Zusammenfassung Informationssicherheit

Mathis Hermann

November 21, 2022

1 Gesetzliche Grundlagen

Schweizer Recht ist uneingeschränkt anwendbar, wenn Täter, Opfer und Tatort in der Schweiz liegen. Im Internet ist das ein Problem.

1.1 Gesetzestexte

Es gibt keum für das Internet spezifische Gesetzestexte in der Schweiz. Es gibt aber viele Gesetzestexte, die im Zusammenhang mit dem Internet angewendet werden: *1)* Obligationenrecht, *2)* Strafgesetzbuch, *3)* Datenschutzgesetz, *4)* Fernmeldegesetz, *5)* Urheberrechtsgesetz – (Liste nicht abschliessend)

Dabei können auch diverse Unterschiede zwischen CH und EU-Recht gefunden werden.

Recht	CH	EU
Widerrufsrecht	Freiwillig (10 Tage)	14 Tage
Lieferfrist	Keine Obergrenze	maximal 30 Tage; länger kann verabredet werden
Gewährleistung	2 Jahre	2 Jahre
Bestell-Button	Keine Vorgabe	Muss als letzter Punkt des "Vertrages" auf der Seite stehen und mit "Zahlungspflichtig bestellen" *eindeutig* beschriftet sein.
Preise	Tatsächlich zu bezahlender Preis in CHF inkl. aller nicht frei wählbarer Zuschläge jeglicher Art. Einheiten und Verrechnungssätze müssen klar ersichtlich sein.	Gesamtpreis einschliesslich aller Steuern und Abgaben.

Obligationenrecht Definiert Formvorschrift: Es braucht im Allgemeinen keine besondere Form für das Zustandekommen eines Vertrages.

Alle Parteien haben Rechte und Pflichten:

- Vertrag muss eingehalten werden
- Haftbarkeit bei versäumten Pflichten
- Kein Recht ohne Verpflichtungen

Datenschutzgesetz Gilt für das Bearbeiten von Daten natürlicher und juristischer Personen. Informationen können mit Verweis auf Datenschutz Gericht nicht vorenthalten werden.

- Personendaten – alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen
- Betroffene Personen – natürliche oder juristische Personen, über die Daten bearbeitet werden
- Besonders Schützenswerte Personendaten – Daten über:

- die religiösen, weltanschaulichen, politischen, oder gewerkschaftlichen Ansichten oder Tätigkeiten
- die Gesundheit, Intimsphäre oder Rassenzugehörigkeit
- Massnahmen der sozialen Hilfe
- Administrative oder strafrechtliche Verfolgungen und Sanktionen

Jede Person kann vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden. Lässt der Inhaber der Datensammlung Personendaten durch einen Dritten bearbeiten, so bleibt er auskunftspflichtig. Die Auskunft ist in der Regel schriftlich, in Form eines Ausdrucks oder einer Fotokopie sowie kostenlos zu erteilen.

Fernmeldegesetz Es ist eine Meldeplficht für Fernmeldeanlagen definiert – *Fernmeldedienst*: fernmeldetechnische Übertragung von Informationen für Dritte; Senden und Empfangen von Informationen über Leitungen oder Funk etc.

WLAN-Accesspoint, Mailserver, Chatserver Gameserver mit Chatfunktion, Powerline-LAN sind grundsätzlich meldepflichtig – Paragraph 2 bestimmt Ausnahmen.

Urheberrechtsgesetz Werke sind, unabhängig von ihrem Wert pder Zweck, geistige Schöpfungen der Literatur und Kunst, die individuellen Charakter haben. Urheber:in ist Person, welche das Werk geschaffen hat. Urheber:in hat das auschliessliche Recht über das zu bestimmen, ob, wann und wie das Werk verwendet wird.

Wird in einem Arbeitsverhältnis bei Ausübung dienstlicher Tätigkeiten sowie in *Erfüllung vertraglicher Pflichten* ein Computerprogramm geschaffen, so ist Arbeitgeber:in allein zur Ausübung der ausschliesslichen Verwendungsbefugnisse berechtigt.

1.2 revDSG

Per Juni 2023 wird eine Revision des Datenschutzgesetzes eingeführt:

- Nur noch natürliche Personen sind geschützt
- Genetische und biometrische Daten werden besonders schützenswerte Daten
- Grundsätze "Privacy by Design" und "Privacy by Default" werden eingeführt

- Informationspflicht gilt für jede From von Personendaten
- Ein Verzeichnis der Bearbeitungstätigkeiten wird zur Pflicht
- Pflicht zur raschen Meldung bei Verletzung der Datensicherheit

1.3 Praxis

Impressumspflicht gilt typischerweise sobald eine Website gewerblich oder kommerziell ist. Impressum muss leicht auffindbar sein und Vorname und Name (bzw. Firma), Adresse und E-Mail-Adressen beinhalten.

Abschliessend Informatiker:innen unterliegen beim Schreiben eines Programmes oder Aufsetzen eines Servers im Minimum immer der schweizerischen Gesetzgebung. Es existieren viele Gesetze, welche einfach zu übertreten sind, aber nicht übertreten werden dürfen.

Im Internet müssen je nachdem auch Gesetze von Drittstaaten berücksichtigt werden.

Gesetzestexte wurden nicht für Laien und nicht von technischen Fachleuten geschrieben. Gesetzestexte folgen nicht immer der Vernunft oder Logik.

Publikationen können helfen Zweifelsfälle zu beantworten.

2 Sicherheitsvokabular

2.1 Das Sicherheitsvokabular

2.2 Authentication, Authorisation und Accounting

3 Technische und nicht-Technische Angriffe

4 Verschlüsselung (Teil 1: Grundoperationen)

5 Verschlüsselung (Teil 2: PKI und andere Vertrauensmodelle

6 Netzwerkprotokolle für AAA

7 Angriffe und Szenarien (1-3)

8 Malware

8.1 Angriffe Entdecken

Indikatoren Zwei Arten: *1)* Indikatoren für einen Angriff (IOA) und *2)* Indikatoren für eine Kompromittierung. Ist grundsätzlich nicht das Selbe.

Häufigste Gefahr: Verschlüsselnde Ransomware – verschlüsselt alles bevor sie entdeckt werden kann. Höchste Gefährdung.

Die Indikatoren sind abhängig vom eigenen System.

Indikatoren für einen Angriff (IOA) Bei Angriff: *Sammeln* und dann *Analysieren.*

- Versagen eines Dienstes oder Zerstörung eines Assets
- Geänderte Leistung eines Subsystems
- Geändertes Verhalten eines Systems oder Subsystems

Sind nur Indikatoren und müssen nicht erfolgreich sein.

Indikatoren für eine Komprimittierung (IOC) Bei Angriff: *Isolieren* (Netzwerktechnisch nicht mehr erreichbar machen – unabhängig machen von anderen Systemen) und dann Systemzustand *einfrieren* (Snapshot erstellen und sicherstellen; Festplatten stromlos machen; Ausschalten und nicht herunterfahren – e.g. Stromstecker ziehen).

GANZ WICHTIG: Was muss bei einer Kompromittierung eines Systems gemacht werden?

- Andere Zustände eines Systems oder Subsystems
- Geänderte Leistung eines Subsystems
- Geändertes Verhalten eines Systems oder Subsystems
- Wertänderung von Assets durch externe Einflüsse

Bei Kompromittierung muss sofort gehandelt werden, da der Schaden immer grösser werden kann.

Firewall als Angriffsdetektion (und Verteidigung) Zum Netzwerkschutz werden Firewalls häufigst verwendet.

Aufgaben Firewall:

- Portfiltering
- Netzwerkverkehr untersuchen nach verdächtigen Aktivitäten
  - Injektions-Attacken
  - Fehlschlagende Loginversuche
  - Virensignaturen

Firewall macht ihre Aufgaben so gut sie kann und benötigt viele Kenntnisse über die Infrastruktur. Schwach, wenn Firewall nicht genug über Infrastruktur weiss. Meisten Firewalls machen nur Portfiltering.

Firewall muss nicht nur eingerichtet werden. Die Logs auswerten etc. muss auch gemacht werden – Expertenwissen benötigt. In der FW-Administration müssen die korrekten Personen angeheuert sein, damit diese korrekt behandelt wird.

Monitoring als Angriffsdetektion Monitoring erfasst typischerweise IOC und IOA.

- Typische IOAs
  - Logs
  - Fehlschlagende Loginversuche
  - Anormale Aktivitäten – Prozesse, die nicht mehr laufen / neu hinzugekommen sind
- Typische IOCs
  - Vorhandene files mit SUID-Flags – Wenn das File ausgeführt wird, läuft es mit den Rechten des File-Eigentümers
  - Treiber, deren Prüfsumme unbekannt sind – Pakete enthalten: Files, Install-Script, Prüfsummen für jedes File (prüfen ob das Paket korrekt entpackt wurde); Files identifizieren, welche (nicht) aus einer vertrauenswürdigen Quelle kommen

Privilege-Escalation: Berschaffung von höheren Privilegien

Intrusion Detection System Laufen und halten Angriffe innerhalb eines Sicherheitsperimeters fest. Dienen dazu, verdächtige Gegebenheiten aufzudecken. Wird zum *Perimeterschutz* verwendet. Ist passiv – beobachtet und meldet es weiter.

untersucht Informationsquellen nach IOCs oder IOAs; Intrusion Prevention System (IPS) hat zusätzlich Möglichkeit Einbrüche zu unterbinden.

Systeme sind Query-Basierte Firewalls.

Honeypot als Angriffsdetektion Systeme, welche Angreifende gezielt anziehen (e.g. Server, welcher gezielt eine Vulnerabilität hat). Jeder Zugriff auf einen Honeypot ist ein Indikator im Perimeter drin.

Wenn der Honeypot nur als ein solcher konfiguriert ist, kann jeder Zugriff auf den Honeypot als versuchter Angriff gewertet werden.

Tarpit als Angriffsdetektion Normale Dienste oder Geräte, welche Angreifer identifizieren und diese möglichst lange beschäftigen (e.g. wird immer langsamer) – Ziel ist es Angreifer möglichst lange aufzuhalten.

Muss möglichst aussehen, wie ein echtes System.

Beispiele für Tarpit:

- IP-Level-Tarpit – es wird simuliert, dass in einem Netz, alle IP-Adressen von Hosts besetzt sind; alle Hosts müssen betrachtet werden
- SMTP-Tarpit – es wird gewartet, um Antworten zu senden; wenn nächste Anfrage früher kommt als Antwort, kann davon ausgegangen werden, dass Angreifer da ist
- Harvester-Tarpit – (Harvester-Bots beeinträchtigen – e.g. Email-Harvester) Auf Website Link platzieren, welcher ganz viele E-Mail-Adressen anzeigt; Adressen werden unendlich viel zufällig generiert – mit robot.txt kann definiert werden, was bots dürfen (Bots binden, wenn sie sich nicht daran halten)

Aufwand für einen potentiellen Angreifer wird massiv erhöht, ohne legitime Benutzer zu beeinträchtigen.

8.2 Das Vertrauen in die Plattform

Es muss sichergestellt werden, dass die Plattformen vertrauenswürdig sind. Dafür werden *Trusted Plattform Modules* (TPM) verwendet. Mit einer TPM kann ein System verschlossen werden (e.g. Spielekonsolen). TPM kann (und wird) misbraucht werden, um das Digital-Rights-Movement zu umgehen.

Einleitung Es kann eine MITM-Attacke über die Plattform ausgeführt werden; Plattform muss zuerst überprüft werden, bevor ihr vertraut werden kann

Aufgaben eines Trusted Plattform Modules Beim Starten eines Computers wird das BIOS/UEFI geladen. Das TPM sorgt dafür, dass die CPU noch nicht gestartet wird. Das TPM berechnet Prüfsumme von UEFI, nimmt dessen Signatur überprüft sie. Wenn alles okay ist, kann das System gestartet werden.

Im TPM befindet sich:

- CA-Speicher, welcher nicht überschrieben werden kann
- hat eine HMAC (Möglichkeit zum Hashs erstellen)
- kann Signieren / Verify / decrypt / encrypt (RSA, ECC...)
- hat sichere Keystore (kann nicht ausgelesen werden)

TPM stellt sicher, dass keine MITM-Attacke ausserhalb des TPM möglich ist. Es stellt sicher, dass externe Kommunikation bis zur Plattform-Grenze immer sicher ist und dass aller Software vertraut werden kann.

Fähigkeiten der meisten TPM

Unified Extendable Firmware Interface (UEFI) ist ein teilweiser Ersatz für das BIOS. Es bietet:

- Vorteile
  - Unterstützung für Disks ¿2TB
  - Prozessorunabhängige Plattform für Treiber
  - Modularer Aufbau (Inhalt des UEFI kann modifiziert werden)
  - Integrierte Unterstützung eines Bootmanagers (Anstelle der Bootsektoren
- Nachteile
  - Inhalt vom UEFI kann modifiziert werden (Sicherheitstechnisch ein Nachteil)
  - Wenn nur noch speziell signierte Software gestartet werden kann (secure boot), kommt einem "Vendor Lock" gleich.

Sicherheit einer virtuellen Trusted Plattform Bei der Rowhammer-Attacke wird die Volatilität der Bits im dRAM ausgenützt. Somit könnte ein Bit geändert werden im dRAM und diese ausgenützt werden. Es kann mit Glück der private key für ssh verändert werden und somit die Sicherheit dessen verkleinern. Ein TPM kann einen solchen HW-Angriff nicht abwehren.

Trusted Plattform vs. TPM TPM und TP sind nicht dasselbe. Ein TPM stellt eine sichere Plattform in einem nicht vertrauenswerten System zur Verfügung für Teilaufgaben, während TP eine vollständige Plattform ist, die eine Dienstleistung einem Benutzer zur Verfügung stellt.

SIM-Karte eines Mobiltelefons stellt sicher, dass die Identität des Telefons nicht von einer Drittpartei übernommen werden kann.

9 Sicherheit von HW / Plattform / Virtualisierung

10 Sicherheit von OS / Software

11 Sicherheit im Netzwerk

12 Sicherheit beim Endbenutzer