Interreg

EUROPÄISCHE UNION

Österreich-Tschechische Republik

Europäischer Fonds für regionale Entwicklung

INFORMATIK

IT-Security

UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

VŠTE

EUROPÄISCHE UNION

Inhalt

1. Motivation 2
2. Schutzziele der Informationssicherheit 6
2.1. Vertraulichkeit 6
2.2. Integrität 7
2.3. Verfügbarkeit 7
2.4. Authentizität 8
2.5. Zugriffskontrolle 8
2.6. Verbindlichkeit 9
3. Informations- vs. IT-Sicherheit 10
4. Schwachstelle, Bedrohung und Risiko 11
5. Angriffskategorien, -ebenen & Ursachen 12
5.1. Angriffsebenen aktuell (Auszug) 15
5.2. Ursachen 15
6. Angreifertypen & ihre Motivation 16
7. Klassifikation von Sicherheitsmaßnahmen 17
8. Kontinuierliche Ganzheitlichkeit in der Informationssicherheit 18
8.1. Sicherheitsstandards 18
8.2. Rechtsnormen / Gesetze 19
9. Literatur 20

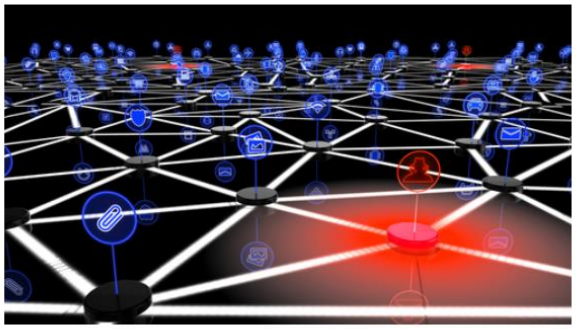
1. MOTIVATION

KrebsonSecurity
In-depth security news and investigation

21 KrebsOnSecurity Hit With Record DDoS

SEP 16

On Tuesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual distributed denial-of-service (DDoS) attack designed to knock the site offline. The attack did not succeed thanks to the hard work of the engineers at **Akamai**, the company that protects my site from such digital sieges. But according to Akamai, it was nearly double the size of the largest attack they'd seen previously, and was among the biggest assaults the Internet has ever witnessed.



The attack began around 8 p.m. ET on Sept. 20, and initial reports put it at approximately 665 Gigabits of traffic per second. Additional analysis on the attack traffic suggests the assault was closer to 620 Gbps in size, but in any case this is many orders of magnitude more traffic than is typically needed to knock most sites offline.

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

RISK ASSESSMENT —

Why the silencing of KrebsOnSecurity opens a troubling chapter for the 'Net

"Free speech in the age of the Internet is not really free," journalist warns.

DAN GOODIN - 9/23/2016, 10:58 PM

DDoS-Attacke

Mit Todessternen auf Spatzen schießen

Die Website eines Journalisten wurde von einem Botnetz aus Haushaltsgeräten bombardiert. Die bisher wohl größte DDoS-Attacke überhaupt war aber nur ein Vorgeschmack.

Von **Patrick Beuth**

ZEIT ONLINE

26. September 2016, 15:18 Uhr / 46 Kommentare

The banker that can steal anything

By Anton Kivva on September 20, 2016. 10:58 am

SECURELIST

MOBILE

BANKING TROJAN | GOOGLE ANDROID | MOBILE BROWSER | MOBILE MALWARE

CONTENTS

Anton Kivva

In the past, we've seen superuser rights exploit advertising applications such as Leech, Guerrilla, Ztorg. This use of root privileges is not typical, however, for banking malware attacks, because money can be stolen in numerous other ways that don't require exclusive rights. However, in early February 2016, Kaspersky Lab discovered Trojan-Banker.AndroidOS.Tordow.a, whose creators decided that root privileges would come in handy. We had been watching the development of this malicious program closely and found that Tordow's capabilities had significantly exceeded the functionality of most other banking malware, and this allowed cybercriminals to carry out new types of attacks.

Technology

Dropbox hackers stole 68 million passwords - check if you're affected and how to protect yourself

share

The Telegraph

The details of tens of millions of Dropbox users are for sale online CREDIT: DROPBOX

By Cara McGoogan

31 AUGUST 2016 • 11:05AM

heise Security

« Vorige | Nächste »

Android-Schädling Tordow: Banking-Trojaner mutiert zum Super-Trojaner

28.09.2016 14:00 Uhr – Dennis Schirrmacher

vorlesen

(Bild: Christoph Scholz, CC BY-SA 2.0)

Sicherheitsforscher warnen vor einer Banking-Malware, deren Funktionsumfang sämtliche Träume von Kriminellen erfüllen dürfte: Der Trojaner kann im Grunde alles mit infizierten Android-Geräten anstellen.

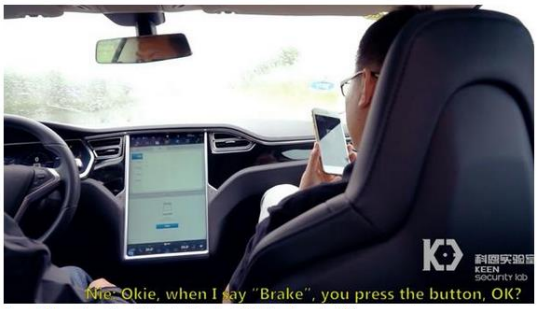
heise Security

« Vorige | Nächste »

Tesla Model S lässt sich von fern kapern

20.09.2016 08:24 Uhr – Andreas Wilkens

vorlesen



Screenshot aus dem Demo-Video der Forscher (Bild: Keen Security Lab)

Forscher des chinesischen Internetunternehmens Tencent demonstrieren, wie sie manche Funktionen eines Tesla Model S unautorisiert von fern steuern. Dabei gelang es ihnen auch, ein fahrendes Auto anzuhalten.

43 million passwords hacked in Last.fm breach

Posted Sep 1, 2016 by John Mannes (@JohnMannes)

Crikey: 43,570,999 user accounts were breached in a hack of Last.fm that occurred in March of 2012, according to a report from LeakedSource. Three months after the breach, in June of 2012, Last.fm issued the following statement:

NEWSLETT

The Daily Cru

Get the top tec to your inbox

TC Weekly R

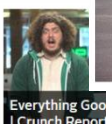
Get a weekly r stories

CrunchBase

The latest start

Enter your email

LATEST CR

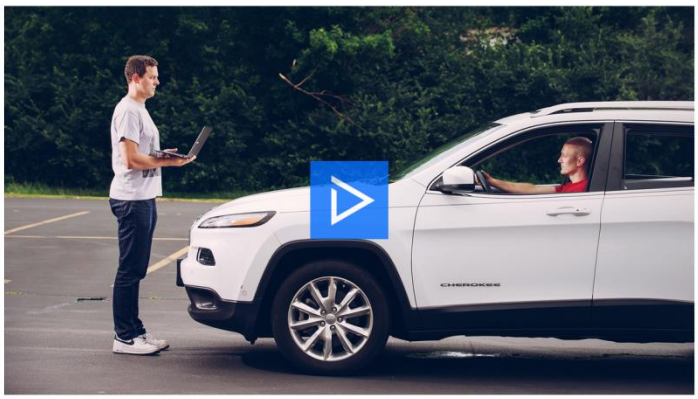


Everything Goo

ANDY GREENBERG SECURITY 07.21.15 8:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

WIRED



derStandard.at

Bis zu fünf Millionen Betroffene bei Facebook-Hack aus EU

2. Oktober 2018, 07:48

3 POSTINGS

foto: dado ruvic / reuters

Der Facebook-Hack sorgt weiter für Aufregung.

Weniger als zehn Prozent der 50 Millionen weltweit – Unternehmen verspricht "bald" neue Informationen

Von den fast 50 Millionen von einem Hacker-Angriff betroffenen Facebook-Nutzer stammen weniger als zehn Prozent, das sind maximal 5 Millionen, aus der Europäischen Union. Das teilte die zuständige irische Datenschutzbehörde am Montagabend bei Twitter mit. Facebook habe zugesichert, "bald" ausführlichere Informationen liefern zu können, hieß es in der knappen Stellungnahme weiter.

Car hacking is the future - and sooner or later you'll be hit

theguardian

Security is finally being taken seriously but the fact that we are increasingly entrusting our lives to self-driving cars creates unease

A Tesla self-driving car on autopilot mode. Researchers explored the potential ways in which such vehicles could be hacked or exploited. Photograph: Bloomberg via Getty Images

DSGVO: Mehr als 1000 US-Portale für Europäer gesperrt

futurezone

08.08.2018

© Bild: Maksim Kabakou - Fotolia / Maksim Kabakou/Fotolia

Noch immer sind mehr als 1000 US-Nachrichtenseiten hierzulande nicht erreichbar, Instapaper ist jedoch wieder verfügbar.

DSG: Verwaltungsstrafe bis EUR 25.000,-- DSGVO: Geldbußen bis EUR 20.000.000,--

https://www.dataprotect.at/info/geldbußen/österreich/

Auch bereits bei **Geltung des Datenschutzgesetzes** (bis 24.5.2018) gibt es **Geldstrafen für Datenschutzverletzungen**; der Strafrahmen ist jedoch (relativ) gering und reicht bis zu **EUR 10.000,--** (für geringe Verstöße) oder bis zu **EUR 25.000,--** (für gröbere Verstöße); es gibt auch **gerichtlich strafbare Handlungen** im DSG (§ 51: Datenverwendung in Gewinn- oder Schädigungsabsicht).
Der **Strafrahmen für Datenschutzverletzungen** steigt mit Geltung der **DSGVO** (25.5.2018) **dramatisch**, und zwar auf 4 % des weltweiten Konzernumsatzes des Vorjahres / EUR 20.000.000,-- als maximale Strafe bzw. 2 % des weltweiten Konzernumsatzes des Vorjahres / EUR 10.000.000,-- bei "geringfügigeren Delikten", wobei dies jeweils die absolute Obergrenze darstellt und immer der Betrag anwendbar ist, der "höher" ist.

dataprotect it-recht

ENTSCHEIDUNGEN ZUM DATENSCHUTZRECHT · 20. September 2018

erste Geldstrafe durch die DSB in Österreich

Die DSB hat die erste **Geldstrafe** verhängt.

EUR 4.800,-- für eine nicht korrekt gekennzeichnete Videoüberwachung, die den öffentlichen Raum mitüberwachte.

https://www.dataprotect.at/2018/09/20/erste-geldstrafe-durch-die-dsb-in-österreich/

Nach Medienberichten (Salzburger Nachrichten, 19.09.2018) wurde gegen einen Betreiber eines Wettlokals in der Steiermark eine Geldstrafe von EUR 4.800,-- verhängt, weil eine **Videoüberwachung nicht ausreichend gekennzeichnet** war und ein **großer Teil des Gehsteigs von der Anlage mitaufgezeichnet** wurde. Die Überwachung des öffentlichen Raums in dieser Art und Weise, nämlich großflächig durch Private ist nicht zulässig.

- Starke Abhängigkeit der modernen Gesellschaft von der IKT (insb. kritische Infrastrukturen).

- IKT wird zur kritischen Informationsinfrastruktur (Critical Information Infrastructure, CII).

- Folgende Trends machen den Schutz der IKT zum zentralen Thema (u. a. nach [Eckert2008]):
    - Globalisierung
    - Mobilität (Smartphone, Information at your fingertips)
    - Vernetzung
    - Ubiquitous/Pervasive Computing, Internet of Things (IoT)
    - Industrie x.0
    - Smart Home/Grid/Car/*
    - Cyber War/Warfare/Espionage/*

- Fazit: Schutz der IKT ist für die Gesellschaft von zentraler Bedeutung!

2. SCHUTZZIELE DER INFORMATIONS-SICHERHEIT

Informationssicherheit (bzw. IT-Sicherheit) hat das Gewährleisten folgender Schutzziele (Grundwerte) zur Aufgabe [Stallings2006]:

1. Vertraulichkeit (engl. confidentiality)
2. Integrität (engl. integrity)
3. Verfügbarkeit (engl. availability)

} C-I-A

4. Authentizität (engl. authenticity)
5. Verbindlichkeit (engl. accountability oder non-repudiation)

2.1. Vertraulichkeit

- **Vertraulichkeit** = engl. Confidentiality
- The protection of data from unauthorized disclosure. [Stallings2006]
- **Traffic Flow Confidentiality** = Schutz vor Verkehrsdatenanalyse
- Vertraulichkeit im täglichen Leben
  - Briefgeheimnis & Fernmeldegeheimnis
  - Amtsverschwiegenheit
  - Beichtgeheimnis
  - Verschwiegenheitspflicht von Rechtsanwälten/Notaren/ Ärzten
  - Geheimhaltungsvereinbarungen/NDAs
- Erreichbar durch Verschlüsselung (Chiffrierung, Encryption)
  - Symmetrische Verschlüsselung
    - ein gemeinsamer geteilter Schlüssel (gleicher Schlüssel für ver- und entschlüsseln) => Schlüsselverteilungsproblem; Strom-/Blockchiffre, Substitution & Transposition
- Asymmetrische Verschlüsselung
  - öffentlicher und privater Schlüssel (öffentlicher Schlüssel für ver- und privater für entschlüsseln) => Schlüsselverteilungsproblem gelöst, algorithmisch aufwändiger und daher langsamer

- Praxis Hybrid: Austausch eines generierten Sitzungsschlüssels über asymmetrische Krypto und dann symmetrische Verschlüsselung

2.2. Integrität

- **Integrität** = engl. Integrity

- The assurance that data received are exactly as sent by an authorized entity (i.e. contain no modification, insertion, deletion, or replay). [Stallings2006]

- Veränderung (z. B. durch Übertragungsfehler oder aktive Angriffe) kann **nicht verhindert** aber **erkannt** werden!

- Authentizität und Integrität werden häufig als Einheit gesehen. Das eine ist ohne das andere nutzlos

- Erreichbar durch den Einsatz von (kryptographischen) Prüfsummen, z. B.
    - CRC (Cyclic Redundancy Check) nur für Übertragungsfehler
    - (Keyed-Hash) Message Authentication Code (MAC, HMAC)
    - Digitale Signaturen

Eine **kryptologische Hashfunktion** oder **kryptographische Hashfunktion** ist eine spezielle Form der Hashfunktion, welche kollisionsresistent oder eine Einwegfunktion (oder beides) ist.

Eine Hashfunktion ist eine Funktion, die eine Zeichenfolge beliebiger Länge auf eine Zeichenfolge mit fester Länge abbildet. Mathematisch ist diese Funktion nicht injektiv (linkseindeutig) und nicht notwendigerweise surjektiv (rechtstotal).

2.3. Verfügbarkeit

- **Verfügbarkeit** = engl. Availability

- Availability is the property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system. [Stallings2006]

- Welche Arten von Performance?
    - Verwendbar bzw. anwendbar
    - Genügend Kapazität
    - Klarer Fortschritt und/oder klar definierte Wartezeiten
    - Vollendung in einem akzeptablen Zeitrahmen
    - ...

- Ansätze zur Realisierung/Garantie von Verfügbarkeit
    - Technisch: Fehlertoleranz und Redundanz durch z. B. RAID, Clustering, ..., gespiegelte Rechenzentren, unterbrechungsfreie Stromversorgung (USV), ...
    - Organisatorisch: Service Level Agreements (SLAs), Verfügbarkeitsklassen

- Verfügbarkeitsklassen
    - 2-6: 99% (Ausfall von ~ 90 Stunden pro Jahr)
    - 99,9%, ... bis 99,9999% (= Ausfall von ~ 30 Sekunden pro Jahr!).

2.4. Authentizität

- Authentizität = engl. Authenticity
    - Entity authenticity= Ich weiß, mit wem ich kommuniziere
    - Data origin authenticity= Ich weiß, von wem die Daten kommen

- Authentifizierung und Authentisierung (authentication)

    - The assurance that the communicating entity is the one that it claims to be. [Stallings2006]

- Authentifizierungsmerkmale = Merkmal mit dem ein Teilnehmer authentifiziert werden kann
    - Basierend auf Wissen (PIN, Passwort)
    - Basierend auf Besitz (Schlüssel, Karte)
    - Basierend auf Eigenschaft (Biometrische Merkmale wie Fingerabdruck, Iris, Stimme, Unterschrift, Retina, ...)
        - Retina = Augenhintergrund (Scan mittels Infrarot)
        - Iris Scan (mittels normaler optischer Kamera)

- Zugangs-/Zugriffskontrolle (Access Control)
    - Authentizität ist Voraussetzung für Zugangs-/Zugriffskontrolle!

2.5. Zugriffskontrolle

- Zugriffskontrolle = engl. access control

- The prevention of unauthorized use of resources. [Stallings2006]

- Die Authentizität der zugreifenden Entität muss sichergestellt sein.

- Es wird geprüft

    - wer Zugriff auf eine Ressource haben darf,
    - unter welchen Bedingungen der Zugriff erfolgen darf und
    - welche Rechte die zugreifende Entität haben darf.

- Prinzip des notwendigen Wissens (Need-to-know principle)

- Grundmodelle
    - Discretionary Access Control (DAC)
        - Festlegung der Rechte ausschließlich auf Basis der Nutzeridentität

- Mandatory Access Control (MAC)
    - Nicht nur Nutzeridentität sondern zusätzliche Regeln und Eigenschaften

- Role Based Access Control (RBAC)
    - Rollenbasierte Rechtvergabe, d. h. nicht auf Basis Nutzeridentität sondern auf Basis von Nutzerrolle (Gruppenzugehörigkeit)

2.6. Verbindlichkeit

- Verbindlichkeit = engl. accountability oder non-repudiation

- Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. [Stallings2006]

- Verbindlichkeit des Sender = Sender kann den Versand der Nachricht nicht abstreiten.

- Verbindlichkeit des Empfängers = Empfänger kann den Empfang der Nachricht nicht abstreiten.

- Erreichbar durch Einsatz von digitale Signaturen (nicht durch [H]MACs!).

3. INFORMATIONS- VS. IT-SICHERHEIT

- Informationssicherheit (Information Security, InfoSec) beschäftigt sich mit Daten jeglicher Form (elektronisch, schriftlich, verbal).
- IT-Sicherheit (IT Security, IT-Sec) konzentriert sich ausschließlich auf die elektronische Datenverarbeitung.
- Definition IT-Sicherheit (übertragbar auf InfoSec, nach [BSI1992]):

IT-Sicherheit ist der Zustand eines IT-Systems, in dem die **Risiken**, die beim Einsatz dieses IT-Systems aufgrund von **Bedrohungen** vorhanden sind, durch **angemessene Maßnahmen** auf ein **tragbares (akzeptables) Maß** beschränkt sind.

- Höchst wichtige (!!) Konsequenz: Es gibt keine absolute Sicherheit!

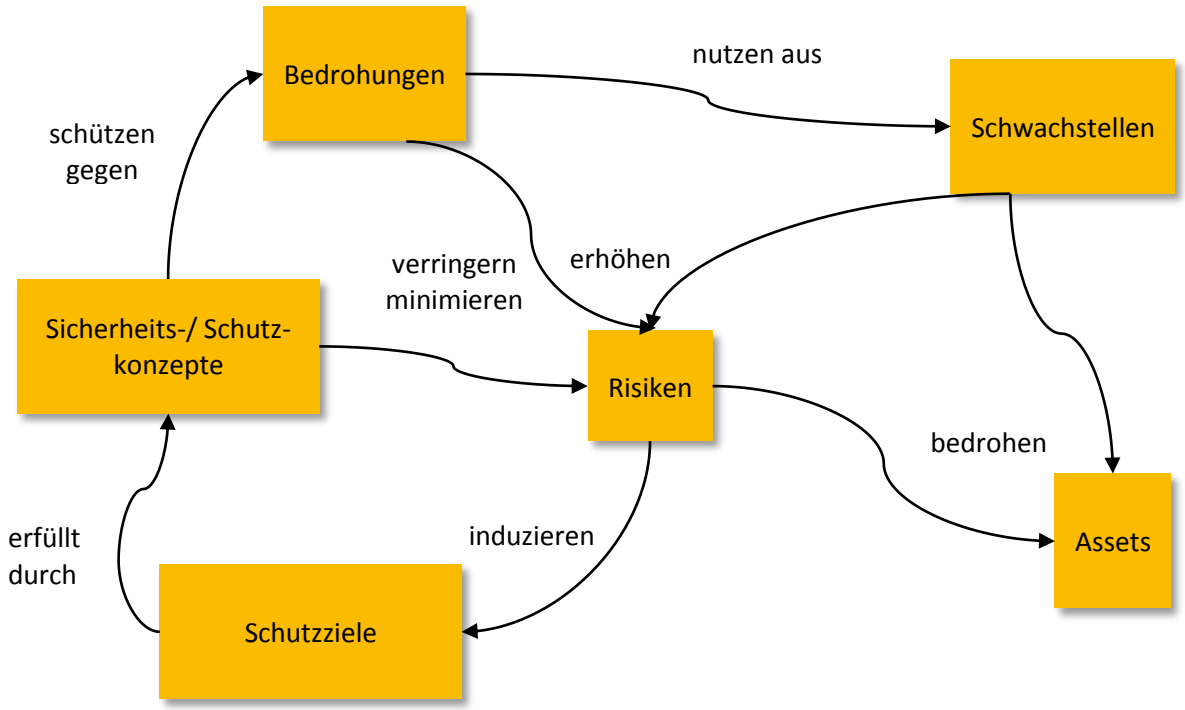
4. SCHWACHSTELLE, BEDROHUNG UND RISIKO

- Eine Schwachstelle/Verwundbarkeit (eng. weakness/vulnerability) ist eine Schwäche des Systems oder ein Punkt, an dem das System verwundbar sein kann (durch einen Exploit).

- Bedrohungen (eng. threat) ergeben sich aus möglichen Angriffen, die eine oder mehrere Schwachstellen eines Systems ausnutzen, um ein oder mehrere Schutzziele zu gefährden.

- Das Risiko R (eng. risk) einer Bedrohung ist die Wahrscheinlichkeit E des Eintritts eines Schadensereignisses und die Höhe des potentiellen Schadens S, der daraus resultieren kann: $R = E \cdot S$

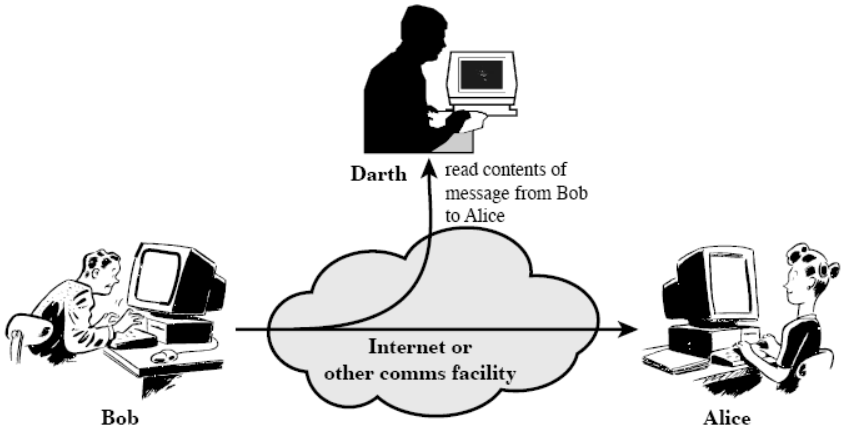
Zusammenhänge



5. ANGRIFFSKATEGORIEN, -EBENEN & URSACHEN

Passive Angriffe – Eavesdropping

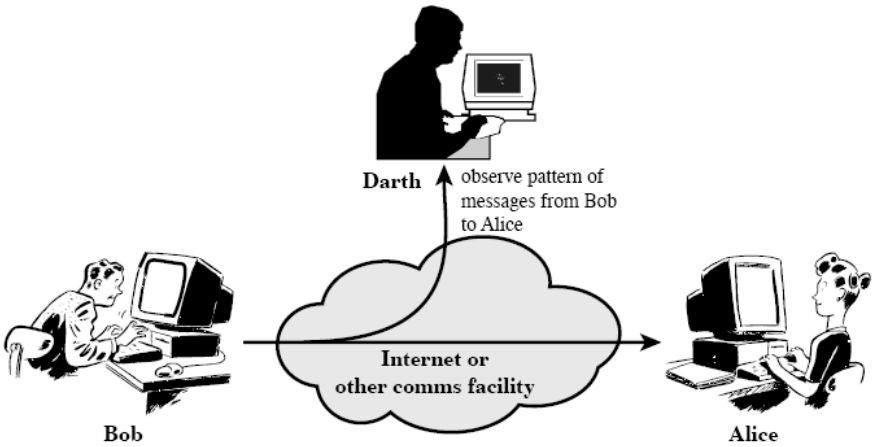
Angreifer hört den Kommunikationskanal ab, greift aber nicht aktiv in die Kommunikation ein.



(a) Release of message contents

Passive Angriffe – Traffic Analysis

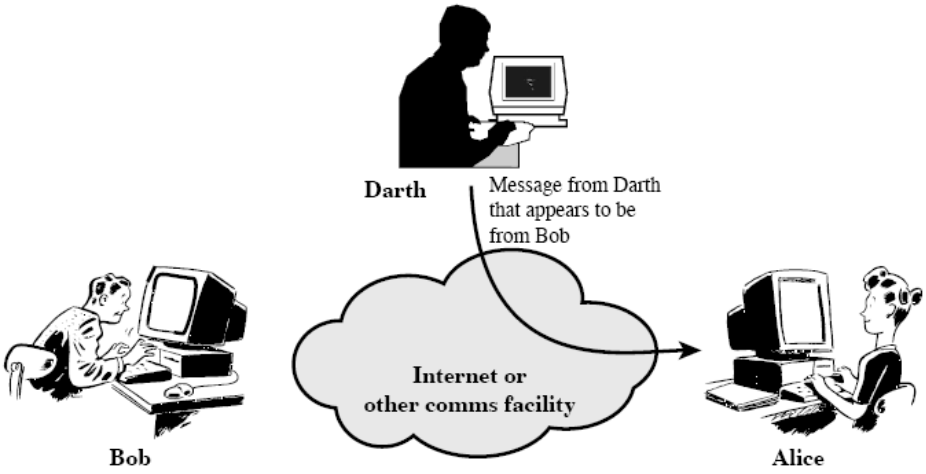
Bei einem verschlüsselten Datenkanal kann ein passiver Angreifer möglicherweise eine Verkehrsdatenanalyse (Traffic Analysis) durchführen (wer kommuniziert wann mit wem?)



(b) Traffic analysis

Aktive Angriffe – Masquerade

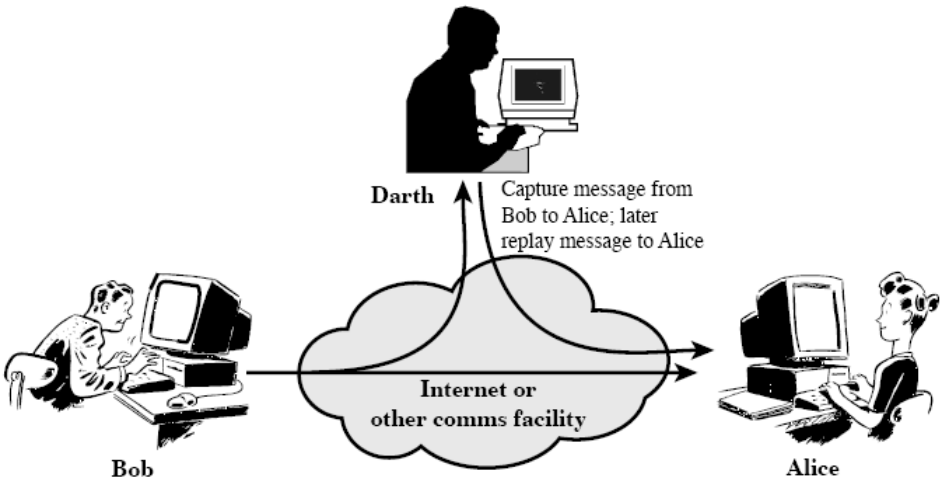
Masquerade: Angreifer gibt sich als jemand anderer aus.



(a) Masquerade

Aktive Angriffe – Insertion & Replay

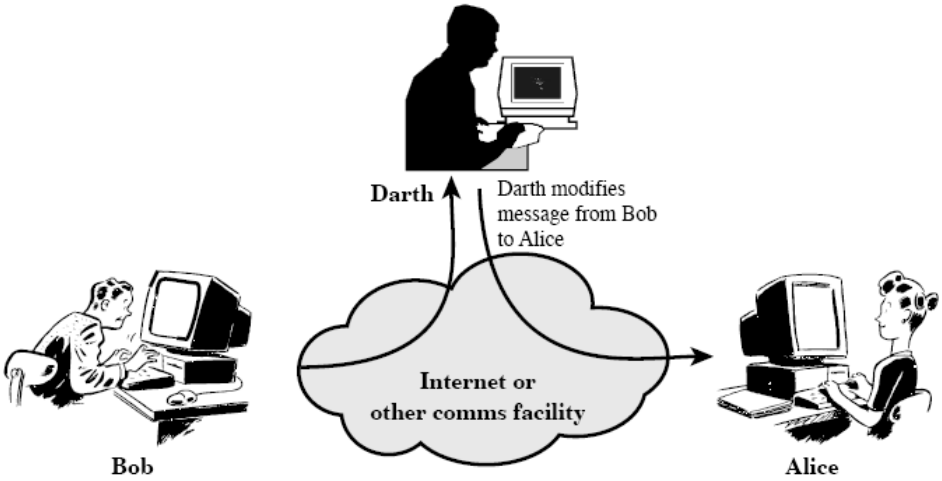
- Insertion: Angreifer fügt Nachrichten(teile) zu einer Kommunikation hinzu.
- Replay: Angreifer sendet aufgezeichnete Daten zu einem späteren Zeitpunkt noch einmal.



(b) Replay

Aktive Angriffe – Modification

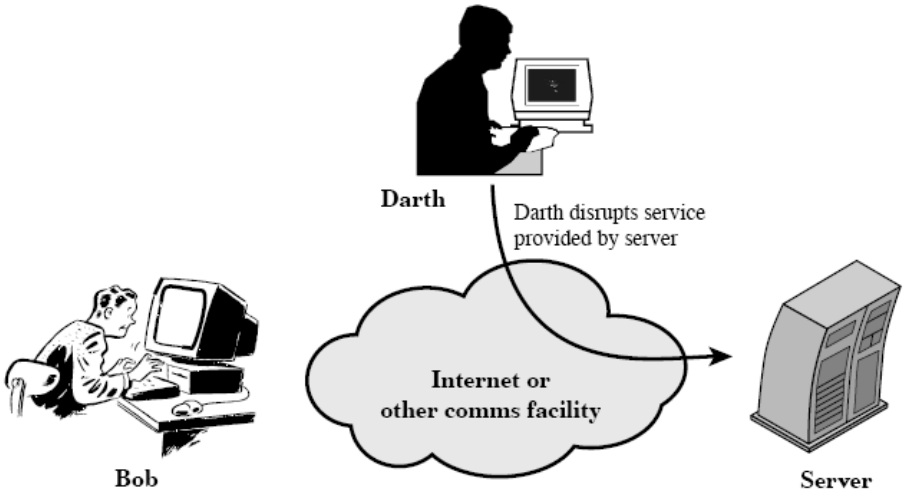
Angreifer verändert eine Kommunikation indem er Nachrichten verzögert, ändert oder löscht.



(c) Modification of messages

Aktive Angriffe – Denial of Service

Angreifer stört die Verfügbarkeit von Kommunikationseinrichtungen



(d) Denial of service

5.1. Angriffsebenen aktuell (Auszug)

- Netzwerk
  - Botnetze
  - (Distributed) Denial of Service (Dienstverweigerung), Reflection, Amplification
  - Spam (Unsolicited Commercial/Bulk E-Mail, Social Media Spam)
  - Man-in-the-Middle-Angriffe (z. B. zum Mitlesen/Modifizieren von Kommunikation)

- Anwendungen (v. a. Web-Anwendungen, s. OWASP Top 10), z. B.
  - Injection (z. B. SQL Injection, Command Injection)
  - Cross-Site Scripting (XSS)
  - Cross-Site Request Forgery (CSRF)
  - Defacements
  - Buffer Overflows

- Benutzer
  - Social Engineering
  - (Spear) Phishing
  - Scareware, Ransomware
  - Spam

5.2. Ursachen

- Fehlende/Mangelnde Identitätsprüfung
  - z. B. schwache Authentifizierungsverfahren, unilaterale Authentifizierung, …

- Fehlende/Mangelnde Input-Validierung
  - z. B. Nutzereingaben in Web-Anwendungen werden server-seitig nicht geprüft

- Psychologische Mängel und Hemmnisse
  - z. B. Social Engineering

- Faktoren Kosten und Zeit in der Produktentwicklung
  - z. B. Kurze Release-Zyklen, fehlende Tests, Sicherheit nicht in Entwicklungsprozesse integriert

- Organisatorische Mängel
  - z. B. fehlendes Sicherheitsmanagement, fehlende Benutzer-Awareness, …

6. ANGREIFERTYPEN & IHRE MOTIVATION

- Amateure (Script Kiddies)
  - Für die meisten (automatisierten) Angriffe verantwortlich
  - Wenige tiefgehendes Wissen Anwendung von fertigen Angriffstools
  - Motive: Prestige, persönliche Rache, Langeweile

- Crackers vs. Hackers (Blackhats vs. Whitehats)
  - Cracker sind bösartige Hacker (Begrifflichkeiten unklar)
  - Tiefes technisches Verständnis (Studenten, Informatiker)
  - Motive: Prestige, intellektuelle Herausforderung

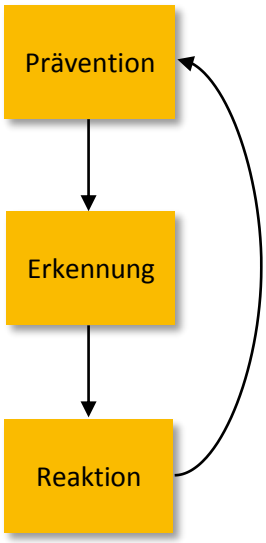
- Kriminelle (Cybercrime)
  - Klassische Kriminelle, die nur aus Profitgründen das Metier wechseln
  - Spamming, Online-Erpressung, Bulletproof-Hosting/-Services, Botnetze (Vermietung), …
  - Gut organisierte Netzwerke mit Verbindungen zum organisierten Verbrechen (z. B. Russian Business Network, Silk Road, …)
  - Motive: Profite

- Terroristen (Cyber-Terrorismus)
  - IT als Angriffsziel Infrastruktur des Zieles schädigen/zerstören
  - Propagandazwecke
  - Kommunikation und Organisation

- Länder und ihre militärischen/nachrichtendienstlichen Apparate (Cyber-War(fare), Cyber-Espionage)
  - Ausschalten der IT-Infrastruktur als Ziel von militärischen Angriffen
  - Wirtschaftliche, politische und militärische Spionage (→ China, USA)
  - Das Internet als Waffe
  - Beispiele: Stuxnet, Flame, Regin, NSA-Überwachungsskandal

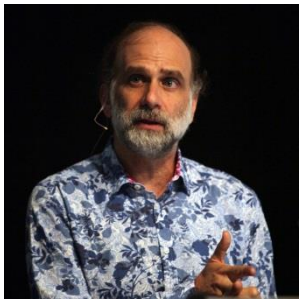
7. KLASSIFIKATION VON SICHERHEITS-MAßNAHMEN

- Maßnahmen zur Verhinderung (a priori)
  - z. B. Authentifizierung, Zugangskontrolle, Einsatz von Verschlüsselung, Firewalls, Härten von Systemen, Sicherheitskonzept, Sicherheitspolitik, Awareness schaffen, …
- Maßnahmen zur Erkennung
  - Dynamisch zur Laufzeit
    z. B. Firewalls, Intrusion Detection Systeme, Log-Analyse, …
- Maßnahmen zur Schadensbegrenzung (a posteriori)
  - z. B. Verschärfen von Kontrollen, Verbesserung von Sicherheitsmaßnahmen, Kappen der Internetverbindung, …



8. KONTINUIERLICHE GANZHEITLICHKEIT IN DER INFORMATIONSSICHERHEIT

Security is not a product; it's process!



Bruce Schneier

Photograph by Rama, Cc-by-sa-2.0-fr, from Wikimedia Commons

- Ganzheitlichkeit ist ein kritischer Erfolgsfaktor für IT-/ Informationssicherheit
  - z. B. Firewall zur Filterung von Datenverkehr, aber Benutzer können WLAN Access Points an das Netzwerk anschließen
  - z. B. Zugänge zu den Systemen sind mit Passwörtern geschützt, die am schwarzen Brett angeschlagen sind
  - z. B. Benutzer notieren ihre Windows-Passwörter auf Post-It's auf ihren Monitoren

- IT-/Informationssicherheit erfordert ein Zusammenspiel aus technischen und organisatorischen Maßnahmen!

- IT-/Informationssicherheit im Unternehmen muss vom Management getragen werden!

- IT-/Informationssicherheit muss kontinuierlich gelebt und verbessert werden (Beispiele?)!

8.1. Sicherheitsstandards

- Sicherheitsmanagement/Sicherheitsprozess, z. B.
  - ISO 27000er Familie
  - BSI Grundschutzstandards 100-1, 100-2, 100-3 und 100-4

- Systemsicherheit (Zertifizierung von Produkten), z. B.
  - TCSEC (Trusted Computer System Evaluation Criteria)
  - ITSEC (Information Technology Security Evaluation Criteria)

    - Common Criteria for Information Technology Security Evaluations (ISO 15408)

- Maßnahmenkataloge (technisch/organisatorisch), z. B.
    - BSI Grundschutzkataloge

- Weitere relevante Standards ([IT]-Governance, Compliance), z. B.
    - COBIT (Control Objectives for Information and Related Technology)
    - ITIL (IT Infrastructure Library)

8.2. Rechtsnormen / Gesetze

- Österreichische Strategie zur Cybersicherheit (ÖSCS)
    - Zukünftig: Österreichisches Cybersicherheitsgesetz

- EU Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit (NIS-Richtlinie)
    - Inkorporation in das Österreichische Cybersicherheitsgesetz

- EU Datenschutzgrundverordnung

9. LITERATUR

[Eckert2008] Eckert, C., Vorlesungsskript zur VO IT-Sicherheit, TU Darmstadt, SS 2008

[Stallings2006] Stallings, W., Cryptography and Network Security, 4th edition, Prentice Hall, 2006

[BSI1992] Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik, Version 1.0, März 1992,

[BSI2005] Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutzhandbuch, Stand 2005