Sicherheit im Heimnetzwerk

Beitrag von Vimes

Nachdem MobyDuck ein Sicherheitskonzept für den Einzelarbeitsplatz vorgestellt hat, geht es heute um das Heimnetzwerk.

Prinzipiell gilt hier das für den Einzelarbeitsplatz gesagte, ich wiederhole kurz die wichtigsten Punkte:

- Nicht benötigte Dienste abschalten
- Keine Nutzung von anfälliger Software (IE, OE und Konsorten)
- Updaten / Patchen ist Pflicht
- Strikte Rechtetrennung
- Nur Software aus "vertrauenswürdigen Quellen" nutzen (z.B. von Herstellern, MS selbst)

Netzwerke sind allerdings noch ein klein wenig komplexer.

Wir unterscheiden hier drei verschiedene Arten von Netzwerken (die Einteilung ist natürlich willkürlich):

a) Das unechte Netzwerk
b) Das echte Netzwerk
c) Das Funknetzwerk (WLAN)

a) Das unechte Netzwerk

Beispiel: Mein Arbeitszimmer. Hier stehen zwei Rechner herum, die über einen Router an das Internet angebunden sind. Technisch gesehen ist das bereits ein Netzwerk. Da ich aber keinerlei Freigaben aktiviert habe, sind die Rechner voneinander getrennt. Damit handelt es sich nicht um ein echtes Netzwerk im Sinne dieser Lektion.

Hier genügt es, alle Anweisungen aus der Lektion "Sicherheitskonzept Einzelarbeitsplatz" umzusetzen.

b) Das echte Netzwerk

Mehrere Rechner sind miteinander verbunden und teilen ihre Ressourcen. Hier können wir zwei weitere Fälle unterscheiden:

1) Das Netzwerk ist nicht an das Internet angebunden
2) Das Netzwerk hat eine Verbindung in das Internet

Fall 1) soll uns nicht weiter interessieren. Uns interessiert hier die Gefahrenquelle Internet.

Jetzt müssen wir danach trennen, wie der Internetzugang hergestellt wird:

a) Über einen eigenen Rechner
b) Über einen Router (das sei ein PC mit einem geeigneten OS oder eine kleine Box, wichtig ist nur, daß er nur zu diesem Zweck dient)

Internet über einen eigenen Rechner

Im ersten Falle spielt ein eigener Rechner das Gateway zum Internet. Ein Beispiel wäre die Möglichkeit unter Windows, die Internet-Verbindung durch einen anderen Rechner mitbenutzen zu lassen.
Das funktioniert mit Windows 98 aufwärts.

Der "Hostrechner", über den auf das Internet zugegriffen wird, braucht dann entsprechend viele Netzwerkkarten.

Ein erster, wichtiger Schritt ist es, auf dem "Hostrechner" an der Schnittstelle, mit der ins Internet gegangen wird, die Netbios-Protokolle zu entfernen. Man möchte Netbios nicht über das Internet anbieten. Wie das geht, erfährt man hier: www.ntsvcfg.de

Als zweites sollte man auf dem Hostrechner von außen kommende Zugriffe auf die "üblichen Verdächtigen" sperren, d.h. auf die Ports 135, 137-139, 445 und 1025-1027. Das sind Ports, die man nur im eigenen Netzwerk (wenn überhaupt) ansprechen können möchte. Die XP-Firewall kann diese Ports von außen blockieren.

Sind ansonsten die Hinweise in der Lektion zum Thema "Einzelarbeitsplatz" umgesetzt, können wir es dabei belassen. Ich halte allerdings diese technische Lösung nicht für optimal.

Internetzugang über einen Router

Sämtliche Rechner, die auf das Internet und einander zugreifen sollen, hängen hier an einer eigens dafür konfigurierten Hardware. Das kann ein PC sein, auf dem ein geeignetes Mini-Betriebssystem läuft oder eine kleine Box z.B. von Linksys.

Auf das grundlegende zum Thema "Router" gehe ich ganz am Schluß ein, hier interessiert nur das Heimnetzwerk, d.h. Netzwerkfreigaben etc.

Es gilt, das Heimnetzwerk vom Internet sauber zu trennen. Dafür gibt es zwei Möglichkeiten:

1) Jeder Client überprüft selbständig, ob ein Zugriff aus dem Internet oder dem Intranet erfolgt und handelt entsprechend
2) Die Zugriffe aus dem Internet werden an der Netzgrenze abgefangen - über den Router

Welche Lösung ist vorzuziehen? Ganz klar: die zweite. Begründung: An der Netzgrenze zwischen Internet und Intranet (Heimnetzwerk) lassen sich Täuschungsversuche noch erkennen. Was ist damit gemeint? Ein Beispiel soll das erläutern:

Wir haben den Router mit der IP 192.168.0.0. Darüber hinaus haben wir vier Clients mit den IPs 192.168.0.1 bis 192.168.0.4.

Möchte jetzt ein Angreifer Zugriff auf einen der Netzwerk-Clients haben, so täuscht er vor, er gehöre zum Netzwerk dazu. Dafür gibt er bei seinem Zugriff als Absender-IP eine lokale IP an, z.B. zum Zugriff auf Client 2 (192.168.0.2) die von Client 3 (192.168.0.3).

Fall 1: Jeder Client prüft selbst

Client 2 hat keine Möglichkeit, den Zugriff als illegal zu erkennen, da die angegebene (gefälschte) IP ja korrekt ist. Auf die Ports, die lokale (verwundbare) Dienste anbieten (135, 137-139, 445, 1025-1027) kann er nicht filtern, weil er sonst ja seinen "Kollegen" den Zugriff verweigern würde.

Fall 2: Zentrale Prüfung durch den Router

Der Router ist so eingestellt, daß er von außen kommende Pakete, die auf lokale Dienste zugreifen möchten (135, 137-139, 445, 1025-1027) wegwirft. Folge: Die gefälschten Pakete erreichen ihr Ziel nicht. Der Angriff wurde abgewehrt.

Noch besser ist es, wenn der Router die Möglichkeit bietet, auf lokale IPs zu filtern. In diesem Falle verwirft er alle Pakete, die "von draußen" (Internet-Seite) eingehen und als Absender eine lokale IP (d.h. eine aus dem Heimnetzwerk) haben.

Fazit: Eine Trennung zwischen Heimnetzwerk und Internet hat stets an der Netzgrenze zu erfolgen.
Sinnvoll ist hierfür, die einschlägigen Ports (s.o.) per Paketfilter-Regeln auf dem Router zu filtern.

Das gilt auch, wenn man eigene Server im Heimnetzwerk laufen hat, die nicht von außen erreicht werden sollen. Auch diese Ports sind dann an der Netzgrenze wegzufiltern. Sinnvollerweise nimmt man diese Filterung in beide Richtungen vor. So vermeidet man, daß eine "Wurmschleuder" im eigenen Netz z.B. mit dem Blaster das Internet vollballert.

c) Das Funknetzwerk (WLAN)

Es gilt das unter b) bereits gesagte. WLAN bietet allerdings eine weitere Angriffmöglichkeit. Ein Angreifer kann versuchen, sich in das lokale Netzwerk einzuklinken. Ziel kann dabei sein, die bestehende Internet-Verbindung

mitzubenutzen oder aber Zugriff auf die lokalen Freigaben im Netzwerk zu erhalten (inkl. Serverdienste und anderes...)

Welche Möglichkeiten gibt es, unerwünschte Eindringlinge aus dem WLAN herauszuhalten?

WEP
WEP ist seit längerem als geknackt zu betrachten. Der Aufwand, in ein WEP-gesichertes Netzwerk einzubrechen, wird auf 20 Minuten geschätzt. Ist der Angreifer erst einmal "drin", ist er ein lokaler Client - er kann dann auf die lokalen Freigaben zugreifen!

WPA-PSK
WPA mit "Pre-Shared-Key" ist zur Zeit als sicher zu betrachten. Dabei wird ein Schlüssel festgelegt, der dann auf Router und Client eingetragen wird.
Wichtig: Der Schlüssel muß
a) eine gewisse Länge aufweisen (deutlich mehr als 8 Zeichen sind zu empfehlen, Maximum sind 63 Ascii-Zeichen)
b) nicht-trivial zu ermitteln sein. D.h. Name und Vorname sind ebenso tabu wie die meisten Wörter aus dem Wörterbuch. Sonst wird WPA anfällig für eine Brute-Force-Attacke nach dem Wörterbuch-Prinzip.

MAC-Adressen-Filterung
Dieses Feature bieten die meisten Router an. Jede Netzwerkkarte verfügt über eine einmalige, physische Adresse, die MAC-Adresse. Ist diese auf dem Router in eine Liste eingetragen, bekommt die Netzwerkkarte Zugriff (von WPA oder sonstigem einmal abgesehen). Ansonsten nicht.
Dieses Feature bietet absolut keine Sicherheit. Eine MAC-Adresse läßt sich innerhalb von Minuten mitschnüffeln und dann auf der eigenen Netzwerkkarte (WLAN-Karte) fälschen.

Abschalten des SSID-Broadcasts
Es wird verhindert, daß der Name des Funknetzwerks durch die Gegend gebrüllt wird. Auch das verhindert absolut nichts, da die SSID in jedem Paket drinsteht, das per Funk über den Äther geht. Es bietet also keine Sicherheit

VPN
Die "Königslösung" für ein WLAN: Aufbau eines "Virtual Private Network". Noch sicherer als WPA, aber für den Heimanwender idR zu komplex. Dabei werden alle Daten, die zwischen Client und Router übertragen werden, über einen verschlüsselten Tunnel geleitet. Bei guten Implementationen ist die Sicherheit so hoch, daß schon gewitzelt wurde, der NSA (National Security Agency der Amerikaner) könnte das knackern, aber sonst kaum jemand.

Fazit: Für WLAN halte ich im Moment WPA für die geeignetste Lösung. Bei Wahl eines hinreichend langen und komplexen Schlüssels (Beispiel: @EW#xj-b82,3g.bkw382l*+ nur ein bißchen länger...) ist man vor Angriffen auf das WLAN an sich gut geschützt.

Kurze Einführung zum Thema Router
Zum Schluß gehe ich noch kurz darauf ein, was gängige Router können - und was sie nicht können.

NAT
Abkürzung für "Network Adress Translation". Dadurch wird es möglich, daß mehrere Rechner gleichzeitig ins Internet gehen können, obwohl man nur einen Zugang hat. Man bekommt eine öffentliche IP zugewiesen. Der Router modifziert nun alle ein- und ausgehenden Pakete so, daß er die öffentliche IP darin durch die lokale IP des jeweiligen Clients ersetzt. (Lokale IPs sind die aus dem Adressbereich 192.168.X.X, siehe oben)
Ein Nebeneffekt von NAT ist damit, daß ein Zugriff von außen auf die Clients im Netzwerk schwierig wird, weil der von außen zugreifende nicht wissen kann, wer sich hinter der öffentlichen IP verbirgt. Um es in aller Deutlichkeit zu sagen: NAT ist kein Sicherheitsfeature. Warum nicht? Wird nicht immer mit "NAT-Firewalls" geworben, wenn man einen Router kaufen möchte?
Eine NAT-Firewall ist ein schwarzer Schimmel. Der Sinn von NAT ist es, eine Kommunikation von innen nach außen und umgekehrt zu ermöglichen. Eine Firewall dagegen soll zwei Netze voneinander trennen. Ein Widerspruch. Ja, NAT verhindert idR, daß man von außen Zugriff auf einen Client bekommt. Außer, das Paket wurde vom Client angefordert. Aber da NAT der Kommunikation dient, bauen manche Hersteller da Funktionen ein, die zur Not auch wild raten, wo ein Paket hingehen sollte... und schon wandert etwas ins Internet, das man dort nicht haben möchte.

Router-Paketfilter

Das ist, im Gegensatz zu NAT, ein Sicherheitsfeature. Das ganze funktioniert so wie (würg) eine PFW. Man kann IPs und Ports angeben, die dann geblockt werden.
Es empfiehlt sich hier, für das Heimnetzwerk alle Ports anzugeben, hinter denen Dienste lauschen, die nur aus dem Heimnetzwerk (LAN) selbst erreichbar sein sollen. Dann werden alle Zugriffe von außen verworfen. Das funktioniert idR sehr zuverlässig.
Außerdem empfiehlt es sich, wenn möglich, alle lokalen IP-Adressen zu filtern. D.h., wenn ich die Adressen 192.168.0.1 bis X.X.X.4 benutze, dann lasse ich diese vom Router von außen kommend verwerfen. Wer diese Adressen von außen vor sich herträgt, der hat nichts Gutes im Sinne.

Router-Passwort

Dieser Punkt wird sehr gerne übersehen.
Alle mir bekannten Router haben bei Auslieferung ein Standard-Passwort wie z.B. "Admin", "Passwort" oder ähnliches.
Ein solches Passwort ist ASAP (so schnell wie möglich) gegen ein sicheres Passwort (siehe WPA) zu ersetzen!

Begründung: Man stelle sich folgenden Fall vor. Jemand schafft es, sich in mein Netzwerk einzuschleichen (egal, ob LAN oder WLAN). Da das voreingestellte Passwort auf dem Router ein Witz ist, klinkt er sich dort ein, klaut meine Zugangsdaten, löscht meine gesamten Paketfilter-Regeln, richtet mir ein nettes Port-Forwarding ein (damit die Würmer, die er mir dann sendet, auch meine Clients treffen und nicht vom NAT aussortiert werden), ändert dann das Passwort, so daß ich die Änderungen nicht rückgängig machen kann und stiehlt sich dann davon.

Paranoid? Ach was. Gerade bei WLAN ist das ein ernstzunehmendes Szenario. Ruck-Zuck sind alles Sicherheitsmaßnahmen dahin.
Hat man Glück, richtet der Angreifer nur Schabernack an, z.B. löscht meine Zugangsdaten und ändert das Passwort, so daß ich nicht mehr ins Internet komme und einen Hard-Reset auf dem Router durchführen muß.

Abschließend:

Es gilt, wie auch in der Lektion zum Thema "Einzelarbeitsplatz" gesagt wurde: Niemals in Sicherheit wiegen! Egal, wie gut meine Absicherung ist, das darf kein Grund für mich sein, fahrlässig zu werden.

- Regelmäßige Kontrolle der laufenden Dienste / Programme
- Regelmäßiges Ändern der Freigabe-Passwörter (Du hast keine??)
- Auch bei einem tollen Router-Paketfilter: Patchen, Patchen, Patchen