

# FIT FÜR ... meine IT-Sicherheit

**Stefan Hessel, Dipl.-Jur.**

Geschäftsführer der Defendo GbR – Möllers & Hessel



# Über uns

- 2017 als Start-up an der UdS gegründet
- Ziel: Forschung und Praxis in Informatik und Recht verbinden
- Technische und juristische Expertise
- Kunden: Privatunternehmen, Justiz, öff. Verwaltung

# Geschäftsfelder



IT-Sicherheit



Datenschutz



Legal Tech



Vorträge &  
Schulungen

# „Haftungsausschluss“

- Der Vortrag erhebt keinen Anspruch auf Vollständigkeit
- IT-Sicherheit ist kein statischer Zustand
- Der Vortrag kann keine Einzelfall-Beratung leisten

# Warum IT-Sicherheit?

- Vorteile der Digitalisierung ohne unangemessene Risiken nutzen
- IT-Sicherheit ist gesetzliche Verpflichtung
  - DSGVO
  - IT-Sicherheitsgesetz
  - Sorgfaltspflicht der Geschäftsführung
- Fahrlässig oder grob fahrlässig ist es den „Stand der Technik“ nicht zu berücksichtigen

# Relative Sicherheit

- Professionalisierung der Szene
- Angreifer denken oft wirtschaftlich
  - Auch Amateure
- Sicherer als andere Ziele → Greife anderes Ziel an
- „Zu sicher“ → Greife nicht an

# Konsequenz

- „Wert“ der Daten ermitteln
  - Für Angreifer
  - Für mich selbst
  - Imageschaden berücksichtigen
- Schutzmaßnahmen entsprechend aufstellen
- „Einfache“ Kosten-/Nutzen-Rechnung

# Sicherheitsupdates

Upgrading Windows





# Sicherheitsupdates

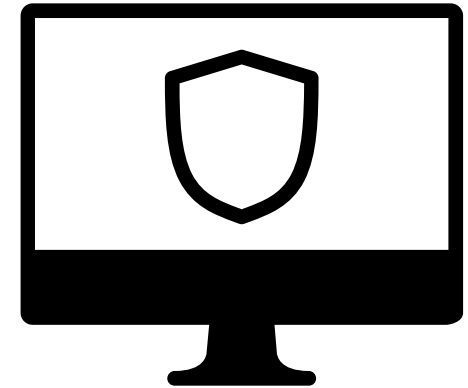
- Lästig, aber unglaublich wichtig
- Schließen Sicherheitslücken
- Problematisch gerade bei Mobilgeräten
- Tipp: Automatische Updates aktivieren

# Demo



# Virenschutz & Firewall

- Virenschutz schützt vor bekannter Schadsoftware
- Windows Defender reicht meist aus
- Firewall schützt vor unerwünschten Netzwerkzugriffen
- In Heimnetzrouter und im Betriebssystem meist integriert



# Sichere Passwörter

- Keine Mehrfachverwendung
- Länge statt Komplexität
- Sicher aufbewahren
- Anlassbezogen ändern
  - Initial
  - Kompromittierung
- Hacks abgleichen: [haveibeenpwned.com](https://haveibeenpwned.com)  
oder <https://sec.hpi.de/ilc>

# Demo

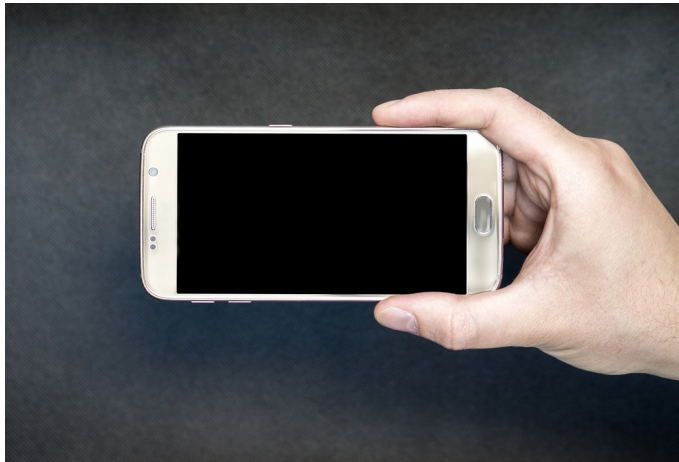


# Nicht als Admin arbeiten!

- Administrator-Rechte erleichtern Angriffe
- Bei mehreren Nutzern: Erschwerte Kontrolle über das Gerät
- Empfehlung: Separates Konto anlegen



# Daten verschlüsseln



- Datenträger-  
verschlüsselung  
schützt wirksam vor  
Diebstahl
- Wichtig  
insbesondere bei  
Mobilgeräten
- Lösungen: Bitlocker,  
VeraCrypt, FileVault

# Demo



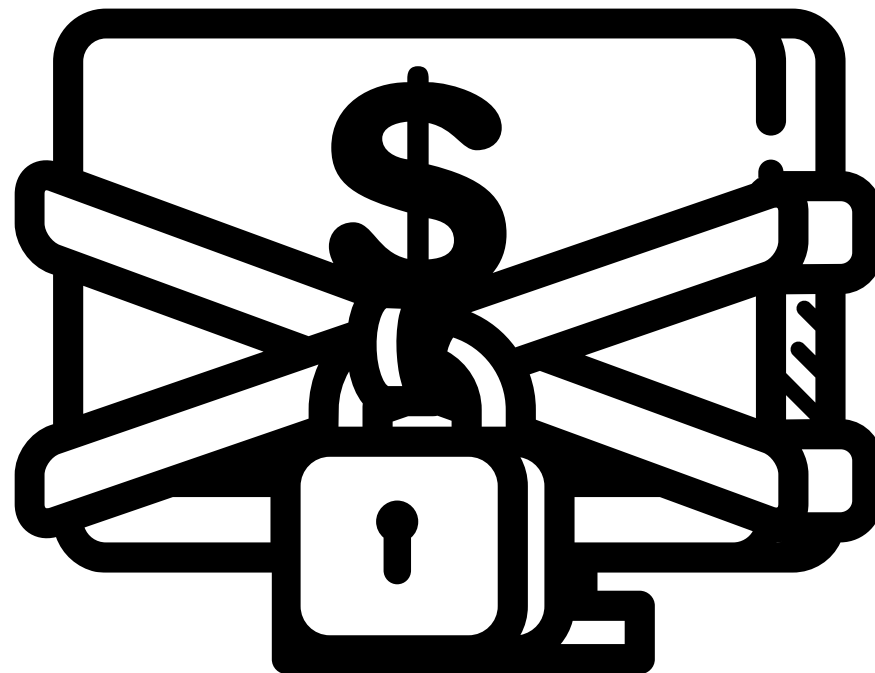


# Backups

- Schutz vor zufälligem Datenverlust
  - z.B. Verschleiß, Feuer, versehentliche Löschung
- Schutz im Fall von Angriffen
  - z.B. Neu-Installation des Systems wg. Trojanerbefall
  - Verschlüsselungstrojaner (sog. Ransomware)

# Ransomware

- Böswillige Verschlüsselung von Daten
- Forderung eines Lösegelds (häufig in Bitcoin)
- Zum Schutz vor Ransomware getrenntes Backup sinnvoll

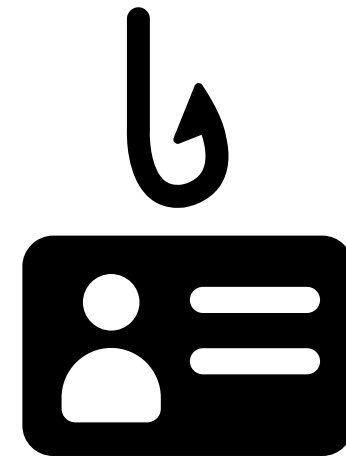


# Demo



# Misstrauisch sein

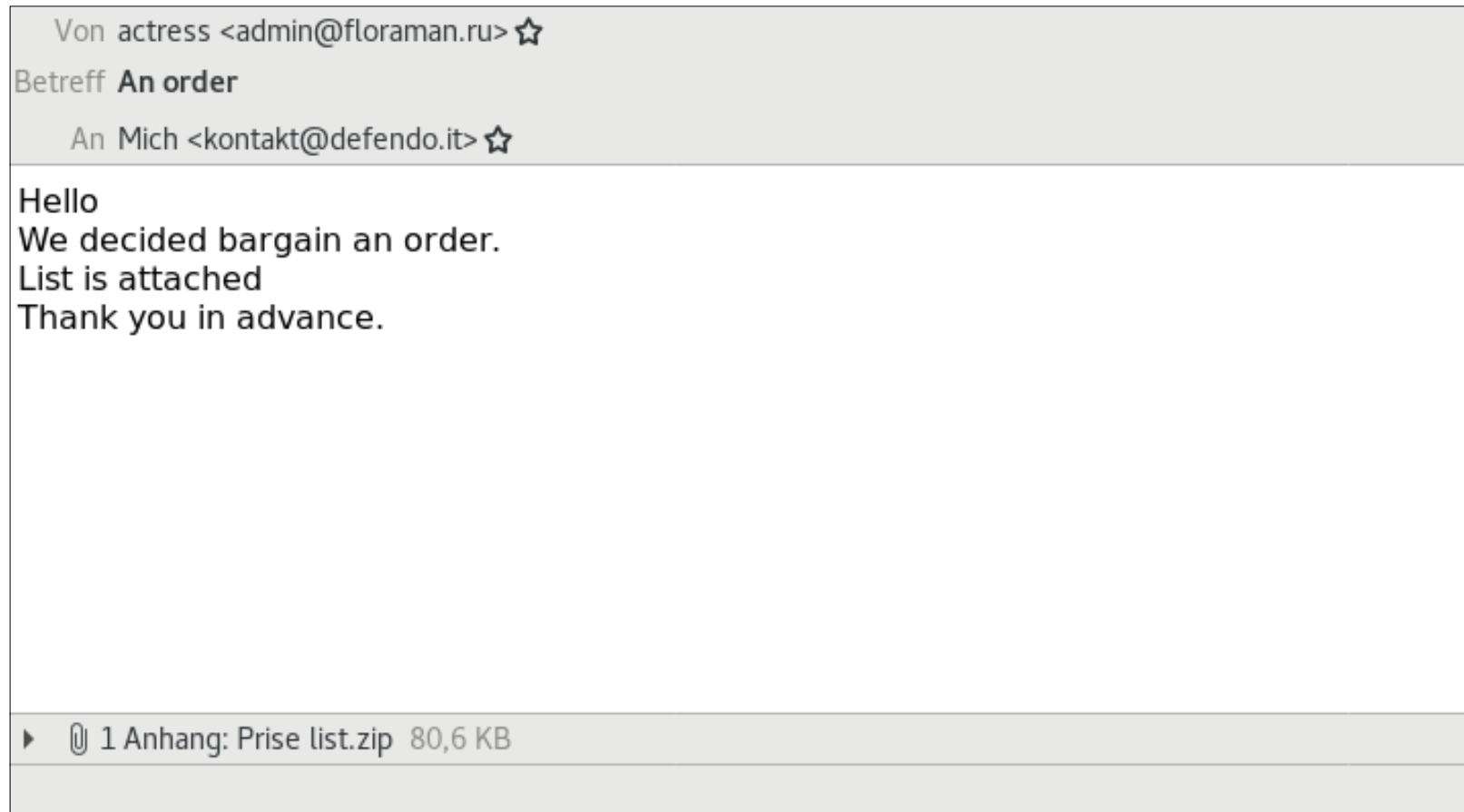
- Immer mehr Angriffe auf den Sicherheitsfaktor „Mensch“ (sog. Social Engineering)
- Technischer Schutz schwierig
- Beispiele:
  - Phishing-Mails
  - Falsche Support-Anrufe
  - USB-Drop
  - Fake-Shops



# Tipps

- Vorsicht bei E-Mails und Anhängen
- Identität oder Anliegen selbst über anderen Kanal (z.B. Anruf) prüfen
- Auf schriftliche Kontaktaufnahme bestehen
- So wenig Informationen wie möglich im Internet preisgeben

# Phishing



# Falsche Supportanrufe

**Verbraucherschützer warnen vor Betrügern, die sich am Telefon als Microsoft-Mitarbeiter ausgeben und falschen Windows-Support anbieten. Die Anrufe kommen häufig von den gleichen gefälschten Telefonnummern.**

Die meisten Heimcomputer laufen auf dem Betriebssystem Windows von Microsoft. Das ruft auch Betrüger auf den Plan. Tatsächlich haben die Fälle, in denen leichtgläubige Windows-Nutzer von falschen Support-Mitarbeiter abgezockt werden, in den letzten Jahren stark zu genommen. Mehr als 7.500 Opfer sollen hierzulande bereits auf die Masche hereingefallen sein, berichtet das Portal [onlinewarnungen.de](http://onlinewarnungen.de).

Die Anrufer sprechen oft nur gebrochen Deutsch oder Englisch mit einem starken Akzent. In Wahrheit sitzen sie in Callcentern in Asien. Der Display zeigt aber eine Rufnummer aus Deutschland, Österreich oder der Schweiz an. Dazu nutzen die Betrüger sogenannte Voice over IP-Anschlüsse (VoIP), bei denen sich die Herkunft des Anrufes leicht verschleiern lässt.

13.08.2018, t-online.de

# Fake-Shops





The screenshot shows a website interface for 'Shopin'. At the top center is the 'Shopin' logo, which consists of a red shopping cart icon above the word 'Shopin' in orange. To the right of the logo is a search bar with the text 'Suche' and a magnifying glass icon. Below the search bar, there is a message: 'Sehr geehrter Besucher, sie können sich **anmelden** oder ein Konto **erstellen**.' Below this is a row of currency symbols: '\$', '\$', 'Col\$', 'kr', '€', '\$', '\$', 'kr', 'zl', '£', '\$', 'kr', 'CHF', '\$'. Below the currency symbols is a horizontal navigation menu with the following items: 'Startseite', 'Damen Pumps', 'Herren Business-Schuhe', 'Herren Freizeitschuhe', 'Niedrige Preismarke', and 'Kontakt'. Below the navigation menu is a section titled 'ANGEBOTE'. Below this section is a row of four product cards. Each card contains an image of a shoe, a small text 'antiquitäten-arr-seeda' below the image, a product description, a price, and a button that says 'In den Warenkorb'. The products are: 1. A red ballerina shoe with gold studs, described as 'A A Klassische Ballerinas von La Ballerina 533481206698' with a price of 43,27€ (original price 209,00€). 2. A grey and tan sandal, described as 'Klassische Pantoletten von Gabor 402334065402' with a price of 45,92€ (original price 235,86€). 3. A brown leather boot, described as 'camel active, Schnürstiefeletten, schwarz 519735832615' with a price of 97,68€ (original price 374,05€). 4. A red and orange Nike sneaker, described as 'Nike Herren Bombax Ic Fußballschuhe - B072XGV6LD' with a price of 70,06€ (original price 320,02€).



# Fazit

- Sicherheitsupdates installieren
- Virenschutz & Firewall aktivieren
- Sichere Passwörter
- Admin- und Nutzerkonten trennen
- Sensible Daten verschlüsseln
- Backups anlegen
- Misstrauisch sein

# Kontakt

-  [www.defendo.it](http://www.defendo.it)
-  [kontakt@defendo.it](mailto:kontakt@defendo.it)
-  0681/41096848
-  @defendo\_it