

Die vorangegangenen Vorträge haben die Bedrohungsmöglichkeiten und deren Darstellung in Tabellen/Checklisten vorgestellt.

Neben den theoretischen Ansätzen soll man auch mitteilen, wie die entwickelte Bedrohungsanalyse für ein Unternehmen in der Praxis umgesetzt werden könnte.

Deshalb das nachfolgende Thema:

Maßnahmen in der Praxis

- Virusscanner, Firewall, VPN, Verschlüsselung –

Zunächst muss man sich immer ins Bewusstsein rufen, dass Datenverlust genauso wahrscheinlich ist wie deren Erhalt..

Bereits Aristoteles sagte: „Das Unwahrscheinliche ist wahrscheinlich“ oder moderner ausgedrückt: „Murphy’s Law: If anything can go wrong – it will“

Hieraus sieht man bereits, dass es nicht einfach damit getan ist, dass man eine Firewall einsetzt und einen Virusscanner laufen lässt.

Der richtige Ansatz ist, dass Datensensibilität entwickelt und hieraus für sein Unternehmen organisatorische und technische Maßnahmen ergreift, um dem gewünschten Ziel der Datensicherheit und Zugriffssicherung immer näher kommt.

Um die technische Umsetzung zu erläutern, wird nachfolgendes Szenario vorgestellt.

A. Szenario

1. Firma A hat 15 Mitarbeiter im Betrieb,
Fileserver, Email-Server, Ethernet LAN, und Internetzugang
Es gibt zwei Gruppen mit höheren Sicherheitsanforderungen:
Geschäftsleitung und Technik/Entwicklungsabteilung
Die dritte Gruppe stellt den Vertrieb dar.
2. Firma A hat 2 Mitarbeiter, die zumeist im Home Office arbeiten
3. Firma A hat eine Partnerfirma B mit
 - Allgemeiner Korrespondenz
 - Arbeiten an gemeinsamen Angeboten
 - Austausch von sensiblen Daten
4. Firma arbeitet mit zwei weiteren Firmen C und D sporadisch zusammen, wobei per eMail vertrauliche Daten (z.B. Angebot, technische Zusammenarbeit in einem Projekt) ausgetauscht werden sollen.

B. Einführen von Sicherheitsmaßnahmen in Stufen

Bei einem Datensicherungs- bzw. Schutzkonzept steht natürlich die Datensicherung im Vordergrund. Hierzu gibt es viele verschiedene Storage Management Möglichkeiten, die in hier nicht weiter erläutern möchten.

Als zweites ist die Firmenstruktur für die umzusetzenden Sicherheitsmaßnahmen notwendig. Diese ist aber bereits durch den Netzaufbau abgebildet. Hier werden im Netz für die einzelnen Benutzer entsprechende Rechte vergeben. Im Allgemeinen muss sich ein Nutzer durch seinen Benutzernamen und Passwort im Netz ausweisen.

Weiterhin sind organisatorische Maßnahmen beim Umgang mit den Firmendaten, sei es firmenintern bzw. bei der Kommunikation mit anderen Unternehmen als dritter nichttechnische Aspekt zu nennen.

Bei der technischen Umsetzung des IT-Schutzmaßnahmen beginnt man mit einem Virenschutzprogramm.

1. Virenschutzprogramme

Ein solches Programm wird über den Server auf die im Netz befindlichen PCs gespielt und automatisch laufend aktualisiert (Up-Date Wartungsvertrag).

Beim Starten der PCs werden die gespeicherten Dateien auf den lokalen Datenträgern gescannt. Das Virenschutzprogramm dann im Hintergrund weiter und überwacht die Arbeiten mit Applikationsprogrammen,

Da die Virenschutzprogramme verschiedener Hersteller, wie z.B. von Norman, Trend Micro und McAfee, unterschiedliches leisten, sollte man nicht nur eine solches Produkt im Firmennetzwerk einsetzen.

So erkennt ein Produkt eher Trojaner oder Würmer mit absoluter Zuverlässigkeit, hat aber vielleicht Probleme bei der Erkennung von Skriptviren. Ein anderer Hersteller ist spezialisiert in solchen Scriptviren.

Einen optimalen Virenschutz kann es daher nur dann geben, wenn gleichzeitig die Produkte unterschiedlicher Hersteller genutzt werden. Die Mehrkosten für die Anschaffung und Pflege mehrerer Virenschutzprogramme werden durch die höhere Sicherheit mehr als nur ausgeglichen.

Die Performance von einem Virenschutzprogramm im Hintergrund wird nur gering beeinflusst. Werden jedoch mehrere solcher Programm gleichzeitig auf einem PC eingesetzt, kann sich die Performance schon merklich reduzieren.

So empfiehlt es sich, das zweite Virenschutzprogramm auf der Firewall mitlaufen zu lassen: So werden die aus dem Internet ankommenden Daten aber auch der interne Datenfluss überwacht.

2. Firewall

Neben den Virenschutzprogrammen sind Firewalls eine bekannte Sicherheitsgrundmaßnahme. Es gibt viele Firewall-Anbieter, wie Checkpoint, Astaro, Gateprotect usw..

Die Aufgaben einer Firewall sind vornehmlich Berechtigungen und Dienste zwischen den einzelnen Rechnern festzulegen. Weiterhin läuft wie vorher erläutert ein Virusschutzprogramm, der den laufenden Verkehr überwacht. Ganz wichtig ist der Einsatz eines IDS (Intrusion Detection System), der die Zugriffsberechtigung der einzelnen Ports überwacht. Dies ist zumindest der erste Grundschutz gegen den Hacker aus dem Internet. Zusätzlich kann auf einer Firewall auch die VPN-Software laufen, was dann später gezeigt wird.

Am Produktbeispiel von Gateprotect werden wir das oben angegebene Szenario umsetzen, da hier aufgrund der graphischen Oberfläche, der Aufbau und die einzelnen Berechtigungen einfach dargestellt werden können.

Zunächst ist die Firewall ein Rechner auf Linux Basis. Linux wird vornehmlich gewählt, da das Betriebssystem überprüfbar bleibt und stabil läuft.

Für unser Beispiel werden 6 Ethernetkarten verwendet, um somit die drei Gruppen untereinander zu trennen und die vierte Ethernetkarte ist für den Internet-Zugang z.B. über DSL vorgesehen. Fileserver-Anbindung und eMail-Server erhalten jeweils eine separate Ethernet-Anbindung zum Firewall. Dadurch können alle Kommunikationswege zwischen den Gruppen überprüft und unterschiedliche Berechtigungen vergeben werden.

Die Firewall wird von einem im Netz befindlichen Rechner programmiert.

ANFANG → Umschalten auf die Oberfläche des Firewalls, wo bereits das Szenario vorbereitet wurde.

a. Rechnergruppen

Die drei Gruppen Vertrieb, Technik und Geschäftsleitung sind bereits eingetragen. Weiterhin ist der Fileserver im inneren Netz

Festlegen von Fileserver und eMailserver

b. Regeleditor

Die Verbindungen (Knoten) entsprechen technisch gesehen dem Firewall, wo die einzelnen Verbindungsrechte zwischen den Rechner(-gruppen), dem Mailserver, dem Fileserver und dem Internet hinterlegt sind.

Anbindung des Mailservers als DMZ (DeMilitarized Zone, Trennung zum lokalen Netz) zum Internet. – über Regeleditor/Zusätzliche Optionen

c. Aktive Dienste

Über diese optische Darstellung kann man übersichtlich sehen, welche Gruppe bzw. Rechner welche Dienste frei geschaltet bekommen hat.

d. Erweitern des Netzes: Rechner hinzufügen, Suchfunktion, Verbindungslinie

Es wird gezeigt, wie man einen neuen Rechner als Einzel bzw. einer Gruppe zuordnet.

e. Statistik – abgewiesene Zugriffe

Über die Statistik kann nachgewiesen werden, wie sinnvoll diese Firewall im Einsatz ist. Die unberechtigten Zugriffe werden hier zahlenmäßig und Graphisch für den vorgegebenen Zeitraum dargestellt.

f. Statistik – Top-Listen im WWW

Über die Statistik lässt sich das Gruppen- aber auch das Einzelverhältn im Netz ablesen.

g. Statistik – Traffic

Es kann der Verkehr über die Firewall für die einzelnen Dienste: Internet, Email und Windows-Daten für einen ausgesuchten Zeitraum einzeln angezeigt werden.

ENDE→ Umschalten auf die Oberfläche des Firewalls, wo bereits das Szenario vorbereitet wurde.

3. VPN – VPN-Client

Mit zum Unternehmen gehören noch die beiden Mitarbeiter, die zumeist vom Home Office aus mit der Firma kommunizieren möchten. Dies könnte über eine gesicherte Standleitung erfolgen. Aber auch eine Dial-In-Telefonverbindung ist denkbar und relativ sicher. Solche exklusive Datenverbindungen sind jedoch zu kostenintensiv

Mit dem Internet ergibt sich die preiswerte Lösung mit der Firma zu kommunizieren. Aber da das Internet öffentlich ist, können Daten, die im Klartext darüber gesendet werden, von jedem gelesen werden können oder sogar manipuliert werden.

Mit einem VPN (Virtual Private Network) wird es jedoch möglich, auch im öffentlichen Internet eine ähnlich hohe Sicherheit wie in einem geschützten privaten Netz zu erreichen.

Über ein kryptographisches Verfahren wird erreicht, dass die Daten, die über das Internet gehen für Mitläuscher aufgrund der Verschlüsselung nicht direkt nutzbar sind. Dieses Verfahren nennt man Tunneling und bedeutet so viel, dass im Internet zwischen den beiden am Datenaustausch beteiligten Punkten ein virtueller Tunnel erzeugt wird, durch den die Informationen übertragen werden. Hierdurch wird wieder eine exklusive (hier jedoch virtuell) Verbindung geschaffen.

Die beiden wichtigsten VPN-Varianten sind:
Point-to-Point-Tunneling Protocol (PPTP) und
IPsec (IP Security), der auf dem Internet-Standardprotokoll IP aufsetzt.

Beide Verfahren verwenden eine Authentifizierung (Passwort beim PPTP und Public-Key-Verfahren bei IPsec) und eine Verschlüsselung (Symmetrische Verschlüsselung, wie 3DES, Blowfish usw.) für die eigentlichen Daten.

a. PPTP

dieses von Microsoft entwickelte Verfahren ist relative einfach zu installieren und werden auch auf älteren Windows-Betriebssystemen direkt unterstützt.

Beide Seiten haben Kenntnis vom gemeinsamen Passwort, welches ausreichend lang und kompliziert sein sollte. Bei jedem neuen Verbindungsaufbau wird von der Software ein neuer symmetrischer Schlüssel erzeugt, dieser wird dann mit dem Passwort nach dem gewählten Verfahren z.B. 3DES verschlüsselt und über das Internet zum Gegenüber geschickt. Somit lernt das Zielsystem den Schlüssel kennen und kann die ankommenden verschlüsselten Daten entschlüsseln.

Wenn jemand diese Schlüsselübersendung abfängt und den Schlüssel daraus entschlüsseln kann, ist er in der Lage bei dieser Verbindung die verschlüsselten Daten zu lesen. D.h. längere Verbindungszeiten von ca. 2 Stunden könnten zur Möglichkeit führen, das ein Angreifer die Informationen mitlesen könnte.

So gibt es ein noch sichereres Verfahren.

b. IPsec

Bei IPsec wird während der Verbindung nach einer gewissen Zeit der symmetrische Schlüssel getauscht. Der Schlüsselaustausch erfolgt über das Public-Key-Verfahren, wobei zuvor der öffentliche Schlüssel des Gegenüber ausgetauscht werden musste, z.B. per Diskette oder Email. Der geheime Schlüssel befindet sich am besten auf einem Token, der dort durch ein Passwort geschützt ist

In unserem vorliegenden Anwendungsfall erhalten die beiden „Heimarbeiter“ jeweils eine Software VPN-Client. Z.B. gibt es ein gutes Produkt von Safenet, wenn mit dem IPsec-Verfahren gearbeitet werden sollte. Ansonsten ist zumeist die PPTP-Software im Windowspaket enthalten.

Auf der Seite der Firma könnte man sich vorstellen, dass die Tunnelung am einzelnen PC eingerichtet wird, In unserem Beispiel kann die Technikergruppe über PPTP direkt mit dem Heimarbeitern kommunizieren.

Man kann aber auch, insbesondere, wenn man IPsec nutzt, ein VPN im Firewall aufsetzen.

Unsere vorliegende Software kann hier die entsprechenden VPNs definieren und die Verbindungsberechtigung festlegen.

ANFANG → Umschalten auf die Oberfläche des Firewalls, wo bereits das Szenario vorbereitet wurde.

Aufzeigen der Eigenschaften der VPN-Rechner, Eigenschaften der Verbindung und Eintrag des Passwortes in das Profil. Hierbei wurde eine netzinterne virtuelle IP-Adresse eingetragen, da der von außen kommende VPN-Client bei jedem Verbindungsaufbau durch den Provider eine neue IP-Adresse erhält, diese wird dann dynamisch im Firewall mit diesem Nutzer hinterlegt.

Die vorliegende Verbindung ist eine Server-Client-Verbindung.

Eine Verbindung mit der Firma B sollte dann über eine Server-Server Verbindung erfolgen. Entsprechende Konfigurationsmöglichkeiten liegen in diesem System ebenfalls vor. Hier ist auf jeden Fall das IPSec Protokoll einzusetzen. Die öffentlichen Schlüssel müssen als Dateien entsprechend getauscht und zugeordnet werden.

ENDE → Umschalten auf die Oberfläche des Firewalls, wo bereits das Szenario vorbereitet wurde.

Anmerkung: Z.B. macht es Sinn, dass der Heimarbeiter sich über das Firmennetzwerk und damit über die Firewall in das Internet einwählt und nutzt somit die Sicherheitsstufe des Firmennetzes.

Anmerkung: Bei WLAN empfiehlt es sich jeweils die Rechner mit VPN-Client Software auszustatten, damit die Luftschnittstelle abgesichert wird. Die derzeitige Sicherheitstechnik WEP (Wired Equivalent Privacy) ist derzeit noch unbefriedigend.

4. Verschlüsselung – Email-Kommunikation

Für die Kommunikation mit den Mitarbeitern der Firma C bzw. D bietet sich die authentische Verschlüsselung der Nachrichten an.

Es gibt das bekannte öffentlich erhältliche Verfahren PGP (Pretty good privacy) oder z.B. das Produkt von Utimaco mit Safeguard. Hierbei werden die Informationen als Anhänge definiert und als gezippte und verschlüsselte Anwendungsdatei versandt. Der Empfänger kann dann diese Nachricht mit dem zuvor vereinbarten bzw. z.B. telefonisch übermittelten Passwort entschlüsseln.

5. Verschlüsselung – Gruppenverschlüsselung auf dem Fileserver

Um Daten von Missbrauch zu schützen oder auch wenn Datenträger (z.B. ein kompletter Laptop) gestohlen werden, sollten die dort gespeicherten Daten verschlüsselt abgelegt werden.

Für die Lokale Anwendung gibt es einerseits eine komplette Verschlüsselung der Festplatte, deren Daten nur in Verbindung mit dem symmetrischen Schlüssel, der Passwort geschützt in einem Token abgespeichert ist, aber auch die Möglichkeit nur Bereiche mit sensiblen Daten verschlüsselt auf der Festplatte bzw. Diskette/USB-Stick abzulegen (Dateiverschlüsselung – FileCrypt).

Im Netz befinden sich auf dem File-Server im Allgemeinen auch sensible Daten, wie Geschäftsberichte, Buchhaltung oder Entwicklungspläne. Diese Daten sind im Klartext abgelegt und können zumindest von den Administratoren gelesen werden.

Hier gibt es die Möglichkeit einer Gruppenverschlüsselung (NetCrypt von Telecrypt) Hierbei wird z.B. von einem NT-Server die Gruppenstruktur mit Benutzernamen übernommen oder es müssen die Gruppenmitglieder, die bei der Gruppenverschlüsselung teilnehmen möchten, manuell eingegeben werden.

Auf dem Netzwerk werden auf dem File-Server die für die automatische Verschlüsselung der Daten vorgesehene Bereiche vom Administrator festgelegt.

Aus jeder Gruppe wird ein Gruppenleiter definiert, der dann seinen Gruppenmitarbeitern eine Zugriffsberechtigung vergeben bzw. verweigern kann. Zuerst muss der Gruppenleiter die Software das erste Mal starten. Daraufhin wird zunächst automatisch ein unsymmetrisches Schlüsselpaar nach dem RSA-Verfahren (oder AES) erzeugt. Der geheime (oder private) Schlüssel wird dann über ein Passwort verschlüsselt entweder auf der Festplatte des PCs oder auf einem Token abgelegt.

Anschließend wird dann automatisch ein symmetrischer Schlüssel z.B. nach dem 3DES-Verfahren erzeugt, der dann mit dem öffentlichen Schlüssel des Gruppenleiters verschlüsselt auf dem File-Server abgelegt wird. Der öffentliche Schlüssel des Gruppenleiters befindet sich dann ebenfalls auf dem File-Server.

Öffnet nun ein Gruppenmitglied die zugehörige Software, wird auch hier ein asymmetrisches Schlüsselpaar erzeugt und entsprechend abgelegt. Gleichzeitig wird eine Schlüsselanforderung zusammen mit dem eigenen öffentlichen Schlüssel an den Gruppenleiter geschickt.

Gibt der Gruppenleiter für dieses Gruppenmitglied die Berechtigung frei, wird hierzu der symmetrische Schlüssel mit dem eigenen geheimen Schlüssel entschlüsselt, um dann diesen mit dem geheimen Schlüssel des Gruppenleiters zu verschlüsseln (Authentifizierung) und zusätzlich mit dem öffentlichen Schlüssel des Gruppenmitglieds zu verschlüsseln. Damit kann dann nur das neue Gruppenmitglied diesen Schlüssel entschlüsseln und er weiß auch, dass dieser Schlüssel vom Gruppenleiter geschickt wurde.

Dieser gleiche symmetrische Schlüssel wird dann mit dem öffentlichen Schlüssel des neuen Gruppenmitgliedes verschlüsselt auf dem File-Server abgelegt.

Werden nun Daten bearbeitet, die in das hierfür vorgesehen Verzeichnis abgelegt werden sollen, tritt automatisch die Verschlüsselung ein. Ein Nebeneffekt ist, dass wenn ein Gruppenmitglied sein Passwort vergessen sollte, kann der Gruppenleiter ihn sozusagen zurücksetzen und er muss sich in der Gruppe wieder neu anmelden, um dann Zugriff auf die Daten der Gruppe zu haben.

So können mehrere Gruppen angelegt werden, die jeweils ihre sensiblen Daten verschlüsselt ablegen. Dies erhöht die Sicherheit gegenüber Datenmissbrauch innerhalb eines Unternehmens aber auch gegen Angriffe von außen, wenn ein Hacker durch die Firewall auf den File-Server gelangt ist.

6. Passwort / Biometrische Erkennung

Im obigen dargestellten Verfahren haben wir gesehen, wie eine Schlüsselverteilung (PKI – Public Key Infrastructure) aussehen könnte. Ein Schwachpunkt in diesem System ist eigentlich das Passwort selbst. Es ist zumeist endlich lang, damit man man sich einfacher merken kann. Aber dies erleichtert das Ausspähen des Passwortes mit geeigneten Programmen. Auch die Unsitte Passwörter z.B. unter die Schreibunterlege zu legen ist dem Authentisierungsgedanken nicht besonders förderlich. Auch werden manchmal Kollegen das Passwort durchgegeben, damit dieser einmal irgend etwas auf seinem Rechner nachsehen kann.

Um eine echte Authentifizierung zu erreichen, können nur biometrische Merkmale zum Einsatz kommen. Es gibt verschiedene Verfahren, wie Gesichtserkennung (Biodata), Iriserkennung oder Fingerprint z.B. Startek.

Es gibt bereits kleine USB-anbindbare Fingerprint Einrichtungen in der Größe von einer Maus oder manche sind in der Tastatur integriert.

Der Fingerprint kann das Passwort ersetzen. Hierzu muss zunächst der Fingerprint als ein Minutiae-File erzeugt werden. Im Minutiae-File werden verschiedene Merkmale – geometrische Orte von Inseln bzw. Verzweigungen der Papillaren codiert abgelegt. Das Fingerprintfile kann entweder auf der Festplatte oder einem Token abgelegt werden. Falls bereits mit dem Public-Key-Verfahren gearbeitet wird, bietet sich der Token vornehmlich an.

Das Einloggen in das System erfolgt nun nach Eingabe des Benutzernamens mit der Aufforderung zum Einscannen des Fingers. Dieser Lifescan wird dann mit dem abgelegten Minutiae-File verglichen und bei Übereinstimmung wird der Zugriff auf das Netz freigegeben werden.

Mit Einführen einer biometrischen Erkennung, wäre dann das Optimum für ein Daten geschütztes Unternehmen gegeben. Zum Abschluss seien erwähnt

7. Digitale Signatur und Trustcenter

Die Digitale Signatur arbeitet ebenfalls mit dem Public Key Verfahren, hierbei werden eMail-versandte Dokumente einmal authentisch mit dem eigenen geheimen Schlüssel verschlüsselt. Hierbei wird nicht unbedingt das Dokument verschlüsselt, sondern nur der Hash auf den Inhalt des Dokumentes. Über diese Hash-Funktion kann festgestellt werden, ob das Dokument verändert wurde. Wird das Dokument selbst verschlüsselt (symmetrische Verschlüsselung), kann dann mit dem öffentlichen Schlüssel des Partners das Dokument nur für den Empfänger zugänglich gemacht werden (Übertragung des symmetrischen Schlüssels).

Ein Trustcenter wird zwischen fremde Unternehmen genutzt, da hier die öffentlichen Schlüssel zentral verwaltet werden. Weiterhin werden dort Zeitstempel vergeben.

Die Digitale Signatur hat sich bis heute kaum durchgesetzt. Zwar ist es bei der digitalen Signatur nicht erforderlich, dass man sich ausschließlich über ein biometrisches Merkmal authentifiziert, aber sicherlich ist dies das Hauptmanko an der derzeitigen Praxis. -- Ende --