ZT WIRTSCHAFT

Mit Umsicht und Know-how gegen digitale Saboteure, Diebe und Späher

Das Internet ist aus dem geschäftlichen Bereich heute nicht mehr wegzudenken. Seine vielen Informations- und Kommunikationsdienste haben herkömmliche Verfahren fast vollständig ersetzt. Die Nutzung des Internets und die Verarbeitung sensibler Daten rücken aber auch das Thema Sicherheit immer mehr in den Mittelpunkt. Autor Thomas Burgard gibt eine umfassende Einführung, die auch Dentallabore für das Thema Internet-Sicherheit sensibilisieren soll.

Einführung

Das Internet ist ein weltumspannendes Netzwerk aus einzelnen Computern und wird heute im professionellen wie auch privaten Bereich immer stärker genutzt, Tendenz steigend. Man kann sich daher sehr leicht vorstellen, dass durch die globale Nutzung des Internets als Informations- und Kommunikationsdienst immer mehr sicherheitsrelevante Daten (z.B. Personendaten, Kontozugangsdaten etc.) auf den miteinander vernetzten Computern gespeichert und verarbeitet werden. Bedingt durch die flächendeckende IT-Vernetzung sind natürlich auch flächendeckende Angriffspunkte vorhanden.

Das Internet wurde bereits in den frühen 70er-Jahren des 20. Jahrhunderts in den USA als reines Forschungsnetz entwickelt. Da das Forschungsnetz ein autarkes, von Forschungseinrichtungen genutztes, Netz war, waren Angriffe von außen nicht möglich. Das technische Grundkonzept des Netzwerkes hat böswillige Angriffe von außen einfach nicht vorgesehen und dies hat sich bis heute prinzipiell nicht geändert. Ein Sicherheitsschutz wird auch heute ausschließlich durch zusätzliche Hardware und Software realisiert. Der Aspekt Sicherheit wurde leider von vielen Softwareanbietern vernachlässigt. In immer kürzeren Abständen kommen neue wirkungsvolle internetbasierte Angriffsmethoden in den Umlauf und somit sind immer mehr Sabotage- und Spionagewerkzeuge auch verfügbar. Erschreckend dabei ist, dass diese Werkzeuge und Hackersoftware für jedermann zugänglich sind. Die Hardware- und Softwareindustrie kommt kaum hinterher und steht immer häufiger vor großen Problemen.

Erschwerend kommt hinzu, dass das Medium Internet von keinem überwacht wird. Es existiert keine übergeordnete Aufsichtsbehörde. Im weltumspannenden Internet ist sich jeder selbst überlassen und kann sehr schnell selbst zum Gefährdungsziel werden. Ist ein Internetnutzer online, d.h. mit dem Internet verbunden, hinterlässt er auf den beteiligten Netzwerkcomputern Spuren, die dann auch böswillig benutzt werden können. Jedem sollte bewusst sein, dass das Internet die gesellschaftlichen Verhältnisse widerspiegelt. Es gibt wie in der realen Welt seriöse und böswillige Anwender.

Somit kann gesagt werden, dass der Seriosität der Internetanbieter eine ganz zentrale Bedeutung zukommt. Jeder Nutzer des Mediums Internet, egal ob geschäftlich oder privat, hat daher die Aufgabe, seine mit dem Internet verbundenen Informations- und Kommunikationssysteme vor Angriffen aus dem Internet zu schützen.

Unter diesen Gesichtspunkten und der Diskussion über das Thema Sicherheit im Internet haben sich drei Schlüsselkonzepte ergeben, die mittels unterschiedlichen Sicherheitsmaßnahmen die Sicherheit gewährleisten soll: **Vertraulichkeit**, **Integrität** und **Authentizität**.

Vertraulichkeit – Wie kann man Daten vor unberechtigten Lesezugriffen schützen?

Integrität – Wie kann man Daten vor unberechtigter Manipulation schützen?

Authentizität – Wer ist der Urheber der Daten? Ist die Datenquelle auch die Richtige (z.B. der E-Mail-Absender)?

Typische Angriffstechniken im Internet

Um Risiken besser zu beurteilen und dann entsprechende Maßnahmen einzuleiten, z.B. Einsatz einer Sicherheitssoftware, möchte ich zuerst gängige Angriffstechniken im Internet vorstellen.

Viren

Computerviren sind die bekannteste Bedrohungsart im Internet. Computerviren sind von Menschen geschriebene Software und hängen sich an Programme an. Die Aktivierung oder auch Reproduktion beginnt nach Start des Programms. Ab diesem Zeitpunkt beginnt die Infizierung des Computer-Betriebssystems oder der Anwendersoftware.

Sogenannte **Stealth-** oder **Slow-Viren** sind die unangenehmsten Viren-Vertreter, denn sie verschleiern sich oder richten den Schaden erst viel später an.

Durch die Installation einer Antivirussoftware auf dem Computer können viele Viren erfolgreich bekämpft werden.

Würmer

Würmer funktionieren ähnlich wie Viren. Der Unterschied ist der, dass Würmer eigenständige Software sind und sich als reguläre Dateien, Dokumente oder sogar Bilddateien ausgeben. Würmer werden meistens als E-Mail-Anhang versendet und bringen so die gefährliche Fracht in den Umlauf, indem sie sich selbsttätig an alle in einem Adressbuch gespeicherten E-Mail-Adressen versenden.

Trojanische Pferde (Trojaner)

Diese Art von Angriffsmethode stellt ein Computerprogramm dar, das sich z.B. hinter einem aus dem Internet heruntergeladenen Programm versteckt, um dann auf dem Fremdrechner bestimmte Funktionen auszuführen. Mit einem Trojaner ist es z.B. möglich, einen Fremdrechner fernzusteuern oder auf dem Fremdrechner Spionage zu treiben.

Spyware/Adware

Spyware ähnelt sehr stark einem Trojanischen Pferd. Der Unterschied ist aber, dass Spyware das Ziel verfolgt, die Surf- und Kaufgewohnheiten des Benutzers auszuspionieren. Mit Spyware kann der Angreifer dann automatische entsprechende Werbung an den Benutzer versenden.

Adware ist zusätzliche Werbesoftware (Werbebanner oder Reklame Pop-ups), die sich z.B. durch eine Installation eines regulären Programms parallel auf dem Computersystem installiert. Die Abgrenzung zwischen Spyware und Adware ist nicht ganz klar definiert.

Denial-of-Service-Attacken

Als Denial-of-Service-Attacken bezeichnet man das gezielte Außerkraftsetzen von Diensten auf einem Server oder Computer im Internet. Als Server bezeichnet man Computer, die in einem Netzwerk (z.B. Internet) bestimmte Dienste anbieten. Der Angriff erfolgt durch Überlastung, d.h. der Zielrechner wird durch eine Flut von Anfragen in Überlast gebracht.

Sniffing

Bei Sniffing wird eine Kommunikationsverbindung in einem Netzwerk ganz gezielt abgehört. Mit Sniffing kann

auch der ganze Datenverkehr innerhalb eines Netzwerkes abgehört werden. Beliebt ist hier das Herausfinden von Passwörtern.

Spoofing
Unter Spoofing versteht man eine ganze Reihe von verschiedenen Angriffsmethoden, die alle ein gemeinsames Ziel haben, nämlich das Verschleiern der eigenen Identität. Das heißt, der angreifende Computer gibt vor, eine anderer zu sein als er wirklich ist.

Source-Routing-Attacken
Diese Angriffsmethode ergattert sich die Route einer Kommunikationsverbindung innerhalb eines Netzwerkes, sodass der Angreifer die Daten zugesendet bekommt.

Man-in-the-Middle-Attacken
Hierbei hängt sich der Angreifer quasi selbst in eine bestehende Verbindung rein, ohne dass die Kommunikationspartner davon etwas bemerken. Der Angreifer kann nun die Datenpakete beliebig manipulieren.

Social Engineering
Diese Angriffsmethode ist relativ einfach durchzuführen. Social Engineering ist die derzeit mit Abstand gefährlichste Angriffsmethode und kann leider nicht abgewehrt werden. Man nutzt die Unwissenheit des Benutzers aus, um z.B. an Geheimwörter zu gelangen. Dazu wird unter anderem eine fingierte E-Mail mit vertrauenswürdiger Aufmachung an den Benutzer gesendet mit der Aufforderung, die geheimen Zugangsdaten wie ein Passwort für das Online-Banking aus angeblichen Sicherheitsgründen einzutragen und zu ändern.

Hoax
Hoax ist ebenfalls eine einfache Angriffsmethode. Der Angreifer versendet gezielt falsche Meldungen mittels E-Mail an Benutzer mit der Aufforderung, diese E-Mail an andere weiterzuleiten. Dadurch entsteht eine höhere Netzlast. Mittels Hoax kann z.B. eine falsche Aktienempfehlung per E-Mail verbreitet werden, um dann einen Aktiencrash zu erreichen.

Pishing
Pishing gehört ebenfalls zu den gefährlichen Angriffsmethoden. Einem Pishing-Angriff geht immer ein Social Engineering voraus. In der E-Mail ist ein Link aufgeführt, der auf eine täuschend echte Bank-Internetseite verweist. Auf dieser Internetseite wird der Benutzer gebeten, die Bankdaten und Bankzugangsdaten einzutragen.

Pharming
Pharming stellt eine Weiterentwicklung des Pishing dar. Hierbei tippt der Benutzer die richtige Internetadresse der Bank ein, landet jedoch auf einer gefälschten Internetseite des Angreifers.

Mailbomben
Hierbei versendet der Angreifer eine Unzahl von E-Mails mit Daten an einen E-Mail-Server oder an einen Benutzer-Computer. Der Angreifer tarnt sich, indem er anonyme Server verwendet. Eine Rückverfolgung ist somit äußerst schwierig.

Kryptografie

Durch den Einsatz von kryptografischen Mitteln lassen sich viele Sicherheitsprobleme im Internet stark verringern. Hierbei kommen sogenannte Verschlüsselungsverfahren zum Einsatz, die einen mathematischen Algorithmus darstellen, um z.B. mittels einer geheimen Zeichenkette (Schlüssel) die komplette Nachricht zu verschlüsseln, also nicht mehr lesbar machen. Für die Entschlüsselung

der Nachricht wird ebenfalls ein Schlüssel benötigt, um den lesbaren Text zu erhalten. Die verwendeten Schlüssel können identisch oder auch unterschiedlich sein.

Verschlüsselungsverfahren

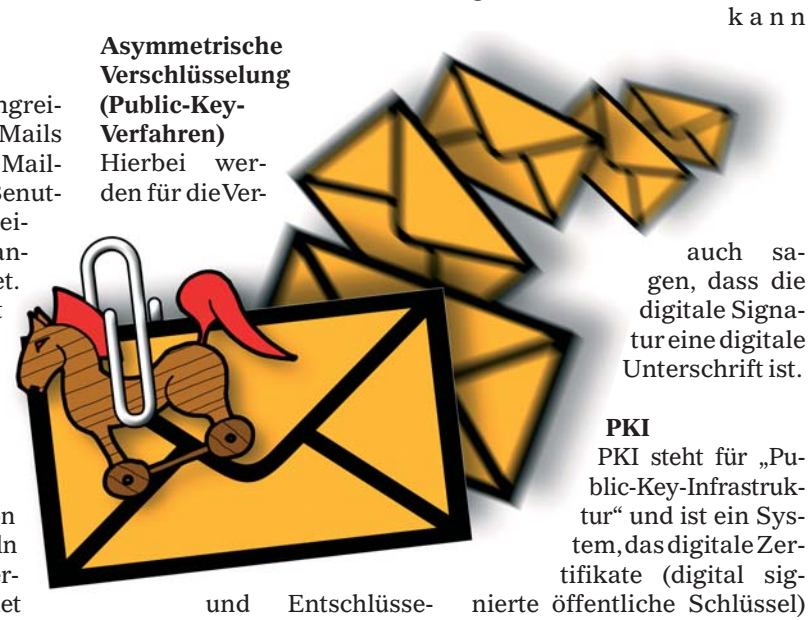
Verschlüsselungsverfahren sind also kryptografische Verfahren, die dafür sorgen, dass nur die wahren Empfänger einer Nachricht diese lesen können. Dabei kommen unterschiedliche Verfahren zum Einsatz:

Symmetrische Verschlüsselung (Private-Key-Verfahren)
Bei der symmetrischen Verschlüsselung wird für die Verschlüsselung und die Entschlüsselung der gleiche Schlüssel verwendet. Dieser muss zwischen den Kommunikationspartnern auf einem sicheren Weg ausgetauscht werden.

Vorteil:
- Nur ein Schlüssel für beide Kommunikationspartner.

Nachteile:
- Der Austausch der Schlüssel ist unsicher, denn ein unbefugter Dritter könnte den Austausch ausspionieren.
- Die Verschlüsselung ist leicht zu brechen.

Asymmetrische Verschlüsselung (Public-Key-Verfahren)
Hierbei werden für die Ver- und Entschlüsselung zwei unterschiedliche Schlüssel verwendet. Die Funktionsweise ist Folgende: Anwender A möchte eine verschlüsselte Nachricht zu Anwender B senden. Zuerst generiert A zwei Schlüssel, von denen einer öffentlich und der andere geheim ist. Die geheime Nachricht von A wird dann mit dem öffentlichen Schlüssel (public key) verschlüsselt. Die Nachricht kommt absolut sicher bei B an, da ja für die Entschlüsselung der geheime Schlüssel (private key) benötigt wird. Nur B kann die Nachricht mit dem geheimen Schlüssel entschlüsseln, da nur er in Besitz des geheimen Schlüssels ist. Die asymmetrische Verschlüsselung wird zur Verschlüsselung, Authentifizierung und Sicherung der Integrität eingesetzt, z.B. beim E-Mail-Verkehr.



Vorteil:
- Die Verschlüsselung ist sehr sicher, da ein zweiter geheimer Schlüssel für die Entschlüsselung notwendig ist.

Nachteil:
- Durch die zwei Schlüssel ist das Verfahren sehr aufwendig.

Digitales Zertifikat und digitale Signatur

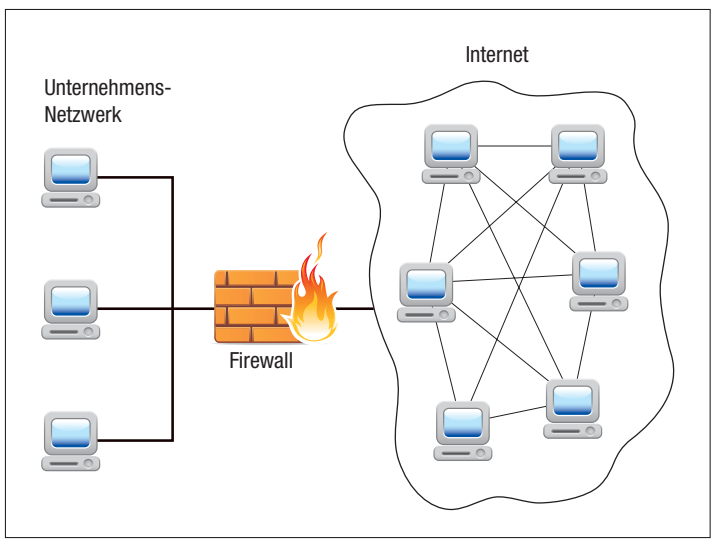
Digitales Zertifikat
Um sicherzustellen, dass der öffentliche Schlüssel auch zum wahren Empfänger gehört und der öffentliche Schlüssel auch mit diesem Verschlüsselungsverfahren und dem entsprechenden Anwendungsbereich verwendet werden darf, muss ein Nachweis dies bestätigen. Genau diesen Nachweis nennt man „digitales Zertifikat".

Digitale Signatur
Eine digitale Signatur basiert auf dem asymmetrischen Verschlüsselungsverfahren und stellt einen Zahlenwert dar, mit dem die Integrität der Daten ermittelt und eine eventuelle Veränderung der Daten aufgedeckt werden kann. Man kann auch sagen, dass die digitale Signatur eine digitale Unterschrift ist.

PKI
PKI steht für „Public-Key-Infrastruktur" und ist ein System, das digitale Zertifikate (digital signierte öffentliche Schlüssel) ausstellen, prüfen und verteilen kann und darf.

Firewalls

Eine (Internet-)Firewall ist prinzipiell ein kontrollierter Übergang zwischen zwei voneinander zu trennenden Netzwerken. In der Regel besteht eine externe Firewall aus einer Hardware und spezieller Firewall-Software. Das zu trennende Netzwerk kann z.B. das Unternehmens-Netzwerk mit den Arbeitsplatz-Computern und das Internet sein. Die Aufgabe der Firewall sind diverse Schutzfunktionen für das Unternehmensnetzwerk gegen Angriffe aus dem Internet und natürlich auch geeignete Schutzfunktionen für die eigene Firewall-Software. Durch umfangreiche Filtereinstellungen kann die Firewall nur ganz bestimmte Datenpakete passieren lassen oder nicht.



Externe Firewall.

Personal Firewalls
Eine Personal Firewall, auch Desktop Firewall genannt, ist eine Software, die auf einem PC installiert wird und ein- und ausgehenden Datenstrom nach bestimmten Regeln filtert. Eine Personal Firewall stellt also keine externe Hardware dar.

Vorteile:
- kostengünstig
- einfach zu installieren und einzustellen
- applikationsspezifische Filter können eingestellt werden

Nachteil:
- Personal Firewall Software kann selbst angegriffen werden.

Geeignete Maßnahmen

Welche geeigneten Maßnahmen kann der Internetnutzer nun gegen die oben beschriebenen Angriffsmethoden treffen? Grundsätzlich lässt sich erst einmal sagen, dass eine große Anzahl von Internetnutzern leider wenige oder gar keine Kenntnisse in Informationstechnologie (IT) besitzen. Auch viele Unternehmer, davon viele Kleinunternehmer, nehmen IT immer noch nicht richtig ernst, obwohl IT heute in keinem vernünftig geführten Unternehmen fehlen kann. Sicherheitsmaßnahmen werden leider dann erst wahrgenommen, wenn Schaden entstanden ist. Unternehmer, aber auch die Mitarbeiter, sollten das Thema Internet-Sicherheit ernst nehmen und zur obersten Pflicht machen.

- Das Unternehmen sollte sich im Bereich Informationstechnik und Internet-Sicherheit weiterbilden (Mitarbeiter müssen unbedingt mit einbezogen werden). Hier ist Eigeninitiative gefordert.
- Das Unternehmen sollte eine Sicherheits-Strategie festlegen und einen Maßnahmenkatalog zusammenstellen.
- Unternehmensdaten müssen immer vertraulich behandelt werden.
- Wichtige Räume mit IT-Technik sollten vor unbefugten Zutritt gesichert sein.
- Ein installiertes IT-System (z.B. ein Unternehmensnetzwerk mit Server und Clients) muss richtig konfiguriert sein.
- Auf einem Netzwerk-Server und auf den Arbeitsplatzrechnern sollte eine geeignete Sicherheitssoftware wie Firewall, Personal Firewall, Antivirussoftware installiert werden.
- Die Firewall muss korrekt eingestellt werden (Filterregeln).
- Antivirussoftware sollte täglich auf Viren, Trojaner etc. überprüfen.
- Einsatz von Open-Source-Software, da hier wesentlich schneller auf gefundene Sicherheitslücken reagiert wird (z.B. Internetbrowser Firefox statt Microsoft Internet Explorer).
- Das Rechner-Betriebssystem sollte regelmäßig auf Sicherheits-Updates überprüft werden. Gleiches gilt für die Internetbrowser-Software.
- Ein Umstieg auf eine neues Betriebssystem oder andere Anwendersoftware sollte vorher gut geplant und getestet sein.
- Der Arbeitsplatzrechner sollte korrekt partitioniert und eine gute Dokumentenstruktur geschaffen werden.
- Die Datenzugriffsmöglichkeiten sollten auf das erforderliche Mindestmaß beschränkt werden.
- Der Zugang zum Arbeitsplatzrechner sollte mit einem Passwort gesichert werden.
- Es sollten regelmäßig Datensicherungen (Back-ups) durchgeführt werden. Die Datensicherungen sind gut und sicher aufzubewahren.
- Passwörter sollten richtig gewählt werden (ausreichende Länge, Sonderzeichen etc.).
- Passwörter und Schlüssel sollten sicher hinterlegt werden.
- Vertrauliche Daten sollten verschlüsselt werden (z.B. E-Mail).
- Nicht vertrauenswürdige E-Mails sollten nicht geöffnet werden.
- E-Mail-Anhänge sollten immer mit Vorsicht behandelt werden, wenn der Absender nicht bekannt ist.
- Um Spam-Mails im E-Mail-Hauptpostfach zu vermeiden, kann eine zweite E-Mail-Adresse angelegt werden. Diese E-Mail nimmt man dann z.B. für die Registrierung in Foren oder für unbekannte Unternehmen.

Fazit

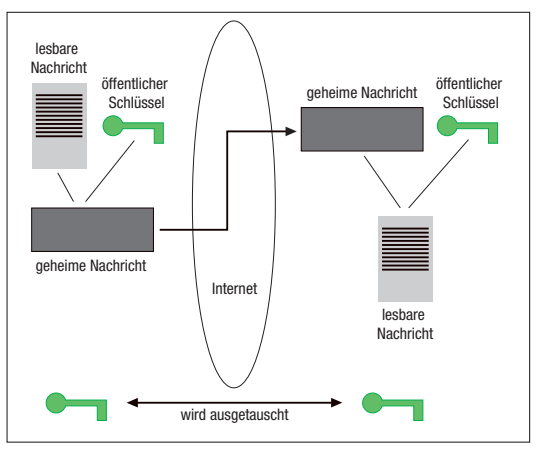
Durch die immer größer werdende IT-Abhängigkeit der Unternehmen und die immer stärkere Computer-Vernetzung weltweit ist eine Internet-Sicherheit unumgänglich. Die Unternehmen müssen sich der Gefahren aus dem Internet bewusst sein und entsprechende Maßnahmen-Strategien und -Kataloge entwickeln. Immer häufiger und in kürzeren Zeitabständen werden Angriffe aus dem Internet getätigt, Daten ausspioniert, Passwörter geklaut. Mit den entsprechenden Maßnahmen (oben beschrieben) lässt sich die Gefahr sehr stark minimieren.
Die Zukunft im Internet ist noch offen, aber eines ist sicher: Die Angriffe aus dem Internet werden massiver und das Thema Internet-Sicherheit wird zu einem zentralen Thema in den Unternehmen. ZT

ZT Der Autor

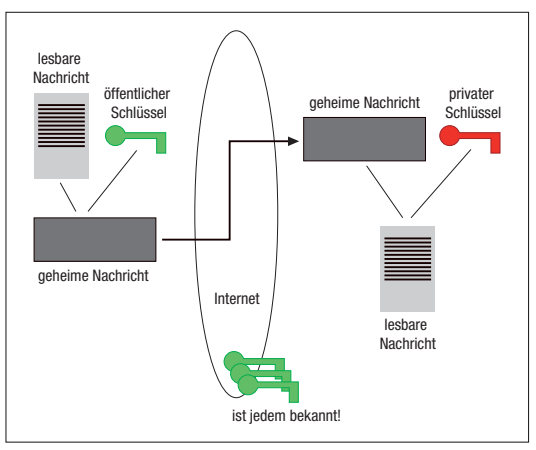
Autor Thomas Burgard entwickelt Dentallabor-Management-Software und erstellt professionelle Internetauftritte für Unternehmen.

ZT Adresse

Thomas Burgard Softwareentwicklung & Webdesign
in Kooperation mit Webexperten24
Dipl.-Ing. (FH) Thomas Burgard
Bavariastr. 18b
80336 München
Tel.: 0 89/54 07 07-00
Fax: 0 89/54 07 07-11
E-Mail:
thomas.burgard@burgardsoft.de
www.burgardsoft.de
www.webexperten24.de



Symmetrische Verschlüsselung.



Asymmetrische Verschlüsselung.