Fachhochschule Kaiserslautern
University of Applied Sciences

Betriebswirtschaft
Zweibrücken

Handout

Die Bedeutsamkeit sowohl privater als auch unternehmensinterner verschlüsselter Netzwerke

Studierende

Bauer, Christof

Beck, Marc Florian

Bröde, Daniel

Korrektor:

Prof. Dipl. Ing. Klaus Knopper

Abgabedatum:

13.12.2013

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
DES	Data Encryption Standard
DTLS	Datagram Transport Layer Security
HTTPS	Hypertext Transfer Protocol Secure
IDEA	International Data Encryption Algorithm
PGP	Pretty Good Privacy
RSA	Rivest, Shamir und Adleman
SSH	Secure Shell
SSL/TLS	Secure Sockets Layer / Tansport Layer Security
TAN	Transaktionsnummer
VPN	Virtual Private Network

1 Technische Grundlagen

1.1 IT-Sicherheit

Sicherheitsdienste sind allgemein beschrieben Dienste, die eine gewünschte Sicherheit bieten. Für die IT-Sicherheit existieren folgende Dienste:

- **Vertraulichkeit:** Bestimmte Informationen sollen nur für bestimmte Personen zugänglich sein
- **Authentizität:** Sicherheit darüber, dass die Informationen auch von der richtigen Person stammen
- **Integrität:** Dass die Informationen nicht geändert wurden (auch von dritten)
- **Verbindlichkeit** (oder auch Nichtabstreitbarkeit): Der Nachweis gegenüber Dritten von wem die Nachricht stammt.
- **Anonymität:** Die Nichtpreisgabe der Identität
- **Zugriffskontrolle:** Verwaltung der Zugriffsrechte auf bestimmte Informationen

1.2 Verschlüsselungstechniken

Mit Hilfe von Verschlüsselungen sollen Klartexte in einen geheimen Chiffretext umgewandelt werden. Hierbei existieren zwei verschiedene Verschlüsselungstechniken: Die symmetrische Verschlüsselung mit einem öffentlichen Schlüssel und die asymmetrische Verschlüsselung mit einem öffentlichen und einem privaten Schlüssel.

1.2.1 Symmetrische Verschlüsselung

Verschlüsselung und Entschlüsselung wird mit dem öffentlichen Schlüssel vorgenommen:

Verschlüsselung: c = f(k, m) = f_c (m)	m: Klartext c: Ciffretext K: Schlüssel f: Verschlüsselungsfunktion f^{-1}: Umkehrfunktion oder Entschlüsselungsfunktion
Entschlüsselung: m = f^{-1} (k, c) = f_k^{-1} (c)	

Beispiele:

- DES (Data Encryption Standard): Von IBM entwickelte 64 Bit Verschlüsselung. Sie ist seit 1981 standard. Die Technik eignet sich für große Datenmengen. Sie wurde unter anderem in UNIX/Linux Systemen verwendet und wird bei EC-Karten aufgrund der Schnelligkeit des Algorithmus verwendet.

- IDEA (International Data Encryption Algorithm): 128 Bit Verschlüsselung, die symmetrisch die Nachricht *m* in 64 Bit - Blöcke aufteilt und der Schlüssel k 128 Bit lang ist.

1.2.2 Asymmetrische Verschlüsselung

Verschlüsselung mit dem öffentlichen Schlüssel; Entschlüsselung mit dem privaten Schlüssel. Bei der asymmetrischen Verschlüsselung können auch digitale Signaturen erstellt werden. Asymmetrische Verschlüsselungsverfahren arbeiten blockweise, eine Nachricht wird in einen Block *m* eingeteilt. Der Block darf nicht länger sein, wie der Schlüssel. Ist die Nachricht länger, wird sie in mehrere Blöcke unterteilt und einzeln verschlüsselt.

Verschlüsselung: c = f(e_B, m) = f_{eB} (m)	m: Klartext c: Ciffretext K: Schlüssel B: Bob f: Verschlüsselungsfunktion f^{-1}: Entschlüsselungsfunktion e: Öffentlicher Schlüssel d: Privater Schlüssel f: Verschlüsselungsfunktion und Entschlüsselungsfunktion
Entschlüsselung: m = f(d_B, c) = f_{dB}(c) = f_{dB}(f_{dB}(m))	

Beispiele:

- **RSA** (Rivest, Shamir und Adleman): Ist eine asymmetrische Verschlüsselungstechnik. Sie kann sowohl Nachrichten verschlüsseln als auch digitale Signaturen erstellen. Der hierbei verwendete öffentliche Schlüssel kann durch ein Zertifikat beglaubigt werden. RSA wird im Block-Algorithmus verschlüsselt.

- **PGP** (Pretty Good Privacy): PGP ist ein Programm, welches früher den RSA-Algorithmus verwendete, heute allerdings den Elgamal-Algorithmus. Bei PGP ist der private Schlüssel durch ein Passwort gesichert. Programme, die die PGP Verschlüsselung anbieten, sind unter anderem PGP Desktop oder OpenPGP. PGP wird eingesetzt, um zum Beispiel Facebook – Nachrichten oder auch Emails zu verschlüsseln.

1.3 Virtual Private Network

Mithilfe von Virtual Private Network (VPN) ist es möglich, den Teilnehmer eines privaten Netzes mit einem anderen privaten Netz zu verbinden. Diese Netze müssen nicht kompatibel sein. Der Computer bzw. das System aus dem externen Netzwerk erscheint dann als Teilnehmer im eigenen Netzwerk. Wenn ein Computer aus dem Netzwerk A sich mit einem Computer aus Netzwerk B verbindet, kann der Teilnehmer A sich mit anderen Geräten aus dem Netzwerk B verbinden, aber nicht umgekehrt, sofern keine entsprechende Konfiguration vorgenommen wurde. Solche VPN-Verbindungen bezeichnet man auch als Tunnel. Daneben ist es möglich mit VPN über den Tunnel im Internet zu surfen. Die Funktionsweise ist folgende: Der Nutzer schickt eine Anfrage an seinen VPN Provider, dieser leitet die Anfrage weiter und weist dem Nutzer eine neue, anonyme IP Adresse zu.

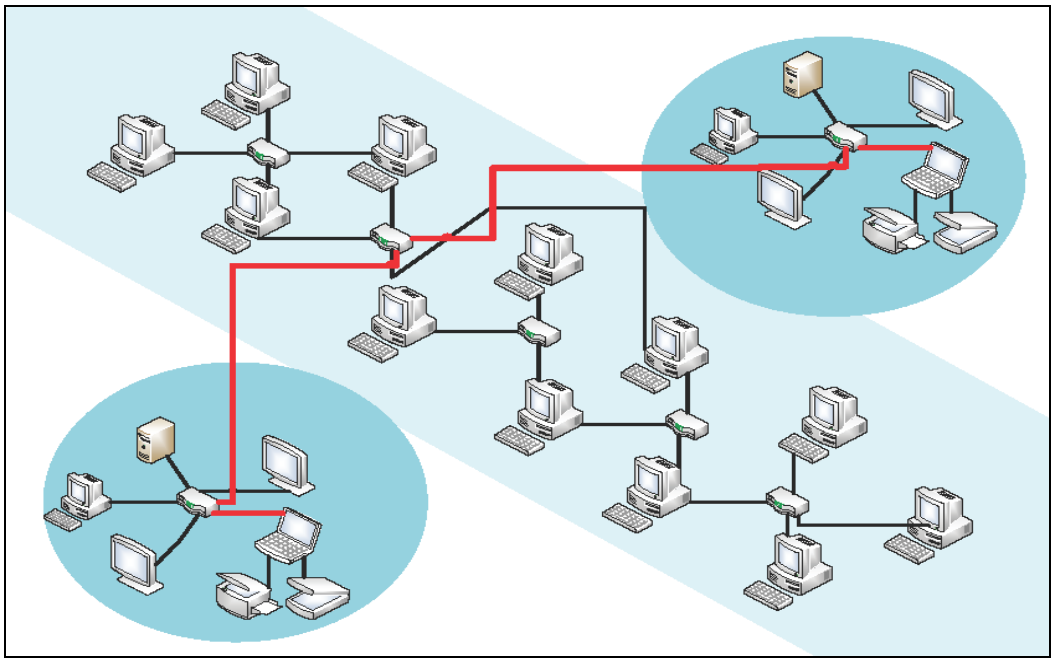


Abbildung 1: VPN-Verbindung im Netzwerk[1]

[1] Eigene Erstellung.

1.4 Sicherheitsprotokolle und Passwörter

1.4.1 Protokolle

Protokolle sind ein Satz von Regeln um Daten auszutauschen. Hierbei sind zwei oder mehrere Parteien beteiligt. Ein Protokoll enthält immer ein Protokollziel, das erreicht werden muss. Üblicherweise werden Protokolle verwendet um Schlüssel auszutauschen, Verschlüsselungsverfahren dazu Identitäten nachzuweisen (Authentifikation).

1.4.2 Passwörter

Bei Passwörtern wird zum einen zwischen einmaligen Passwörtern, z. B. Transaktionsnummern (TAN´s) beim Online Banking und dauerhaften Passwörter unterschieden. Letztere können mehrfach zum Nachweis einer Identität eingesetzt werden.

1.4.3 Challenge-Response-Authentifikation

Ziel ist es, dass eine Partei seine Identität gegenüber einer anderen Partei nachweist. Person B sendet eine Anforderung (challenge) an Person A (response). Die Anforderung ist hierbei eine Aufgabe, die gelöst werden muss. Zunächst wird ein gemeinsamer symmetrischer Schlüssel ausgetauscht. Danach sendet Person B eine Zufallszahl an Person A, Person A verschlüsselt dann die Zufallszahl mit dem gemeinsamen Schlüssel und sendet die verschlüsselte Zahl zurück. Die Zufallszahl wird aus Sicherheitsgründen nur einmal verwendet.

1.4.4 Anwendung

- **HTTPS** (Hypertext Transfer Protocol Secure): HTTPS dient zur Verschlüsselung und Authentifizierung für die Kommunikation zwischen Webserver und Browser.

- **SSH** (Secure Shell): Ist sowohl ein Netzwerkprotokoll als auch ein Programm. Mit SSH kann eine verschlüsselte Netzwerkverbindung aufgebaut werden und somit eine Verbindung zu einem entfernten Gerät hergestellt werden. Häufig wird dies verwendet, um eine Kommandozeile von einem entfernten Gerät aus aufzurufen. Bei der Übertragung werden unsichere Protokolle mit Hilfe von symmetrischer Verschlüsselung gesichert.

1.4.5 Transport

- **SSL/TLS** (Secure Sockets Layer früher, heute Tansport Layer Security): SSL wurde von Netscape entwickelt. Informationen sollen hiermit vertraulich übertragen werden. SSL/TLS wird vor allem bei HTTPS eingesetzt. Die meisten Browser setzen TLS mit RSA oder AES Verschlüsselung ein.
- **DTLS** (Datagram Transport Layer Security): DTLS ist eine Verschlüsselungstechnik, welche auf TLS basiert und zur Übertragung von unzuverlässigen Transportprotokollen wie UDP dient.
- **SRTP/SRTCP** (Secure Real-time Transport Protocol): RTP ist ein Protokoll zur kontinuierlichen Übertragung von Daten, wie Videos und Audiodaten (Streams). SRTP ist hierbei die verschlüsselte Transportvariante.

1.4.6 Schlüsselaustausch

- **ZRTP** („Z“ und Real Time Protocol): Ist ein kryptographisches Schlüsselaustauschprotokoll für RTP.
- **MIKEY** (Multimedia Internet KEYing): MIKEY ist ein Schlüsselaustauschprotokoll, welches zur Initialisierung des Schlüsselaustauschs bei Multimedia - Anwendungen genutzt wird.

1.4.7 Diffie-Hellman-Schlüsselaustausch

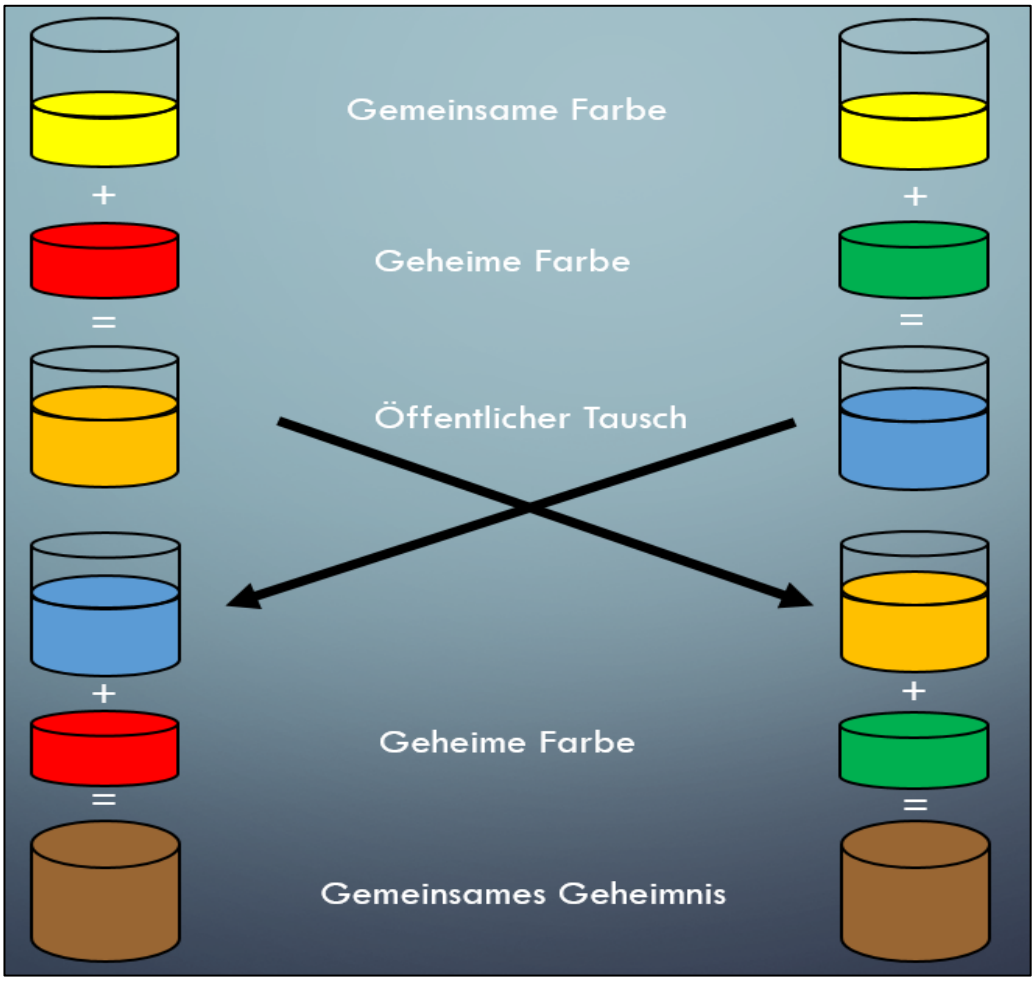


Abbildung 2: Diffie-Hellman-Schlüsselaustausch[2]

1.5 Digitale Zertifikate

Digitale Zertifikate sollen Eigenschaften und Identitäten von Personen und Objekten bestätigen. Ein Zertifikat ist wie ein digitaler Personalausweis. Er soll somit die Vertraulichkeit, Integrität und die Identifizierung gewährleisten. Die

[2] In Anlehnung an: Wikipedia, http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange, Abruf am 2013-12-12.

Zertifikate werden von der Certifikation Authority ausgestellt. Am meisten verbreitet sind die Public-Key-Zertifikate, welche die Identität des Inhabers mit Hilfe öffentlicher kryptischer Schlüssel bestätigen.

1.6 Digitale Signatur

Mit digitalen Signaturen sollen sowohl die Urheberschaft als auch die Zugehörigkeit einer Nachricht geprüft werden. Digitale Signaturverfahren verwenden asymmetrische Verschlüsselungstechniken. Dabei wird entweder die Nachricht selbst mit den privaten Schlüssel signiert (digitale Signatur mit Nachrichten-Rückgewinnung) oder der Hashwert (digitale Signatur mit Hashwert-Anhang). Anschließend wird mit dem öffentlichen Schlüssel die Signatur entschlüsselt und somit die Identität des Senders verifiziert.

1.7 Hash-Funktionen

Eine Hashfunktion berechnet von einer Nachricht beliebiger Länge einen Hashwert mit fester Länge. Bekannte Algorithmen, die die Hashfunktionen anwenden, sind der Secure Hash Algorithm (SHA) und der Message-Digest Algorithm 5 (MD5). Im Folgenden wird die Hashfunktion mit SHA erklärt. Bei SHA wird eine Prüfsumme erstellt. Diese Prüfsumme hat immer die gleiche Länge, unabhänig wie lange die Nachricht ist. So kann eine große Menge an Daten einfach auf Korrektheit überprüft werden. Sobald sich ein Bit ändert, verändert auch sich die komplette Prüfsumme. Die Prüfsumme lässt sich nicht zurückrechnen und wird deswegen auch eingesetzt, um Passwörter zu verschlüsseln. Im Folgenden werden einige Beispiele aufgelistet, welche den SH-Algorithmus veranschaulichen.

SHA1 Prüfsumme zu „Test1234“: dddd5d7b474d2c78ebbb833789c4bfd721edf4bf
SHA1 Prüfsumme zu „test1234“: 9bc34549d565d9505b287de0cd20ac77be1d3f2c
SHA1 Prüfsumme zu „Diese Praesentation dauert schon viel zu lange“: 8abe388aa9401082250a3e0ab236928eb4d13413

1.8 E-Mail Verschlüsselung

1.8.1 Client-basierte E-Mail Verschlüsselung und –Signatur

Bei der Client-basierten E-Mail Verschlüsselung wird beim Client (Sender) die E-Mail verschlüsselt und versendet. Der Client des Empfängers entschlüsselt dann die E-Mail.

1.8.2 Serverbasierte E-Mail Verschlüsselung und –Signatur

Bei der serverbasierten Verschlüsselungstechnik wird von dem E-Mail Server die Verschlüsselung vorgenommen. Die Entschlüsselung der E-Mail kann dann entweder vom Client oder vom Server des Empfängers vorgenommen werden.

1.8.3 PKI-basierte E-Mail Verschlüsselung und –Signatur

PKI steht für Public Key Infrastruktur und verwendet Standards zur Verschlüsselung und wird eingesetzt um entweder die Client- oder die Server-basierte Verschlüsselung zu realisieren. Die Standards sind unter anderem S/MIME (Secure / Multipurpose Internet Mail Extensions) und OpenPGP (Open Pretty Good Privacy).

1.8.4 Passwort-basierte E-Mail Verschlüsselung

Alternativ zur Serververschlüsselung werden E-Mails mit Passwörtern gesichert und auf dem Server des Senders abgerufen. Diese Variante wird statt PKI eingesetzt, wenn der Empfänger entweder selbst über keine Server-basierte Lösung verfügt oder der Client des Empfängers kein PKI unterstützt.

2 Bedeutsamkeit privater und unternehmensbezogenen Daten

Im Folgenden werden Beispiele aus der Realität zur Verdeutlichung der Relevanz der Themenstellung herangezogen.

2.1 Andrej Holm[3]

Andrej Holm absolvierte eine Grundausbildung bei der Staatssicherheit in der ehemaligen Deutschen Demokratischen Republik und war nach dieser Mitarbeiter im Wachregiment Feliks Dzierzynski. Zudem war er Mitglied in einer marxistischen Jugendvereinigung und Hausbesetzerbewegungen.

Nach seinem Studium an der Humboldt-Universität Berlin war er dort als wissenschaftlicher Mitarbeiter tägig. Er promovierte mit der Arbeit „Restrukturierung des Raumes und gesellschaftliche Macht im Sanierungsgebiet“. Er gilt national und international als Experte für Stadtentwicklung und Gentrifizierung.

Holm wurde wegen des Verdachts der Mitgliedschaft in einer „terroristischen Vereinigung“ verhaftet. Er wurde bezichtigt bei der Inbrandsetzung dreier Bundeswehrfahrzeuge beteiligt gewesen zu sein. Der Verdacht begründete sich darin, dass Holm sich mit (anderen) Beschuldigten getroffen hatte, zudem hatte er bei diesen Treffen sein Mobiltelefon nicht bei sich und die Verabredung erfolgte über verschlüsselte Mails. Nach Holms Verteidiger wurden die Ermittlungsbehörden durch eine Internetrecherche mit den Suchbegriffen „Gentrification“ und „Prekarisierung“ auf ihn aufmerksam. Holms steht mit diesen Begriffen jedoch aufgrund seiner Forschungsarbeit im Zusammenhang. Wie bereits zuvor erwähnt, gilt er als Experte auf diesem Gebiet.

Als Fazit ist festzuhalten, dass Daten und Kontakte aus der Vergangenheit in Kombination mit sicherer Kommunikation und einem vergessenen Mobiltelefon schon ausreichend zu sein scheint, um als Beschuldigter in einem Verfah-

[3] Vgl.: Wikipedia: http://de.wikipedia.org/wiki/Andy_Holm, Abruf am 2013-12-12.

ren über Mitgliedschaft in einer terroristischen Vereinigung gelten zu können. Der Haftbefehl wurde vom Bundesgerichtshof im Jahr 2007 aufgehoben.

2.2 Privatperson, Unternehmen und Staat[4]

Der zuvor genannte Fall Andrej Holm zeigt die Notwendigkeit von Datenschutz und die Bedeutsamkeit privater Daten. Datenschutz nimmt aufgrund der zunehmenden Vernetzung einen immer höheren Stellenwert ein. Privatpersonen und Unternehmen lagern zunehmend Daten z.B. in Clouds aus. Durch Verfahren wie die Big-Data-Analysen lassen sich Daten (Gesichter von Fotos, Kontobewegungen, Daten von und in sozialen Netzen, das Kaufverhalten u.v.m.) gezielt Personen, Personenkreisen und Unternehmen zuordnen. Es besteht die Möglichkeit gezielt Profile über Personen und Unternehmen anzulegen und immer weiter zu vervollständigen – sogar Rückschlüsse und Prognosen über das künftige Verhalten sind möglich. Es besteht somit die Gefahr des „Gläsernen Menschen“. Problematisch sind aber auch politische Auswirkungen. Es gibt keine Demokratie ohne Datenschutz. Eine Demokratie zeichnet sich durch die Gewährung von Grundrechten aus, wie beispielsweise die Glaubens- und Meinungsfreiheit. Wer sich jedoch überwacht fühlt, wird sich anders verhalten und ist somit in seiner Freiheit eingeschränkt. Zuletzt gewährleistet der Datenschutz einen Schutz der Unternehmen und des Wirtschaftsstandortes vor dem Diebstahl von Firmengeheimnissen und Industriespionage.

[4] Vgl.: Heise.: http://www.heise.de/tp/artikel/23/23625/1.html, Abruf am 2013-12-12.

3 Privat- und Firmennetzwerke - Risiken, Sicherheitstipps des BSI, Praxisanwendungen von Sicherheitsmaßnahmen und Sicherheitstools

3.1 Gefahren/ Risiken für Privat- und Firmennetzwerke

Privat- und Firmennetze sehen sich im Zuge der immer stärker werdenden Vernetzung einer immer größer werdenden Reihe von Gefahren ausgesetzt. Dabei können grundsätzlich mehrere Gefahrenpotentiale beobachtet werden. Die Gefahren lassen sich dabei auf Gefahrenpotentiale aus dem internen Netzwerk, Gefahren aus dem Internet (externes Netz) und fehlerhaften Netzwerkkonfigurationen zurückführen.

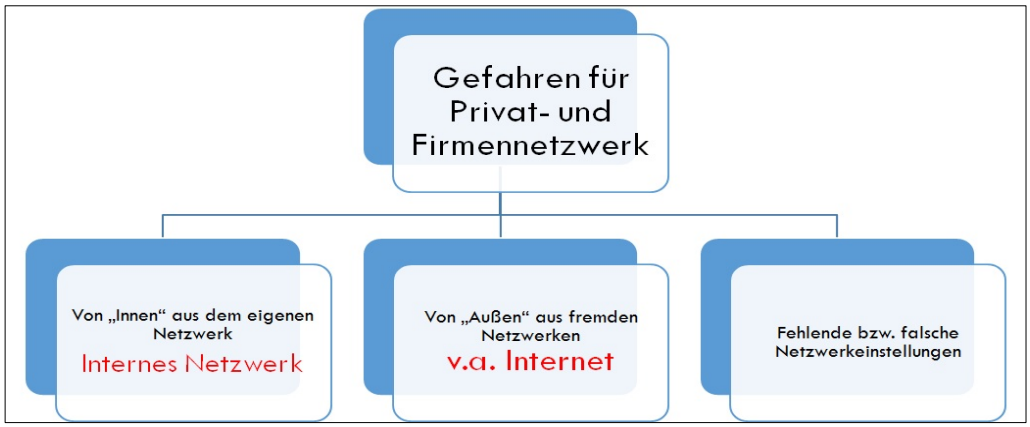


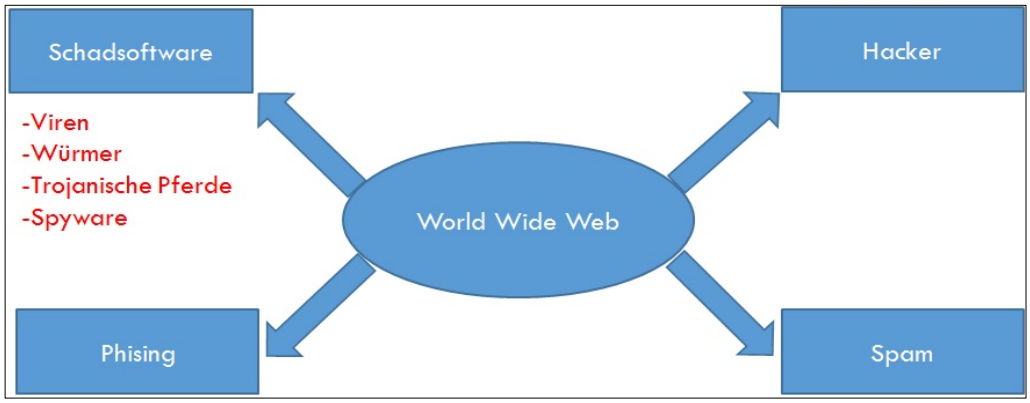
Abbildung 3: Gefahren für Privat- und Firmennetze[5]

[5] Eigene Erstellung.

Gefahren aus dem internen Netzwerk:

- Verbreitung von Schadsoftware über USB, CD/DVD
- Fehlende/Fehlerhafte Zugriffsrechte (Benutzerrechte)
- Fehlende Schutzmechanismen (kein Passwortschutz)

Gefahren im Netz:[6]



Weitere Gefahren: **Botnetzwerke, Falsche Virensoftware, DoS, Gefälschte Absenderadressen, Hoax, Kostenfallen …….**

Abbildung 4: Gefahren im Netz[7]

Beispiel : Flash – Cookies (oder LSO = Local Shared Object)[8]

- stellt ein über das Adobe Flash – Player gebundenes Cookie dar
- Ziel:

  Speicherung von benutzerbezogenen Daten auf dem PC des Nutzers mit dem Ziel diese beim erneuten Wiederaufruf des Webdienstes bereitzustellen.

[6] Vgl. BSI. Quelle: https://www.bsi-fuer-bue-ger.de/BSIFB/DE/GefahrenImNetz/gefahren_node.html;jsessionid=4EAA2338F8320EA32A988F3308F22D19.2_cid369, Abruf am 2013-12-08.
[7] In Anlehnung an BSI.: Gefahren im Netz. Ebenda.
[8] Vgl. Wikipedia.: http://de.wikipedia.org/wiki/Flash-Cookie, Abruf am 2013-12-09.

- längere Verweildauer als herkömmliche Cookies (z.T. als unlöschbare Langzeit - Cookies bekannt)
- browserübergreifend
- → werden durch das eingesetzte Flash – Plug-In verwaltet und i.d.R. browserunabhängig im System abgelegt (meist in den Anwendungsdaten)

Gefahren – Netzwerkeinstellungen

- Offene WLAN – Netze
- Fehlende/Fehlerhafte Firewall-Regeln

3.2 Praktische Anwendung von Sicherungsmaßnahmen

- Sicherung des privaten WLAN (Sicherheitstipps des BSI)

  Sicherheitstipps:[9]

  1) Persönliches Administratorkennwort
  2) Konfiguration des Access-Points über sichere Wege
  3) Änderung des Netzwerknamens (SSID = Service Set Identifier)
  4) Sichere Verschlüsselung (WPA / WPA2) – WEP unsicher
  5) Einrichten von MAC – Filter
  6) WLAN nur bei Gebrauch
  7) Firmware – Aktualisierung

- *Einsatz von **Sicherheitstools** (Beispiele):*

  - Better Privacy zum Schutz vor LSO Cookies
  - No-Script (Schutz vor gefährlichen Skripten)

[9] Vgl. BSI.: https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/WegInsInternet/WLAN/Sicherheitstipps/wlan_tipps.html, Abruf am 2013-11-30.

3.3 Netzwerke professionell absichern[10]

1. Schritt: Netzwerkanalyse:

- Analyse aller Dienste, Geräte und Programme im Netzwerk
  - in kleinen Netzwerken (<= 5 Geräte): Netzwerkcheck i.d.R. mithilfe von Excel-Listen
  - in größeren Netzwerken: Automatischer Netzwerkcheck
- Datenverkehr analysieren
  - dubiosen Datenverkehr erkennen
    → z.B. Wireshark

2. Schritt: Schwachstellen finden

Ausgangssituation: Schwachstellen rühren i.d.R. aus veralteter oder falsch konfigurierter Software

Schwachstellen von Anfang an vermeiden:

→Tatsächlicher Bedarf an Systemen, Diensten etc. ermitteln!

→Abwägung des Risikos der einzusetzenden Ressourcen

Security – Check durchführen:

→Testen der getroffenen Sicherheitsmaßnahmen durch den Einsatz von Software →softwaregestützter Security Check (z.B. Live CD Boss (BSI)

3. Schritt: Schwachstellen beheben

- Nicht immer wird kostenintensive Software benötigt
- Konfigurationen von bestehender Software kann u.U. genügen (z.B. Updateintervalle wichtiger Systeme neu konfigurieren)

[10] Vgl. Chip Online.: http://business.chip.de/artikel/Kleine-Netzwerke-professionell-absichern_39743805.html, Abruf am 2013-11-26.

- Bedarf an grundlegenden Aktivitäten:
    - Updates regelmäßig einspielen; bei großem Netzwerk zentral verteilen, automatisieren
    - Regeln vorgeben (Passwortrichtlinien)
    - Rechte gezielt vergeben (Zugriffsrechte verteilen)

4. Schritt: Warnsysteme einrichten

Einführung eines Monitoringsystems mit dem Ziel

- Hardwareveränderungen
- Softwareveränderungen
- die Benutzerverwaltung
- sowie eine Funktionsprüfung bestehender Systeme

für die IT-Verantwortlichen bereitzustellen.

4 Fazit

Die vorgestellten Sicherheitsmaßnahmen bieten einen guten Grundschutz, um sich vor Gefahren aus dem Netz zu schützen. 100% - Sicherheit existiert nicht.

I.d.R. liegt ein Informationsvorsprung der Angreifer vor, der durch Sicherheitsmaßnahmen auf Hard- und Software-Ebene einzudämmen ist. Die Vorgestellten Verschlüsselungstechniken gelten z.Z. als sicher, jedoch ist es fraglich, ob mit genügender Rechenleistung und Zeit diese Techniken in der Zukunft genügend Sicherheit bieten und ggf. umgangen werden können. Jeglicher Schutz sollte als kurzfristige Maßnahme angesehen werden, da dieser nur so lange als valide gilt, bis die nächste Sicherheitslücke bekannt wird.

Literaturverzeichnis

BSI – Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi-fuer-buerger.de/BSIFB/DE/Home/home_node.html, https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/gefahren_node.html

Chip Online, http://business.chip.de/artikel/Kleine-Netzwerke-professionell-absichern_39743805.html

Heise Online, http://www.heise.de/tp/artikel/23/23625/1.html

www.itwissen.info

Kryptographie und IT-Sicherheit – Joachim Swoboda, Stephan Spitz, Michael Pramateftakis, Springer Verlag 2008

Wikipedia, http://de.wikipedia.org/wiki/Andy_Holm, http://de.wikipedia.org/wiki/Flash-Cookie