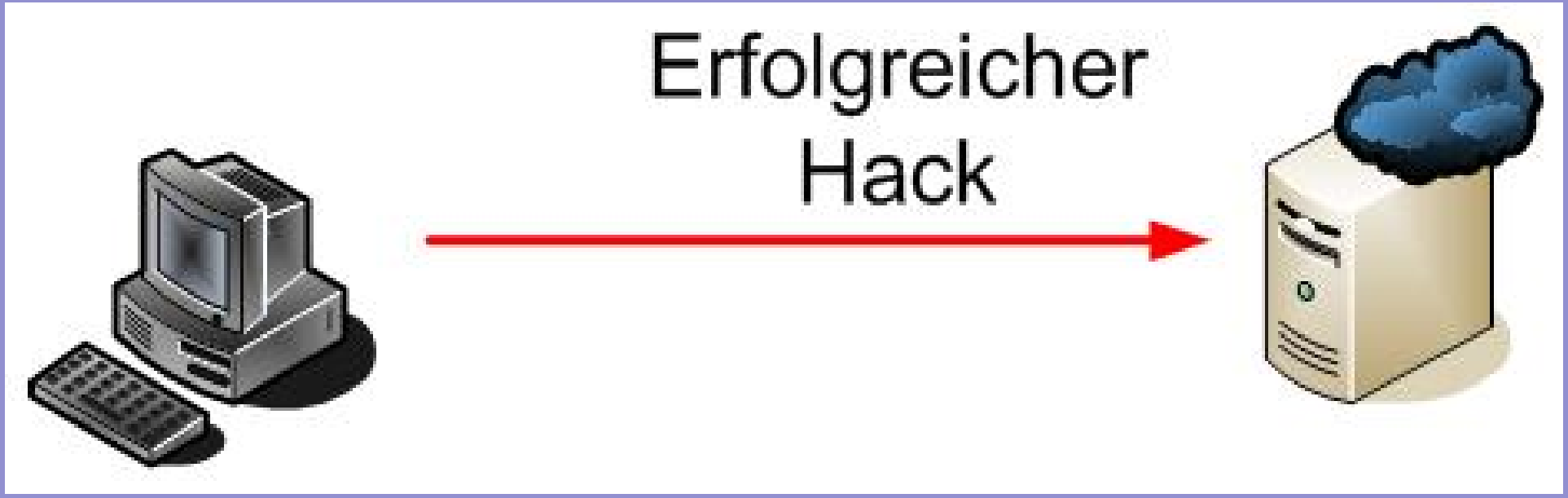
Hacking & Computerstrafrecht

lukas.feiler@lukasfeiler.com
http://teaching.lukasfeiler.com



Was tun?

- Zivilrechtlicher Anspruch auf Schadenersatz (Prozessrisiko!)
- Strafanzeige (Anschluss als Privatbeteiligter)

Struktur des Vortrages

1. Österreichische Strafrechtsdogmatik
2. Die Cyber-Crime-Konvention des Europarates
3. Angriffe auf Computersysteme und ihre rechtliche Beurteilung

Der Zweck des Strafrechts

- Spezialprävention
  nochmalige Begehung der Tat durch denselben Täter verhindern
- Generalprävention
  Begehung der Tat durch andere Täter verhindern

nicht:
- Rache
- Vergeltung („Aug um Aug“)

z.B. X ermordet seine/ihre Mutter:
Spezialprävention: ?
Generalprävention: ?

Der „fragmentarische“ Charakter des Strafrechts

§ 1 StGB: Keine Strafe ohne Gesetz; Analogieverbot
Nur was das Gesetz ausdrücklich unter Strafe stellt, ist strafbar!

z.B. X dringt in meine unversperrte (!) Wohnung ein und durchwühlt meine Privatsachen – strafbar?

Der objektive & subjektive Tatbestand

objektive TB: Handlungen
subjektive TB: Gedanken/Vorstellungen

z.B. X dreht sich ungeschickt um und wirft eine teure Vase des A zu Boden – strafbar?
Objektiv: Wer eine andere Sache zerstört
Subjektiv: § 7 Abs. 1 → „vorsätzlich“ → § 5 Abs. 1 → ernstlich für möglich hält und sich damit abfindet

Rechtswidrigkeit und Verschulden

Rechtswidrigkeit

X hätte sich anders verhalten sollen

Verschulden

X hätte sich anders verhalten können
(„subjektive Vorwerfbarkeit“)
→ § 4 keine Strafe ohne Schuld! (kein Erfolgsstrafrecht)

Die wichtigsten Tatbestände des Computerstrafrechts

§ 118a StGB: Widerrechtlicher Zugriff auf ein Computersystem
§ 119 StGB: Verletzung des Telekommunikationsgeheimnisses
§ 119a StGB: Missbräuchliches Abfangen von Daten
§ 126a StGB: Datenbeschädigung
§ 126b StGB: Störung der Funktionsfähigkeit eines Computersystems
§ 126c StGB: Missbrauch von Computerprogrammen oder Zugangsdaten
§ 51 DSG: Datenverwendung in Gewinn- oder Schädigungsabsicht

StGB… Strafgesetzbuch
DSG… Datenschutzgesetz 2000

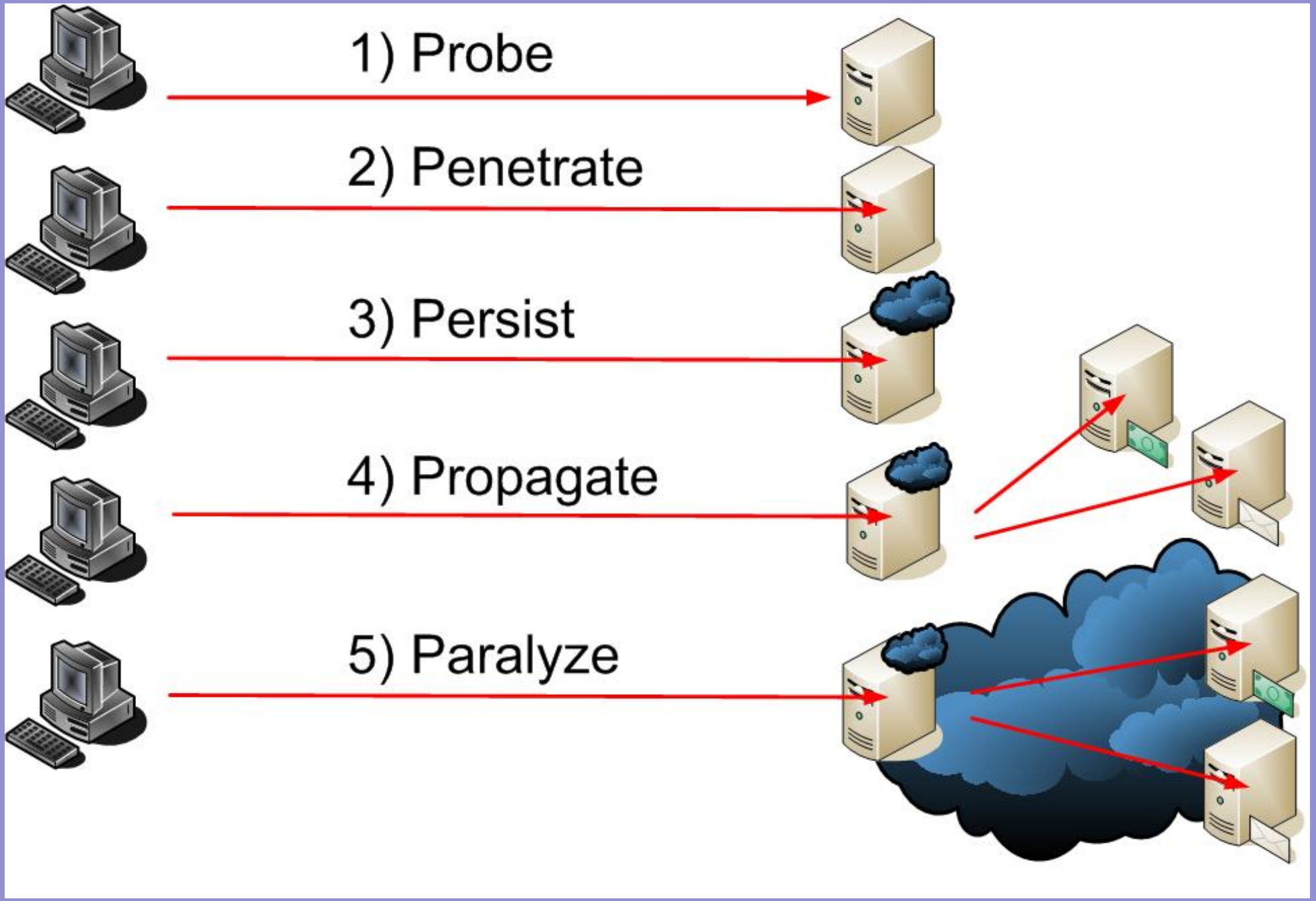
Die Cyber-Crime-Konvention des Europarates

Völkerrechtlicher Vertrag
Europarat: nicht Rat d. Europäischen Union

http://www.lukasfeiler.com/CyCC/

Die Anatomie eines Angriffs: wo beginnt die Strafbarkeit?

1) Probe
2) Penetrate
3) Persist
4) Propagate
5) Paralyze



The 5 Ps: Probe, Penetrate, Persist, Propagate, Paralyze

Tätergruppen

nach Skills:
- Script Kiddies
- IT-Profis
- Underground-Hacker

nach sozialem Umfeld
- Angestellte des Unternehmens
- Ehemalige Angestellte
- Angestellte des Konkurrenten
- Sonstige

Angriffe

auf die Vertraulichkeit (**C**onfidentiality)
auf die Integrität (**I**ntegrity)
auf die Verfügbarkeit (**A**vailability)

Angriffe auf die Vertraulichkeit von Daten & Systemen

Angriffsarten:

- Password Guessing & Bute Force
- Buffer Overflows
- Sniffing

Strafnormen: §§ 118a, 119, 119a StGB, §51 DSG

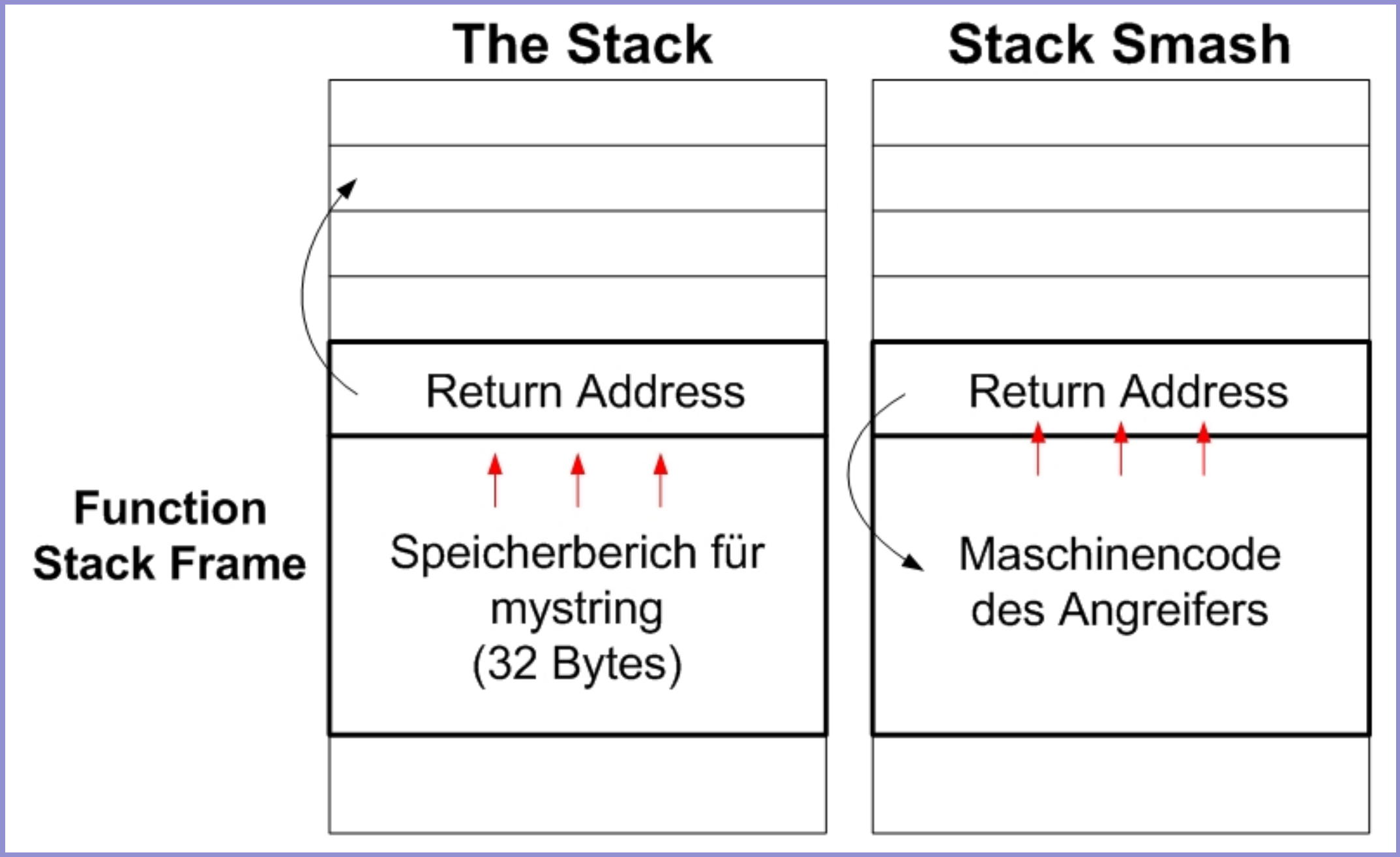
Password Guessing & Brute Force Attacks

Anwendungsfälle:
- Standard-Passwörter
- Leicht zu erratende Passwörter & bekannte Benutzernamen

→ Demonstration: Hacking eines FTP-Account

Buffer Overflows

Bedeutendste Angriffsform



→ Demonstration: CVE-2001-0010 BIND remote root exploit

§ 118a StGB Widerrechtlicher Zugriff auf ein Computersystem

Objektiver Tatbestand des § 118a Abs. 1:

Wer sich […]
zu einem Computersystem,
über das er nicht oder nicht allein verfügen darf,
oder zu einem Teil eines solchen
Zugang verschafft,
indem er spezifische Sicherheitsvorkehrungen im Computersystem verletzt

Objektiver Tatbestand:
- Zugang verschaffen
- Zu einem System über das er nicht (alleine) verfügen darf
- Indem er spezifische Sicherheitsvorkehrungen verletzt

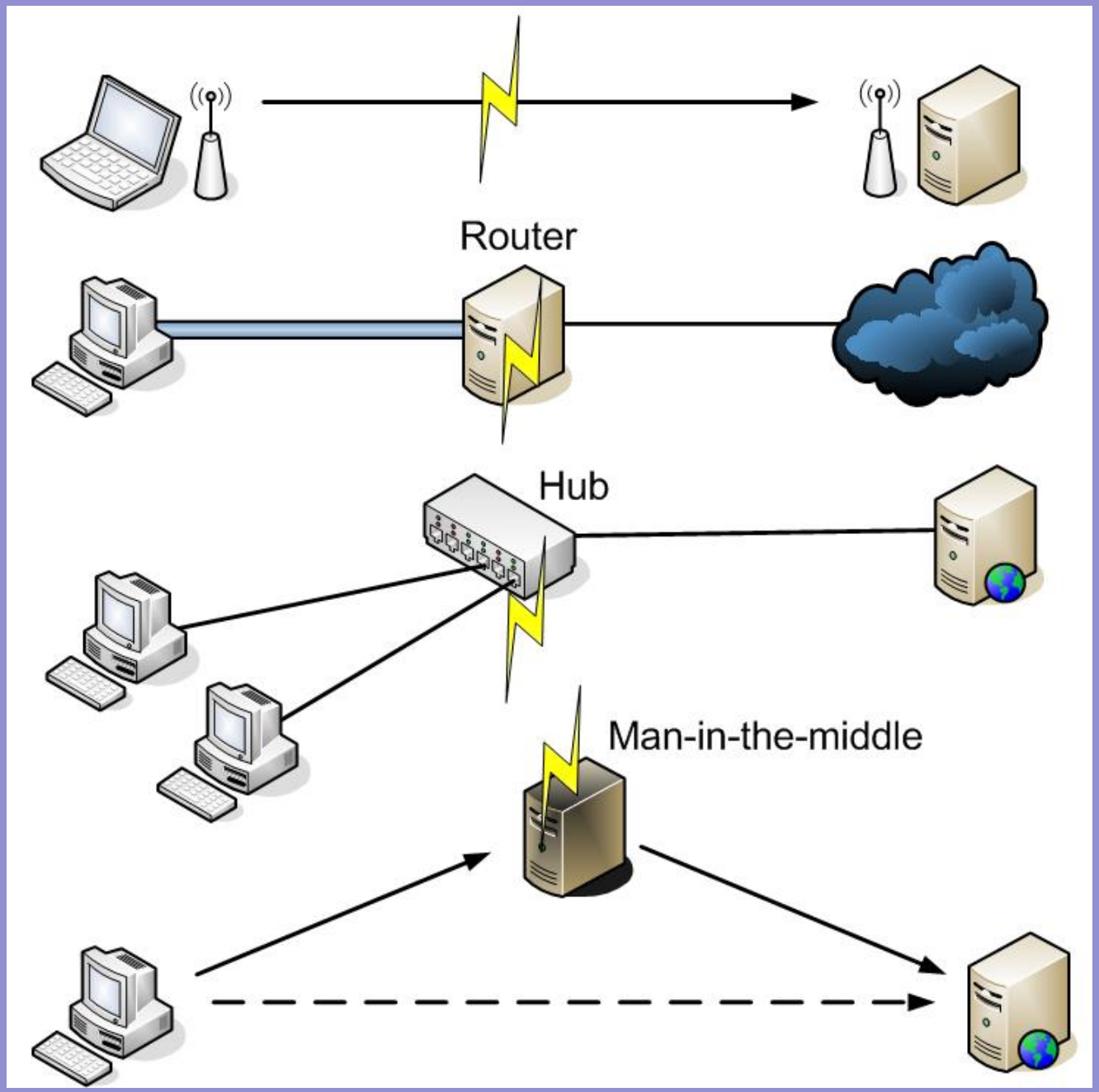
Subjektiver Tatbestand des § 118a Abs. 1:

Wer sich in der Absicht
sich oder einem anderen Unbefugten von in einem Computersystem gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen
und
dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht,
[und]
sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen […]

Subjektiver Tatbestand:
- (Eventual-)Vorsatz bezüglich des objektiven Tatbestandes
- **Absichtlichkeit** (es kommt ihm gerade darauf an) bezügl.
  1. Spionage, 2. **Verwendung** und 3. **Gewinn bzw. Schädigung**

Sniffing

Mitlesen fremden Datenverkehrs



1) WLAN sniffing

2) Hacking eines Routers

3) Promiscuous mode im LAN mit Hub

4) Man-in-the-middle-attack

→ Demonstration: mitlesen des FTP-Logins

§ 119 StGB Verletzung des Telekommunikationsgeheimnisses

Objektiver Tatbestand des § 119 Abs. 1:

§ 119 StGB. (1) Wer eine [Abhör-]Vorrichtung, die an der Telekommunikationsanlage oder an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt,

Objektiver Tatbestand:
- eine Abhörvorrichtung benützen

Subjektiver Tatbestand des § 119 Abs. 1:

§ 119 StGB. (1) Wer in der Absicht, sich oder einem anderen Unbefugten vom Inhalt einer im Wege einer Telekommunikation (§ 3 Z 13 TKG) oder eines Computersystems übermittelten und nicht für ihn bestimmten Nachricht Kenntnis zu verschaffen

Subjektiver Tatbestand:
- (Eventual-)Vorsatz bezüglich des objektiven Tatbestandes
- **Absichtlichkeit** (es kommt ihm gerade darauf an) bezügl. **Spionage des Inhalts der Nachricht am Übertragungsweg**

Problem: Sniffing v. allem, das keine Nachricht mit Inhalt ist; z.B. URLs
http://www.cnn.com/POLITICS/
http://www.example.com/msgBoard.php?nachricht=bin+ganz+deiner+meinung&autor=john_doe

§ 119a Missbräuchliches Abfangen von Daten

Objektiver Tatbestand des § 119a Abs. 1:

§ 119a StGB. (1) Wer
eine [Abhör-]Vorrichtung,
die an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt
oder
die elektromagnetische Abstrahlung eines Computersystems auffängt,

Objektiver Tatbestand:
- eine Abhörvorrichtung benützen

oder
- elektromagnetische Abstrahlung auffangen

Subjektiver Tatbestand des § 119a Abs. 1:

§ 119a StGB. (1) Wer
in der Absicht,
sich oder einem anderen Unbefugten von im Wege eines Computersystems übermittelten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen
und
dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht,
[und]
sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen,

Subjektiver Tatbestand:
- (Eventual-)Vorsatz bezüglich des objektiven Tatbestandes
- **Absichtlichkeit** (es kommt ihm gerade darauf an) bezügl.
  1. **Spionage von Daten am Übertragungsweg**, 2. **Verwendung** und 3. **Gewinn bzw. Schädigung**

§ 51 DSG Datenverwendung in Gewinn- oder Schädigungsabsicht

Objektiver Tatbestand des § 51 Abs. 1 DSG:

§ 51 DSG. (1) Wer personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat

Objektiver Tatbestand:

- **personenbezogene Daten** durch Beruf oder widerrechtlich erlangen
- diese **verwenden**

Subjektiver Tatbestand des § 51 Abs. 1 DSG:

§ 51 DSG. (1) Wer in der Absicht,
sich einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen,

Subjektiver Tatbestand:
- (Eventual-)Vorsatz bezüglich des objektiven Tatbestandes
- **Absichtlichkeit** (es kommt ihm gerade darauf an) bezügl. **Gewinn- bzw. Schädigung**

Sonstige Tatbestände

§ 120 Abs. 2a StGB: Mißbrauch von Tonaufnahme- oder Abhörgeräten

objektiver Tatbestand:

übermittelte Nachricht aufzeichnet, zugänglich macht od. veröffentlicht

subjektiver Tatbestand:

sich od. einem anderen unbefugten Kenntnis zu verschaffen

§ 123 Abs. 1 StGB: Auskundschaftung eines Geschäfts- od. Betriebsgeheimnisses

objektiver Tatbestand:

Geschäfts- oder Betriebsgeheimnis auskundschaften

subjektiver Tatbestand:

(Eventual-Vorsatz) es zu verwerten od. preiszugeben

Probleme beim Schutz der Vertraulichkeit von Daten und Systemen

Hacking ohne Verletzung spezifische Sicherheitsvorkehrungen (nach hA Buffer Overflows, Default-Passwörter)

Hacking ohne Spionage-, Verwendungs- und Gewinn- bzw. Schädigungsabsicht

Sniffing von Daten, die keine Nachrichten sind ohne Spionage-, Verwendungs- und Gewinn- bzw. Schädigungsabsicht

Nicht am Übertragungsweb befindliche E-Mails: nur durch §§ 118a, 123 StGB u. § 51 DSG geschützt
Grund: E-Mail ist kein verschlossener Brief iSd § 118 StGB (Analogieverbot des § 1 StGB); eher eine Postkarte

Phishing & Social Engineering Attacks

Opfer wird durch Täuschung zur Informationspreisgabe bewegt.
In Betracht kommende Tatbestände:

§ 146 StGB „normaler“ Betrug
§ 148a StGB Betrügerischer Datenverarbeitungsmißbrauch
§ 118a StGB erst bei Verwendung der erlangten Daten möglich

Bank of America Higher Standards

Online Banking Alert

Need additional up to the minute account information?
Sign In »

Change of Email Address

Your primary e-mail address for Bank of America Online Banking has been changed.

- Did You Know? You can change your address, order checks and more online. Sign in to Online Banking and click on the "Customer Service" tab.

Because your reply will not be transmitted via secure e-mail, the e-mail address that generated this alert will not accept replies. If you would like to contact Bank of America with questions or comments, please sign in to Online Banking and visit the customer service section.

Angriffe auf die Integrität von Daten & Systemen

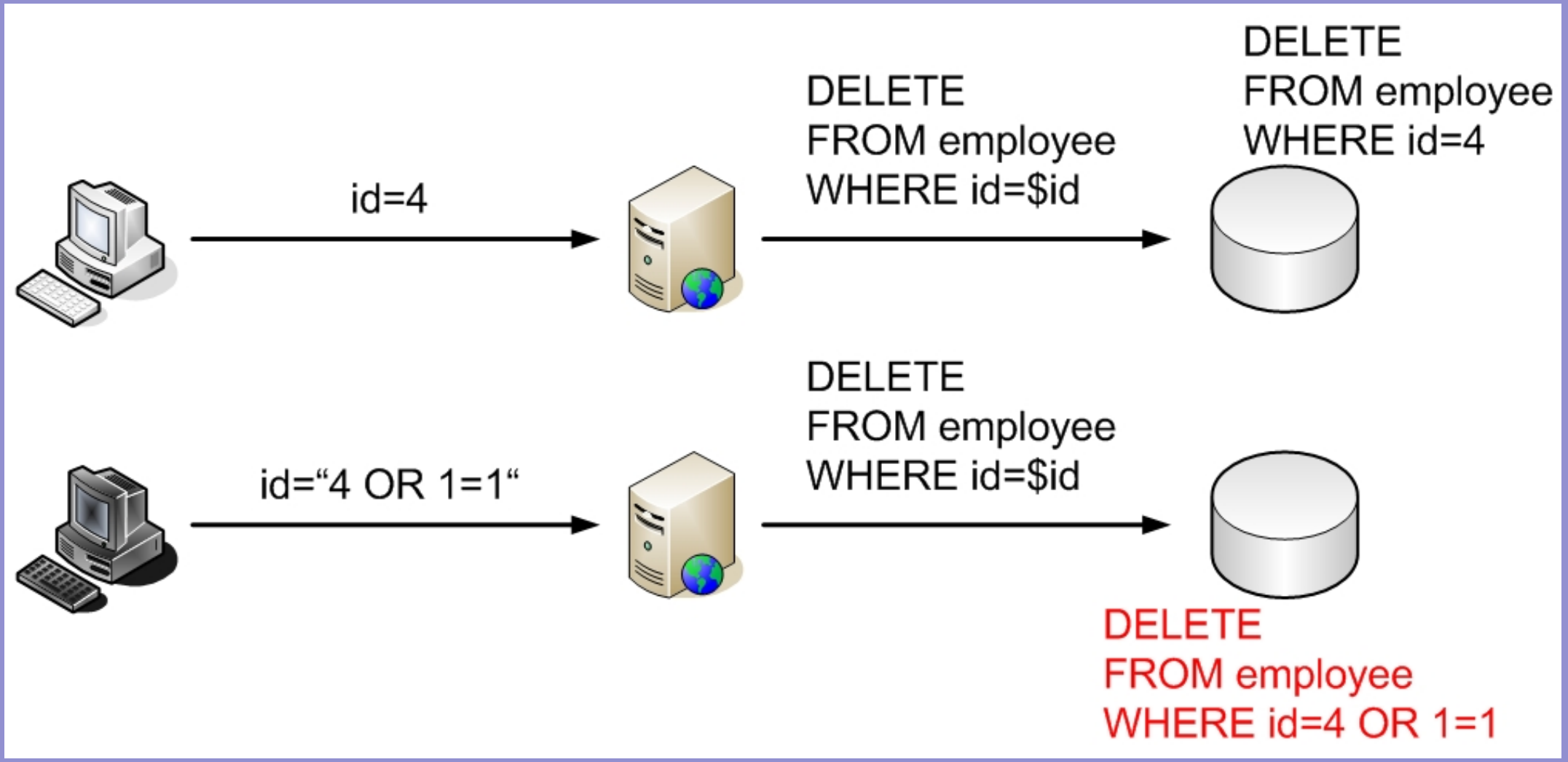
Angriffsarten:

- SQL-Injection
- nach erfolgreichem Hack einfach:
  Datenlöschung, Verschlüsselung

Strafnormen: § 126a StGB

SQL-Injection

Einschleusen von Code in eine Datenbankabfrage



→ **Demonstration: deleteEmployee.php**

§ 126a StGB Datenbeschädigung

Objektiver & subjektiver Tatbestand des § 126a Abs. 1:

§ 126a StGB. (1) Wer [vorsätzlich] einen anderen dadurch schädigt, daß er automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die er nicht oder nicht allein verfügen darf, verändert, löscht oder sonst unbrauchbar macht oder unterdrückt,

ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Objektiver Tatbestand:

- Daten verändern, löschen, unbrauchbar machen, unterdrücken

Subjektiver Tatbestand

- (Eventual-)Vorsatz bezüglich des objektiven Tatbestandes

Angriffe auf die Verfügbarkeit von Daten & Systemen

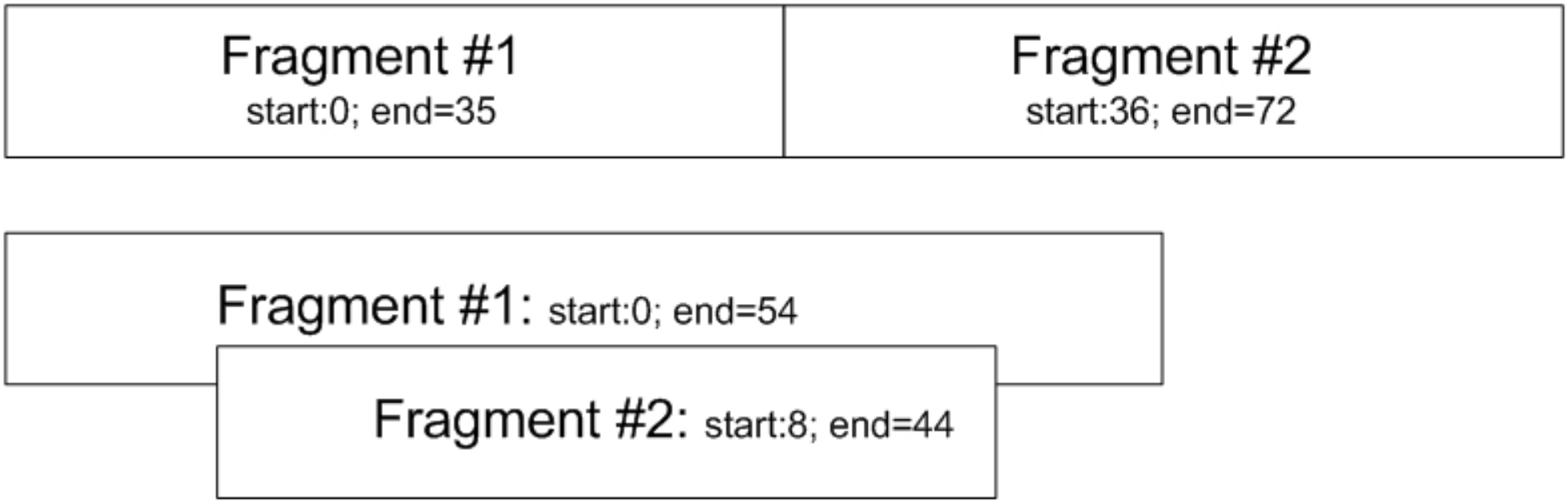
Erscheinungsformen:

- Denial of Service (DoS) Attacks
- Distributed Denial of Service (DDoS) Attacks

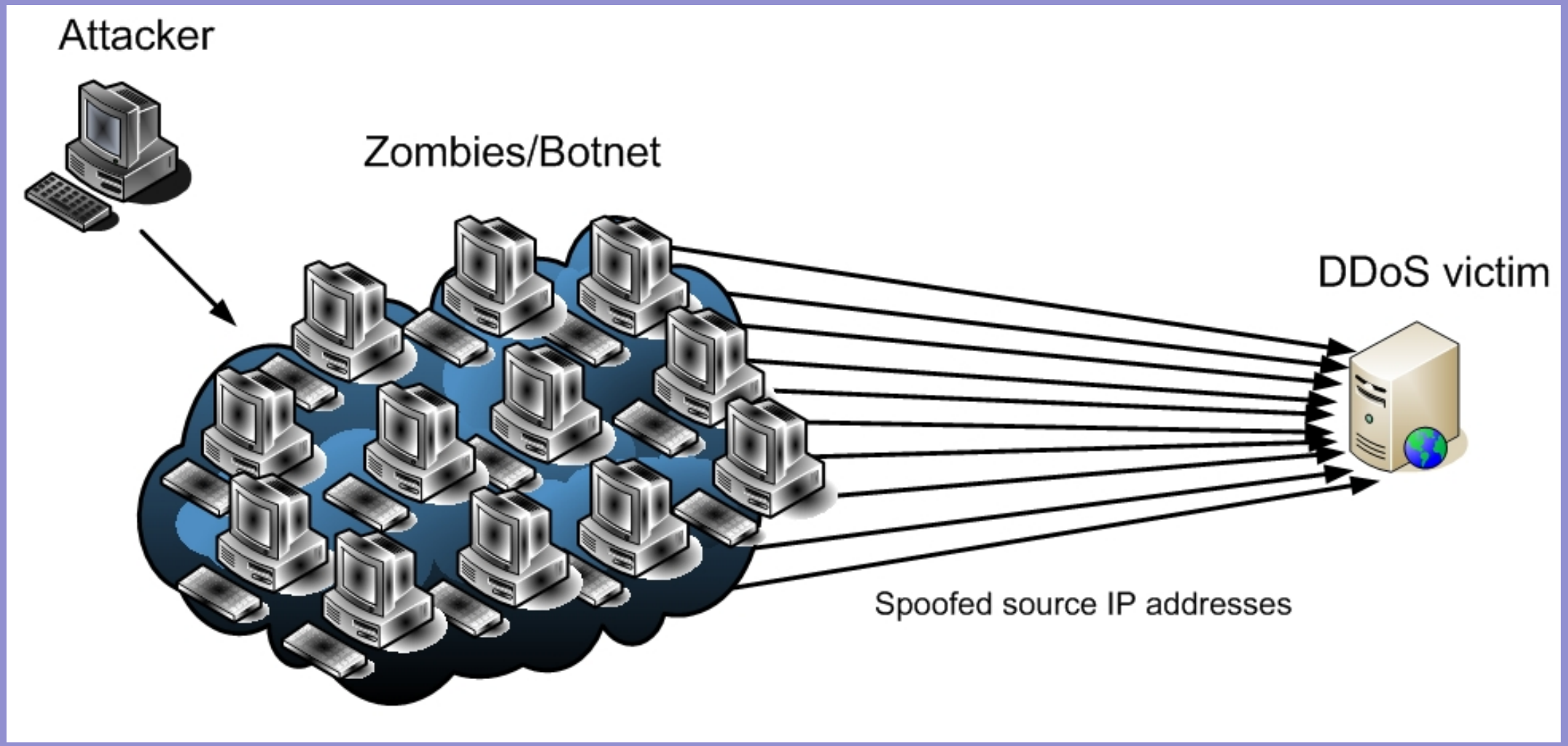
Strafnormen: § 126b StGB

Denial of Service (DoS) Attacks

- durch Überbeanspruchung der endlichen Resourcen
- durch ausnützen von Sicherheitslücken
  (insbes. Buffer Overflows)



→ **Demonstration: „teardrop attack“ CVE-1999-0015**



DDoS: der Angreifer verwendet zuvor gehackte “Zombies” um einen Server anzugreifen

Distributed Denial of Service (DDoS) Attack

§ 126b StGB Störung der Funktionsfähigkeit eines Computersystems

Objektiver & subjektiver Tatbestand des § 126b:

§ 126b StGB. (1) Wer [vorsätzlich] die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt

Objektiver Tatbestand:
- Funktionsfähigkeit durch Dateneingabe- od. Übermittlung schwer stört

Subjektiver Tatbestand
- (Eventual-)Vorsatz bezüglich des objektiven Tatbestandes

Problem: physische Angriffe

Strafbarkeit erfolgloser/unterbliebener Angriffe?

Strafnormen:
§ 15 StGB Strafbarkeit des Versuches
§ 126c StGB Missbrauch von Computerprogrammen oder Zugangsdaten

Strafbarkeit des Versuches

z.B: A versucht mittels Brute Force Attack einen Server der BAWAG zu hacken
Delikt: § 118a StGB iVm § 15 StGB

z.B: A versucht mittels Exploit einen Server der Este Bank zum Absturz zu bringen. Der Server weist die entsprechende Sicherheitslücke jedoch nicht auf.
Problem: Untauglichkeit des Tatobjekts

Port Scanning & Vulnerability Scanning

→ grundsätzlich Straflos

z.B: A scannt alle offenen Ports des BAWAG-Servers
z.B: A scannt nach Sicherheitslücken des Erste Bank-Servers

→ **Demonstration: Portscan mit nmap**

§ 126c StGB Missbrauch von Computerprogrammen oder Zugangsdaten

Objektiver Tatbestand des § 126c Abs. 1 StGB:

§ 126c StGB. (1) Wer
ein Computerprogramm,
das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung [der §§ 118a, 119, 119a, 126a, 126b] […] geschaffen oder adaptiert worden ist, oder eine vergleichbare solche Vorrichtung oder
ein Computerpasswort,
einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen
herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt

Objektiver Tatbestand:

Programm od. Passwort herstellen, zugänglich machen, besitzen, …

Subjektiver Tatbestand des § 126c Abs. 1:

§ 126c StGB. (1) Wer mit dem Vorsatz […], dass sie zur Begehung [der §§ 118a, 119, 119a, 126a, 126b] […] gebraucht werden

Subjektiver Tatbestand:
- (Eventual-)Vorsatz bezüglich des objektiven Tatbestandes
- (Eventual-)Vorsatz bezüglich Verwendung für genannte Straftaten

Rechspolitische Überlegungen

Ist der strafrechtliche Schutz von
- Vertraulichkeit
- Integrität
- Verfügbarkeit

ausreichend?

Danke

lukas.feiler@lukasfeiler.com
http://teaching.lukasfeiler.com