abc
nformation
IT Solution Company

Security Products

- Unsere IT-Spezialisten haben langjährige Erfahrung mit Netzwerken und IT-Security.
- Wir bieten Unterschützung bei der Planung, Realisierung bis zur Betreuung von IT-Systeme.

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

1 Unser Know-how

Unsere IT-Spezialisten haben langjährige Erfahrung mit Netzwerken und IT-Security.

- Firewalls (Packetfilter, Application Gateway, Hybridsysteme...)
- Intrusion Detection und Prevention
- Virenschutz und Content Security
- Verschlüsselung / VPN
- Ausfallsicherheit, Hochverfügbarkeit
- Betriebssysteme, Hardware
- Netzwerkinfrastrukturen

2 Unsere Dienstleistungen

Die Planung, Konzeption und Betreuung für IT-Systeme sind unsere Stärken

Vielfältige Aufgaben gehören ebenso dazu, u.a.:

- neue Trends sind zu erkennen und zu nutzen,
- strategische Entscheidungen sind zu fällen,
- Geschäftsprozesse sind in IT-Strukturen abzubilden,
- der maximalen Nutzen ist aus den Systemen zu ziehen,
- Systeme sund sicher und anwenderfreundlich zu gestalten,
- die permanente Verfügbarkeit ist zu gewährleisten,

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

3 Information Secret Management

Mit zunehmender elektronischen Vernetzung der Unternehmen werden ungeahnte Möglichkeiten der Informationsflut geschaffen sowie Geschäftsprozesse transparenter abgebildet. Das Online-Business trägt wesentlich zur Markterweiterung bei. Kommunikation in den Bereichen B2B, B2C und auf Mitarbeiterebene wird ermöglicht.

Damit verbunden sind aber auch zunehmende Risiken und Gefahren der Manipulation.

Der Zugriff auf wertvolle Unternehmensdaten, kritische Business Applikationen sowie personenbezogener Kundeninformationen muss daher abgesichert werden.

Heute reicht allerdings die routinemäßige Installation von Firewalls oder Intrusion Detection- Systemen nicht mehr aus, um der Gefahr eines Missbrauchs zu begegnen. Zudem kommen die meisten Gefahren nicht von außen. Denn im Vergleich zu unautorisierten Systemzugriffen von außerhalb stellen Verletzungen interner Sicherheitsrichtlinien durch eigene Mitarbeiter das weitaus größere Sicherheitsproblem von Unternehmen dar. Wenn die Mitarbeiter kein Bewusstsein für die Anforderungen einer modernen Security-Strategie entwickeln, versagt auch die beste Technologie.

Hier gilt es, technische und organisatorische Vorkehrungen zu treffen. Doch oft setzen die Maßnahmen nur Blockaden nach außen und ignorieren das Problem internen Unwissens oder der Fahrlässigkeit. Der Bedarf an ausgebildeten Fachkräften in Unternehmen sowie Behörden steigt enorm. Diese bilden das Bindeglied zwischen dem Management und den Mitarbeitern.

Im Information Security Management muß man über die Fähigkeit verfügen, in großen Zusammenhängen sicher und zielgerichtet zu agieren. Im technischen Bereich können die Probleme nur durch Qualifikation gelöst werden. Die Mitarbeiter und Manager müssen über ein hohes Maß an Bewußtsein und Gruppendynamik verfügen. Kommunikation zwischen diesen ist unabdingbar und setzt prozessorientiertes Umsetzen voraus. Projektmanagement, Controllingaktivitäten und Rechtssicherheit runden den Prozess ab.

4 Sicherheit gibt es nicht von der Stange

Mit All-in-one-Lösungen versuchen immer mehr Anbieter, alle wesentlichen Sicherheitsfunktionen in einem Gerät zu vereinen. Derartige Spezial- Appliances sind in erster Linie auf die Bedürfnisse kleiner und mittlerer Unternehmen ausgerichtet. Für Großbetriebe sind diese Lösungen weniger geeignet.Hier sind eindeutige Sicherheitsanalysen notwendig. Unterschiedliche Faktoren wie Verfügbarkeit, Sicherheitsbedürfnis (z.B. geschützte Kundendaten), Bedienerpersonal werden klassifiziert und Security_Levels zugeordnet.

5 Content Security

Content Security umfasst eine Vielzahl verschiedener Technologien

5.1 Überwachung und Verwaltung von Daten

- Überwachung und Verwaltung von Daten, um zu gewährleisten, dass sie frei von bösartigen Codes wie zum Beispiel Viren, vertraulichen Informationen oder beleidigendem Inhalt sind

5.2 Spam-Mails

- Eindämmung der wachsenden Menge an Spam-Mails und Sicherstellung der Mail- Verbindungen der Organisation (keine missbräuchliche Nutzung)

5.3 Mitarbeiter

- Verringerung der gesetzlichen Haftung in Bezug auf die Nutzung von E-Mail und Internet durch Mitarbeiter für die das Unternehmen haftet.

5.4 Authentifizierung

Authentifizierungslösungen stellen sicher, dass nur autorisierte Nutzer Zugang zu unternehmenskritischen Anwendungen, Datenbanken, Dateien oder Webseiten bekommen können. Wenn die Authentifizierung erfolgt ist, lässt sich mit dem System der Zugang einzelner Nutzer zu bestimmten Ressourcen und Dienstleistungen genau steuern und kontrollieren (Autorisierung). Gleichzeitig wird ein Protokoll erstellt, dass die Zugangsversuche und tatsächlichen Zugänge einzelner Nutzer zu Systemen, Dateien und Diensten revisionssicher aufzeichnet.

Viele Organisationen verlassen sich noch immer auf den Einsatz von Benutzernamen und Passwörtern, auch beim Zugang zu extrem sensiblen Firmendaten. Einfache Passwörter können durch eine Vielzahl von Attacken ausgespäht bzw. erraten werden, darunter „Brute Force Attacks“ (Dictionary-Angriffe) und das Erraten von Passwörtern oder Passwortdaten. Andere Formen von Angriffen verfolgen heimlich das Surfen oder greifen Informationen im Netz mit Hilfe entsprechender Geräte (Sniffer) ab. Und schließlich gibt es noch die klassischste aller Varianten, das „Social Engineering“ worunter gewöhnlich alle herkömmlichen Spionagetechniken, Trickbetrügereien und der Missbrauch von Vertrauen zusammengefasst werden.

Starke Authentifizierungslösungen, die einmalige Passwörter - wie zum Beispiel Tokens oder Smart Cards - verwenden, werden immer häufiger von größeren Organisationen eingesetzt.

5.5 Verwaltung der Internetnutzung

Ein weiterer Vorteil von Content Security-Lösungen ist die Verwaltung der Internetnutzung der Mitarbeiter. Diese Lösungen bieten einen Schutz gegen den Missbrauch des Internetzugangs. Produktivitätsverluste während der Arbeitszeit durch den Missbrauch des Internetzugangs gehören der Vergangenheit an.

5.6 Speicheranforderungen

Gleichzeitig steigen die Speicheranforderungen drastisch an. Content Security Tools können dabei helfen, das Speichern von Videos, Musikdateien und heruntergeladener Shareware auf die Festplattenlaufwerke der firmeneigenen IT- Umgebung zu verhindern.

5.7 Bandbreiten-Management

Durch Bandbreiten-Management gewährleisten Sicherheitsprodukte und -lösungen die Hauptgeschäftsprozesse. Es wird verhindert, daß durch gelegentliches Surfen oder nicht geschäftsbezogene Anwendungen (wie zum Beispiel Streaming Media, Peer-to-Peer ((P2P))- Anwendungen und Instant Messaging) Netzwerkressourcen abgezogen werden.

5.8 Schwachstellen Erkennung

Schließlich sind die Lösungen bereits im Stande, Schwachstellen zu bearbeiten, die sich durch die Verwendung unlizensierter, nicht autorisierter und nicht unterstützter Desktop- Anwendungen ergeben; z.B. wird Spyware für viele Unternehmen zu einem immer größeren Problem.

- Virenschutz-Lösungen sowohl für den Desktop als auch für das Gateway
- Web (URL) Filter-Lösungen
- Content Solutions für HTTP und FTP (webbasierten) Verkehr
- Content Solutions für SMTP (E-Mail)

-

5.9 Verschlüsselung von Informationen

Immer mehr Firmen erwägen den Einsatz von Verschlüsselungen zum Schutz der Daten während der Übertragung. Die Verwendung von Kryptografie kann die Unversehrtheit der Daten gewährleisten, indem eine Veränderung oder Komprimitierung durch nicht autorisierte Manipulationen verhindert wird. Die Verschlüsselung kann außerdem Datenschutz gewährleisten, indem nicht autorisierte Nutzer vom Lesen der Daten abgehalten werden.

In Kombination mit der digitalen Signatur von Dateien wird außerdem ein unbestreitbarer Ursprungsnachweis für E-Mails geboten: Der Sender einer E-Mail kann im Nachhinein weder das Senden noch den Inhalt der Sendung leugnen.

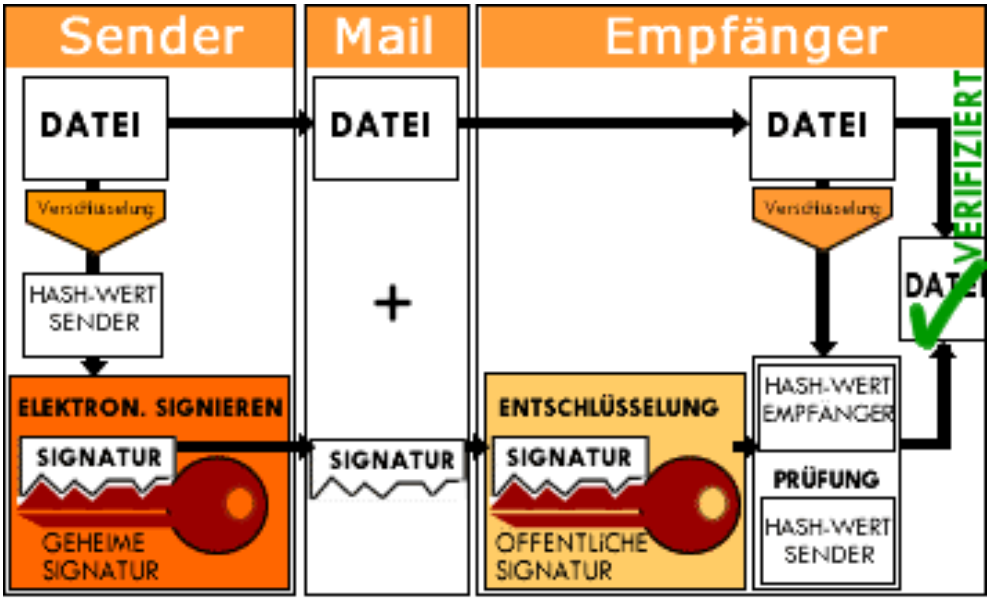
Natürlich ist dieses Verfahren auch auf die Übertragung von Daten anwendbar, da jedes erfolgreiche Unternehmen eine geschützte VPN Lösung benötigt.

Wir haben durch eine Vielzahl von Lösungen Unternehmen unterstützt, die ihren Mitarbeitern sichere (verschlüsselte) E-Mail-Lösungen und einen sicheren Remote-Zugang zur Verfügung stellen.

5.10 Verschlüsselung mit Signaturen

Das Funktions-Prinzip der digitalen Signatur

Die elektronische Signatur gewährleistet die Unverändertheit (Integrität) der Daten und die Identität des Versenders (Authentizität). Mit der elektronischen Signatur werden Manipulationen am Inhalt erkennbar. So lassen sich Sender und Empfänger einer Nachricht eindeutig identifizieren.



Anforderungen an Signaturen

Von einer Unterschrift oder Signatur erwartet man eine Reihe von speziellen Eigenschaften:

- Die Signatur soll authentisch sein:
  Sie ist ein Zeichen dafür, daß der Unterschreibende das Dokument persönlich und absichtlich unterschrieben hat.
- Die Signatur soll nicht fälschbar sein.
- Die Signatur soll nicht wiederbenutzbar sein:
  Sie ist Teil des Unterschriebenen; man kann sie nicht auf ein anderes, nie unterschriebenes Dokument übertragen.
- Das Unterschriebene ist nicht veränderbar:
  Nach erfolgter Unterschrift kann keine Änderung am Text mehr erfolgen.
- Die Signatur kann nicht abgestritten werden:
  Niemand kann nachher behaupten, der Unterschriftsapparat sei ihm abhanden gekommen.

Es ist nicht schwer zu erkennen, daß die meisten dieser Eigenschaften von den heute verbreiteten "physischen" Signaturen nicht voll erfüllt werden; so ist es zum Beispiel relativ leicht, eine Unterschrift auszuschneiden und unter ein anderes Dokument zu plazieren, das Unterschriebene im Nachhinein zu verändern oder auch den Finanzbehörden glaubhaft zu machen, man habe nicht gewußt, was mit der eigenen Unterschriftsmaschine alles unterzeichnet wurde.

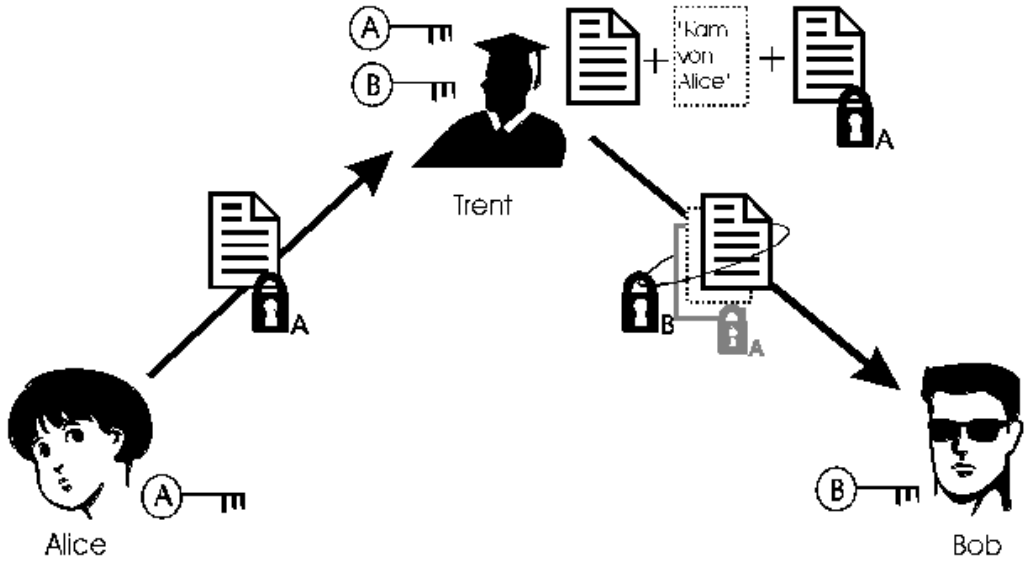
Wir werden zu prüfen haben, inwiefern die digitalen Signaturen in diesen Punkten an die Sicherheit der heute verbreiteten Unterschrift heranreichen oder diese sogar übertreffen.

Signatur mit symmetrischen Kryptoverfahren und einem vertrauenswürdigen Dritten

Die einfachste denkbare Signatur basiert auf symmetrischen Kryptoverfahren und einem "vertrauenswürdigem Dritten", der in der englischsprachigen Literatur meist "Trent" genannt wird (für "Trusted Arbitrator").

Trent ist im Besitz aller geheimen Schlüssel. Möchte Alice nun Bob glaubhaft versichern, daß ein bestimmtes Dokument von ihr ist, verschlüsselt sie es und sendet es an Trent. Dieser entschlüsselt es mit Alices Schlüssel und weiß daraufhin, daß es tatsächlich von Alice gekommen sein muß (sonst wäre die Entschlüsselung fehlgeschlagen). Er zertifiziert diesen Tatbestand in einer separaten Nachricht ("Das anliegende Dokument habe ich von Alice erhalten"), verschlüsselt beides mit Bobs Schlüssel und sendet es an Bob.

Bob wiederum kann sicher sein, daß die Nachricht von Trent kam, denn nur Trent und Bob selbst kennen den Schlüssel. Da Bob Trent vertraut, nimmt er aufgrund von Trents angehängter Nachricht nun an, daß das erhaltene Dokument ursprünglich von Alice kam.



Dieses Verfahren erinnert an zuweilen übliche notarielle Unterschriftsbeglaubigungen, bei denen der Notar als "vertrauenswürdiger Dritter" bestätigt, daß die Unterschrift unter einem Dokument tatsächlich von einer bestimmten Person, die sich ihm ausgewiesen hat, ist.

Die *Authentizität* und *Nichtfälschbarkeit* sind hier trivialerweise erfüllt, da jeweils nur die Beteiligten und der vertrauenswürdige Trent den untereinander benutzten Schlüssel kennen; nur Alice kann also das Ursprungsdokument verschlüsselt haben, nur Trennt kann die Nachricht an Bob abgesandt haben, und Bob glaubt Trent dessen Zertifikat "dies erhielt ich von Alice".

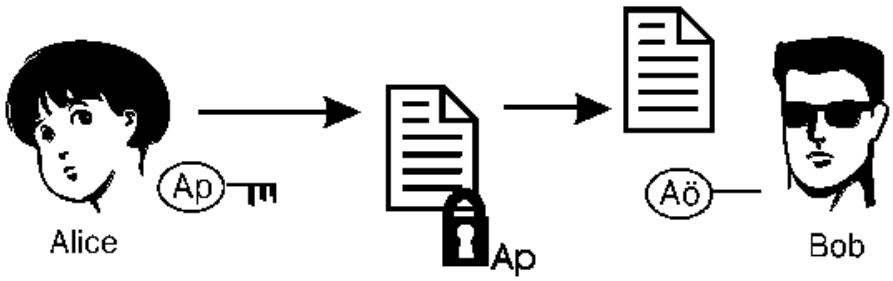
Für die anderen drei Kriterien ist es von Bedeutung, daß Bob zusätzlich von Trent das mit Alices Schlüssel verschlüsselte Originaldokument erhält. Mit diesem kann er zwar nichts anfangen, aber es gewährleistet die *Nichtabstreitbarkeit:* Behauptet Alice später, das Dokument nie abgesandt zu haben, so müssen sie oder Trent in einer Gerichtsverhandlung das bei Bob gelagerte, verschlüsselte Dokument entschlüsseln, und es ergibt sich, daß es tatsächlich mit dem Schlüssel A verschlüsselt war, also von Alice kam. Die *Nichwiederbenutzbarkeit* der Unterschrift bzw. *Unveränderbarkeit* des Dokuments sind ebenfalls dadurch gewährleistet: Wenn Bob eine Änderung am Dokument vornimmt und nun behauptet, das geänderte Dokument von Alice über Trent erhalten zu haben, wird Alice Einspruch einlegen. Bob muß nun in der Lage sein, das verschlüsselte Dokument vorzuweisen, und nach der Entschlüsselung mit dem Schlüssel A zeigt sich, daß das Ergebnis nicht identisch ist mit dem, was Bob erhalten zu haben vorgab.

Die Nichtabstreitbarkeit ist natürlich nur in Grenzen gewährleistet. Ebenso, wie es möglich ist, eine physische Unterschrift dadurch abzustreiten, daß man behauptet, der eigene Unterschriftsapparat oder -Stempel sei mißbraucht worden, kann man auch "versehentlich" seinen geheimen Schlüssel veröffentlichen oder verlieren, und schon kann jedes signierte Dokument theoretisch von jedermann kommen. Es gibt jedoch erweiterte Protokolle, die nicht diesem Manipulationsrisiko ausgesetzt sind.

Signatur mit Public-Key-Verfahren

Bisher wurde im Rahmen dieses Seminars nur auf den Einsatz der Public-Key-Kryptographie zur Verschlüsselung von Nachrichten an einen bestimmten Empfänger eingegangen: Möchte Alice Bob ein Dokument senden, das sonst niemand lesen kann, so verschlüsselt sie es mit Bobs öffentlichem Schlüssel; nur der Inhaber von Bobs privatem Schlüssel - also Bob - kann die Nachricht lesen. Über den *Absender* ist damit jedoch nichts gesagt; die Nachricht kann von jedem kommen, der Bobs öffentlichen Schlüssel kennt.

Public-Key-Kryptographie ist jedoch auch zum Signieren von Dokumenten geeignet. Hierbei verschlüsselt Alice eine Nachricht mit ihrem privaten Schlüssel. Jeder, der Alices öffentlichen Schlüssel kennt, kann diese Nachricht lesen und weiß im selben Augenblick, daß sie von Alice kommen muß, da niemand sonst Nachrichten erzeugen kann, die nach der Entschlüsselung mit Alices öffentlichem Schlüssel Sinn ergäben.



Bei diesem Verfahren sind *Authentizität* und *Nichtfälschbarkeit* ebenfalls trivialerweise erfüllt, da nur Alice selbst ihren geheimen Schlüssel kennt und jede Nachricht, die sich mit ihrem öffentlichen Schlüssel entschlüsseln läßt, daher von ihr kommen muß. Auch die *Unveränderbarkeit* ist gewährleistet, denn wenn Bob die erhaltene Nachricht verändert, paßt Alices öffentlicher Schlüssel nicht mehr, und jeder kann das feststellen.

Für die *Nichtwiederverwendbarkeit* der Unterschrift unter anderen Dokumenten gilt dasselbe; es ist für Bob jedoch möglich, einfach zu behaupten, er habe dasselbe Dokument (beispielsweise eine Bestellung) zehnmal (statt nur einmal) erhalten. Um dem vorzubeugen, könnte Alice eine Datums- und Zeitangabe oder eine laufende Nummer in alle von ihr versandten Dokumente einbauen.

5.11 Verschlüsselung der Datenübertragung

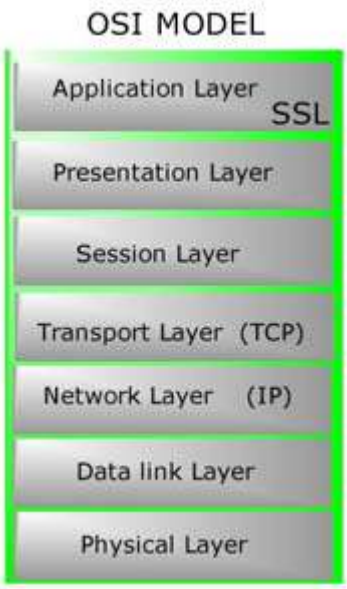
Datensicherheit

Die Verschlüsselung von Daten mittels SSL ist ein Weg zu einem sicheren Datenverkehr. Es gibt dafür zahlreiche, weitere Möglichkeiten,die von den einzelnen Bedürfnissen abhängig sind. Diese reichen von der Client Server Anbindung bis hin zum **VPN-Tunnel.** Fragen Sie uns, wir beraten Sie gern.

SSL-Verschlüsselung

Die Datenübertragung erfolgt im Internet ohne entsprechende Vorkehrungen unverschlüsselt. Damit ist sie für jedermann einseh- und manipulierbar. Je nach Anwendungsgebiet ist dies sehr gefährlich. Mittels der SSL-Verschlüsselung können die Daten sicher und vollständig übertragen und der Web-Server kann eindeutig identifiziert werden

Und wieder kommt das uns bekannte OSI Model zum Einsatz:



SSL (Secure Socket Layer)

Beim Secure Socket Layer (SSL) handelt es sich nicht, wie bei SHTTP, um eine Erweiterung eines existierenden Protokolls, sondern um eine zusätzliche Kommunikationsschicht, die zwischen Transaktionsschicht und Applikationsschicht liegt (siehe Abbildung) und sichere Kommunikation über TCP/IP Netzwerke ermöglichen soll. Die Nutzung von SSL muss allerdings nicht auf TCP/IP Verbindungen beschränkt bleiben. Da es sich bei SSL um eine zusätzliche Schicht zwischen Transportschicht und Applikationsschicht handelt, ist es ebenfalls möglich eine SSL Implementation zu erstellen, die auf einem anderen Netzwerkprotokoll aufsetzt, wie etwa SPX/IPX.

Der Ansatz, der mit SSL verfolgt wird, ist wesentlich flexibler als der von SHTPP, da auch andere Applikationsschicht- Protokolle wie FTP oder telnet die Funktionalitäten der SSL-Schicht nutzen können um eine sichere Kommunikation zu erreichen.

Die Idee, die hinter SSL steht, ist für die Kommunikation zwischen Client und Server einen **sicheren Kanal** bereitzustellen, der den Austausch sensibler Daten über ein unsicheres Netzwerk ermöglicht. Damit ein solchen Ansatz auf breiter Front und vor allem im WWW einsetzbar ist, muss sicher gestellt sein, dass ein sicherer Kanal auch dann zwischen einem Client und Server aufgebaut werden kann, wenn diese zum ersten Mal miteinander kommunizieren. Die Lösung dafür liegt in der Nutzung von Public-Key-Methoden.

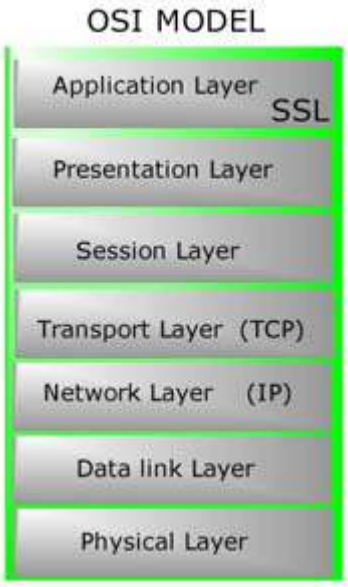
5.11.1 Datensicherheit

Die Verschlüsselung von Daten mittels SSL ist ein Weg zu einem sicheren Datenverkehr. Es gibt dafür zahlreiche, weitere Möglichkeiten,die von den einzelnen Bedürfnissen abhängig sind. Diese reichen von der Client Server Anbindung bis hin zum **VPN-Tunnel.** Fragen Sie uns, wir beraten Sie gern.

5.11.2 SSL-Verschlüsselung

Die Datenübertragung erfolgt im Internet ohne entsprechende Vorkehrungen unverschlüsselt. Damit ist sie für jedermann einseh- und manipulierbar. Je nach Anwendungsgebiet ist dies sehr gefährlich. Mittels der SSL-Verschlüsselung können die Daten sicher und vollständig übertragen und der Web-Server kann eindeutig identifiziert werden

Und wieder kommt das uns bekannte OSI Model zum Einsatz:



5.11.3 SSL (Secure Socket Layer)

Beim Secure Socket Layer (SSL) handelt es sich nicht, wie bei SHTTP, um eine Erweiterung eines existierenden Protokolls, sondern um eine zusätzliche Kommunikationsschicht, die zwischen Transaktionsschicht und Applikationsschicht liegt (siehe Abbildung) und sichere Kommunikation über TCP/IP Netzwerke ermöglichen soll. Die Nutzung von SSL muss allerdings nicht auf TCP/IP Verbindungen beschränkt bleiben. Da es sich bei SSL um eine zusätzliche Schicht zwischen Transportschicht und Applikationsschicht handelt, ist es ebenfalls möglich eine SSL Implementation zu erstellen, die auf einem anderen Netzwerkprotokoll aufsetzt, wie etwa SPX/IPX.

Der Ansatz, der mit SSL verfolgt wird, ist wesentlich flexibler als der von SHTPP, da auch andere Applikationsschicht- Protokolle wie FTP oder telnet die Funktionalitäten der SSL-Schicht nutzen können um eine sichere Kommunikation zu erreichen.

Die Idee, die hinter SSL steht, ist für die Kommunikation zwischen Client und Server einen **sicheren Kanal** bereitzustellen, der den Austausch sensibler Daten über ein unsicheres Netzwerk ermöglicht. Damit ein solchen Ansatz auf breiter Front und vor allem im WWW einsetzbar ist, muss sicher gestellt sein, dass ein sicherer Kanal auch dann zwischen einem Client und Server aufgebaut werden kann, wenn diese zum ersten Mal miteinander kommunizieren. Die Lösung dafür liegt in der Nutzung von Public- Key-Methoden.

6 Systems Security

Systems Security beinhaltet primär folgende Themen:

- **Intrusion Detection und Intrusion Prevention**
- **Betriebssystemsicherheit**
- **Schwachstellen-Analyse und -Management.**

6.1 Betriebssystemsicherheit

Die Härtung von Betriebssystemen umfasst die Neukonfiguration von Systemen zur Erhöhung der Sicherheit, über das bei der Installation des Betriebssystems und/oder der fertigen Anwendung angebotene Maß hinaus. Weitere Beispiele: SMTP ist auf Webservern nicht erforderlich, ebenso wenig wie Rlogin auf den meisten Unix-Systemen. Diese Service sollten deshalb abgeschaltet werden.

Unsere Berater können bei den meisten der heute führenden kommerziell erhältlichen Betriebssystemen eine Vor-Ort-Härtung durchführen.

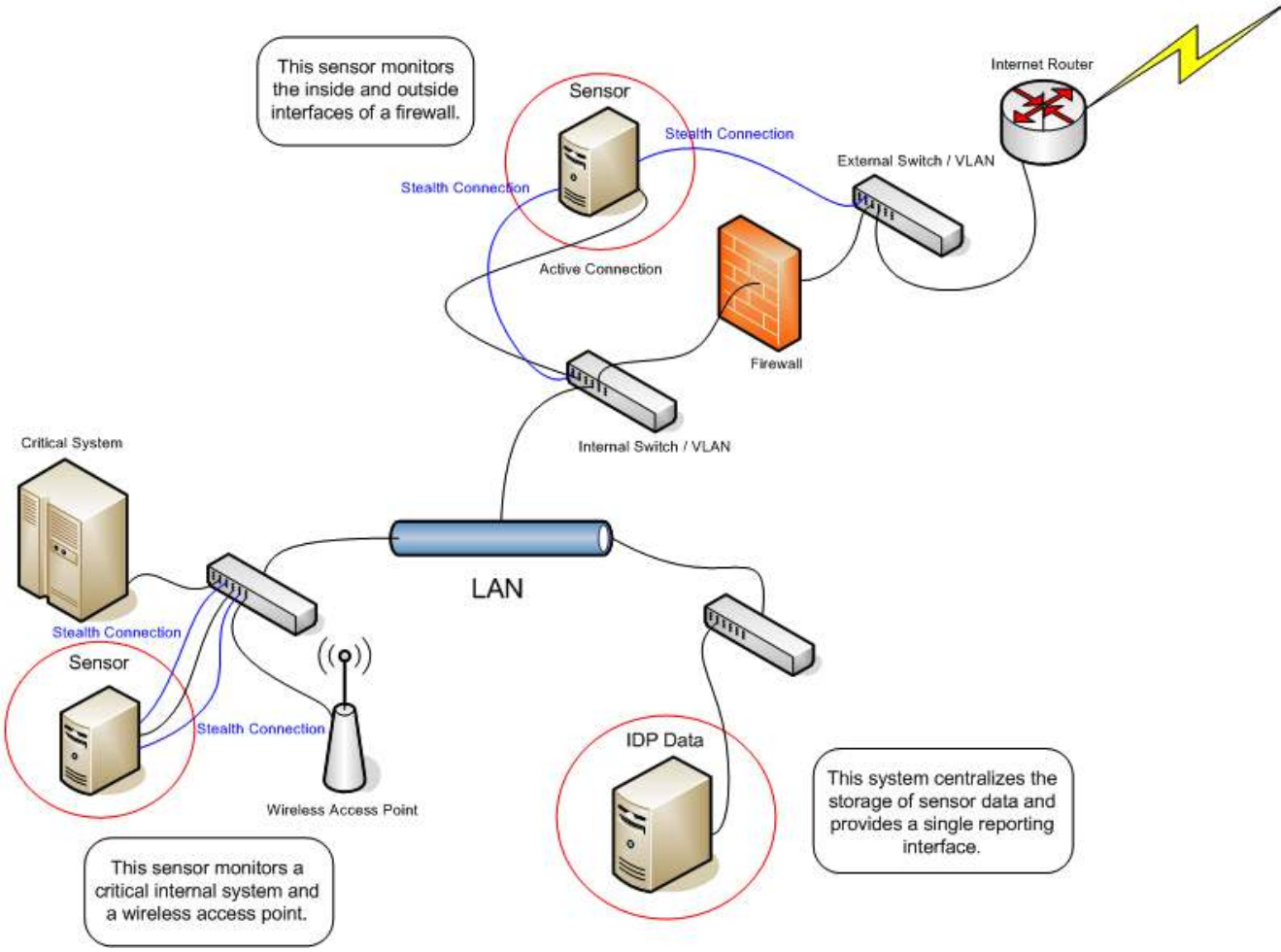
6.2 Intrusion Detection

Intrusion Detection-Systeme (IDS) sind ein weiteres Tool, mit dem Sicherheitsadministratoren ihre Ausstattung für die Netzwerkabsicherung verstärken können. Die heutigen IDS lassen sich in zwei grundsätzliche Kategorien einteilen: Erstens die passiven Systeme, die lediglich den Datenverkehr, der über sie geleitet wird, überwachen und anhand von Richtlinien und Regeln alle verdächtigen Daten erfassen und protokollieren. Diese können dann vom Sicherheitsteam analysiert werden, entweder als Sicherheitsrisiko erkannt oder freigegeben werden.

Die zweite Kategorien von Intrusion Detection-Systemen sind aktive Strukturen, die nicht nur Vorgänge erfassen und protokollieren, sondern auch versuchen, potenzielle Bedrohungen und Angriffe seitens der Eindringlinge abzuwehren. Diese Systeme werden mittlerweile allgemein entweder als IPS (Intrusion Prevention Systems) oder als IDP (Intrusion Detection and Prevention) bezeichnet.

Sowohl die IDS als auch die IDP wenden ähnliche Verfahren an, um voraussichtliche Angreifer oder Gefahren im Netzwerk aufzuspüren. Grundlage der meisten Systeme bildet dabei eine Datenbank mit Signaturen, die bei der Entdeckung neuer Bedrohungen aktualisiert wird.

Intrusion Detection and Prevention – Multiple Sensor Implementatio



Herkömmliche Firewalls filtern den Datenverkehr, aber sie analysieren bekanntlich nicht den Inhalt eines Datenpakets. Sie können nicht feststellen, ob die Nutzlast destruktive Code-Elemente enthält oder nicht. Das können nur IDS-Systeme. Beide Systeme und Mechanismen sind also komplementär und die Firewall-Regelbasis kann sogar bei der Planung der Filter und Festlegung der Sicherheitsrichtlinien für die Sensoren innerhalb des IDS gute Dienste leisten. Seit Einführung des ersten IDS in den 80er-Jahren ist der Markt erheblich gewachsen.

Netzwerk und Host basierte IDS

Traditionell gibt es zwei grundlegende Typen von Intrusion Detection Systemen: Netzwerk basierte Intrusion Detection Systeme und Host basierte Intrusion Detection Systeme mit Agenten oder Sensoren im ganzen Netzwerk, die von einer Zentralkonsole aus verwaltet werden.

Ein Netzwerk IDS bietet vor allem Schutz gegen externe Bedrohungen. Ein Host IDS untersucht die Log-Files und Dateien auf dem Ziel- Server und konzentriert sich somit auf die Aktionen der Anwender, mögen diese nun authentifiziert sein oder nicht.

Ein Netzwerk IDS beobachtet den gesamten Netzwerkverkehr auf einem Segment. Man benötigt dazu Hardware – typischerweise ein dediziertes Windows NT System mit zwei Netzwerkkarten. Die zweite Netzwerkkarte ist mit dem VLAN Management verbunden. Das Netzwerk IDS überprüft jedes Paket und vergleicht den Inhalt mit bekannten Angriffs- Signaturen auf der Basis von Mustern, Sequenzen und Protokollen. Sobald ein Netzwerk IDS eine verdächtige Signatur identifiziert, löst es unverzüglich Alarm aus. Wenn ein solches System korrekt implementiert ist, kann es wirksam gegen netzwerkbasierte Denial-of-Service Attacken, gegen Port-Scans, die Nutzung von Hintertür- Programmen (wie zum Beispiel Back Office), gegen DNS- und ICMP-Angriffe, um nur ein paar Möglichkeiten zu nennen, eingesetzt werden.

Neben Netzwerk IDS gibt es auch noch so genannte Hybrid IDS. Im Gegensatz zu Netzwerk IDS werden Hybrid IDS direkt auf einem individuellen Zielsystem installiert. Ein Hybrid IDS analysiert dann den gesamten Datenverkehr von und zu diesem Gerät. Hybrid IDS haben zum Beispiel in geswitchten Umgebungen deutliche Vorteile gegenüber Netzwerk IDS. In geswitchten Umgebungen wäre nämlich bei einem Netzwerk IDS ein entsprechendes Sensorelement auf jedem einzelnen Segment erforderlich.

Mittlerweile gibt es auch Sensoren, die beispielsweise Host IDS mit Hybrid IDS zusammenbringen. Auch stack-orientierte IDS-Sensoren, also solche, die eng mit dem TCP/IP-Protokollstack zusammenwirken, sind im Kommen. Mit solchen Sensoren können Pakete über sämtliche Schichten des OSI-Modells hindurch analysiert werden. Auf diese Weise kann das IDS selbst Pakete aus dem Stack entfernen, bevor das Betriebssystem oder die Anwendung die destruktive Sequenz verarbeiten und dadurch ein Sicherheitsproblem produzieren. Stack-basierte IDS können auch gegenüber einigen Formen der Verschlüsselung sehr effizient sein. Dies ergibt sich aus dem engen Zusammenspiel von TCP/IP-Stack und IDS. Der TCP/IP Stack entschlüsselt ein destruktives Paket, danach erkennt dann das stack- basierte IDS die Schadsoftware und schlägt Alarm.

6.3 Application-Layer IDS

Application-Layer IDS Lösungen sind jetzt speziell für Web-Anwendungen erhältlich. Diese Software-Lösungen sitzen typischerweise auf dedizierten Systemen und schützen die Webserver gegen jede Art von Manipulation aus Richtung der Online-Anwendung, zum Beispiel den Versuch, einen Buffer- Overflow auf dem Server zu erzeugen, auf dessen Basis dann die Kontrolle über den Server erschlichen werden kann.

Für den Angreifer wird durch die IDS-Technologie verhindert, dass in großem Maße bereits veröffentlichte Sicherheitsrisiken ausgenutzt werden können. Beim Entdecken eines Angriffs blockiert das Application-Layer IDS die Aktion und loggt sie gleichzeitig. Das IDS kann einen Alarm auslösen und eine Warnung ausgeben, das Netz ggf. unterbrechen damit der Angriff entdeckt und protokolliert wird.

6.4 Intrusion Prevention

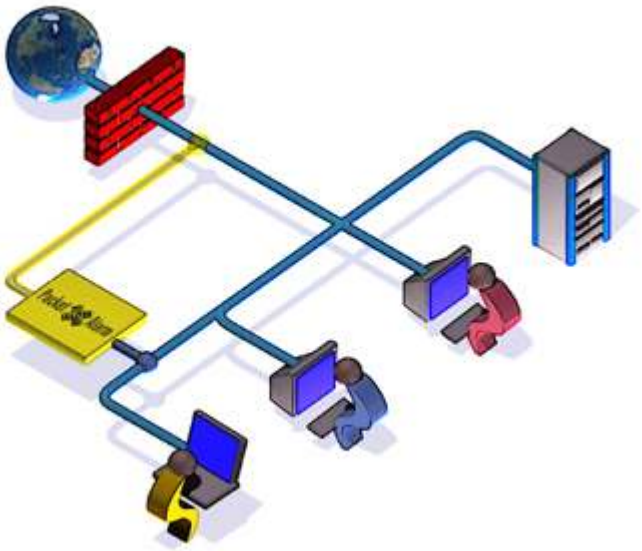
Immer mehr Security-Hersteller sprechen über Intrusion Prevention anstatt Intrusion Unter den Produkten gibt es Lösungen von Herstellern wie Internet Security Systems, Top Layer Networks und Sanctum, die in diesem Security-Sektor technisch führend sind.

Da bei diesem Funktionsprinzip gefährliche Inhalte für jeden Request einzeln betrachtet werden, kann es nicht zu Denial-of- Service-Angriffen wie bei klassischen IDS- bzw. IPS-Lösungen kommen. Bei korrekter Konfiguration sind Blockaden von unschuldigen Anwendern nahezu ausgeschlossen.

Eine ganze Reihe von Services können zur Unterstützung hinsichtlich Dimensionierung, Design, Implementierung und Feinabstimmung von IDS-Lösungen angeboten werden

Ein völlig anderer Bereich der Intrusion Prevention Welt sind die hostbasierten Systeme. Sie laufen als Agenten auf allen zu sichernden Servern und Desktops und kontrollieren dort möglichst im Betriebssystemkern alle Ressourcen-Zugriffe der Applikationen. Bösartige Zugriffe wie beispielsweise ein schreibender Zugriff auf System- Bibliotheken oder Registry- Einträge, können direkt verhindert werden.

Sniffing Mode



Im Sniffing Modus lauscht Packet Alarm am Netzwerk und liest alle vorbeifließenden Daten mit. Alle Attacken werden aufgezeichnet und können alarmiert werden. Wird das Prevention System aktiviert, werden Angriffe mittels TCP Reset oder einem Firewall-Hardening verhindert. Um auch ein Firewall-Hardening mit den Systemen anderer Hersteller oder mit selbstentwickelten Systemen zu ermöglichen, wird über eine spezielle Schnittstellen Definition, der Open PacketAlarm Architecture (OPA), kommuniziert.

6.5 Schachstellen-Analyse und -Management

Angreifer nutzen bekannte Sicherheitslücken in Betriebssystemen und Anwendungen aus. Sobald ein Angriff in Gang gesetzt ist, können Intrusion Detection Systeme (IDS) diesen Angriff entdecken und sogar verhindern. Die andere Aufgabe von IDS ist das Schließen von Sicherheitslücken und Schwachstellen, bevor sie von kriminellen Angreifern innerhalb oder außerhalb des Unternehmens ausgenutzt werden können. Es klingt vielleicht trivial, aber in Wirklichkeit müssen Unternehmen, die einen strukturierten und praxiserprobten Ansatz zur Schwachstellenbeurteilung entwickeln möchten, einiges an „Gehirnschmalz“ aufwenden.

Nach den Zahlen des Computer Emergency Response Team (CERT) der Carnegie Mellon University beläuft sich die Zahl der im Jahr 2002 entdeckten neuen Schwachstellen auf insgesamt 4129 – das entspricht knapp 80 neuen Sicherheitslücken pro Woche.

Das wichtigste Hierbei ist der Mensch, dessen Sicherheitsrisiko nicht vernachlässigt werden darf. Denn Irren ist menschlich und wer hat nicht schon einmal einen Fehler gemacht.

Jährliche Audits können kaum verhindern, dass allgemein bekannte Schwachstellen als Einfalltor für Angriffe genutzt werden. Das dürfte für die meisten Unternehmen ein nicht zu akzeptierendes Risiko darstellen.

Die Anfälligkeit gegenüber möglichen Schwachstellen wird also umso kleiner, je häufiger Scans durchgeführt werden. Falls die zu scannenden Systeme Teil einer unternehmenskritischen Web- Infrastruktur sind, die entscheidend zum Umsatz beiträgt, ist eine fortlaufende Evaluation mit täglich durchgeführten Scans vermutlich die einzige akzeptable Option.

Die Installation von fünf Patches an jedem Arbeitstag auf 17 Servern erfordert schon fast eine eigens dafür bereitstehende Ressource. Mit angenommenen 1700 Servern ist ein derartiges Vorgehen praktisch unmöglich. Eine Schwachstellen- Analyse kann aber zumindest eine Prioritätenliste derjenigen Patches zu erstellen suchen, die aus der Perspektive der Sicherheit besonders wichtig sind.

Das Durchführen der erforderlichen Sicherheits-Scans im Unternehmen erfordert also Zeit und Ressourcen. Mit ziemlicher Sicherheit müssen mehrere einschlägige Tools eingesetzt werden.

Automatisierte Services werden typischerweise über das Web durchgeführt. Hierbei werden Systeme mit Verbindung nach außen, die über das Internet sichtbar sind, gescannt. Das Scannen wird in einem solchen Fall blind oder zumindest fast blind hinsichtlich bestimmter Ziele durchgeführt. Die meisten automatisierten Scanning- Services sind für das Scannen einer kleinen Zahl von IP- Adressen ausgelegt. Schwachstellenanalysen sind im Großen und Ganzen auf die Netzwerk- und die Betriebssystem-Layer beschränkt. Zur Bewertung aller Layer der Kommunikations-Architektur sind vermutlich auch unternehmenseigene Spezialisten notwendig, welche die Ergebnisse bewerten können. FoundScan von Foundstone ist übrigens einer der ausgeklügelsten Services, die auf dem Markt erhältlich sind. Eine wachsende Anzahl von Firmen bietet manuelle Analysen an. Da diese mit hochspezialisierten Beratern durchgeführt werden, welche die einzelnen Systeme sehr detailliert kennen, liefern deren Berichte meist eine Flut von Details. Bei manuellen Analysen können die Prüfmethoden als Reaktion auf Output von einzelnen Werkzeugen und Programmen bei laufendem Betrieb modifiziert werden. Jedes Output-Element wird sozusagen von Hand angefasst und unterliegt der Analyse und Interpretation durch Menschen. Derartige Services werden entweder aus der Ferne („remote“) oder vor Ort erbracht. Letzteres hat den Vorteil, dass ein Blick auf die internen Systeme geworfen werden kann. Vermutlich sind auch Vor-Ort-Inspektionen einiger Systeme notwendig, bei denen Fehlkonfigurationen behoben und Programmfehler beseitigt werden müssen. Bei einigen Analyse-Produkten und Services erhalten die Verantwortlichen im Unternehmen auch zusätzlich Hilfestellung in Form von Informationen zur Durchführung der Fehleinstellungen und zur Fehlerbeseitigung. Desgleichen wird eine Erfolgskontrolle der durchgeführten Aktionen durchgeführt. Einige Services bieten auch Alarmmeldungen über E-Mail an, wenn bei der Fehlerbehebung auf einmal neue Schwachstellen auftritt. Wir bieten ein vollständiges Sortiment an Produkten und Dienstleistungen im Bereich Schwachstellenanalyse und - management an. Es stehen sowohl automatisierte als auch manuelle Service zur Verfügung.

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de