

DATENSICHERHEIT

VORLESUNG AM SAE INSTITUTE

DOZENT: BJOERN ZAPADLO

ABOUT ME

Bjoern Zapadlo
Konstanz
35 Jahre

Engineering Manager / Consultant @ HolidayCheck AG

Informatik Studium 1999 - 2002
3 Agenturen in Stuttgart

HolidayCheck International Websites / neue Architektur
Neckermann / Thomas Cook

Dozent an der SAE, Dualen Hochschule Stuttgart, Hochschule
Furtwangen

PHP, Java, Scala, Javascript, CSS, Html, MySQL, MongoDB,
Elasticsearch, ...

CONTACT ME

bjoern.zapadlo@gmail.com

<http://www.zapadlo.de>

@BjoeZap

https://www.xing.com/profile/Bjoern_Zapadlo

<http://de.linkedin.com/pub/bjoern-zapadlo/36/889/1a5>

Facebook

Google+

HOLIDAYCHECK AG

Größtes deutsches Meinungsportal für Reise und Urlaub

Vermittlung von Reisen

Hauptsitz in der Schweiz, direkt am Bodensee

Weiterer Sitz in München

Börsennotiert über Tomorrow Focus AG

Existiert seit 1999

Ausgründungen in mehreren europäischen Ländern

Über 300 Mitarbeiter

YES, WE HIRE ;)

[HTTP://WWW.HOLIDAYCHECK.DE/
JOBS](http://www.holidaycheck.de/jobs)

JETZT ABER SCHLUSS MIT DER
WERBUNG...

UND IHR?

Name

Erwartungen

Wünsche

ORGANISATORISCHES

Skript

Pausen

...

AGENDA

1. Definition von Datensicherheit
2. Bedrohungen
3. Verteidigung
4. Datenschutz
5. Rechtliches
6. Standards
7. A closer look:
 - Newsletter
 - Passwörter
 - Authentifizierung
 - Authorisierung
8. Misc / Q&A

BEFORE WE START

ÜBUNG

Wo kommt ihr mit den Themen Datensicherheit und -schutz in Berührung?

THEMENSAMMLUNG

Welche Themen interessieren euch?

DEFINITIONEN

INFORMATIONSSICHERHEIT

Als Informationssicherheit bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden Systemen, welche die **Vertraulichkeit**, **Verfügbarkeit** und **Integrität** sicherstellen. Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von Schäden und der Minimierung von Risiken.

Datensicherheit und Informationssicherheit werden synonym gebraucht, oft wird die Thematik auch schlicht mit der Begrifflichkeit „Security“ bezeichnet.

Informationssicherheit bezieht sich auf alle relevanten Informationen einer Organisation oder eines Unternehmens einschließlich personenbezogener Daten

VERTRAULICHKEIT

Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden, dies gilt sowohl beim Zugriff auf gespeicherte Daten wie auch während der Datenübertragung.

INTEGRITÄT

Daten dürfen nicht unbemerkt verändert werden. Respektive es müssen alle Änderungen nachvollziehbar sein.

VERFÜGBARKEIT

Verhinderung von Systemausfällen; der Zugriff auf Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet werden.

DATENSCHUTZ

Es geht hierbei nicht um den Schutz von allgemeinen Daten vor Schäden, sondern um den Schutz persönlicher Daten vor Missbrauch.

Der Schutz personenbezogener Daten stützt sich auf das Prinzip der informationellen Selbstbestimmung. Diese wurde im BVerfG-Urteil zur Volkszählung festgeschrieben. Geschützt werden muss dabei die Privatsphäre, d. h. Persönlichkeitsdaten bzw. Anonymität müssen gewahrt bleiben (Geregelt in Datenschutzgesetzen (zum Beispiel Bundesdatenschutzgesetz)).

RANDTHEMEN & VERWANDTE BEGRIFFE

AUTHENTIZITÄT

Echtheit und Glaubwürdigkeit einer Person oder eines Dienstes müssen überprüfbar sein.

ZURECHENBARKEIT

(engl. accountability)

„Eine durchgeführte Handlung kann einem Kommunikationspartner eindeutig zugeordnet werden.“

VERBINDLICHKEIT/NICHTABSTREITBARKEIT

(engl. non-repudiation)

Sie erfordert, dass „kein unzulässiges Abstreiten durchgeführter Handlungen“ möglich ist. Sie ist unter anderem wichtig beim elektronischen Abschluss von Verträgen. Erreichbar ist sie beispielsweise durch elektronische Signaturen.

NICHT-ANFECHTBARKEIT

Der Nachweis, dass eine Nachricht versendet und empfangen worden ist (Authentizität/Nachweisbarkeit)

ZUGRIFFSSTEUERUNG

Reglementierung des Zugriffes von außen

ANONYMITÄT

ANYWAY? WHY? ME?

Gefahren durch Vernetzung / neue Endgeräte

Sicherheit hat eine besondere, immer größer werdende Bedeutung

Früher waren nur Firmen und Behörden Ziel von Hackerangriffen. Heute Gefahr für alle, die sich im Internet „tummeln“

Jeder trägt ein Stück Verantwortung

Extrem weites Feld

UND WO JETZT?

EIGENER PC

PROGRAMMIERSPRACHE

EIGENES VERHALTEN

HARDWARE SERVER

BETRIEBSSYSTEM NETZWERK

SOFTWARE APPLIKATION

DATENBANK ...

WELCHE GEFAHREN KENNT IHR?

VIREN XSS TROJANER
HACKERANGRIFFE PHISING
DNS-SPOOFING SPAM
DIALER DDOS-ATTACKE
SPYWARE TAN DIEBSTAHL
CLICKJACKING CSRF
HEARTBLEED

SCHADENSZENARIEN

GELD WEG

KUNDENDATEN WEG

IMAGESCHADEN

MEIN DATEN WEG

SOFTWARE / HARDWARE DEFFEKT

...

WER TUT DENN SOWAS?

HACKER

Werden oft als „die Guten“ hingestellt, da sie meist ohne kriminellen Hintergrund, sondern nur aus akademischem Interesse in Netze einbrechen. Allerdings kriegt man von denen, die dies mit anderen Interessen tun ja nichts mit.

CRACKER

Die „Bösen“. Versuchen Kopierschutzmechanismen kommerzieller Computerprogramme zu knacken und die Programme dann in Umlauf zu bringen.

CRASHER

Legen den Schwerpunkt darauf, fremde Computersysteme zum Absturz zu bringen (z.B. Durch DoS-Attacken).

SCRIPT KIDDIE

Der Dummie unter den Hackern. Nutzt schon bekannte Sicherheitslücken aus, um mit ihnen das Internet unsicher zu machen. Meist haben sie kein besonderes technisches Wissen, sondern handeln, um Aufmerksamkeit auf sich zu ziehen

UND WARUM?

Systemmissbrauch, durch illegitime Ressourcennutzung, z.B.
Bitcoin Mining

Veränderung von publizierten Inhalten, etc.

Sabotage

Spionage

Betrug und Diebstahl

IT'S ALL ABOUT
THE BENJAMINS

UND WIE OFT?

<http://map.ipviking.com/>

BEDROHUNGEN

ELEMENTARSCHÄDEN

Feuer

Überschwemmung

Sturm

Stromausfall

Systemausfall / Hardwaredefekt

MENSCH

Fehlbedienung

Löschen

Verschieben

“Überspeichern“

Schwache Passwörter

Aufschriebe

Weitergabe von Daten

Bequemlichkeit

Verlust von Notebooks, Handys, USB-Sticks

London pro Jahr in Taxis: >3000, >6000, >2000

Social Engineering => Emails

MAN IN THE MIDDLE

Zwischenschalten zwischen Sender und Empfänger

Einsehen / Manipulieren der Daten

ARP- / Gateway-Spoofing

WLAN-Snarfing

Host-Datei

Kontrolle über Netzwerk-Hardware

Ziel: z.B. Online Banking

BOTNETZE

Ein Botnet oder Botnetz ist eine Gruppe von automatisierten Computerprogrammen, sogenannten Bots. Die Bots (von englisch: robot „Roboter“) laufen auf vernetzten Rechnern, deren Netzwerkanbindung sowie lokale Ressourcen und Daten ihnen zur Verfügung stehen. In Deutschland gab es 2010 über 470.000 solcher Bots, von denen im Durchschnitt etwa 2.000 pro Tag aktiv waren.[1] Betreiber illegaler Botnetze installieren die Bots ohne Wissen der Inhaber auf Computern und nutzen sie für ihre Zwecke.

Einsatz als Proxy, SPAM, Phising, DDOS und Passwort Brute Force

DENIAL OF SERVICE

Als Denial of Service (kurz DoS, englisch für: Dienstverweigerung oder -ablehnung) wird in der digitalen Datenverarbeitung die Folge einer Überlastung von Infrastruktursystemen bezeichnet.

Solch eine Dienstverweigerung kann durch unbeabsichtigte Überlastungen verursacht werden oder durch einen mutwilligen Angriff auf einen Host (Server), einen Rechner oder sonstige Netzkomponenten in einem Datennetz. Dies geschieht in der Regel mit der Absicht, einen oder mehrere bereitgestellte Dienste arbeitsunfähig zu machen. Erfolgt solch ein Angriff koordiniert von einer größeren Anzahl anderer Systeme aus, so spricht man von Verteilter Dienstblockade oder englisch Distributed Denial of Service (DDoS). Normalerweise werden solche Angriffe nicht per Hand, sondern mit Backdoor-Programmen oder Ähnlichem durchgeführt, die sich von alleine

DISTRIBUTED DENIAL OF SERVICE

Wird die Überlastung von einer größeren Anzahl anderer Systeme verursacht, so wird von einer Verteilten Dienstblockade oder englisch Distributed Denial of Service (DDoS) gesprochen.

Mutwillige DDoS-Angriffe werden oft mit Hilfe von Backdoor-Programmen oder Ähnlichem durchgeführt. Diese Backdoor-Programme werden in der Regel von Computerwürmern auf nicht ausreichend geschützten Rechnern installiert und versuchen selbstständig, weitere Rechner im Netzwerk zu infizieren, um so ein Botnetz aufzubauen. Je größer das Botnetz, desto wahrscheinlicher ist, dass der Angriff selbst gegen gut geschützte Systeme durchdringt. Die Steuerung des Angriffs erfolgt über IRC, HTTP oder mittels eines Peer-to-Peer-Netzes.

DISTRIBUTED-REFLECTED-DENIAL-OF-SERVICE-ANGRIFF

Eine besondere Form stellt der Distributed-Reflected-Denial-of-Service-Angriff (DRDoS-Angriff) dar. Hierbei adressiert der Angreifer seine Datenpakete nicht direkt an das Opfer, sondern an regulär arbeitende Internetdienste, trägt jedoch als Absenderadresse die des Opfers ein (IP-Spoofing). Die Antworten auf diese Anfragen stellen dann für das Opfer den eigentlichen DoS-Angriff dar. Durch diese Vorgehensweise ist der Ursprung des Angriffs für den Angegriffenen nicht mehr direkt ermittelbar. Ein Beispiel für einen solchen Angriff ist die DNS Amplification Attack, bei der das Domain Name System als Reflektor missbraucht wird.

Weitere bekannte Methoden sind der Smurf- und der Fraggle-

TRACKING

Angriff auf die Privatsphäre

Tracking (Google Analytics, Omniture, ...)

Cookies

Web-Bugs

Sniffing

Webspoofing

Spyware

Adware

Keylogger

SURFSPUREN AUF DEM EIGENEM RECHNER

Surfhistorie / Bookmarks / Cache des Browsers mit
zwischengespeicherten Web-Seiten

E-Mails und -Adressen im Mailprogramm

Daten von Cookie-Servern

AUF EINEM PROXY-RECHNER BZW. BEIM PROVIDER

verschickte/empfangene Daten (unverschlüsselt)

Logfile: „Wer (welcher Rechner) rief wann welche Seite auf?“

AUF EINEM DER BESUCHTEN SERVER

Logfile: "Von welchem Rechner wurden wann welche Seiten
aufgerufen

Benutzerdaten, Session,

SPAM

Massenhaftes Senden vor allem von Emails

97% aller Emails sind Spam

Schaden: Arbeitszeit, Rechenzeit, ...

Rechtliches Problem: Keine einheitliche Regelung

Extrem hoher Schaden: (> 30 Milliarden EURO pro Jahr)

PHISHING

„password fishing“

Ausspähen der Daten

Gefälschte WWW-Seiten

(HTML-)Emails

Auch per Spionage-Software auf dem Rechner

Pharming => DNS / Host-Spoofing

Skimming => in Hardware (z.B. Geldautomaten)

XSS

Cross-Site Scripting

Angriff auf die Webapplikation

Über URL / Formulare

Code-Ausführung (Javascript)

Remote-Include (PHP)

BEISPIEL - PHP

```
<?php
if ( isset( $_GET[ 'COLOR' ] ) ) {
    include( $_GET[ 'COLOR' ] . '.php' );
}
?>

<form method="get">
    <select name="COLOR">
        <option value="red">red</option>
        <option value="blue">blue</option>
    </select>
    <input type="submit">
</form>
```

```
/vulnerable.php?COLOR=/etc/passwd%00
```

BEISPIEL - JAVASCRIPT

```
<?php  
$name = $_GET[ 'name' ];  
echo "Welcome $name<br>";  
echo "<a href='http://xssattackexamples.com/'>Click to Download</a>";  
?>
```

```
index.php?name=guest<script>alert( 'attacked' )</script>
```

```
index.php?name=<script>window.onload = function() {var link=document.getElemen
```

SQL-INJECTION

Angriff auf die Datenbank

Anlegen von Benutzern

Löschen von Daten

Ausgabe von Daten auf der Webseite erzwingen

CSRF

Cross-Site Request Forgery

Ausnutzen der Rechte eines echten Benutzers

über gefäkte Links

z.B. angemeldeter Benutzer legt neuen Benutzer an

VIREN / TROJANER / WÜRMER VIRUS

Richtet meist Schaden an

Verbreitung passiv via Datenträger / Email

TROJANER

Tarnt sich als nützliche Anwendung

Wird meist zum Ausspionieren genutzt

WURM

Verbreitet sich aktiv selber, meist via Internet

Oft kein direkter Schaden, sondern erst zeitverzögert

WER HAT EINEN
VIRENSCANNER
INSTALLIERT?
UND AUF DEM HANDY?

MOBBING / JUGENDSCHUTZ / ANBIETERKENNZEICHNU NG / BETRUG

Rechtlich relevante Themen

Sicherstellung des Alters durch Verfahren (PostIdent,
Personalausweis, Konto, ...)

Redaktionelle Prüfung und Freigabe von Beiträgen

Vollständiges Impressum falls es doch Beschwerden gibt

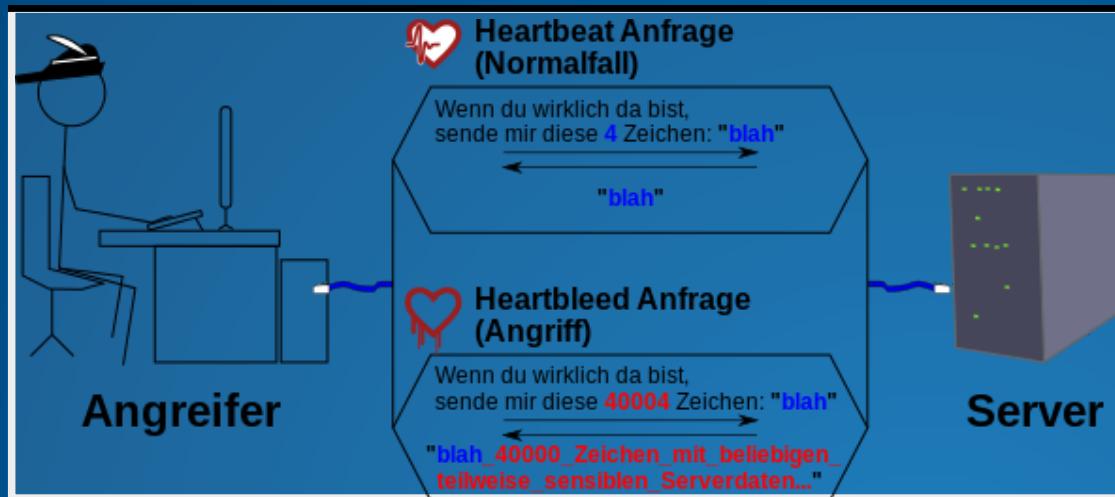
Logging von Aktivität zur nachträglichen Aufspüren von
Straftaten (Tracking)

HEARTBLEED

Der Heartbleed-Bug ist ein schwerwiegender Programmfehler in älteren Versionen der Open-Source-Bibliothek OpenSSL, durch den über verschlüsselte TLS-Verbindungen private Daten von Clients und Servern ausgelesen werden können. Der Fehler betrifft die OpenSSL-Versionen 1.0.1 bis 1.0.1f und wurde mit Version 1.0.1g am 7. April 2014 behoben. Ein großer Teil der Internetdienste, darunter auch namhafte Websites wie auch VoIP-Telefone, Router und Netzwerkdrucker waren dadurch für Angriffe anfällig.

Der Fehler befindet sich in der OpenSSL-Implementierung der Heartbeat-Erweiterung für die Verschlüsselungsprotokolle TLS und DTLS. Die Heartbeat-Erweiterung sieht vor, dass ein Kommunikationsteilnehmer eine bis zu 16 kByte große Menge an beliebigen Daten (Payload und Padding) an die Gegenseite schickt, die anschließend den Payload-Teil unverändert zurücksendet, womit periodisch abgeprüft werden kann, ob die Verbindung zum Server noch besteht.

Bei der fehlerhaften Implementierung dieser Funktion wird nicht überprüft, ob die angegebene Länge der Daten mit der tatsächlichen Länge der mitgelieferten Daten übereinstimmt. Ist die angegebene Länge größer als die tatsächliche Länge, so kopiert die OpenSSL-Implementierung über das Ende des Eingabepuffers hinaus Daten aus dem Heap in den Ausgabepuffer. Aufgrund der fehlenden Überprüfung kann ein Angreifer mit einer Anfrage bis zu 64 kByte des Arbeitsspeichers der Gegenstelle auslesen. Der Angriff kann



CLICKJACKING

Clickjacking ist eine Technik, bei der ein Computerhacker die Darstellung einer Internetseite überlagert und dann deren Nutzer dazu veranlasst, scheinbar harmlose Mausklicks und/oder Tastatureingaben durchzuführen.

Dabei lassen Angreifer die ahnungslosen Anwender – scheinbar – auf die überlagerten Objekte klicken. Tatsächlich jedoch wird der ursprüngliche Inhalt (Button/Link) der Internetseite ausgelöst. So geschieht es, dass der User – anstatt lediglich auf die ihm vorgegaukelten Links an einer Stelle zu klicken – eine vom Hacker definierte, beliebige Aktion auslöst.

Dies betrifft Seiten, die beispielsweise Links und Schaltflächen zur Konfiguration von Systemeinstellungen enthalten. Während der Nutzer also denkt, er tätige harmlose Eingaben in einer Internetseite, ändert er in Wahrheit, ohne es zu merken, z. B.

Dies wird meist mit Hilfe von Frames oder IFrames vorgenommen.

Ein Schutz ist u.a. die Verwenung von Framekiller Javascript-Code und X-Frame-Options-Headers.

[YouTube Demo](#)

VERTEIDIGUNG

THINK!
GEHIRN EINSCHALTEN
GESUNDES MISSTRAUEN

FAKTOR MENSCH

Sensibilisieren z.B. arbeiten mit eingeschränkten Benutzerrechten

Planung von Maßnahmen / Strategie

Ständige Schulung von Mitarbeitern

"Interne" Angriffe vornehmen

Passwörter

Richtiges Löschen

Richtes Aufbewahren von Dateien

Risikoanalysen

Disaster-Recovery

FIREWALLS

Abgrenzung von sicheren und unsicheren Netzen

Barriere für unerwünschte Daten

Ggf. Überprüfung der durchgelassenen Daten

Ansätze

- Paketfilterung
- Stateful Inspection
- Überprüfung auf Applikationsebene

Personal Firewalls

IDS

Intrusion Detection System

Software / Appliance

Prüf-Ebenen

- Netzwerk
- Applikation
- Datenbank

Warnehmung > Mustererkennung > Reaktion

Statisch vs. Heuristisch

Probleme: Falschmeldungen / Aufwändig

HONEYBOT

Als ein Honigtopf oder auch englisch Honeypot (früher auch Iron Box genannt) wird in der Computersicherheit ein Computerprogramm oder ein Server bezeichnet, das Netzwerkdienste eines Computers, eines ganzen Rechnernetzes oder das Verhalten eines Anwenders simuliert. Honeypots werden eingesetzt, um Informationen über Angriffsmuster und Angreiferverhalten zu erhalten. Erfolgt ein Zugriff auf einen derartigen virtuellen Dienst oder Nutzer, werden alle damit verbundenen Aktionen protokolliert und gegebenenfalls ein Alarm ausgelöst.

ANONYMISIERUNG

Verschleierung von Software, Cookies, Herkunft, ...

Private Modus in Firefox und Chrome

Browser-Addons z.B. für Chrome / FF

Proxy-Services aka Anonymizer

TOR-Netzwerk

@ HOME

Viruskiller / Adware / Spyware und automatische Signatur-
Updates

Firewall installieren (Test mit Online-Portscanner)

Firewall auf Router einschalten

Regelmässig Sicherheitsupdates einspielen

(Surf)verhalten an die Gefahren anpassen

Passwörter verwenden: Passwort-Regeln

WPA(2) bei WLAN

(Surfaccount mit wenigen Rechten einrichten.)

(Browser / Email-Client abdichten)

REMOTE ACCESS

VPN

SSH

FTPS BZW. SFTP

WEBAPPLIKATION

AKTUELLE KOMPONENTEN
BENUTZEN:

Betriebssystem / Datenbank / Programmiersprache /
Frameworks

SICHERE
PROGRAMMIERRICHTLINIEN
BEACHTEN

Escaping / Filtern / Validierung

SECURITY BEST PRACTICES /
HÄRΤEN DER APPLIKATION

Session / Formulare (Token, Captcha) / URL (Checksumme) /

BIOMETRISCHE
VERFAHREN
FINGERABDRUCK
RETINA

...

PROBLEM: TEUER UND NOCH
UNAUSGEREIFT BZW.
ANGREIFBAR

2 FAKTOR AUTHENTIFIZIERUNG

Die Zwei-Faktor-Authentifizierung (kurz 2FA) dient dem Identitätsnachweis eines Nutzers mittels der Kombination zweier verschiedener Komponenten. Das kann etwas sein, was er weiß, etwas, was er besitzt, oder etwas, was untrennbar zu ihm gehört. Aus dem Alltag ist dies z. B. vom Geldautomaten bekannt. Erst die Kombination aus Bankkarte und PIN ermöglicht die Transaktion.

Die Zwei-Faktor-Authentifizierung als Identitätsnachweis ist nur dann funktionsfähig, wenn beide benötigten Faktoren eingesetzt werden und korrekt sind. Fehlt eine Komponente oder wird sie falsch verwendet, lässt sich die Identität nicht zweifelsfrei feststellen. Der Zugriff, der durch die Zwei-Faktor-Authentifizierung geschützt ist, bleibt verweigert. Die Faktoren können sein:

- etwas, was der Nutzer besitzt: z. B. ein Token (USB-Stick etc.), eine Bankkarte, ein Schlüssel u. Ä.,
- etwas, was der Nutzer weiß: z. B. sein Benutzername, Passwort, PIN, TAN u. Ä., sowie
- etwas, was als körperliches Charakteristikum untrennbar zum Nutzer gehört: z. B. sein Fingerabdruck, die Regenbogenhaut (Iris) seines Auges, seine Stimme u. Ä.

WELCHEN TOKEN HABEN WIR
WOHL HEUTE IMMER DABEI?

MOBILTELEFON

Google Authenticator App Android (Ja, gibt's auch für iPhone)
Wordpress

ONLINE BANKING - TAN

TAN-LISTE

Beim klassischen TAN-Verfahren erhält der Teilnehmer beim Electronic Banking, meist per Post, eine Liste von Transaktionsnummern. Bei jedem Buchungsvorgang – der Transaktion – muss eine beliebige TAN der aktiven Liste eingegeben werden. Sie ist eine Ergänzung zur Persönlichen Identifikationsnummer (PIN). falls die Bank nach Eingabe der korrekten PIN einen Buchungsauftrag mit korrekter TAN erhält, geht sie davon aus, dass der Auftrag vom Kunden abgesendet wurde. Die TAN wird von der Bank als Quasi-Unterschrift interpretiert. Sie verfällt nach einmaligem Gebrauch. Wenn die TAN-Liste zur Neige geht, erhält der Kunde von der Bank nach Anforderung oder automatisch eine neue.

Auf Grund von stark anwachsenden Phishing-Angriffen wird

INDIZIERTE TAN-LISTE

Einen Schritt weiter geht das Verfahren der indizierten Transaktionsnummern, kurz iTAN: Der Kunde kann hier seinen Auftrag nicht mehr mit einer beliebigen TAN aus seiner Liste legitimieren, sondern wird von der Bank aufgefordert, eine bestimmte, durch eine Positionsnummer (Index) gekennzeichnete TAN aus seiner zu diesem Zweck nun durchnummerierten Liste einzugeben. Der TAN-Aufforderung muss der Kunde innerhalb weniger Minuten folgen. Außerdem wird die angeforderte TAN auch im Falle einer Nichtverwendung im Bankrechner als verbraucht gekennzeichnet.

Auch dieses Verfahren wird mittlerweile von Hackern auf zwei verschiedene Weisen angegriffen:

MTAN

Die Variante Mobile TAN (mTAN) oder smsTAN besteht aus der Einbindung des Übertragungskanals SMS. Dabei wird dem Onlinebanking-Kunden nach Übersendung der ausgefüllten Überweisung im Internet seitens der Bank per SMS eine nur für diesen Vorgang verwendbare TAN auf sein Mobiltelefon gesendet. Der Auftrag muss anschließend mit dieser TAN bestätigt werden.

TAN GENERATOR

Mit einem TAN-Generator können TANs elektronisch erzeugt werden. Hierzu muss dieser mit der Bank synchronisiert und bei jeder Transaktion mit der EC-Karte autorisiert werden. Anschliessend wird aus den Daten der Transaktion bei der Bank und via Generator eine TAN erzeugt und diese wird abgeglichen. Die Eingabe der benötigten Daten (meist Kontonummer und Betrag) kann dabei über eine Tastatur, Flicker-Codes oder QR Codes erfolgen.

WORDPRESS

BELIEBTESTES TOOL IM INTERNET

Daher sehr beliebtes Angriffsziel

HAUPTANGRIFFSPUNKT SIND DIE
PLUGINS

Aktuell halten

nicht benötigte Plugins deinstallieren

Security Plugins nutzen (Google Authenticator)

HARDWARE

RECHENZENTRUM

Schutz vor Elementarschäden

Geheimer Ort

Zweites RZ

Zugangskontrolle

SERVER

Doppelt ausgeführt

Standardkomponenten

Virtualisierung

Monitoring

BACKUP

WIE SICHERT IHR EURE DATEN?

BACKUP

Medien

Festplatte / Bänder / DVD / BlueRay / Online-Backup

Backup vs. Archivierung vs. Image

Strategien

Full-Backup / Differentiell / Inkrementell / Mischtaktik

Was ist zu sichern?

Lagerung der Backups

Frequenz der Backups

BACKUP SPANNUNGSVERHÄLTNISS

Kosten

vs.

Geschwindigkeit

vs.

Sicherheit

vs.

Lebenszeit

RAID

REDUNDANT ARRAY OF INDEPENDENT DISKS

RAID 0: Geschwindigkeit

RAID 1: Sicherheit

RAID 5: Geschwindigkeit + Sicherheit

Raid ist kein Ersatz für ein Backup

VERSCHLÜSSELUNG - SYMMETRISCH

Ver- und Entschlüsselung erfolgen mit ein und demselben
(geheimen) Schlüssel

Bsp.: vertrauliche Speicherung von Daten eines Benutzers oder
gemeinsam benutzter Daten einer Benutzergruppe lokal, auf
Disketten oder einem Server.

Problem:

Einsatz im Netz, da Schlüssel paarweise vereinbart, geheim
gehalten und sicher übertragen werden müssten

VERSCHLÜSSELUNG - ASYMMETRISCH

Eine Nachricht wird nicht mehr mit ein und dem gleichen Schlüssel ver- und entschlüsselt, sondern mit zwei unterschiedlichen, einander zugeordneten Schlüsseln:
Öffentlich und **privater** Schlüssel

Öffentlicher Schlüssel öffentlich bekannt Digitale Unterschriften
(Beweis der Originalität eines elektronischen Dokuments)

Der öffentliche Schlüssel einer Person wird verwendet, um eine Nachricht an diese Person zu verschlüsseln

Der private Schlüssel wird zur Decodierung der verschlüsselten Nachricht verwendet und steht nur dem Empfänger zur Verfügung

Besitz des öffentlichen Schlüssels einer Person ermöglicht

VERSCHLÜSSELUNG - ASYMETRISCH

Mit Hilfe des öffentlichen Schlüssels kann diese Nachricht nicht gelesen werden

Austausch der Schlüssel häufig symmetrisch verschlüsselt

Worst case: Verlust / Kompromitierung des persönlichen Schlüssels

100 - 1000 mal langsmaer als symmetrische Verschlüsselung

VERSCHLÜSSELUNG - ALGORITHMEN

UNSICHER

Data Encryption Standard, DES

Md5

Sha1

(RELATIV) SICHER

Sha256

Sha3

Triple DES, 3DES

AES

Blowfish / Twofish

VERSCHLÜSSELUNG

KERCKHOFFS-PRINZIP

Die Sicherheit eines Verfahrens darf nicht von der Geheimhaltung des Verfahrens abhängen, sondern nur von der Geheimhaltung des Schlüssels.

*[Auguste Kerkhoffs: *La Cryptographie militaire. Journal des Sciences Militaires*, Januar 1883.]*

VERSCHLÜSSELUNG VS.
HASHING

UMKEHRBARKEIT

ZIEL: VERTRAULICHKEIT VS.
INTEGRITÄT

KRYPTOANALYSE

DURCH BIGDATA UND AKTUELLE
RECHENPOWER IMMER
EINFACHER

SPRACHE IST NICHT NORMAL
VERTEILT

SICHERER ALGORITHMUS UND
AUSREICHEND LANGER
SCHLÜSSEL BLEIBEN DIE
VORAUSSETZUNG FÜR
SICHERHEIT

STEGANOGRAPHIE

VERSTECKTE INFORMATION Z.B.
IN BILDERN

ZUSÄTZLICH VERSCHLÜSSELUNG
MÖGLICH



STEGANOGRAPHIE VS. KRYPTOGRAPHIE

STEGANOGRAPHIE BIETET EINE
WEITERE STUFE VON
VERTRAULICHKEIT

- Kryptographie: Vertraulichkeit der Nachricht
- Steganographie: Vertraulichkeit der Existenz der Nachricht
- Steganographisches System wird als unsicher betrachtet,
wenn die Existenz der eingebetteten Nachricht erkannt
werden kann

HTTPS

Das HTTPS-Protokoll (HyperText Transfer Protocol Secure) wird zur Verschlüsselung und zur Authentifizierung der Kommunikation zwischen Webserver und Browser im World Wide Web verwendet.

Standard-Port ist 443 und die Verschlüsselung der Daten geschieht mittels SSL/TLS.

Unter Verwendung des SSL-Handshake-Protokolls findet zunächst eine geschützte Identifikation und Authentifizierung der Kommunikationspartner statt.

Anschließend wird mit Hilfe asymmetrischer Verschlüsselung oder des Diffie-Hellman-Schlüsselaustauschs ein gemeinsamer symmetrischer Sitzungsschlüssel ausgetauscht. Dieser wird schließlich zur Verschlüsselung der Nutzdaten verwendet.

SECURITY AUDIT / PENETRATIONTEST

Einbruchversuche

TÜV (Gütesiegel) / Bundesamt für Sicherheit in der
Informationstechnik / Externe Dienstleister

Betrachtung von

- Netzwerk
- Server
- Software
- Applikation
- Organisation
- ...

Auf aktuellem Stand bleiben

Blind für die eigene Sicherheit

DATENSCHUTZ

DEFINITION

Datenschutz bezeichnet den **Schutz des Einzelnen vor dem Missbrauch personenbezogener Daten.**

Der Begriff wurde auch verwendet für Schutz wissenschaftlicher und technischer Daten gegen Verlust oder Veränderung – und Schutz gegen Diebstahl dieser Daten.

Heute bezieht sich der Begriff meist auf den Schutz personenbezogener Daten.

Bei personenbezogenen Daten wurde er auch für Schutz vor „Verdatung“ verwendet.

Im englischen Sprachraum spricht man von „privacy“ (Schutz der Privatsphäre) und von „data privacy“ oder „information privacy“ (Datenschutz im engeren Sinne).

Im europäischen Rechtsraum wird in der Gesetzgebung auch der Begriff „data protection“ verwendet.

Heute wird der Zweck des Datenschutzes darin gesehen, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird.

Datenschutz steht für die Idee, dass jeder Mensch grundsätzlich selbst entscheiden kann, **wem wann welche** seiner persönlichen Daten zugänglich sein sollen. Der Datenschutz will den so genannten gläsernen Menschen verhindern.

Regelungen in jedem Land anders:
USA vs. Europäische Union vs. Deutschland

Hauptprinzipien des Datenschutzes sind

- Datensparsamkeit und Datenvermeidung
- Erforderlichkeit
- Zweckbindung

Der Datenschutz bezieht sich auf die **Erhebung** (= Beschaffen), die **Verarbeitung** (= Speichern, Verändern, Übermitteln, Sperren, Löschen) und die **Nutzung** (=Verwenden) personenbezogener Daten.

PRINZIPIEN

Auf der Internationalen Datenschutzkonferenz 2005 haben die Datenschutzbeauftragten in ihrer „Erklärung von Montreux“ darüber hinaus an die international anerkannten Datenschutzprinzipien erinnert. Diese sind:

1. Prinzip der Zulässigkeit und Rechtmäßigkeit der Erhebung und Verarbeitung der Daten
2. Prinzip der Richtigkeit
3. Prinzip der Zweckgebundenheit
4. Prinzip der Verhältnismäßigkeit (vgl. Verhältnismäßigkeitsprinzip)
5. Prinzip der Transparenz
6. Prinzip der individuellen Mitsprache und namentlich der Garantie des Zugriffsrechts für die betroffenen Personen
7. Prinzip der Nicht-Diskriminierung
8. Prinzip der Sicherheit
9. Prinzip der Haftung
10. Prinzip einer unabhängigen Überwachung und gesetzlicher Sanktionen
11. Prinzip des angemessenen Schutzniveaus bei grenzüberschreitendem Datenverkehr

DATENSCHUTZ IST EIN ZWEISCHNEIDIGES SCHWERT

Datenschutz vs. Informationsfreiheit

Kosten des Datenschutzes (Datenschutzbeauftragter)

Datenschutz und Kriminalitätsbekämpfung

Datenschutz und Wissenschaft / Medizin

Nur was der Kunde gezielt verbietet ist verboten, z.B. der Verkauf von Daten

RECHTLICHES

STRAFRECHT

Jegliches rechtswidrige Verändern, Löschen, Unterdrücken oder Unbrauchbar-Machen fremder Daten erfüllt den Tatbestand nach § 303a StGB (Datenveränderung). In besonders schweren Fällen ist dies auch nach § 303b I Nr. 1 StGB („Computersabotage“) strafbar und wird mit Haftstrafe von bis zu fünf Jahren oder Geldstrafe bestraft. Die Durchführung von DDOS-Attacken stellt seit 2007 ebenfalls eine Computersabotage dar, gleiches gilt für jegliche Handlungen, die zur Beschädigung eines Informationssystems, das für einen anderen von wesentlicher Bedeutung ist, führen.

Das Ausspähen von Daten (§ 202a StGB), also die Erlangung des Zugangs zu fremden Daten, die hiergegen besonders geschützt sind, wird mit Haftstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. Das Abfangen fremder Daten in Netzen oder aus elektromagnetischen Abstrahlungen ist seit 2007 ebenfalls strafbar, anders als bei § 202a StGB kommt es hier nicht auf eine besondere Zugangssicherung an. Das sich Verschaffen, Erstellen, Verbreiten, Öffentlich-Zugänglichmachen etc. von sog. „Hackertools“ steht ebenfalls seit 2007 unter Strafe, wenn damit eine Straftat vorbereitet wird (§ 202c StGB).

Daten sind nach § 202a Abs. 2 in Verbindung mit Abs. 1 aber nur vor dem Ausspähen geschützt, wenn sie „besonders gesichert“ sind, um ein Ausufern des Tatbestandes zu vermeiden. Das heißt, erst wenn der Nutzer seine Daten technisch schützt genießt er auch den strafrechtlichen Schutz. Die frühere Debatte, ob das „Hacken“ ohne Abruf von Daten strafbar sei, ist hinfällig, seit der Wortlaut der Norm 2007 derart geändert wurde, dass Strafbarkeit bereits mit Erlangung des Zugangs zu Daten einsetzt. Weiter ist umstritten, ob die Verschlüsselung zur besonderen Sicherung zählt. Sie ist zwar sehr effektiv, aber es wird argumentiert, die Daten seien ja nicht gesichert sondern lägen nur in „unverständlicher“ bzw. schlicht „anderer“ Form vor.

Als Computerbetrug wird nach § 263 a StGB mit Geldstrafe oder Freiheitsstrafe bis zu fünf Jahren bestraft, wenn Datenverarbeitungsvorgänge zur Erlangung von Vermögensvorteilen manipuliert werden. Schon die Erstellung, Verschaffung, Anbietung, Verwahrung oder Überlassung dafür geeigneter Computerprogramme ist strafbar.

ZIVILRECHT

Nach § 33 DSG 2000 besteht ein Anspruch auf Schadenersatz der Betroffenen, wenn Daten schuldhaft entgegen den Bestimmungen des DSG 2000 verwendet werden. Ein derartiger Schadenersatzanspruch setzt den Eintritt eines Schadens voraus, der durch den Betroffenen oft schwer nachzuweisen sein wird. Aus diesem Grunde wurde für besondere Fälle, nämlich dann, wenn durch eine öffentlich zugängliche Datenverwendung von sensiblen Daten, Daten über die Kreditwürdigkeit des Betroffenen oder strafrechtlich relevante Daten schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt wurden, die zu seiner Bloßstellung führen, ein Anspruch auf angemessene Entschädigung unabhängig vom tatsächlichen Schadenseintritt festgelegt.

Für die Verpflichtung zum Schadenersatz haftet der Auftraggeber auch dann, wenn das schädigende Ereignis durch einen Mitarbeiter oder eine Mitarbeiterin herbeigeführt wurde. Das DSG normiert eine Beweislastumkehr, sodass die Haftung nur dann auszuschließen ist, wenn bei Feststehen einer Übertretung des Gesetzes der Beklagte nachweist, dass ihn an der Übertretung der Norm kein Verschulden trifft.

In den §§ 51 f DSG sind gerichtliche Strafbestimmungen normiert. So wird etwa die, in der Absicht, sich einen vermögensrechtlichen Vorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen, durchgeführte missbräuchliche Verwendung von personenbezogenen Daten, die dem Täter ausschließlich in seiner beruflichen Beschäftigung zugänglich geworden sind, mit Freiheitsstrafe bis zum einem Jahr bedroht. Auch im Strafgesetzbuch sind das missbräuchliche Abfangen von Daten, Datenbeschädigung und betrügerischer Datenverarbeitungsmissbrauch mit

KONSEQUENZEN FÜR UNTERNEHMEN

Die Nichteinhaltung angemessener Datensicherheitsmaßnahmen kann auch sonstige rechtliche Konsequenzen für das Unternehmen nach sich ziehen. In aller Regel ist die Einhaltung von Datensicherheitsmaßnahmen wenigstens vertragliche Nebenpflicht in geschäftlichen Beziehungen, in denen Zugang zu Daten gewährt wird.

Handelt es sich um sensible oder vertrauliche Daten, so wird vielfach mit Hilfe sogenannter Vertraulichkeitsvereinbarungen oder „Non Disclosure Agreements“ (NDAs) die Verpflichtung zur Geheimhaltung zum Datenschutz ausdrücklich festgeschrieben. In NDAs wird oft eine empfindliche Schadenersatzzahlung für jene Fälle vereinbart, in denen eine (auch nur fahrlässige) Weitergabe oder gar Veröffentlichung der relevanten vertraulichen Daten erfolgt. Dabei wird

Trifft den Datenverarbeiter jedoch ein Verschulden an der mangelnden Datensicherheit und sei dies auch nur fahrlässig, so besteht nach allgemeinem Zivilrecht die Verpflichtung zum Schadenersatz. Der Kläger hat dabei nur nachzuweisen, dass der Schädiger anwendbare gesetzliche und/oder vertragliche Normen nicht eingehalten hat und ein Schaden tatsächlich entstanden ist. Die Einhaltung der Mindestschutzvorschriften des Datenschutzgesetzes wird - wie bereits oben gezeigt - in vielen Fällen als Handelsbrauch auch bei nicht personenbezogenen Daten obligatorisch sein.

STANDARDS

ZERTIFIZIERUNG

Zur Bewertung und Zertifizierung (Qualitätsmanagement) der Sicherheit von Computersystemen existieren internationale Normen. Wichtige Normen in diesem Zusammenhang sind vor allem die amerikanischen TCSEC- und die europäischen ITSEC-Standards sowie der neuere Common Criteria-Standard. Die Zertifizierung erfolgt in Deutschland in der Regel durch das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Die IT-Grundschutz-Kataloge des BSI definieren für die verschiedenen Aspekte einer IT- Landschaft konkrete Maßnahmen, die zur Erhaltung der Sicherheit bei niedrigem und mittlerem Schutzbedarf erfüllt werden müssen (Waschzettel). Die Grundschutz-Kataloge sind primär in Deutschland bekannt, liegen allerdings auch englischsprachig vor.

ISO/IEC 27001: Normenreihe für
Informations Sicherheitsmanagementsysteme

ISO/IEC 27002:2005: Leitfaden für das
Informationssicherheitsmanagement

BS 7799-1 / BS 7799-2

ITIL

BS 15000

ISO 20000: IT-Service-Management

CobiT

ISO 13335: Normenreihe zum Sicherheitsmanagement in der
Informations- und Kommunikationstechnik

...

A CLOSER LOOK

NEWSLETTER

Schutz des Formulars vor automatischer Eintragung

Captcha

Token

Checkboxen nicht per default an

Erst eintragen nach Bestätigung via Email

Gefahr als Spam verschrien zu sein

Html vs. Plaintext => Multipart

Impressum & Abmeldelink in der Email

PASSWÖRTER

WAS MÜSSEN WIR ALS APPLIKATIONSENTWICKLER BEACHTEN?

Passwörter sollten möglichst sicher sein

Sicheres Speichern der Passwörter

SICHERE PASSWÖRTER

Mindestlänge

Nicht der Benutzername oder Teile des Benutzernamens

Nicht in einem Wörterbuch

Gross- und Kleinbuchstaben & Zahlen & Sonderzeichen

Zahlen und Sonderzeichen möglichst in der Mitte

Z.B. Keine 3 anstatt E

Passwort Rotation

Automatisch generierte Passwörter

Verschieden pro Applikation (Password-Tool)

Nicht aufschreiben

SICHERES ABSPEICHERN

Besonders gesicherte Datenbank / Server

Passwörter **NICHT** im Klartext abspeichern

Sicherer Verschlüsselungsalgorithmus benutzen (SHA256, AES, ...)

Zusammengesetzten Salt verwenden

- Applikation
Zufällige Zeichenkette in Programmcode / Konfiguration
- Per User
Zufall und nicht Usernamen und in DB speichern

AUTHENTIFIZIERUNG

OAuth Style

Eigenes System zur Authentifizierung

Authentifizierung via Username / Passwort

Benutzung von zeitlich begrenzten Tokens

Refresh Token in Client

Muss man das selber programmieren? Kann man, muss man aber nicht.

Provider benutzen => Facebook / Google / Twitter

<http://en.wikipedia.org/wiki/OAuth>

AUTHORISIERUNG

WAS DARF EIN BENUTZER TUN?

Rechte vs. Rollen vs. Zuordnung

Zugriff analog Dateisystem: pageA/edit/read...

Mehrfach-Rollen & Vererbung

Abschauen bei anderen bzw. Bibliotheken / Frameworks benutzen

MISC / Q & A

WAS TUN WENN'S DOCH PASSIERT IST?

Die guten Angriffe bleiben lange unentdeckt.

Sofort vom Netz trennen

Ermittlungsbehörden benachrichtigen

Computer-Forensik

Spurensuche in Logfiles, Betriebssystem, ...

Extrem teuer und aufwändig!

WEB 2.0

Applikationen werden mächtiger und komplizierter

Social Networks machen Daten überall verfügbar

Persönliche Daten meist Grundlage

Vernetzung von Applikationen

Speichern von Daten bei User, in der Cloud oder als Service

IN A NUTSHELL

Sicherheit ist ein kontinuierlicher Prozess!

Wir sind immer einen Schritt hinterher!

Klartext speichern vermeiden!

Verschlüsselt übertragen!

Man kann nicht überall sofort gut sein. Ein Schritt nach dem anderen!

Rechtlicher / professioneller Beistand schadet nicht!

Planung!

Gehirn einschalten!!!

DATENSICHERHEIT UND
DATENSCHUTZ SIND UND
BLEIBEN EIN DAUERBRENNER
UND DIE WICHTIGKEIT WIRD
NOCH WEITER ZUNEHMEN

BEREITS HEUTE BESCHÄFTIGEN
SICH UNTERNEHMEN MIT NICHTS
ANDEREM ALS SICHERHEIT IM IT-
UMFELD.

LINKS

www.phpids.org

de.wikipedia.org/wiki/Datenschutz

de.wikipedia.org/wiki/Informationssicherheit

sicherheitskultur.at/Eisbergprinzip.htm

www.bsi.bund.de

www.sektioneins.com

FRAGEN?

THE END

VIELEN DANK FÜR DIE
AUFMERKSAMKEIT UND
STIMMUNG!

Made with [reveal.js](#)