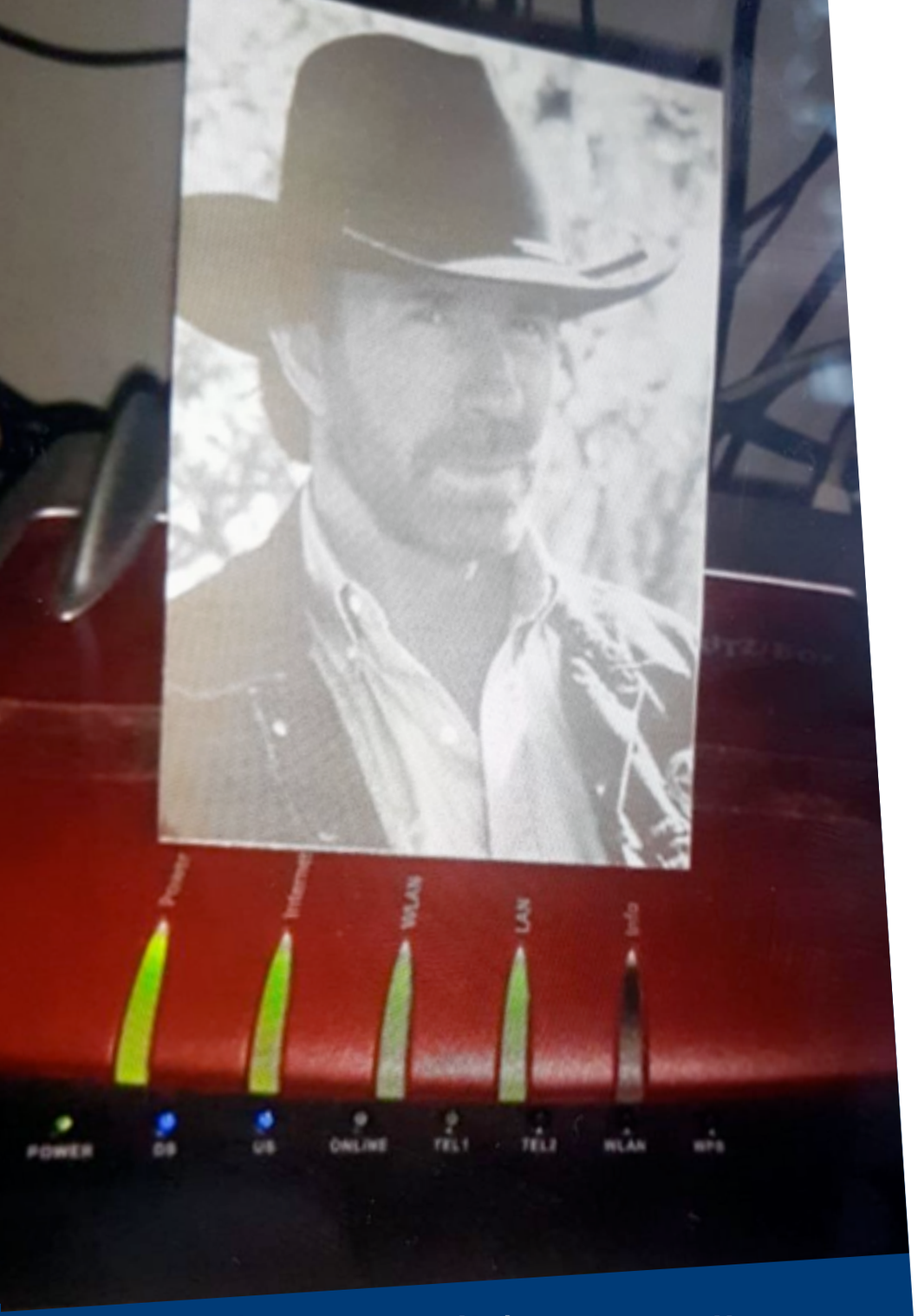


Meine Persönliche Firewall

MediaClick®
Kommunikation und
Software GmbH

IT-Sicherheit

in Web-Anwendungen

Produzieren für Morgen

12. Norddeutsche Fachtagung für die Qualitätssicherung

Markus Roppiler
MediaClick! Kommunikation und Software GmbH

Agenda

- Fakten und Hilfe
- Live Hacking?
- Risiko von Web-Anwendungen
- IT-Sicherheit und Passworte
- DIN ISO 27001
- Anwendungsbeispiele der ISO 27001
- Fazit

MediaClick® Kommunikation und Software GmbH

Fakten zur IT-Sicherheit

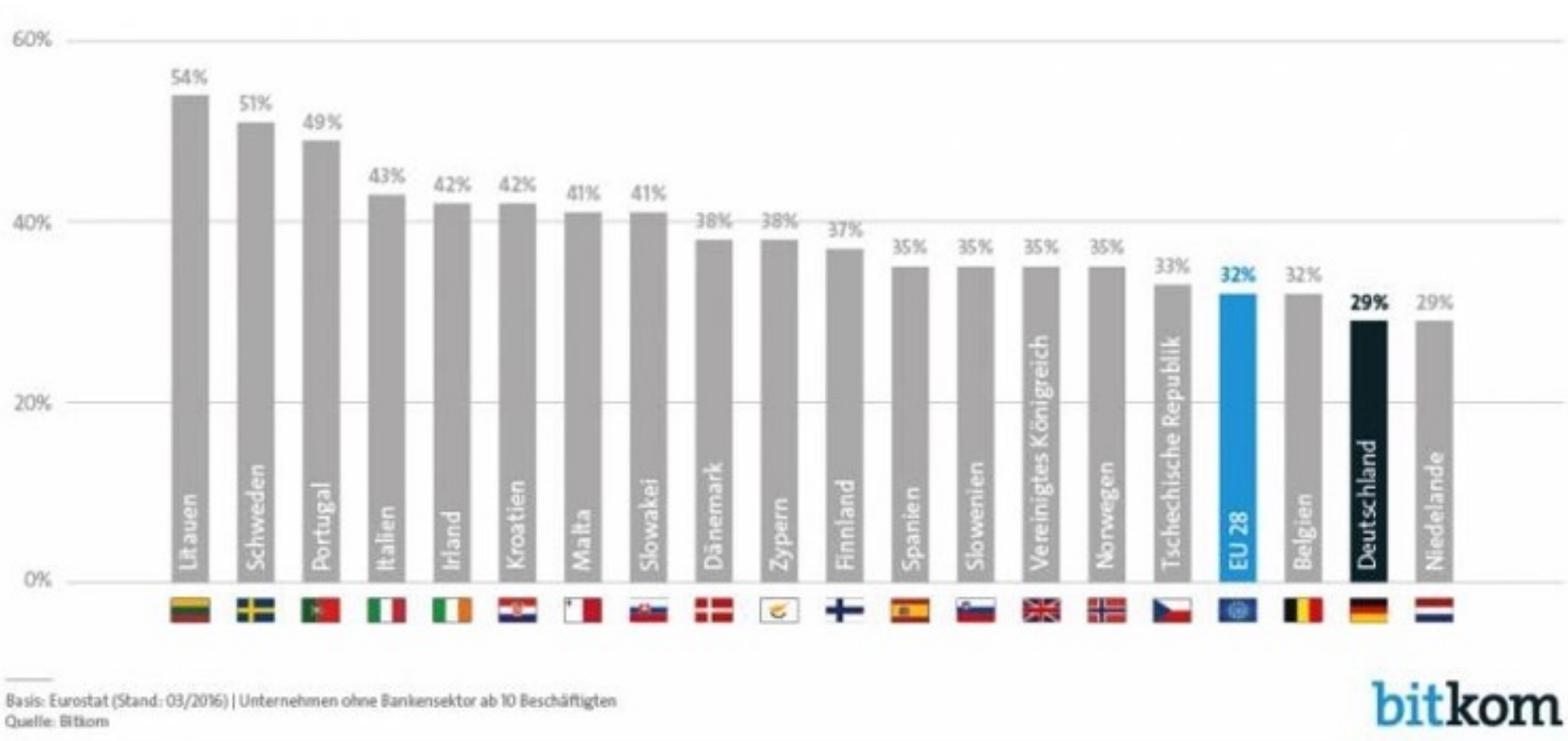
- **Digitale Wirtschaftsspionage in Deutschland:**
  Jedes 2. deutsche Unternehmen wurde zwischen 2013 und 2014 Opfer*.
- **Jährlicher Schaden:**
  Rund 51 Mrd. Euro
- **Maßnahmen:**
  Organisatorische Sicherheit, Personelle Sicherheit, Sicherheitszertifizierungen

---

*) Umfrage der Bitkom: 1.074 Unternehmen ab 10 Mitarbeitern

Fakten zur IT-Sicherheit

Anteil der Unternehmen mit einer formell festgelegten IT-Sicherheitspolitik (in Prozent)



Basis: Eurostat (Stand: 03/2016) | Unternehmen ohne Bankensektor ab 10 Beschäftigten
Quelle: Bitkom

bitkom

Staatliche Unterstützung

- BSI:

  Bundesamt für Sicherheit in der Informationstechnik

- Jährlicher Lage- / Gefährdungsbericht:

  Cloud-Computing:
  Große Kumulation von sensiblen Daten, aber relativ gute Pflege

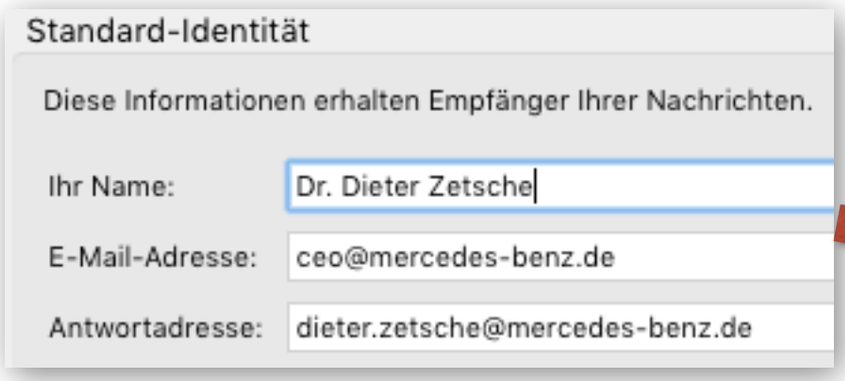
  Desktop-Software:
  Größte Schwachstellen: Adobe Reader, Flash Player sowie Apple OS X.

  Mobilkommunikation:
  Veraltete BS (besonders Android), ungeprüfte Apps im Store, öffentliche Hotspots, Ortung in Mobilfunknetzen durch Dritte, Telefonate nicht abhörsicher

- DIN ISO/IEC 27001 und 27002

Live-Hacking?

- Diesmal nicht
- Aber, was ist CEO-Betrug?
- Glauben Sie E-Mail Absendern?



MediaClick® Kommunikation und Software GmbH

Was ist eine Web-anwendung?

- Unverzichtbares Medium:

  soziale Dienste, Lesen und Versenden von E-Mails, Online-Shopping, Internet-Banking, Auktionen,…

- begehrtes Angriffsziel:

  Eingabefelder für Code, unverschlüsselte FTP-Zugänge, Platz 1 des DBIR*

- Kaum Schutz durch etablierte Sicherheitsmaßnahmen

  z.B. Firewalls

---

*) Data Breach Investigation Report: 42.000 Sicherheitsvorfälle in 20 Branchen und 84 Ländern.

Risiko von Web-anwendungen

- Individuell entwickelt
- direkte Verbindung zu Datenbankserver
- Rund um die Uhr öffentlich verfügbar
- wenig Sensibilität für Schutzmaßnahmen

  z.B. Verwendung von SSL
- Open Web Application Security Project (OWASP)

Angriffs-techniken auf Weban-wendungen

MediaClick®
Kommunikation und
Software GmbH

SQL-Injection

Normal:

`http://shop.de/books.php?ID=60`

Manipuliert:

`http://shop.de/books.php?ID=60;UPDATE+USER+SET+TYPE=”administrator“`

Fehler bei Authentifizierung und Session-Management

`http://fluege.de/booking;sessionid=FFDD349XVDDFLKDG?dest=Wien`

Cross Site Scripting (XSS)

z.B.: Cookie-Grabber, um in einem Forum Cookies zu sammeln

Tipps für mehr IT-Sicherheit

1. Regelmäßige Updates
2. Der Umgang mit Passwörtern
3. Backups
4. Browser aktualisieren / härten
5. Awareness (Hirn einschalten)
6. ISMS

MediaClick® Kommunikation und Software GmbH

Passwörter

- Altbekannte Regeln:
  Alle 5 Wochen wechseln
  Mindestens 8 Zeichen
  Mind. 1Klein-, 1Großbuchstabe, 1Sonderzeichen, 1Ziffer
  Keine Jahreszahlen, Vornamen, etc.
  Niemals auf Zetteln in Computernähe
- Geänderte neue Erkenntnisse*)

  Verwendung von Wortlisten (Diceware)

  mehrere Worte würfeln und verbinden

  Bsp.: `merken boom ekd zonen ragt hurra`

MediaClick® Kommunikation und Software GmbH

DIN ISO 27001, 27002

- Nutzung von Management-Prozessen
- Grundsätze:
  Bewusstsein, Verantwortung, Reaktion, Risikoeinschätzung, Sicherheitsgestaltung, Sicherheitsmanagement, Neufestlegung
- Sicherheit als Managementprozess:

  Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung

  ISMS als strategische Entscheidung
- 27001 = Anforderungsstandard
- 27002 = Umsetzungsleitfaden

konkrete Anwendung der ISO 27001

Thema Passwörter

- Benutzer-Zugänge von Ex-Mitarbeitern
- Auffinden alter Zugangsdaten in DB einer Web-Anwendung
- Schlampigkeit / Sicherheitslücke
- ISO 27001, Anhang 9.2.6:

  Entzug oder Anpassung von Zugangsrechten

MediaClick® Kommunikation und Software GmbH

konkrete Anwendung der ISO 27001

Thema Datensicherung

- Anhang 12.3: Erstellung eines Datensicherung-Plans

  …dokumentiertes Wiederherstellungsverfahren

  Aufbewahrung an einem externen Ort

  Schutz vor physischen und Umweltfaktoren

  Regelmäßige Prüfung der Medien

  Evtl. Verschlüsselung

- Audit könnte z.B. Schreibrechte auf Sicherungen feststellen…

MediaClick® Kommunikation und Software GmbH

Fazit

Web-Anwendungen sind verbreitet und gefährdet

Wichtig: Updates, Awareness, Gefahr durch E-Mail

Auf aktuellem Stand bleiben

Anti-Viren-Software (AV-Scanner) nicht immer beste Möglichkeit

ISO 27001 aufwendig, aber wirkungsvoll

Danke für Ihre Aufmerksamkeit

Fragen?

roppiler@mediaclick.de

MediaClick®
Kommunikation und
Software GmbH