GOETHE UNIVERSITÄT FRANKFURT AM MAIN

ATHENE National Research Center for Applied Cybersecurity

Wie Hacker Sicherheitslücken für Cyberangriffe missbrauchen und was Zero Trust verbessern kann

Prof. Dr. Haya Schulmann

ATHENE | Goethe-Universität Frankfurt a.M.

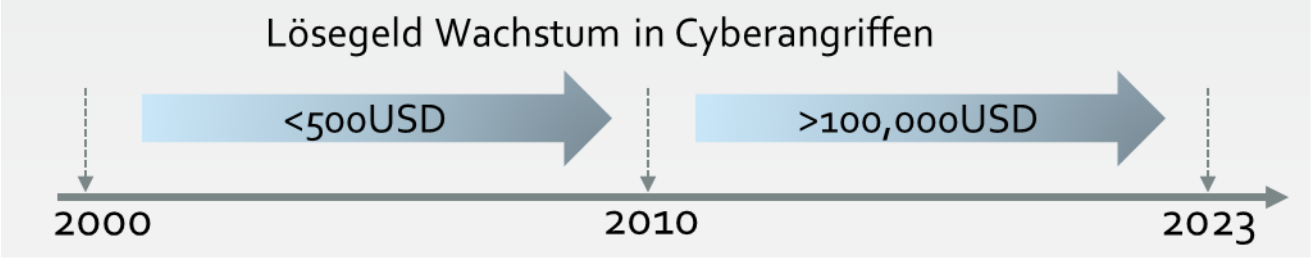
Ringvorlesung Cybersicherheit
Wiesbaden, 29. November 2023

„Die Bedrohungslage im Cyber-Raum ist angespannt, dynamisch und vielfältig und damit so hoch wie nie.“

Bundesamt für Sicherheit in der Informationstechnik

Nov. 2023

- Digitalisierung und Fortschritte in der Informationstechnologie vergrößern die Angriffsoberfläche und das Schadenspotenzial



- Geopolitische Konflikte und wirtschaftliche Lage erhöhen die Motivation für Cyberangriffe

bitkom research

Sept. 2023

„206 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen“

Sicherheitsstudien – Werkzeuge und Lagebilder

- **Entwicklung von Werkzeugen**
  zum Finden von Schwachstellen
  in Netzen, HW, SW, Diensten

- **Nicht-intrusive groß angelegte Studien**
  - Politische Parteien (2020)
  - Forschungsorganisationen (2022)
  - Bundesländer (2022)
  - KMUs (2020-2022)
  - und so weiter …

Studie der 16 Bundesländer (2022)

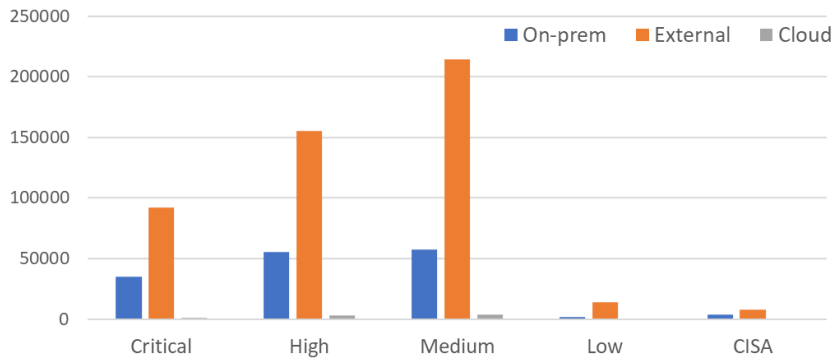
Schwächen im IT-Management: veraltete SW, Domänen auf schwarzen Listen, …

- Geringe Cloudnutzung
- > 25.000 Software-Komponenten mit Sicherheitslücken
- >10% von 40.000 sind ungültige Zertifikate
- >1000 Abhängigkeiten von Assets eines Landes zu externen Assets mit bekannten kritischen Sicherheitslücken
- 92 kritische Probleme + mehrere laufende Angriffe

Studie der 16 Bundesländer (2022)

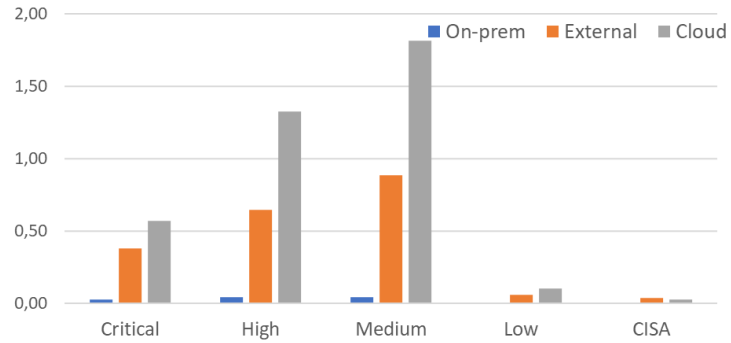
Die Verwaltung der IT-Infrastruktur on-premise ist besser

Software und Versionen

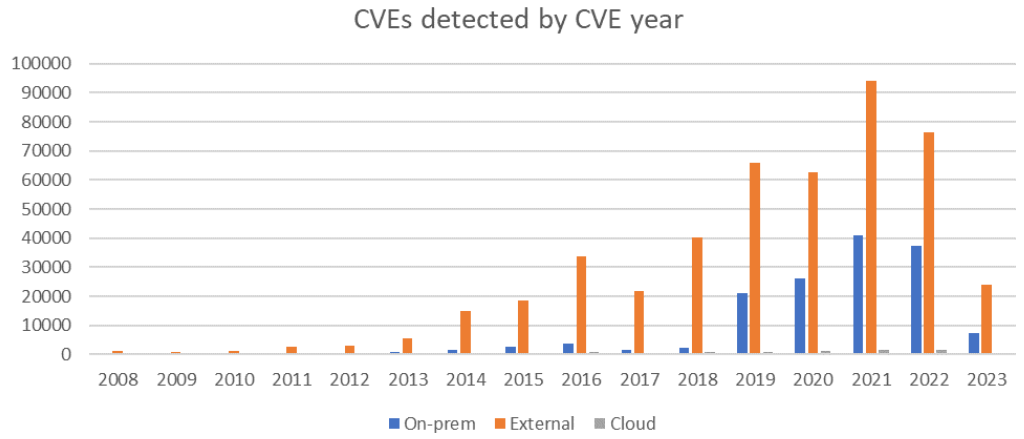


CVE Kritikalität

Software und Versionen / #Assets in Hosting-Modell



CVE Kritikalität



#Gefundene CVEs pro Jahr der Entdeckung

Studie der 16 Bundesländer (2022)

Angreifbare IT: Geheime Schlüssel, Passwörter, Konfigurationen & Backup-Dateien, Tokens, DB Dumps, …

*.env Datei enthält Umgebungsvariablen des Benutzers

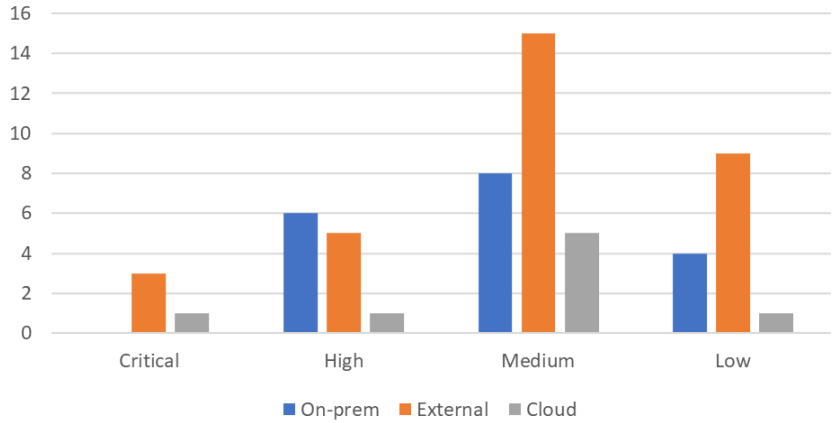
[redacted] .env

```
# The environment Craft is currently running in ('dev', 'staging', 'production', etc.)
ENVIRONMENT="production"

# The secure key Craft will use for hashing and encrypting data
SECURITY_KEY="[redacted]

# The database driver that will be used ('mysql' or 'pgsql')
DB_DRIVER="mysql"

# The database server name or IP address (usually this is 'localhost' or '127.0.0.1')
DB_SERVER="db1"

# The database username to connect with
DB_USER=[redacted]

# The database password to connect with
DB_PASSWORD=[redacted]

# The name of the database to select
DB_DATABASE=[redacted]

# The database schema that will be used (PostgreSQL only)
DB_SCHEMA="public"

# The prefix that should be added to generated table names (only necessary if multiple things are sharing the same database)
DB_TABLE_PREFIX=""

# The port to connect to the database with. Will default to 5432 for PostgreSQL and 3306 for MySQL.
DB_PORT=""
```

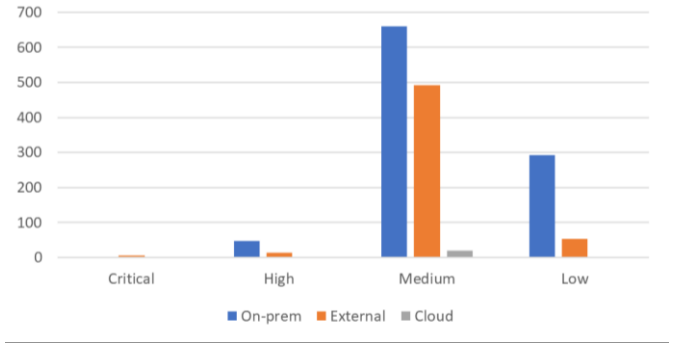
Beispiel: .private Key

```
-----BEGIN RSA PRIVATE KEY-----
[redacted]
2+nCVmFgWUjXzCH6OMrg9358Bo/CLcVrIcTR7trg6w==
-----END RSA PRIVATE KEY-----
```

Betroffene Bundesländer



Data Exposure



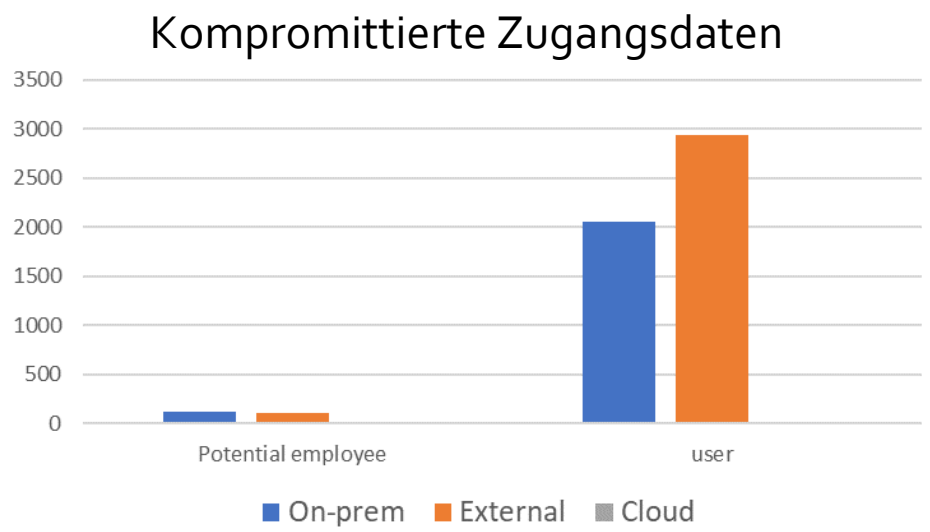
Studie der 16 Bundesländer (2022)

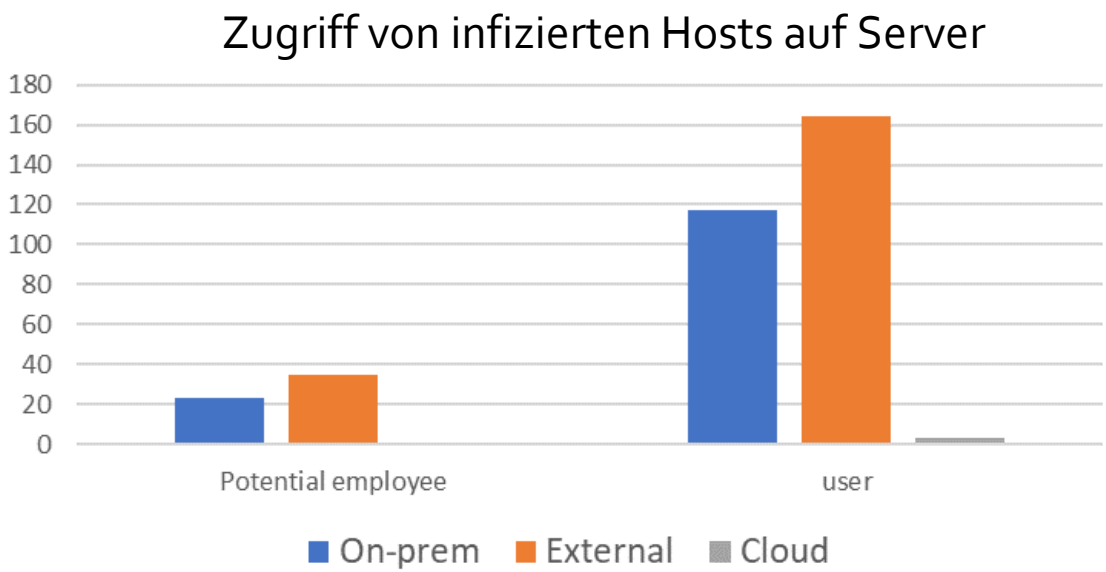
Entdeckte Kompromittierungen und laufende Angriffe

- Mit Schadsoftware infizierte Hosts
- Kompromittierte Zugangsdaten
- Manipulation von Daten und Konfigurationen auf Servern
- Code Injection-Angriffe
- Erzeugen von Webseitenverkehr
- Manipulation von Suchmachinenergebnissen
- Übernahme von „„stale Ressourcen“,

Studie der 16 Bundesländer (2022)

Kompromittierte Zugangsdaten und infizierte Hosts

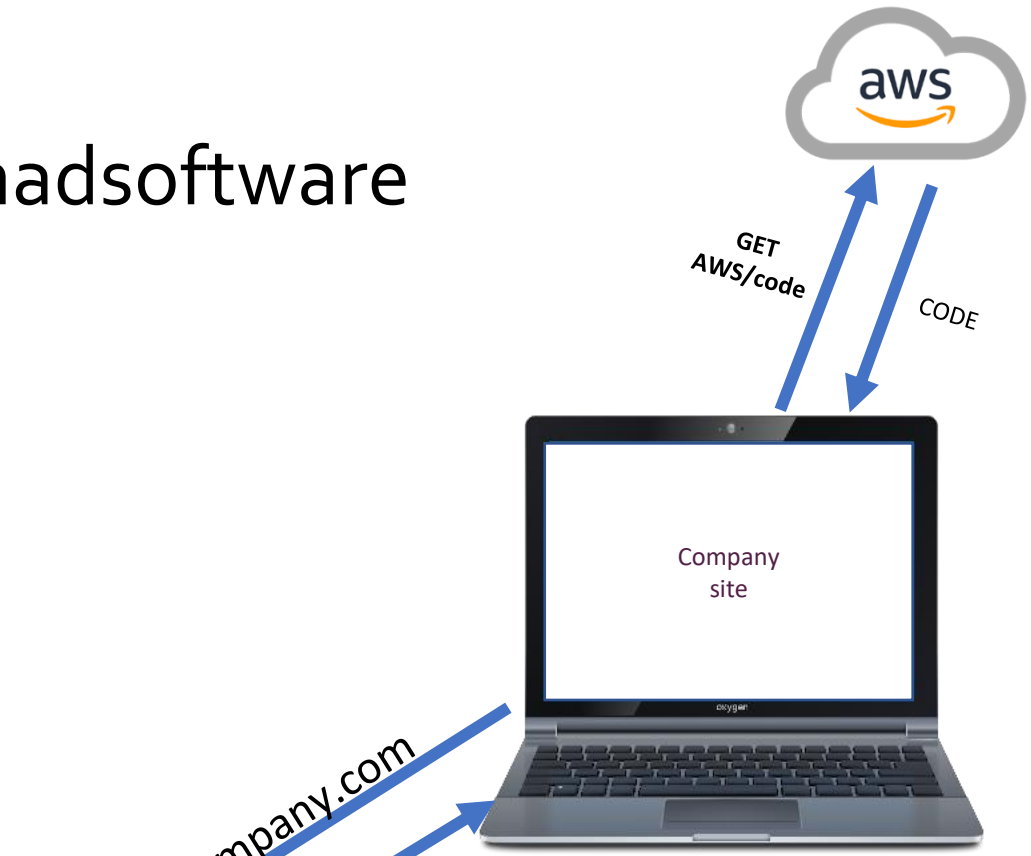




Code Injection Angriffe
Datendiebstahl, Verteilung von Schadsoftware

- Angriff auf Dritten →
  Kompromittiertes Javascript wird von dort heruntergeladen
- Code des Dritten wird in Webseite eingebunden
- Wie kann man damit Daten vom Client stehlen?
  - Schwachstellen in der Webseite
  - Fehlkonfigurierter S3 Bucket
  - Stale/released Ressourcen
- Daten des Clients gehen zum Server des Angreifers
  - Kreditkarten, Passwörter, Cookies, …
    -

Company server

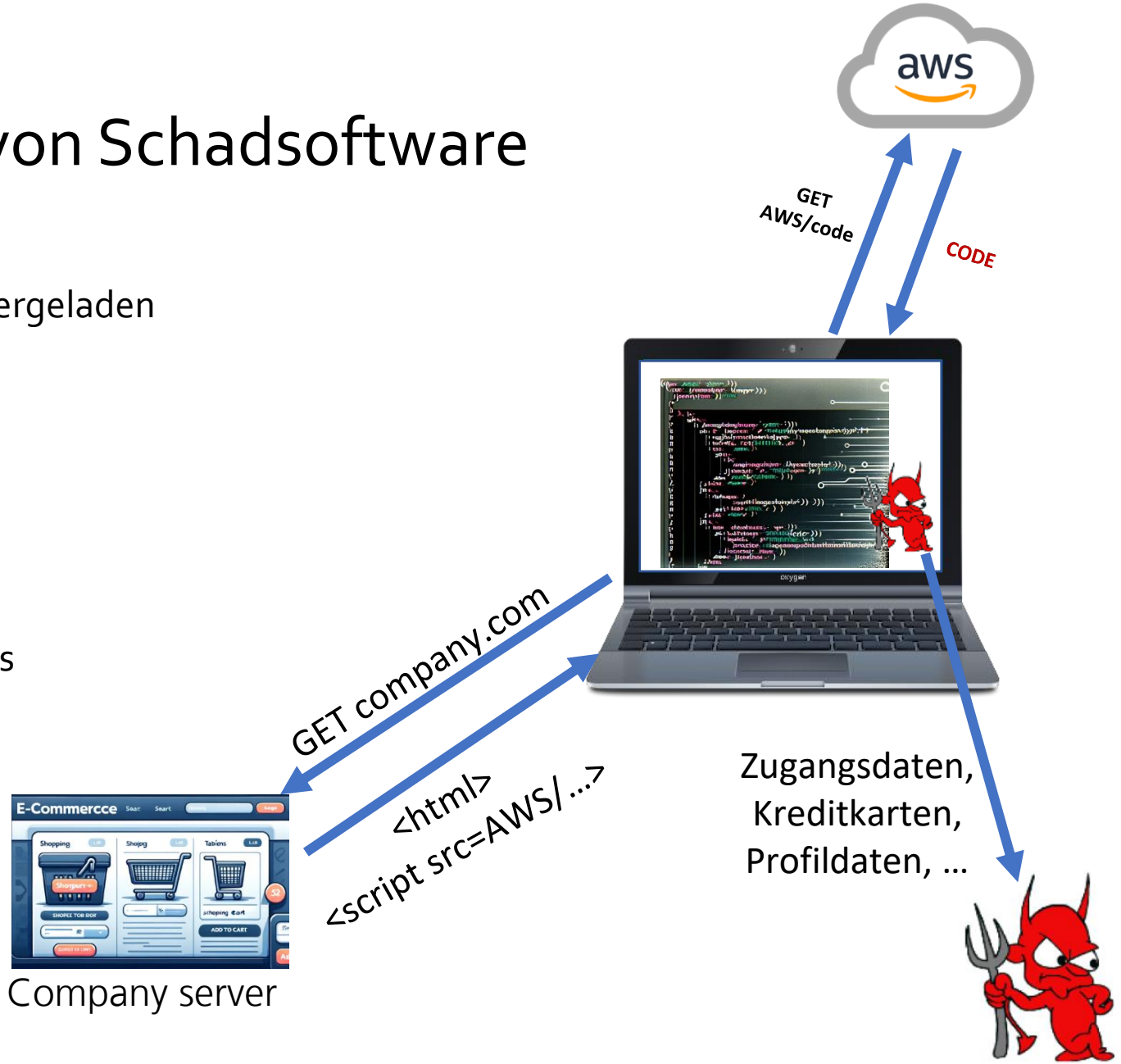


Code Injection Angriffe
Datendiebstahl, Verteilung von Schadsoftware

- Angriff auf Dritten →
  Kompromittiertes Javascript wird von dort heruntergeladen
- Code des Dritten wird in Webseite eingebunden
- Wie kann man damit Daten vom Client stehlen?
  - Schwachstellen in der Webseite
  - Fehlkonfigurierter S3 Bucket
  - Stale/released Ressourcen
- Daten des Clients gehen zum Server des Angreifers
  - Kreditkarten, Passwörter, Cookies, …

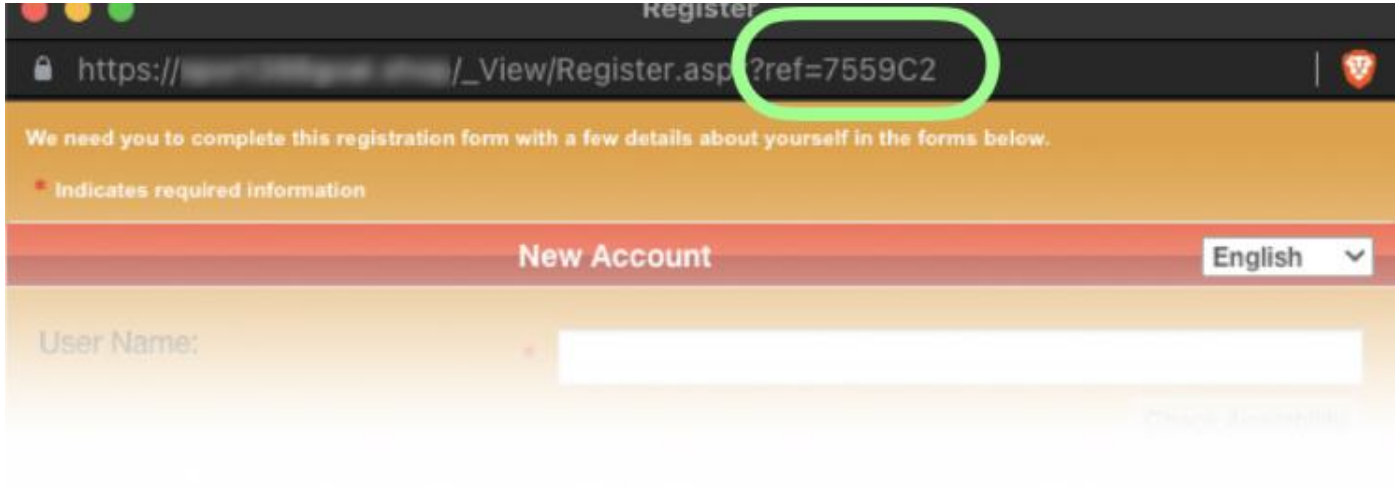
Gefahr durch Drittanbieter-Scripte

British-Airways-Hack: 205 Millionen Euro Strafe



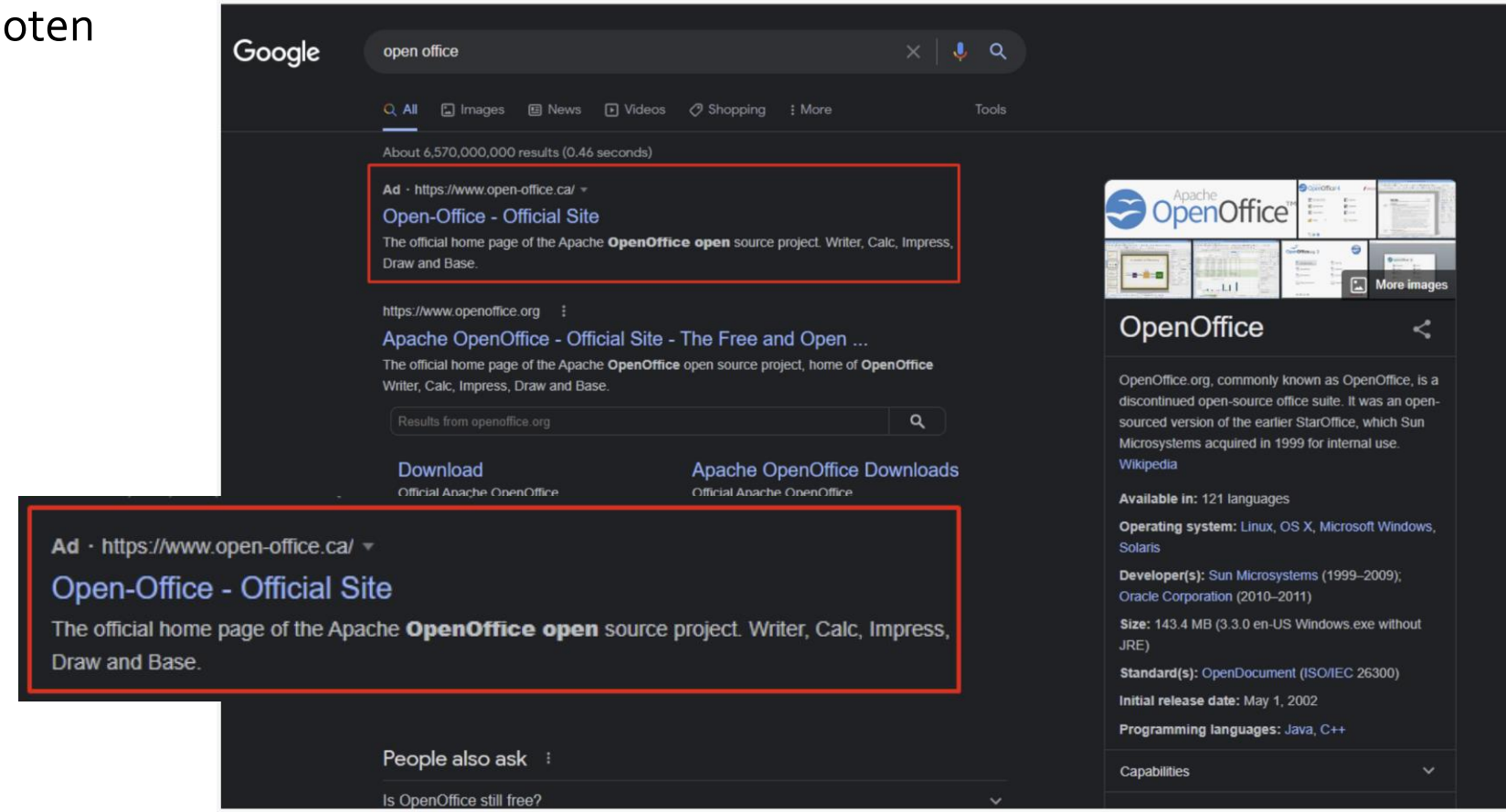
Erzeugen von Webseitenverkehr

Clients abfangen, die eine beliebte Domäne besuchen, um dadurch einen finanziellen Gewinn zu erzielen



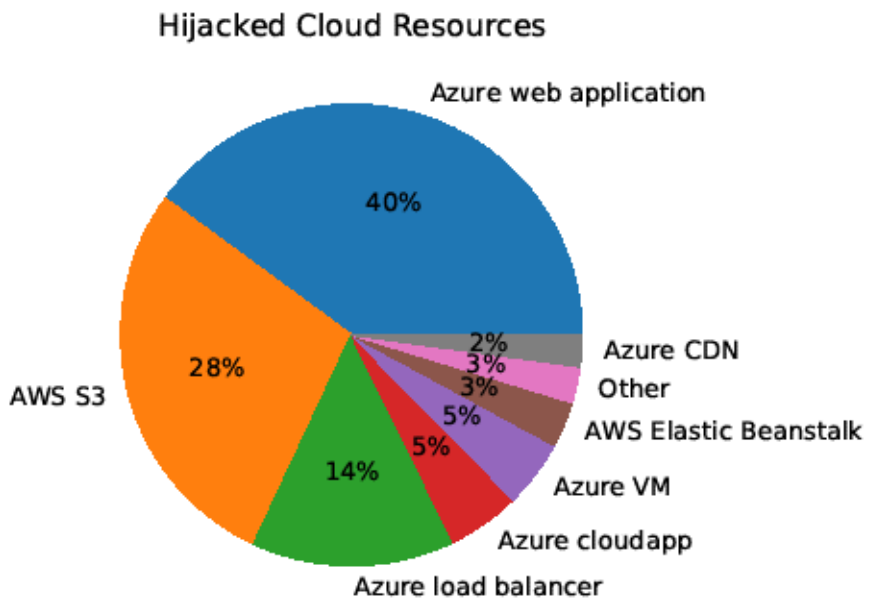
Manipulation von Suchmaschinenergebnissen
Um Schadsoftware zu verteilen über gefälschte Webseiten

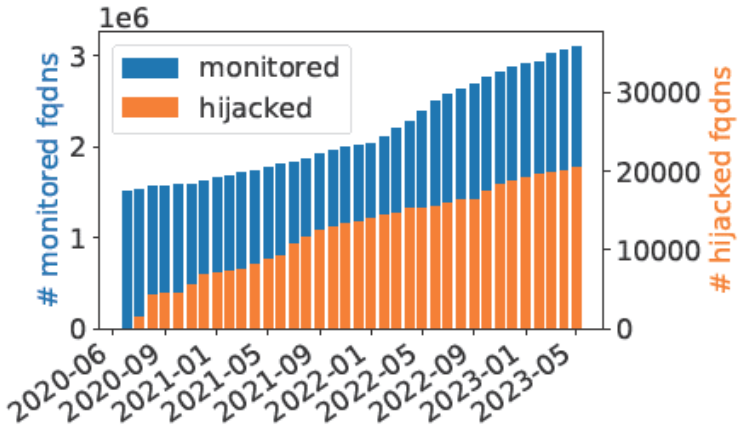
- 2628 Seiten mit Download-Angeboten
- 181 verschiedene Android- (.apk) and Windows-Apps (.exe)
- Virus Total erkannte **nur zwei** davon als Trojaner



Ad · https://www.open-office.ca/
Open-Office - Official Site
The official home page of the Apache **OpenOffice open** source project. Writer, Calc, Impress, Draw and Base.

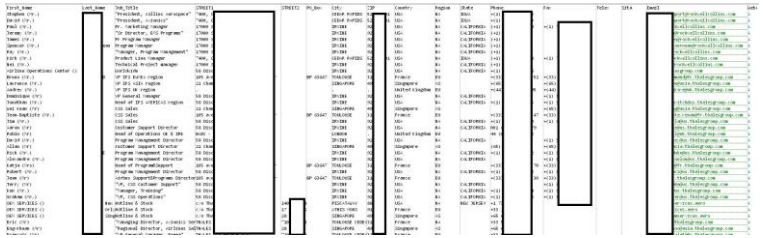
Übernahme von „stale Ressourcen“ und auch in der Cloud





Ziele: Zugangsdaten Diebstahl (SSO/VPN/RDP/…) , Cookies Diebstahl, persönliche Daten, Schadsoftware Verteilung, ….

Airbus Cyberattack (Sept. 2023)
Hacker „USDoD" veröffentlicht Datensätze von 3200 Mitarbeitern von Airbus-Kunden



Infostealer Malware

↓ **Verändertes .net**

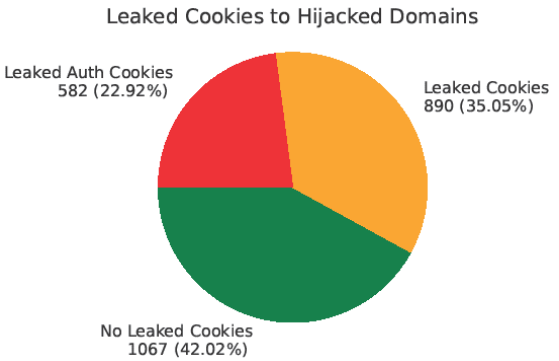
TURKISH AIRLINES

↓ **Passwort**

AIRBUS

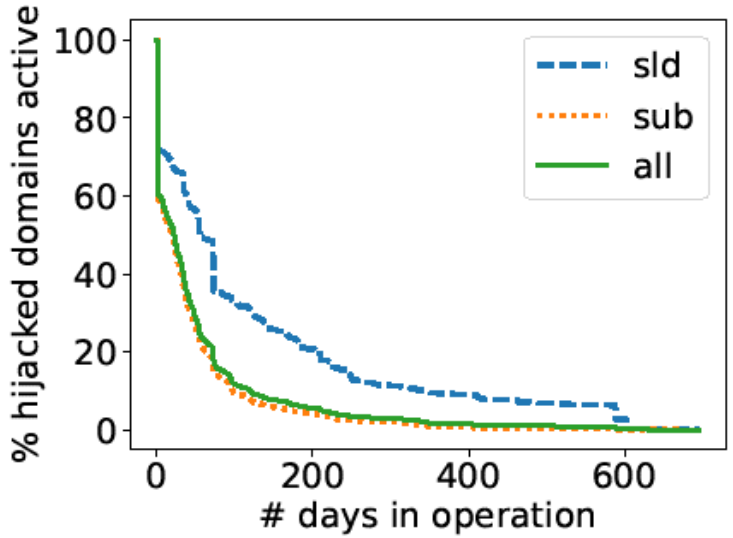
↓

Rockwell Collins, Thales, …



Häufige Angriffe, die selten entdeckt werden
Cookies/Zugangsdaten Diebstahl, Schadsoftware Verteilung, ….

- Nur 135 of 20.000 übernommenen Domänen waren geblacklisted



1/3 der Angriffe in unserer Studie laufen länger als 65 Tage, manche über ein Jahr!

Traditionelle Sicherheitsarchitektur
Perimeter + unterschiedlich vertrauenswürdige Netzzonen

Traditionelle IT-Sicherheitsarchitektur

- Fokus auf Perimeterschutz
- Dienste in DMZ haben direkte Anbindung an das Internet
- In jeder Zone sind alle Hosts implizit vertrauenswürdig

Problem 1: Schutz des Perimeters ist mangelhaft

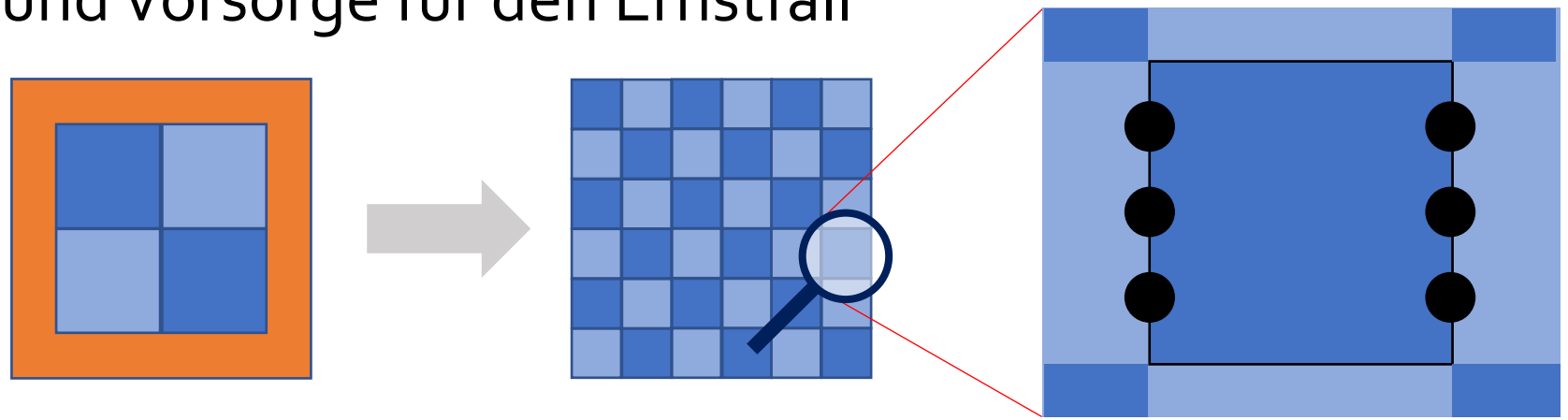
- Sicherheitslücken, Zero Days
- Kompromittierte Konten
- Mitarbeiter
- VPNs / WLAN
- …

Problem 2: In einer Zone kann sich Angreifer ungehindert ausbreiten

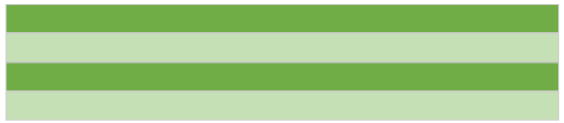
- Zugangsdaten Diebstahl (Uber, Colonial Pipeline,…)
- Lücken in Lieferketten (Solarwinds,…)

Zero Trust Architektur

Feingranulare Segmentierung, minimale Rechte, gesunde Systeme und Vorsorge für den Ernstfall

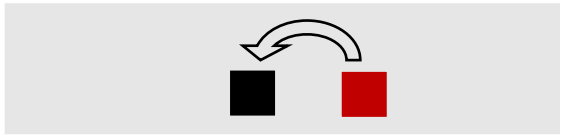


- Starke Authentifizierung
- Minimale Rechte für begrenzte Zeit
- Minimale Daten
- Verschlüsselung innen und außen
- Logging und Prüfung



- Auf allen Schichten
- Entlang Supply Chain

- Security by Design
- Scans & Tests im Betrieb
- Vulnerability & Patch Mgmt



- Redundanz, keine SPOF
- Schnelle Recovery

- **Werkzeuge für große Lagebilder**
  - Schwachstellen
  - Probleme im IT-Management
  - Laufende Angriffe
  - Häufig übersehene Angriffe
- **Patch & Vulnerability Mgmt**
  - Nicht trivial, aber kritisch
- **Zero Trust**
  - Kann Probleme mildern

תודה רבה!

Merci beaucoup!

çok teşekkürler

谢谢

Thank you very much!

Vielen Dank!

Dank je wel!

Muchas gracias

ありがとうございます

Dziękuję!

zor spas

شكرا لك

Grazie mille!