# Gefahr durch Cookies

**Antonio Kulhanek**
Security Consultant
Dipl. Techniker HF, Kommunikationstechnik
MCSE, ITIL Foundation
kulhanek@goSecurity.ch



goSecurity
EXPERTEN FÜR IHRE IT-SICHERHEIT

# Rechtliche Hinweise

- **Art. 143 StGB „Unbefugte Datenbeschaffung“**
  Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, sich oder einem andern elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind, wird mit Zuchthaus bis zu fünf Jahren oder mit Gefängnis bestraft.

- **Art. 143$^{bis}$ StGB „Unbefugtes Eindringen in ein Datenverarbeitungssystem“**
  Wer ohne Bereicherungsabsicht auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.

# Rechtliche Hinweise

- **Art. 144$^{bis}$ StGB „Datenbeschädigung“**
  [1] Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft. Hat der Täter einen grossen Schaden verursacht, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden. Die Tat wird von Amtes wegen verfolgt.

  [2] Wer Programme, von denen er weiss oder annehmen muss, dass sie zu den in Ziffer 1 genannten Zwecken verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonstwie zugänglich macht oder zu ihrer Herstellung Anleitung gibt, wird mit Gefängnis oder mit Busse bestraft. Handelt der Täter gewerbsmässig, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden.

# Themen

- Cookies allgemein
- Tracking
- Cookies stehlen
- Persistent XSS
- Wichtige Massnahmen

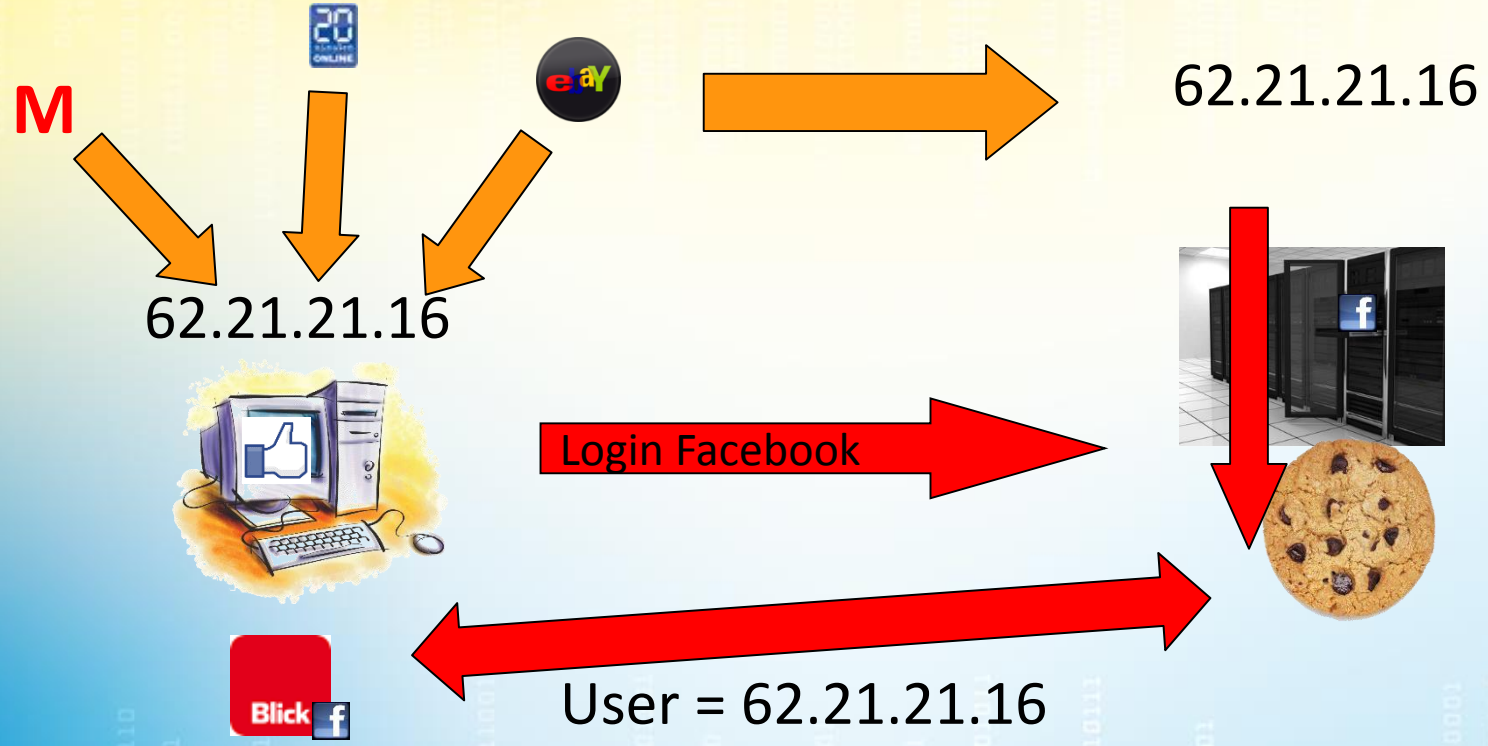
# Cookies

- HTTP-Cookies
  - Spezifiziert im RFC 6265 (Stand 2011)
  - Wird über den HTTP-Header übertragen
  - Kommt auch bei anderen Skriptsprachen zum Einsatz (JavaScript, Flash)

- Supercookies
  - Web Storage
    - Weiterentwicklung, Speicherplatz pro Domain (5-10MB)
  - Flash Cookies
    - Inhalte Browserunabhängig speichern, ohne Verfallsdatum, schwierig zu löschen
    - Datenschutzrechtlich problematisch

# Cookie Tracking

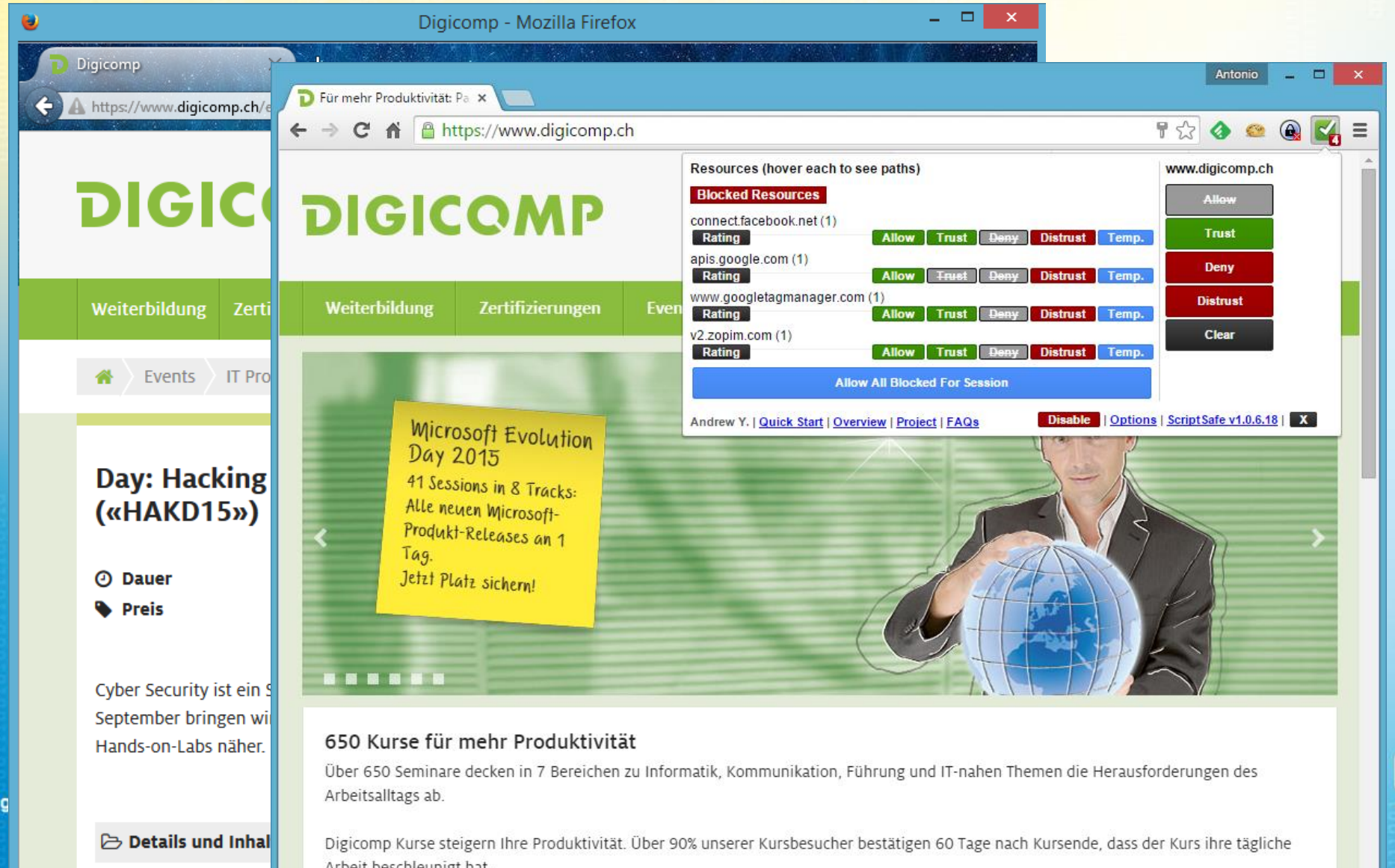
# Cookie Tracking




# Cookie Tracking

- Demo Lightbeam

# Schutz vor Cookie Tracking



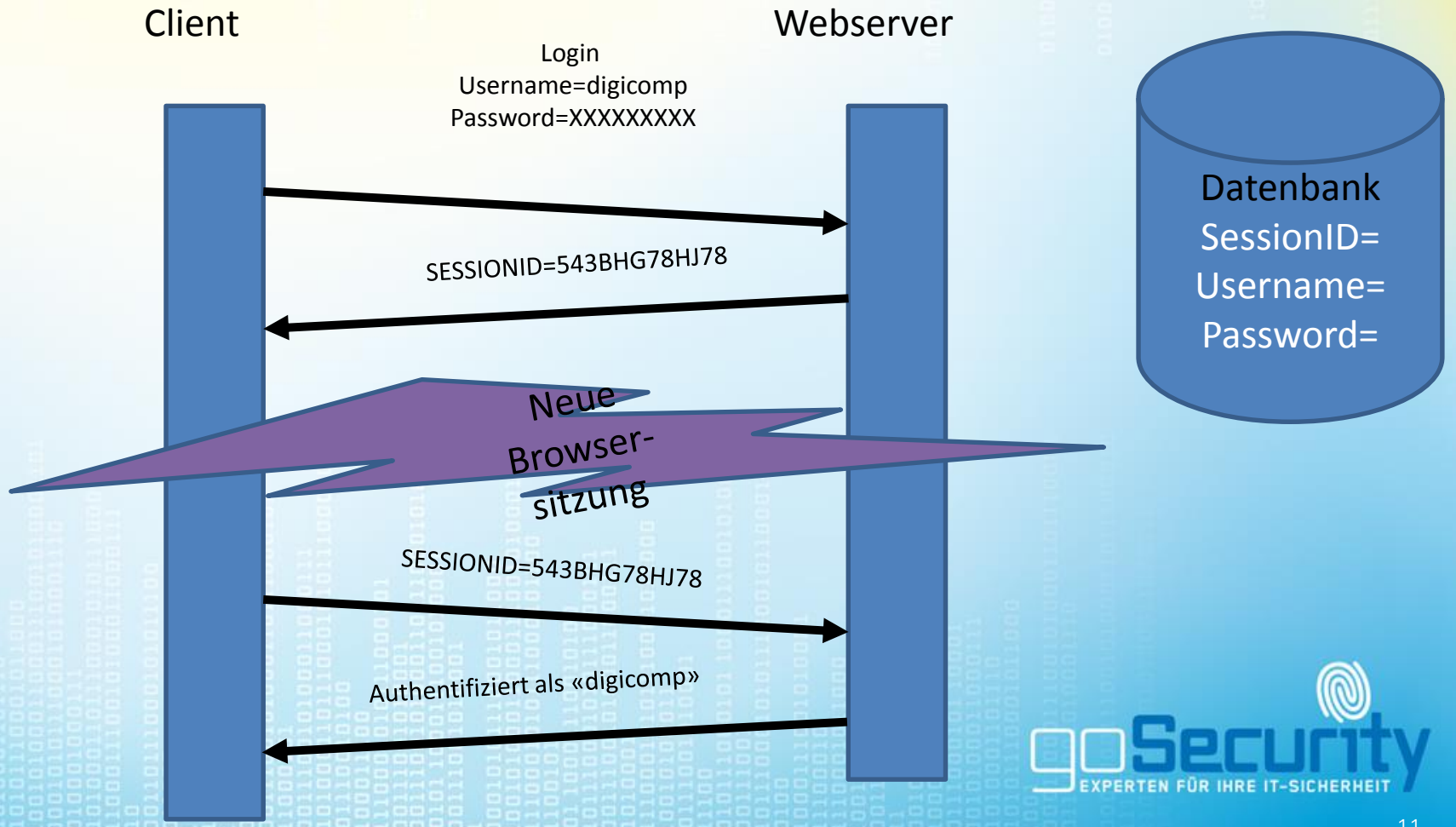

goSecurity
EXPERTEN FÜR IHRE IT-SICHERHEIT

# Session Hijacking

- Session eines angemeldeten Benutzers «klauen»
  - Man-in-the-Middle-Angriff
  - Persistent XSS Schwachstelle in einer Webseite

# Session Hijacking

- Demo MitM



# Session Hijacking

- HTTPS für die gesamte Webseite einsetzen
- Vertrauenswürdige Zertifikate verwenden
- Aktuelle Empfehlungen zur SSL-Sicherheit beachten

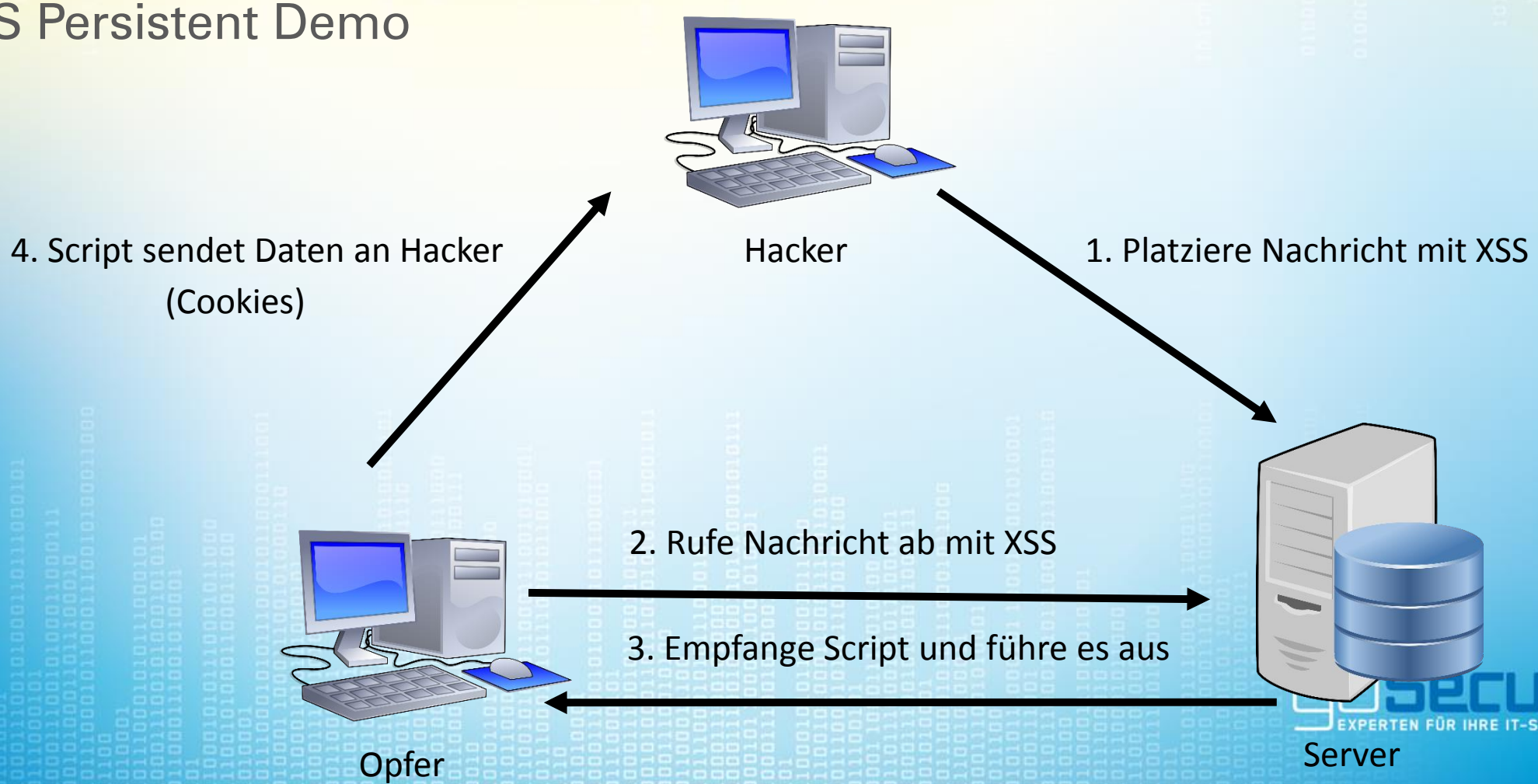
| Ciphers | | Protokolle | | |
|---|---|---|---|---|
| Algorithmus | Stärke | TLSv1 | TLSv1.1 | TLSv1.2 |
| AES-GCM | 256, 128 | | | sicher |
| AES-CCM | | | | sicher |
| AES-CBC | | | sicher | sicher |
| Camellia-GCM | 256, 128 | | | sicher |
| Camellia-CBC | | | sicher | sicher |
| ARIA-GCM | 256, 128 | | | sicher |
| ARIA-CBC | | | sicher | sicher |
| SEED CBC | 128 | | sicher | sicher |
| GOST-28147-89-CNT | 256 | sicher | sicher | sicher |
| IDEA-CBC | 128 | | sicher | |
| ChaCha20-Poly1305 | 256 | | | sicher |

Stand September 2015

- OWASP: Session Management

# Session Hijacking

- XSS Persistent Demo



# Session Hijacking

- XSS
  - CMS und Plugins regelmässig aktualisieren
  - Eigene Plugins auf XSS-Schwachstellen testen

# Session Hijacking

- HTTP und HTTPS Angriffe automatisieren
  - HTTPS über Angreifer auf HTTP umleiten
  - HSTS umgehen (wwww.google.com)

Tools:

| | |
|---|---|
| sslstrip | > Hijack HTTPS trafffc |
| mitmf | > Kombiniert MitM mit HTTPS Hijack |
| mana-toolkit | > Kombiniert MitM **über WLAN** mit HTTPS Hijack |

# Massnahmen

- Tracking
  - Skript- und AD-Blocker verwenden
  - Vorsicht im Umgang mit persönlichen Daten
- Hijacking Clientseitig
  - IMMER auf HTTPS achten
- Hijacking Serverseitig
  - HTTPS
  - CMS und Plugins regelmässig aktualisieren
  - Session Management verbessern

# Nützliche Tools

- Your online Choices (Tracking)
  http://www.youronlinechoices.com/ch-de/
- Firefox, Lightbeam (Tracking)
  https://www.mozilla.org/de/lightbeam/
- Firefox BetterPrivacy (Flash Cookies)
  https://addons.mozilla.org/de/firefox/addon/betterprivacy/
- Firefox ADD-ONS, NoScript
  https://addons.mozilla.org/de/firefox/addon/noscript/
- Chrome Web Store, ScriptSafe
  https://chrome.google.com/webstore/detail/scriptsafe/
- OWASP Session Management
  https://www.owasp.org/index.php/Session_Management_Cheat_Sheet

# Informieren Sie sich!

- http://www.melani.admin.ch
  - Infoseite zu den Gefahren im Internet
- http://www.ebankingabersicher.ch
  - Infoseite für sicheres e-Banking
- http://www.geschichtenausdeminternet.ch
  - Infoseite zu den Gefahren im Internet
- http://www.switch.ch/de/saferinternet/
  - Sichere Websites für ein sicheres Internet

# Experten für Ihre IT-Sicherheit


A. Wisler


Th. Furrer


S. Müller


A. Kulhanek


M. Hamborgstrøm


M. Hennet


C. Wehrli


S. Walser

# Unsere Dienstleistungen