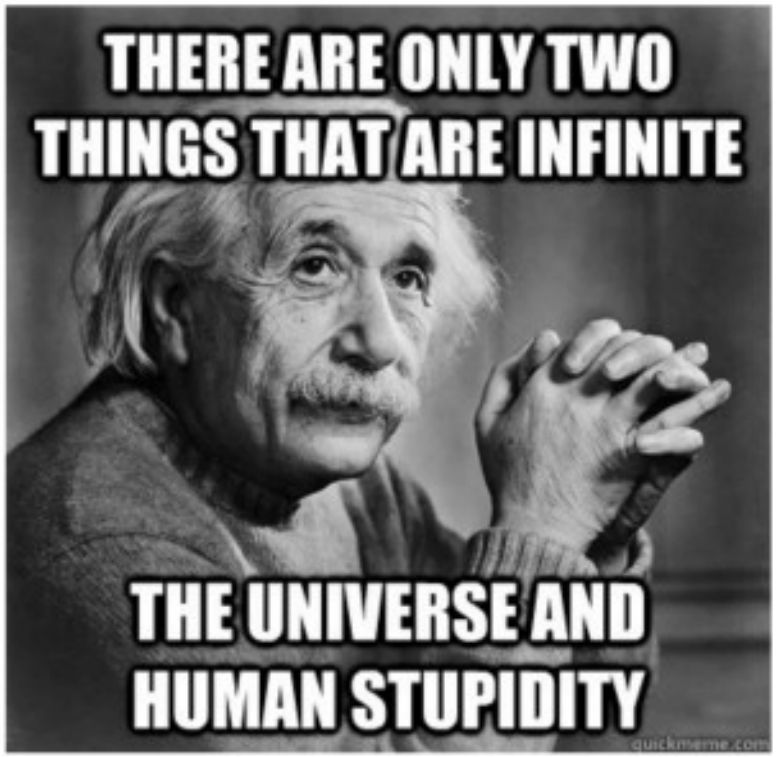
Greenbone – Professionelles Schwachstellen Management

- Einsatzbereit in 10 Minuten
- Appliance versorgt sich selbstständig mit Updates
- Lösung läuft bei Ihnen im Netzwerk (keine Cloud-Abhängigkeit/keine sensiblen Daten in der Cloud)
- Personelle Ressourcen können dort eingesetzt werden, wo sie oft dringender benötigt werden

Nicht alle Angriffsvektoren können technisch entkräftet werden!

Faktor Mensch

- E-Mail Phishing
  - Erschleichen von Zugangsdaten mittels gefälschter Webseiten / gefälschter
- Social Engineering
  - Vortäuschung falscher Tatsachen...
    - mittels Telefon-Anrufen
    - mittels E-Mail Nachrichten
    - mittels persönlicher Kontakte (z.B. in Verkleidung)
  - z.B. CEO-Betrug
- Abhilfe durch Mitarbeiterschulung
  - Wie können Angriffe erkannt werden?
  - Welche Methoden verwenden Angreifer?



Strukturierung von Sicherheits-Maßnahmen

Prozessorientierung

- ISO 27001
  - Aufbau eines ISMS
  - Risiko-Management
  - Vorgabe von Richtlinien
  - Planung + Umsetzung von Sicherheits-maßnahmen
  - Zuweisung von Verantwortung
  - Regelmäßige Überprüfung (Audits)

Wirtschaftskammer Österreich to the Rescue!

www.it-safe.at – Sicherheit für KMU

it-safe.at

- IT-Sicherheitshandbuch für KMU
  - https://www.wko.at/site/it-safe/sicherheitshandbuch.html
- Cyber-Security-Hotline
  - 0800 888 133 (kostenfreie „Erste Hilfe“)
- IT-Security Experts Group
  - 180 aktive Mitglieder
  - Anlaufstelle für Security-Herausforderungen
  - Plattform für Sicherheitsaktivitäten

Kommen Ihnen vielleicht bekannt vor!

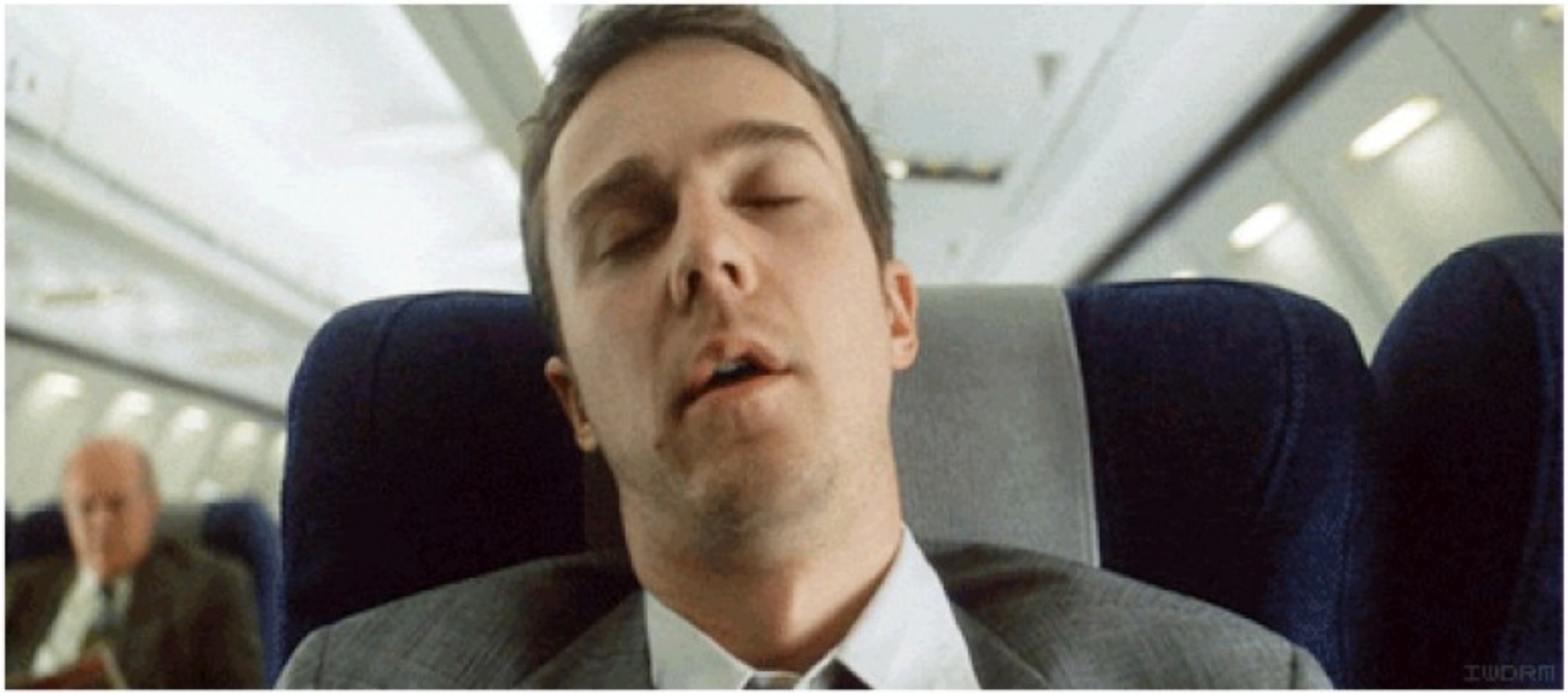
Gartners Top 10 Security Mythen (Famous last Words)

- **It won't happen to me.**
  - Mir passiert das nicht.
- **Infosec budgets are 10% of IT spend.**
  - Das Security-Budget beträgt 10% der IT Ausgaben.
- **Security risks can be quantified.**
  - IT-Sicherheitsrisiken können quantifiziert werden.
- **We have physical security (or SSL) so we know your data is safe.**
  - Weil wir physische Sicherheit (oder SSL) haben wissen wir, dass ihre Daten sicher sind.
- **Password expiration and complexity reduces risk.**
  - Die Gültigkeit und die Komplexität von Passwörtern reduzieren das Risiko.
- **Moving the CISO outside of IT will automatically ensure good security.**
  - Wenn die Rolle des CISO außerhalb der IT besetzt wir, hat man automatisch gute IT-Sicherheit.
- **Adhering to security practices is the CISO's problem.**
  - Die Rolle des CISO muss dafür sorgen, dass alle sicherheitstechnischen Maßnahmen eingehalten werden.
- **Buy this 'tool' and it will solve all of your problems.**
  - Kaufe dieses 'Tool' und es wird alle deine Probleme lösen.
- **Let's get the policy in place and we are good to go.**
  - Definieren wir eine Richtlinie und dann ist alles gut.
- **Encryption is the best way to keep your sensitive files safe.**
  - Mit Verschlüsselung ist alles sicher.

https://www.networkworld.com/article/2167176/gartner-reveals-top-10-it-security-myths.html

Es ist nie zu spät für Veränderung

Vielen Dank für die Aufmerksamkeit!



“If you wake up at a different time, in a different place, could you wake up as a different person?”

Fight Club (1999)