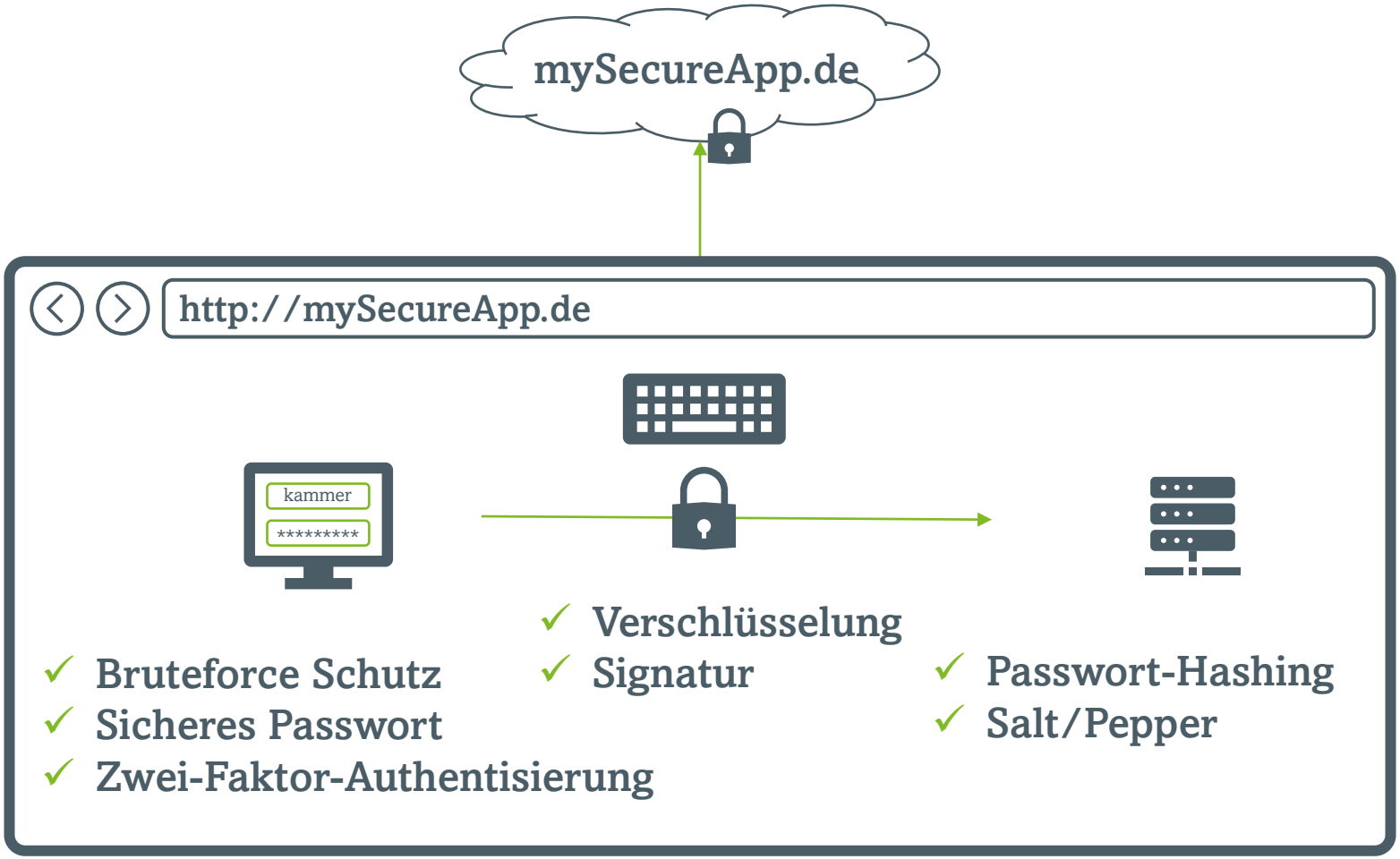
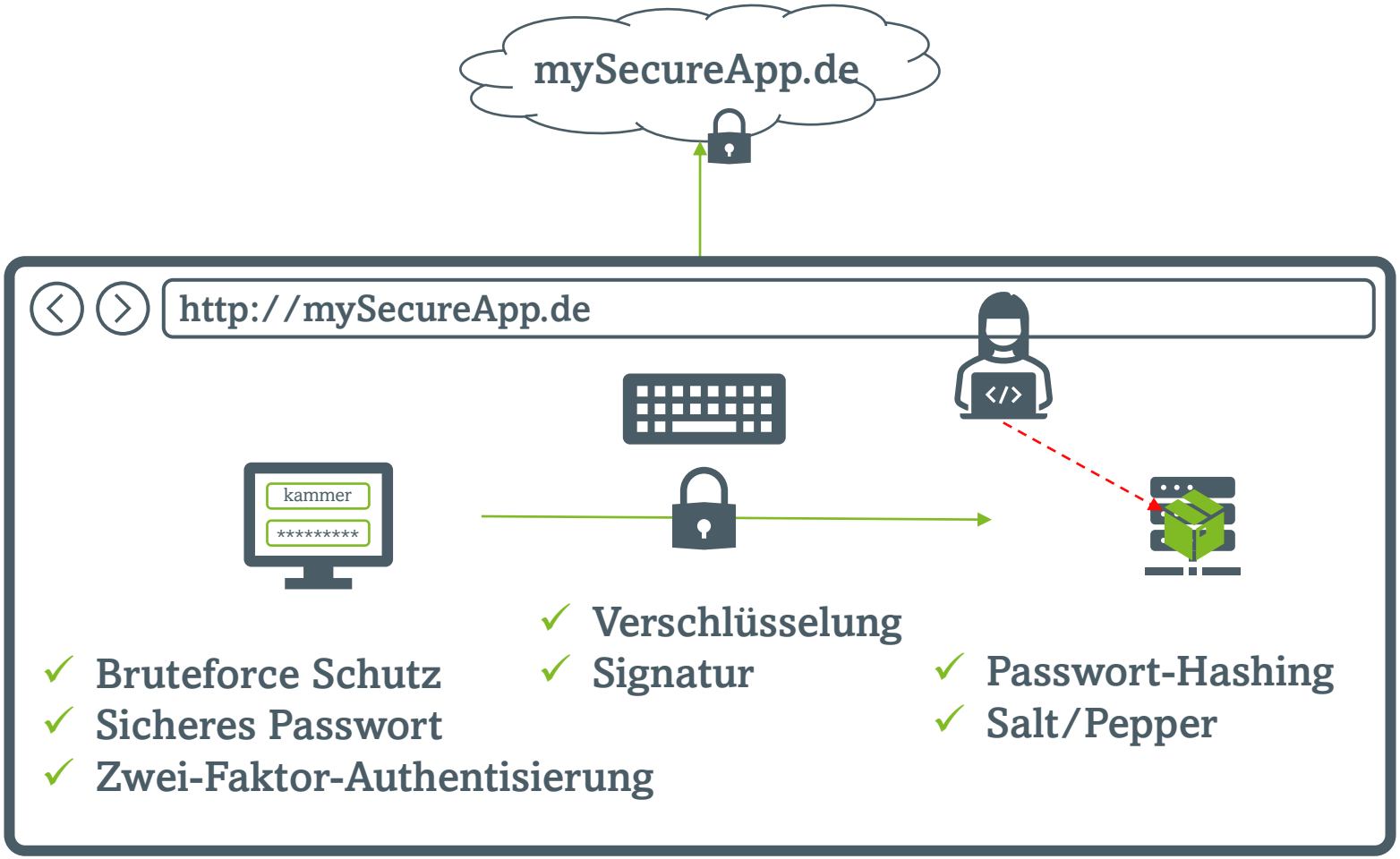
Sicherheitsrisiken

Rückblick


mySecureApp.de
http://mySecureApp.de
kammer
****
✓ Verschlüsselung
✓ Signatur
✓ Bruteforce Schutz
✓ Sicheres Passwort
✓ Zwei-Faktor-Authentisierung
✓ Passwort-Hashing
✓ Salt/Pepper

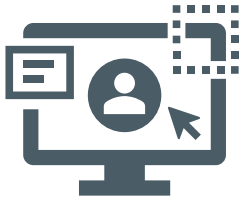
Rückblick


mySecureApp.de
http://mySecureApp.de
kammer
****
✓ Bruteforce Schutz
✓ Sicheres Passwort
✓ Zwei-Faktor-Authentisierung
✓ Verschlüsselung
✓ Signatur
✓ Passwort-Hashing
✓ Salt/Pepper

OWASP Top Ten

1.  Broken Access Control
2.  Cryptographic Failures
3.  Injection
4.  Insecure Design
5.  Security Misconfiguration
6.  Vulnerable and Outdated Components
7.  Identification and Authentication Failures
8.  Software and Data Integrity Failures
9.  Security Logging and Monitoring Failures
10.  Server-Side Request Forgery (SSRF)

Warum IT-Sicherheit?



- **Für einen selbst**
  - Besserer Schlaf und weniger Sorgen
  - Weniger Datenverlust → Weniger Arbeit

- **Es gibt Verpflichtungen**
  - Moralisch
  - Juristisch

Schutzziele

- Grundziele der IT-Sicherheitsmaßnahmen
- CIA-Triade

Schutzziele – CIA-Triade

Schutzziele

- Grundziele der IT-Sicherheitsmaßnahmen
- CIA-Triade
- Es existieren weitere Schutzziele:
  - Revisionsfähigkeit, Authentizität, Zurechenbarkeit, ...

Haftungsrisiken für Administratoren

c‘t Ausgabe 12/2013

- Administratoren definieren Spielregeln für Unternehmen / Organisationen
- Beweislast liegt beim Administrator
- Ggf. persönliche Haftung (wegen grober Fahrlässigkeit)
- Theorie und Praxis: Theoretisch sicher, praktisch …
- Zwischen den Stühlen: Anwendbarkeit und Sicherheit
- Meist keine schriftlichen Weisungen
- Meist ohne externe Unterstüzung

Besonderheiten des Cybercrime

Kriminelle Tätigkeiten

- Es gibt einen zentralen Tatort
- Es existiert ein Tatmittel
- Unmittelbares (physisches) Zusammentreffen von Täter, Opfer und Tatmittel am Tatort
- Es gibt eine zentrale Spurenlage

Beim Cyber-Crime ist das alles anders!

Besonderheiten des Cybercrime

Paralleler Zugriff

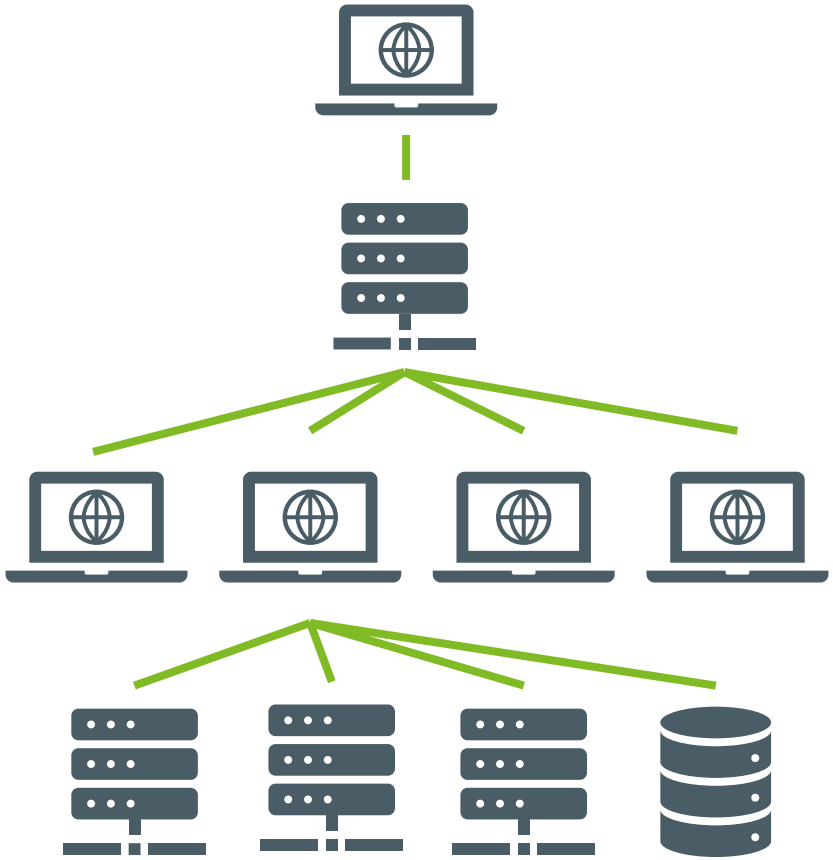
- Hunderte Rechner gleichzeitig manipulieren

Hunderte Tatorte

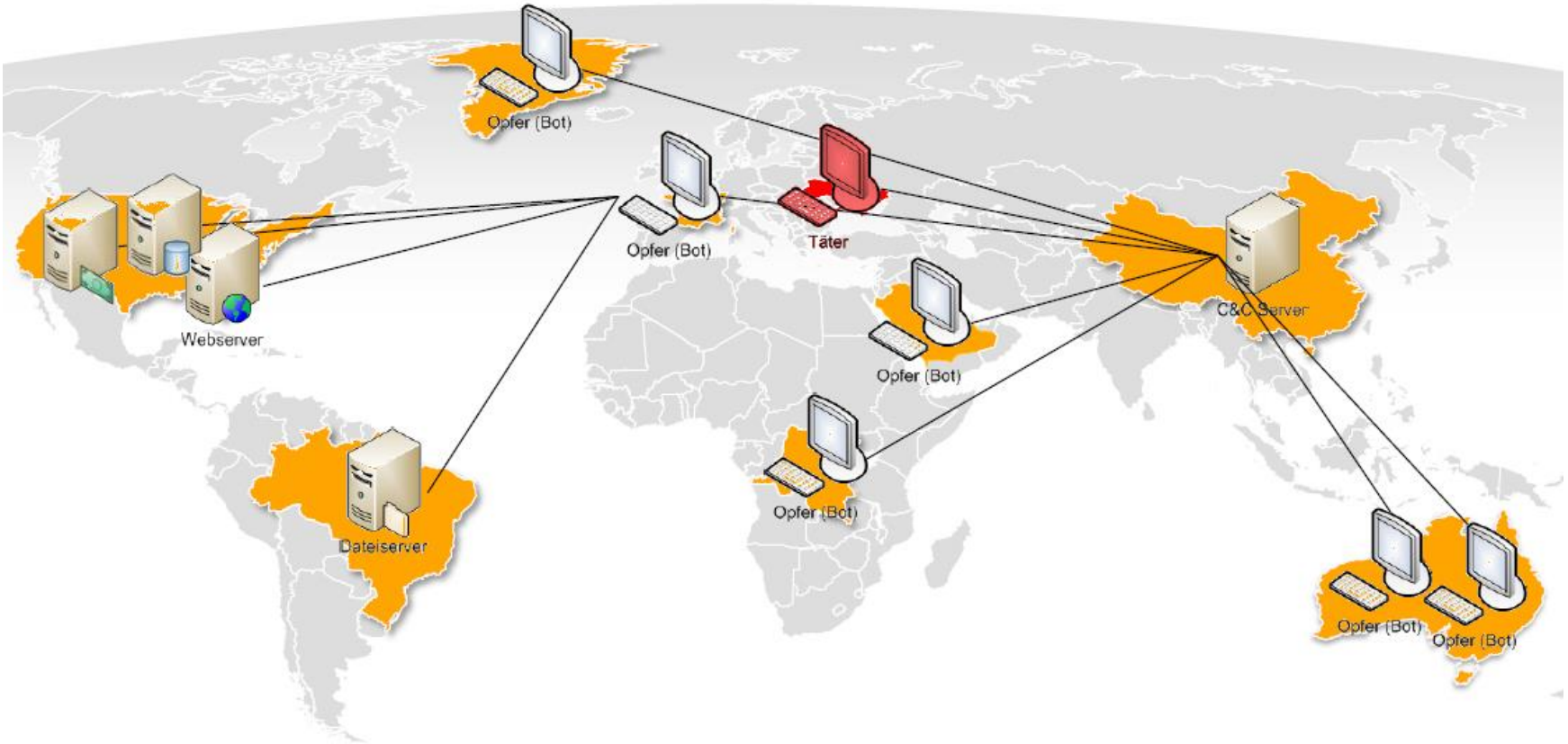
- An keinem vor Ort

Mehrere Rechner manipulieren

- Kein zusätzlicher Aufwand



Besonderheiten des Cybercrime



Besonderheiten des Cybercrime

- „Globales Dorf“ → Datenübertragung im Internet kennt keine Grenzen
- Einkommensunterschiede → Auch größter Zeitaufwand kann lukrativ sein
- Operieren aus dem Ausland → Es muss selten mit Strafen gerechnet werden

Wenn man Opfer wurde …

- Zusammenarbeit mit Behörden vorbereiten
- Protokolle (Logdaten) der betroffenen Netzwerkkomponenten / des zentralen Logservers
- Mitschnitt des Datenverkehrs (.pcap-Dateien)
- Datensicherung betroffener Email-Accounts
- Ergebnisse eigener Auswertungen (Motiv, Vorgehensweise, Schaden…)
- Ergebnisse von Auswertungen externer Dienstleister anfordern
- Behörden kontaktieren

Behördliche Ansprechpartner

Bundesamt für Sicherheit in der Informationstechnik

Aufgabenschwerpunkte

- generelle Beratung und Unterstützung
- keine Verfolgung von Straftaten bzw. Abwehr konkreter Gefahren durch Zwangsmaßnahme

Behördliche Ansprechpartner

Bundeskriminalamt

Aufgabenschwerpunkte

- Übernahme von Ermittlungen im Sinne einer Strafverfolgung in besonderen Fällen (v.a. länderübergreifende Ermittlungsverfahren von besonderer Bedeutung).

Behördliche Ansprechpartner

Zentrale Ansprechstellen Cybercrime

Aufgabenschwerpunkte

- Zuständigkeit bei örtlichen Polizeibehörden, ggf. auch beim LKA
- Strafverfolgung als auch Abwehr konkreter Gefahren
- Ansprechpartner für die Wirtschaft

Behördliche Ansprechpartner

Landesämter für Verfassungsschutz (LfV) und Zentrale Ansprechstelle Cybercrime (ZAC)

- Beratung, Aufklärung und Unterstützung im Bereich der Spionageabwehr und des Wirtschaftsschutzes

Unterliegen nicht dem Legalitätsprinzip

Behördliche Ansprechpartner

Legalitätsprinzip

- Verpflichtung der Strafbehörde ein Ermittlungsverfahren zu eröffnen, wenn sie hinreichende Kenntnisse einer (möglichen) Straftat hat
- Offizialdelikte: Legalitätsprinzip findet stehts Anwendung
- Antragsdelikte: Strafantrag des Geschädigten ist Voraussetzung für Strafverfolungsmaßnahmen

OWASP Top Ten

1.  Broken Access Control
2.  Cryptographic Failures
3.  Injection
4.  Insecure Design
5.  Security Misconfiguration
6.  Vulnerable and Outdated Components
7.  Identification and Authentication Failures
8.  Software and Data Integrity Failures
9.  Security Logging and Monitoring Failures
10.  Server-Side Request Forgery (SSRF)

Wiederholung

CWEs/CVEs

- **Common Weakness Enumeration ist eine von der Gemeinschaft entwickelte Liste von Software- und Hardware-Schwachstellen**
  - Katalogisieren von Schwachstellen
  - mehr als 600 Kategorien
- **Common Vulnerabilities and Exposures**
  - Liste der derzeit bekannten Probleme in Bezug auf bestimmte Systeme und Produkte

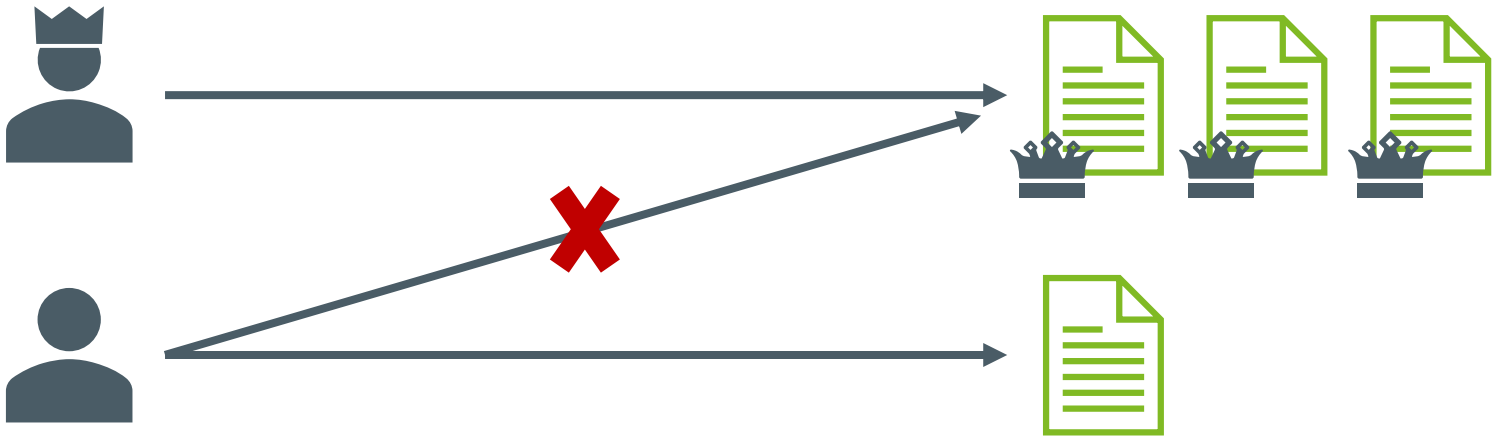
Broken Access Control

Erfasste CWEs	max. Inzidenzrate	Ø Inzidenzrate	Ø gewichtete Ausnutzung	Ø gewichtete Auswirkung
34	55,97%	3,81%	6,92	5,93

max. Abdeckung	Ø Abdeckung	gesamtes Vorkommen	gesamte CVEs
94,55%	47,72%	318.487	19.013

Broken Access Control

Fehler führen in der Regel zur unbefugten Offenlegung von Informationen, zur Änderung oder Zerstörung aller Daten oder zur Ausführung einer Geschäftsfunktion außerhalb der vom Benutzer festgelegten Grenzen.



Broken Access Control

- **Zugriff außerhalb der zugewiesenen Rechte**
- **Häufige Schwachstellen**
  - Kein standardmäßiges Verweigern
  - Umgehen der Zugriffsrechte durch Manipulation der URL
  - CORS-Fehlkonfiguration
  - Manipulation von Metadaten

Beispiel

Broken Access Control

Datenleck im Legoland (2022)

- mehrere tausend Datensätze von Buchungen mit
  - Namen
  - Anschriften
  - Reisezeitraum
- Daten seit Mai 2015

https://www.heise.de/news/Datenleck-im-Legoland-Reisedaten-tausender-Kunden-seit-2015-betroffen-6668852.html

Beispiel

Broken Access Control

https://mylogin.legolandholidays.de/api/buchung/document/100001/...

LEGOLAND Holidays Deutschland GmbH
LEGOLAND Allee 1
89312 Günzburg

BESTÄTIGUNG

KD.NR.: [redacted]

Buchungsnummer: [redacted]
Buchungsdatum: [redacted]
Bearbeiter: Online LEGOLAND Holidays

Frau
[redacted]
Deutschland

https://www.heise.de/news/Datenleck-im-Legoland-Reisedaten-tausender-Kunden-seit-2015-betroffen-6668852.html

Beispiel

Broken Access Control

https://mylogin.legolandholidays.de/api/buchung/document/100002/...

LEGOLAND HOLIDAYS

LEGOLAND Holidays Deutschland GmbH
LEGOLAND Allee 1
89312 Günzburg

BESTÄTIGUNG

KD.NR.: [redacted]

Buchungsnummer: [redacted]
Buchungsdatum: [redacted]
Bearbeiter: Online LEGOLAND Holidays

Frau
[redacted]
Deutschland

https://www.heise.de/news/Datenleck-im-Legoland-Reisedaten-tausender-Kunden-seit-2015-betroffen-6668852.html

Broken Access Control

Prävention

- **Zugriff auf Ressourcen standardmäßig verweigern**
  - Ausnahmen speziell angeben
- **Verwendung von Zugriffskontrollmechanismen**
- **Loggen von Fehlern bei der Zugangskontrolle**
  - gegebenenfalls Alarmierung der Administratoren
- **Begrenzen Sie den API- und Controller-Zugriffe**

Broken Access Control

https://mylogin.legolandholidays.de/api/buchung/document/100002/...

Mögliche Lösungen:

- Backen Identifier hashen
  - *Hash(100002 + salt)*
- kryptografisch sichere IDs verwenden
  - Z.B. UUID V4
- Zusätzlich auch die Authentifizierung überprüfen

100002

44d83b1251bb50bd3616
bfcd6f7992ae34926471

https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html

Cryptographic Failures

Erfasste CWEs	max. Inzidenzrate	Ø Inzidenzrate	Ø gewichtete Ausnutzung	Ø gewichtete Auswirkung
29	46,44%	4,49%	7,29	6,81

max. Abdeckung	Ø Abdeckung	gesamtes Vorkommen	gesamte CVEs
79,33%	34,85%	233.788	3.075

Cryptographic Failures

- Es wird keine Verschlüsslung für die Übertragung verwendet
- Verwendung von verschlüsselten Verbindungen auch zwischen den internen Systemen
- Verschlüsselung wird nicht erzwungen (z.B. http/s)
- Sensible daten werden nicht zusätzlich verschlüsselt
- Unsichere Secrets / Keine Secret Rotation
- Validierung der SSL-Zertifikatskette
- …

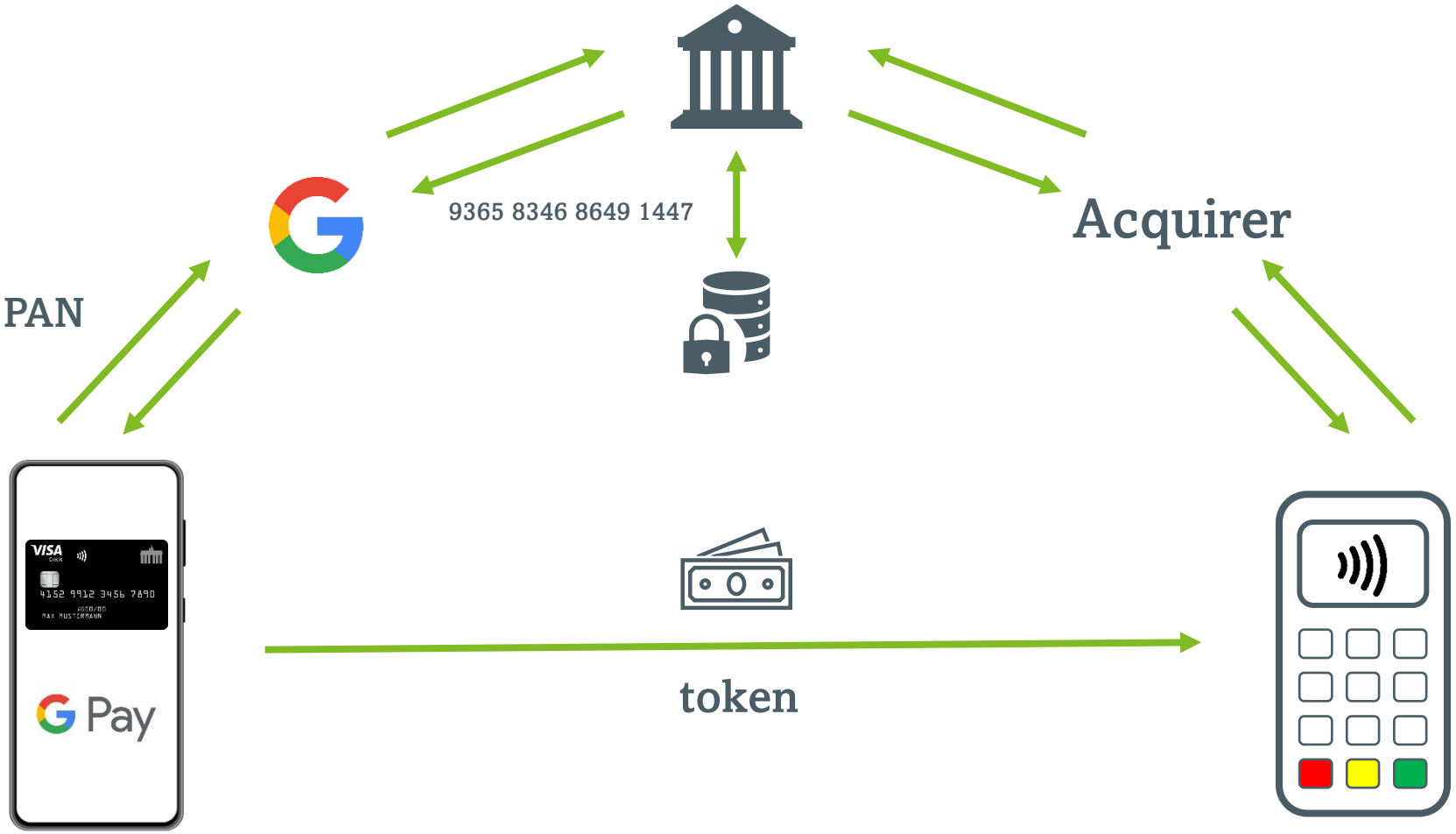
https://owasp.org/Top10/A02_2021-Cryptographic_Failures/#description

Cryptographic Failures

Prävention

- Klassifizieren von Daten
- Keine unnötige Speicherung von Daten
- Tokenization (Ersetzen von sensiblen Daten)

Tokenization



Cryptographic Failures

Prävention

- Klassifizieren von Daten
- Keine unnötige Speicherung von Daten
- Tokenization (Ersetzen von sensiblen Daten)
- Deaktivieren caching von sensiblen Antworten
- Vermeiden von veralteten kryptographischen Algorithmen
  - MD5, SHA1, PKCS

Injection

Erfasste CWEs	max. Inzidenzrate	Ø Inzidenzrate	Ø gewichtete Ausnutzung	Ø gewichtete Auswirkung
33	19,09%	3,37%	7,25	7,15

max. Abdeckung	Ø Abdeckung	gesamtes Vorkommen	gesamte CVEs
94,04%	47,90%	274.228	32,078

Injection

- Daten eines Benutzers werden von der Anwendung nicht validiert, gefiltert oder bereinigt
- Dynamische Queries werden direkt im Interpreter verwendet

SQL-Injection

```
"SELECT * FROM users
        WHERE user = $user ";
```

```
$user = "; "DROP DATABASE db
```

```
"SELECT * FROM users
        WHERE user = ";
        DROP DATABASE db";
```

XSS-Injection

```
<script>alert(1)</script>
```

```
document.getElementById(„id“)
    .innerHTML = input;
```

SQL-Injection

- Escaping

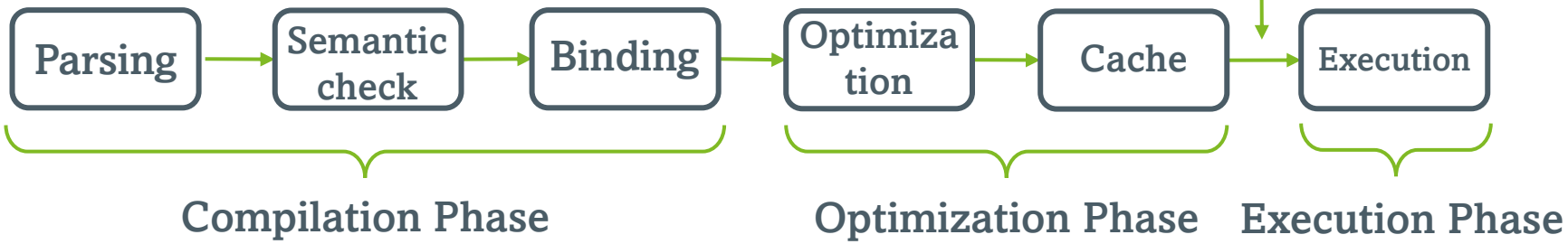
```
"SELECT * FROM users WHERE user = $user ”;
```

  - $user = test\“

- Prepared Statements

```
"SELECT * FROM users WHERE user = ? ”;
```

Parameter: $user



XSS-Injection

- Sicherstellen dass keine Inputs als HTML gerendert werden
- Filtern von bestimmten HTML-Tags, die erlaubt sind
- Bereinigen von Eingaben

XSS-Injection

DOMPurify

- XSS-Sanitizer für HTML, MathML und SVG
- Erlauben und Verbieten von HTML-Tags

https://cure53.de/purify

Insecure Design

Erfasste CWEs	max. Inzidenzrate	Ø Inzidenzrate	Ø gewichtete Ausnutzung	Ø gewichtete Auswirkung
40	24,19%	3,00%	6,46	6,78

max. Abdeckung	Ø Abdeckung	gesamtes Vorkommen	gesamte CVEs
77,25%	42,51%	262.407	2.691

Insecure Design

- Risiken durch Design- und Architekturfehler
- Sicheres Design kann trotzdem zu Implementierungsfehlern führen
- Ein unsicherer Entwurf kann nicht durch eine perfekte Implementierung behoben werden
- Anforderungen und Ressourcenmanagement
- Secure Design
- Secure Development Lifecycle

Insecure Design

Prävention

- Aufbau und Nutzung einer Bibliothek mit sicheren Entwurfsmustern oder gebrauchsfertigen Komponenten
- Robuste Trennung von Mandanten durch Design auf allen Ebenen
- Begrenzung des Ressourcenverbrauchs nach Benutzer oder Dienst

Security Misconfiguration

20	 19,84%	4,51%	8,12	6,56
Erfasste CWEs	max. Inzidenzrate	Ø Inzidenzrate	Ø gewichtete Ausnutzung	Ø gewichtete Auswirkung

 89,58%	 44,84%	208.387	789
max. Abdeckung	Ø Abdeckung	gesamtes Vorkommen	gesamte CVEs

Security Misconfiguration

- Unnötige Funktionen aktiviert oder installiert sind (z. B. unnötige Ports, Dienste, Seiten, Konten oder Berechtigungen).
- Standardkonten und deren Kennwörter sind weiterhin aktiviert und unverändert.
- Den Benutzern werden Stack Traces oder andere übermäßig informative Fehlermeldungen angezeigt.
- Die Software ist veraltet oder anfällig

Security Misconfiguration

Prävention

- sichere Installationsprozesse implementieren
- keine ungenutzten Funktionen und Frameworks installieren
- Automatische Überprüfung von Konfigurationen und Aktualisierungen
- Senden von Security-Headers

Security Misconfiguration

Security-Headers

- Verhaltensregeln für den Browser

X-Frame-Options: DENY

~~X-XSS-Protection: 1; mode=block~~

X-XSS-Protection sollte nicht mehr verwendet werden

Content-Security-Policy: <policy-directive>; <policy-directive>

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Security Misconfiguration

Security-Headers

- Verhaltensregeln für den Browser

Strict-Transport-Security: max-age=<expire-time>; includeSubdomains

Referrer-Policy: no-referrer

Portscanner

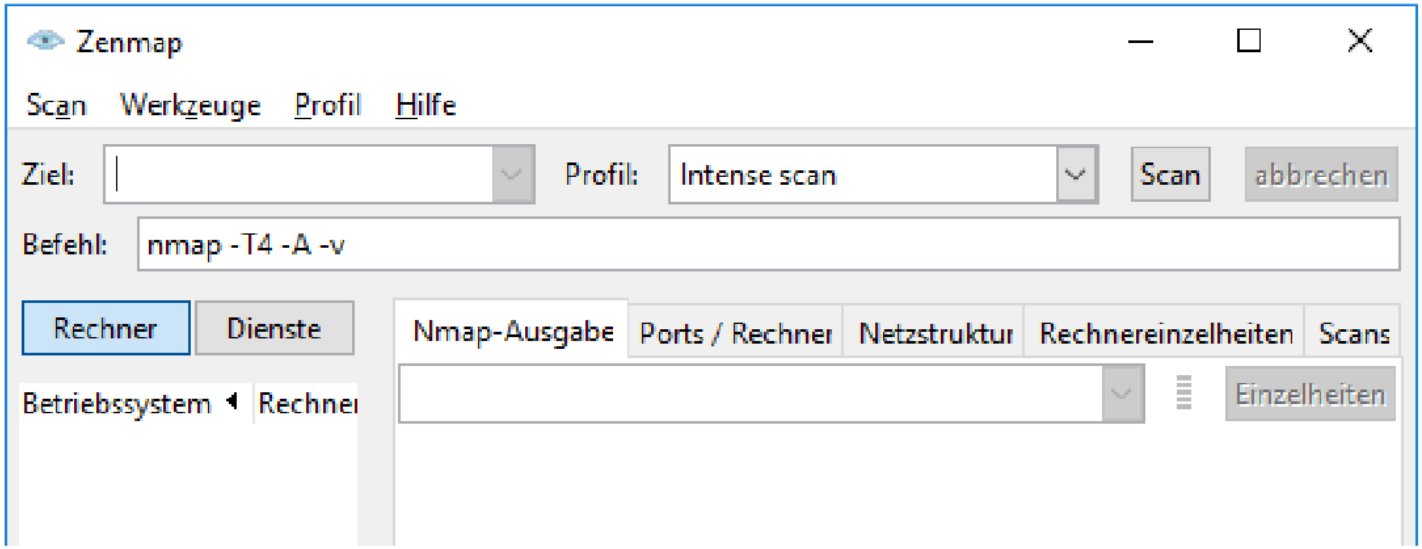
- Software zum Überprüfen, welche Dienste ein System über das Protokoll TCP oder UDP anbietet.
- Der Portscanner nimmt dem Anwender dabei die Arbeit ab, das Antwortverhalten eines Systems mit telnet oder mit einem Sniffer zu untersuchen und zu interpretieren.
- Oft bieten Portscanner auch Zusatzfunktionen wie Betriebssystem- und Diensterkennung an. (Ist eigentlich nicht die Aufgabe eines Portscanners.)
- Portscanner Programm für Windows/Linux/MAC: nmap

Gegenmaßnahme:

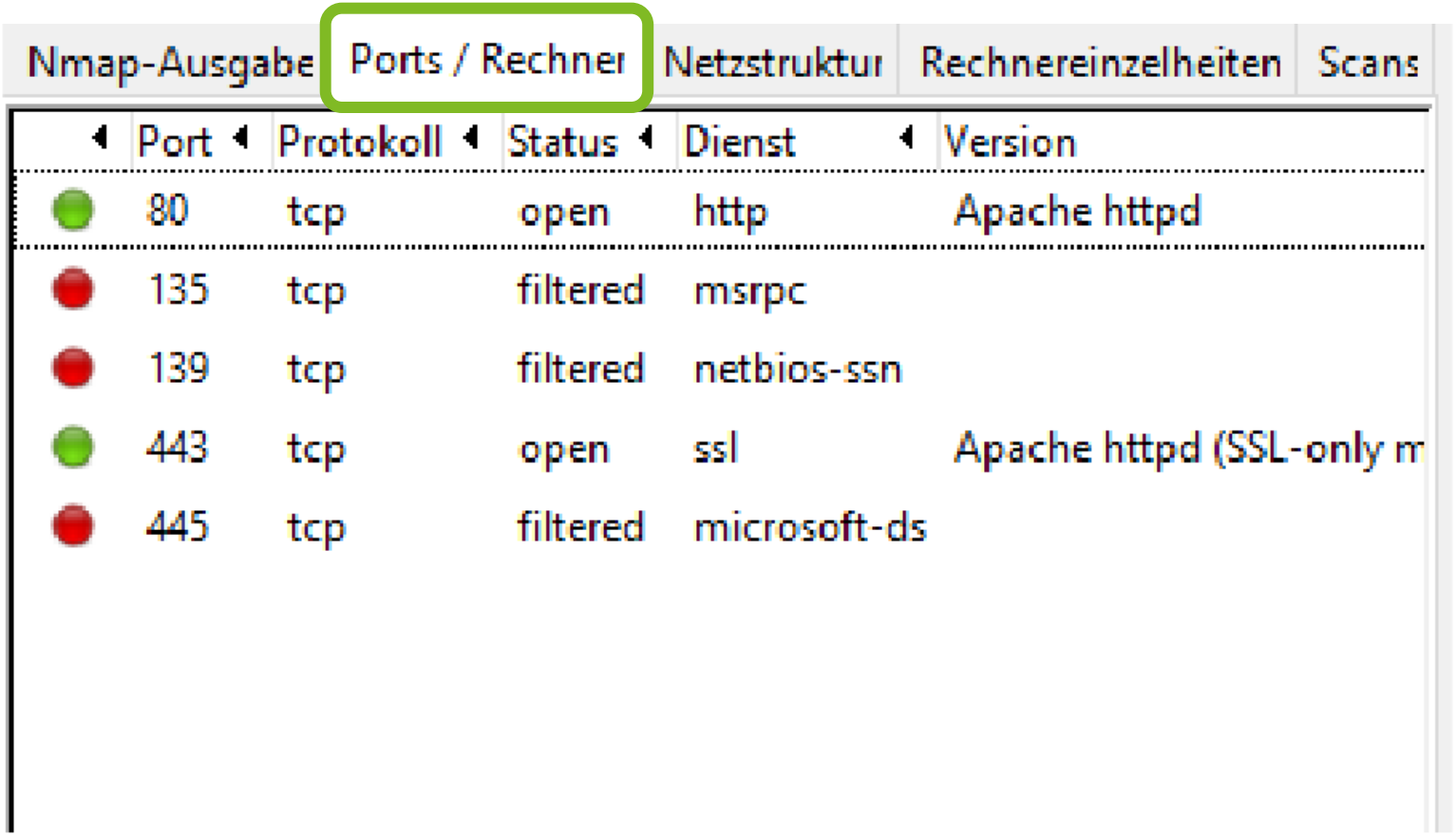
z.B. Portscan Attack Detector psad

Nutzung von Zenmap

- Ziel: Der zu prüfende Host
- Profil: Art des durchzuführenden Scans
- Befehl: nmap T4 –A –v wie er in der Konsole ausgeführt werden kann

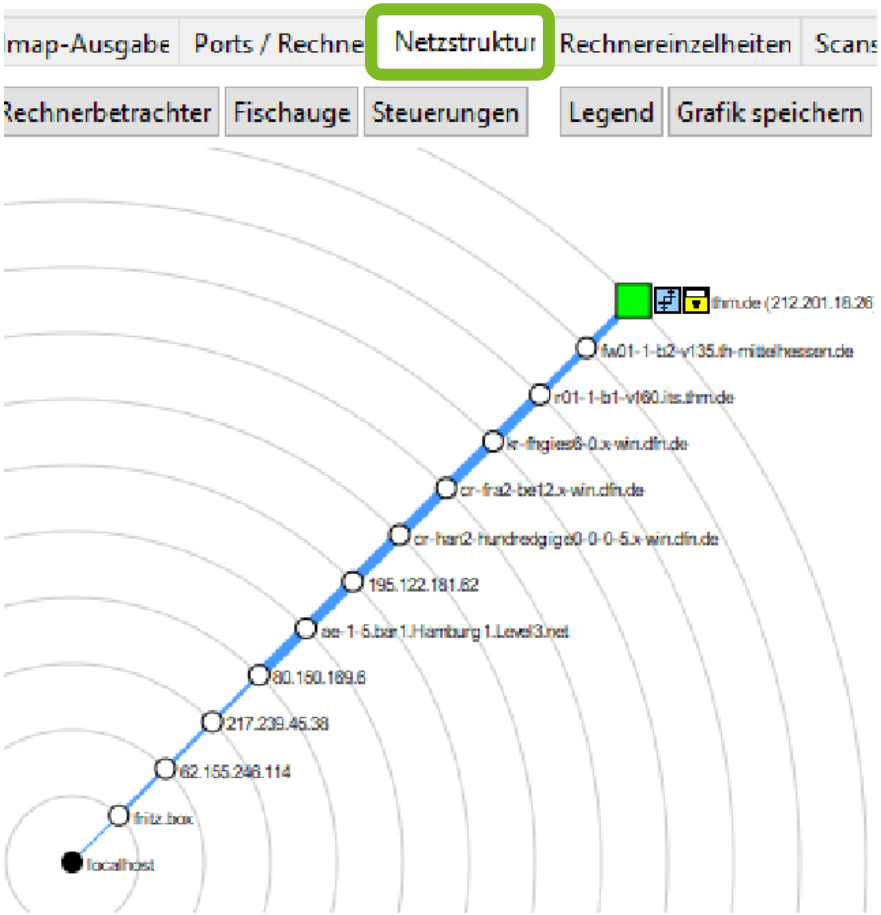


Zenmap: Ports / Rechner



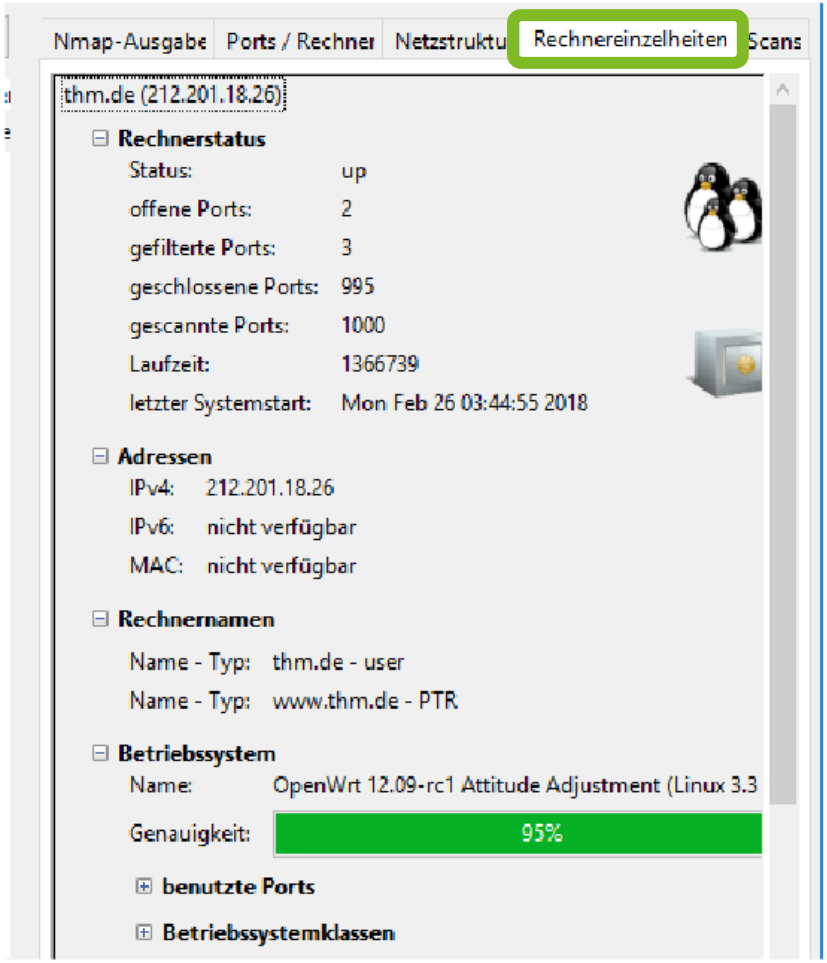
Zenmap: Netzstruktur

- Gibt einen grafischen Überblick über die aufgebaute Netzwerkstruktur beim Anfragen des Hosts.



Zenmap: Rechnereinzelheiten

- Gibt aufschlussreiche Informationen über den angefragten Rechner/Server.



Portscanner: Fall Suprema

- Klappt das auch bei echten Systemen? Wer ist denn so unsicher??

UNVERSCHLÜSSELT:
Nutzernamen und Passwörter

> 1 Million Fingerabdrücke sowie eine ungenannte Zahl an Gesichtsbildern

Biometriedatenbank mit 27,8 Millionen Einträgen ungesichert im Netz

Israelische IT-Sicherheitsexperten konnten auf 23 Gigabyte an Daten inklusive über einer Million Fingerabdrücke in einer ungeschützten Datenbank zugreifen.

Lesezeit: 4 Min. In Pocket speichern 161

Mit prominenten Namen wirbt Suprema für die mobile Daseinsform seines biometrischen Zugangssystems. Ob diese von dem Datenleck betroffen sind, wurde nicht bekannt. (Bild: supremainc.com)

14.08.2019 14:19 Uhr | Security

Von Stefan Krempl

Vulnerable and Outdated Components

Erfasste CWEs	max. Inzidenzrate	Ø Inzidenzrate	Ø gewichtete Ausnutzung	Ø gewichtete Auswirkung
3	27,96%	8,77%	5,00	5,00

max. Abdeckung	Ø Abdeckung	gesamtes Vorkommen	gesamte CVEs
51,78%	22,47%	30.457	0

Vulnerable and Outdated Components

- Wenn die Software anfällig ist, nicht unterstützt wird oder veraltet ist
- nicht regelmäßig nach Schwachstellen suchen
- die Konfigurationen der Komponenten nicht absichern

Identification and Authentication Failures

Erfasste CWEs	max. Inzidenzrate	Ø Inzidenzrate	Ø gewichtete Ausnutzung	Ø gewichtete Auswirkung
22	14,84%	2,55%	7,40	6,50

max. Abdeckung	Ø Abdeckung	gesamtes Vorkommen	gesamte CVEs
79,51%	45,72%	132.195	3.897

Identification and Authentication Failures

- Bestätigung der Identität des Benutzers
- Zulassen von Brute-Force- oder andere automatisierte Angriffen (Credential Stuffing)
- Zulassen von Standardpasswörtern, schwachen oder bekannten Passwörtern
- Sitzungskennungen werden nicht korrekt ungültig gemacht

Software and Data Integrity Failures

Erfasste CWEs	max. Inzidenzrate	Ø Inzidenzrate	Ø gewichtete Ausnutzung	Ø gewichtete Auswirkung
10	16,67%	2,05%	6,94	7,94

max. Abdeckung	Ø Abdeckung	gesamtes Vorkommen	gesamte CVEs
75,04%	45,35%	47.972	1.152

Software and Data Integrity Failures

- Anwendung auf Plugins, Bibliotheken oder Module aus nicht vertrauenswürdigen Quellen angewiesen
- Angreifer laden eigene Updates hoch und verteilen diese

Beispiel

Software and Data Integrity Failures

Hacks verschiedener Firmen

- IT-Sicherheitsfirma FireEye
- US-Regierung (Finanz- und Handelsministerium)
- …

SolarWinds Hack

- kompromittiertes Update der Plattform Orion
- 33 000 Kunden
- 18 000 installierte Updates
- Hack des Build-Prozesses und Einschleusung eines Trojaners

Software and Data Integrity Failures

Prävention

- Verwendung von digitalen Signaturen
- Sicherstellung das die Dependencies aus Vertrauenswürdigen repositories stammen
- Automatische Überprüfung der Dependencies auf Sicherheitslücken
- Reviews von gemachten änderungen
- Sichere Konfiguration der CI/CD Pipelines

Security Logging and Monitoring Failures

Erfasste CWEs	max. Inzidenzrate	Ø Inzidenzrate	Ø gewichtete Ausnutzung	Ø gewichtete Auswirkung
4	19,23%	6,51%	6,87	4,99

max. Abdeckung	Ø Abdeckung	gesamtes Vorkommen	gesamte CVEs
53,67%	39,97%	53.615	242

Security Logging and Monitoring Failures

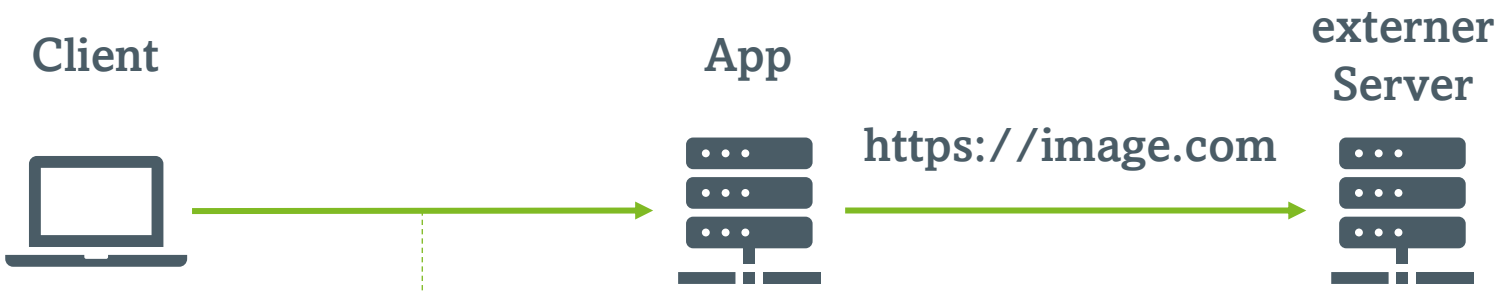
- Ohne Protokollierung und Überwachung können Sicherheitsverletzungen nicht erkannt werden
- Warnungen und Fehler erzeugen keine, unzureichende oder unklare Protokollmeldungen.
- Nachvollziehbare Ereignisse wie Anmeldungen, fehlgeschlagene Anmeldungen und Transaktionen mit hohem Wert werden nicht protokolliert.

Server-Side Request Forgery (SSRF)

Erfasste CWEs	max. Inzidenzrate	Ø Inzidenzrate	Ø gewichtete Ausnutzung	Ø gewichtete Auswirkung
1	2,72%	2,72%	8,28	6,72

max. Abdeckung	Ø Abdeckung	gesamtes Vorkommen	gesamte CVEs
67,72%	67,72%	9.503	385

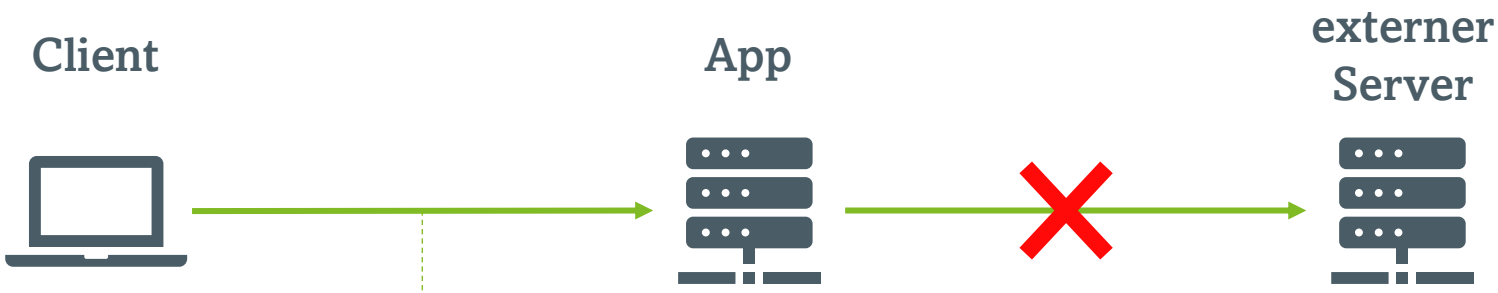
Server-Side Request Forgery (SSRF)




```
POST /images/dog HTTP/3
Content-Type: …

Body: {
      ImageAPI: https://image.com
}
```

Server-Side Request Forgery (SSRF)




```
POST /images/dog HTTP/3
Content-Type: …

Body: {
      ImageAPI: https://localhost/admin
}
```

Server-Side Request Forgery (SSRF)

Prävention

- Bereinigung und Validierung aller vom Kunden bereitgestellten Eingabedaten
- keine rohen Antworten an Clients senden
- Segmentierung des Fernzugriffs auf Ressourcen in getrennten Netzen, um die Auswirkungen von SSRF zu verringern