Sicherheitskonzept für Einzelplatzrechner

Beitrag von MobyDuck

In Beiträgen zu Firewalls liest man häufig das gut gemeinte Schlagwort, eine Firewall sei kein Stück Software, sondern ein Sicherheitskonzept. „Na gut“, denkt sich der User, „aber wie sieht denn so ein Konzept aus?“ Gute Frage. Eins vorneweg, ein allgemein gültiges Sicherheitskonzept gibt es nicht. Auch nicht für Heimanwender, denn der Computernutzer, der Homebanking betreibt und vielleicht auch noch seine Steuererklärung am PC bearbeitet sollte andere Vorstellungen über Sicherheit pflegen als der User, der vor allem zocken möchte.

So gibt es auch viele unterschiedliche Ansätze, den Umgang mit dem Rechner sicherer zu machen. Am weitesten verbreitet ist die Methode, über Antivirenprogramme und Personal Firewalls die Sicherung des Computers eben doch der Software zu überlassen. Dahinter steckt vereinfacht gesagt der Gedanke, Angriffe von außen per Firewall abzuwehren und die Installation von Malware über das AV-Programm zu verhindern, bzw. eingedrungene Schädlinge zu entfernen. Wir haben in den vorherigen Lektionen gesehen, dass dies nicht zuverlässig funktionieren kann, ganz abgesehen davon, dass man diese Vorgehensweise nur schwerlich als „Konzept“ bezeichnen kann. Andere setzen zusätzlich auf regelmäßige Überprüfung. So hat eine Umfrage hier im Forum ergeben, dass viele User regelmäßig wöchentlich ihr System auf Viren scannen. Kontrolle ist gut, aber letztendlich auch nicht ausreichend, da nun mal auch Virenscanner nicht fehlerlos sind und trügerische Sicherheit vermitteln können. Hierauf kommen wir weiter unten beim Thema „Risikokompensation“ zurück.

Jedenfalls müssen wir einen anderen Ansatz wählen. Wir werden uns daher in diesem Beitrag mit einem Konzept beschäftigen, das man schlagwortartig mit „Verringerung der Angriffsfläche, Überschaubarkeit und Datensicherung“ beschreiben kann. Letztendlich setzen wir damit nur praktisch um, was wir in den vorherigen Lektionen besprochen haben.

Verringerung der Angriffsfläche

Hier greifen wir den Stoff der Lektion „Einstellungen in Windows, Browser und Mailprogramm" auf. Wir haben gesehen, dass es Schädlinge gibt, die zu ihrer Ausführung und Verbreitung Schwachstellen in Diensten und Programmen ausnutzen. Es liegt auf der Hand, dass man die Gefahr, mit derartigen Schädlingen Bekanntschaft zu machen, schon dadurch drastisch verringert, indem man anfällige Dienste und Programme gar nicht erst anbietet bzw. nutzt. Weiter verkleinern wir die Angriffsfläche dadurch, dass wir unsere Software aktuell halten und schließlich unwillkommenen Besuchern Administratoren-Rechte versagen.

Wir schalten daher zunächst nicht benötigte Dienste ab.
Wie es geht, ist in der Lektion "Einstellungen in Windows, Browser und Mailprogramm" beschrieben.

Weiter sollten wir auf die Nutzung potentiell anfälliger Programme verzichten.
Hierzu zählen vor allem der Internet Explorer 6.0 (ob es mit der angekündigten Version 7.0 besser wird werden wir sehen), Outlook Express und Outlook. Wer die Programme nicht missen kann oder möchte, sollte zumindest versuchen, sie halbwegs sicher zu konfigurieren. Wie es geht steht ebenfalls in der erwähnten Lektion 2

Immer wieder gelangen jedoch auch andere Programme wegen Sicherheitsmängel ins Gerede. Wenn der Hersteller nicht zeitnah Patches zur Verfügung stellt, sollte sich der User fragen, ob der Software-Produzent seine Sicherheitsbedürfnisse nicht ernst nimmt oder ob die Software so schlecht ist, dass sie nicht nachgebessert werden kann. Egal, in beiden Fällen sollte man sich nach Alternativen umsehen.

Ohnehin ist es unabdingbar, laufend das System durch Updates und Patches aktuell zu halten. Dies gilt vor allem für Windows und den darin tief eingebetteten Internet Explorer, aber auch für alle anderen Programme. Der Grund liegt auf der Hand, mit jedem beseitigten Fehler wird das System weniger angreifbar.

Schließlich verringert man auf NT-Systemen die Angriffsfläche noch dadurch, dass man unter Windows NT/2000 oder XP eine Arbeitsumgebung mit eingeschränkten Rechten nutzt und den Administrator –soweit möglich- nur das machen lässt, wozu er da ist: Administrieren. Zugegeben ist die Rechteverwaltung unter Windows für weniger erfahrene User wenig durchsichtig und schlecht programmierte Anwendungen verlangen nach Admin-Rechten. Es ist jedoch schon viel gewonnen, wenn man sich wenigstens angewöhnt, konsequent mit eingeschränkten Rechten zu surfen. Wie ein eingeschränkter Benutzer eingerichtet wird, steht in Lektion 2

Wenn wir die vorstehenden Punkte konsequent beachten, dann sind wir in der Umsetzung unseres Konzeptes schon ein ganzes Stück weiter und können uns in Teil 2 den weiteren Aspekten zuwenden.

Überschaubarkeit

Der Begriff der Überschaubarkeit hat für unser Sicherheitskonzept eine doppelte Bedeutung: Zum einen ist die Überschaubarkeit des Systems gemeint, zum anderen die Vermeidung von Verborgenem wie etwa Trojanern und Spyware. Beide Punkte bedingen sich. Doch der Reihe nach, es ist gar nicht kompliziert:

Ich mache mit meinem Computer und den installierten Programmen, was ich will und nicht umgekehrt.

Das sollte eigentlich selbstverständlich sein, ist es aber nicht. Wenn ich mir in den einschlägigen Foren die üblichen Hijackthis-Logs anschaue, dann werde ich regelmäßig von den nicht enden wollenden Listen von Autostart-Einträgen geradezu erschlagen. Wie sich dann in der Problembehebung herausstellt, haben die betroffenen User nur einen Bruchteil wissentlich selbst installiert, viele wissen überhaupt nicht, was sich alles das Recht herausnimmt, per Autostart ein Eigenleben zu führen. Das muss nicht sein, nur die wenigsten Programme müssen automatisch beim Booten gestartet werden. Wir sollten uns daher angewöhnen, nach jeder Programminstallation unter

start -> ausführen: msconfig -> Systemstart

nachzusehen, ob sich das neue Programm einen Autostart genehmigen möchte. Falls wir diesen automatischen Start nicht ausdrücklich wünschen (etwa bei bestimmten Drucker- oder Maustreibern), dann sollten wir dem Programm diese Eigenmächtigkeit durch Abstellen der entsprechenden Option oder durch Entfernen des Häkchens in msconfig austreiben.

An dieser Stelle sollten wir uns auch fragen, wann wir zum letzten mal von einem wildfremden Menschen ohne Hintergedanken etwas geschenkt bekamen. Lange her? Im Internet gibt es so etwas noch in den zahlreichen Open Source Projekten wie Linux oder der Mozilla Stiftung. Aber das ist nicht die Regel. Viele auf den ersten Blick kostenlose Programme werden durch die Beigabe von Ad- oder Spyware finanziert, wenn nicht gar Trojanische Pferde eingebaut sind. Bevor wir daher kostenlose Software installieren, recherchieren wir im Internet, ob das Programm „sauber“ ist. Auch die zu Beginn der Installation regelmäßig auftauchenden „Nutzungsbedingungen“ klicken wir nicht einfach weg, sondern schauen nach, ob irgendwo vom Einverständnis zur Installation weiterer Programme oder Features die Rede ist.

Selbst große Software-Anbieter schrecken nicht davor zurück, dem User mit ihren Trial-Versionen aus Werbezwecken weitere Trials oder Adware unterzujubeln. Aufmerksamkeit bei der Installation und ein Blick in den Programm-Ordner und/oder in Systemsteuerung -> Software nach der Installation geben hierzu Aufschluss.

Wenn wir gerade beim Thema Aufräumen sind: Auf den Einsatz von Filesharing-Programmen sollten wir verzichten. Sie sind häufig selbst Spyware-verseucht und darüber hinaus eine beliebte Plattform zur Verbreitung von Schädlingen aller Art.

In diesen Zusammenhang gehört ohnehin jeder Download aus nicht vertrauenswürdigen Quellen. Das gebietet bereits der gesunde Menschenverstand. Wer sich von dubiosen Seiten irgendwelche Daten herunterlädt, braucht sich nicht zu wundern, wenn er anschließend sein Sicherheitskonzept an einem wegen Malware-Befall frisch aufgesetzten System ausprobieren darf, oder besser muss. Welche Seiten nun als vertrauenswürdig einzuschätzen sind, ist nicht immer einfach zu entscheiden. Mit einem gesunden Schuss Misstrauen und mit Nachdenken kommt man jedoch schon weiter. Vielleicht fragt man sich einfach, ob man von dem Betreiber der Seite auch einen Gebrauchtwagen kaufen würde.

Bei der Gelegenheit noch ein Wort zu Messenger-Programmen wie ICQ und Co. Mir persönlich hat sich der Nutzen dieser Programme nie erschlossen. Wer mir etwas mitteilen will, kann mir eine E-Mail schicken und muss mich nicht durch eine ICQ-Meldung aus dem Büroschlaf reißen. Gemessen an dem Gefährdungspotential und dem tatsächlichen Nutzen sind diese Programme in meinen Augen nicht ganz ungefährliches Spielzeug. Man sollte daher abwägen, ob man so etwas wirklich haben muss.

So, wenn wir uns dann noch grundsätzlich überlegen, welche Programme wir tatsächlich brauchen und Unnützes ausmisten, dann haben wir die nötige Überschaubarkeit erreicht. Dem ungewollten Installieren von Code durch den Internet Explorer haben wir bereits durch das Ausweichen auf andere Browser oder das Abschalten aktiver Inhalte im IE vorgebeugt. Durch die Beschäftigung mit den soeben genannten Punkten lernen wir unser System genauer kennen, wissen, welche Programme installiert sind und was sie machen. Da wir auf Überflüssiges verzichten, wird das System übersichtlicher und man erkennt schneller, wenn sich etwas ungewollt einnistet. Außerdem schließt sich der Kreis zu Punkt 1: Durch die Beschränkung auf das Benötigte haben wir die Angriffsfläche erneut verkleinert.

Da wir uns schon in vorherigen Lektionen abgewöhnt haben, unkritisch auf jeden Link oder jeden E-Mail-Anhang zu klicken, sind wir mit dem vorbeugenden Teil unseres Konzepts auch schon fertig. Eine Personal Firewall brauchen wir als Sicherheitsmaßnahme nicht mehr, obwohl nichts dagegen spricht, die XP-Firewall mitlaufen zu lassen. Sie stört zumindest nicht. Virenscanner und Anti-Spyware-Tools haben jetzt die Rolle, die ihnen zusteht: Nämlich als zusätzliches Werkzeug und nicht als Rückgrat eines Sicherheitskonzeptes. Wir halten diese Tools ständig aktuell und scannen regelmäßig die Festplatte - eigentlich nur noch zur Beruhigung.

Risikokompensation

Damit sind wir jedoch nicht fertig, leider. Das aus dem Arbeitsschutz bekannte Phänomen der Risikokompensation könnte uns noch einen Strich durch die Rechnung machen. Darunter versteht man den Ausgleich, einer hoch eingeschätzten Gefahr mit vorsichtigem Verhalten zu begegnen und in subjektiv ungefährlichen Situationen ein geringeres Sicherheitsverhalten zu zeigen.
http://www.bgfe.de/aktuell/motivation_arbeitsschutz.html

Jeder kennt das hierzu immer wieder bemühte Beispiel von dem unerfahrenen User, der sich zunächst ganz vorsichtig im Internet bewegt und sich mit der Programmsammlung seines Komplett-PC bescheidet. Bis er eine der üblichen Sicherheitspakete kauft. Im Vertrauen auf die Rundum-Sorglos-Reklame verhält er sich von jetzt an völlig fahrlässig und wundert sich, was so alles in trügerischer Sicherheit passieren kann.

Doch was hat das mit unserem Konzept zu tun? Eine ganze Menge. Auch wenn wir das Konzept gewissenhaft umgesetzt haben, besteht keine Veranlassung, leichtsinnig zu werden. Alle Punkte greifen ineinander und sind gleich wichtig. So macht es zum Beispiel wenig Sinn, alle Dienste abgeschaltet zu haben, wenn man sich bei nächster Gelegenheit einen Wurm mit Kazaa zieht oder Programme von Warez-Seiten runterlädt. Ständige Vorsicht – oder wie es in den Foren gern genannt wird: „Brain. 1.0“ – sind unabdingbar. Doch das gilt erst recht für die Nutzer der „Rundum-sicher“-Pakete. Nur mit dem Unterschied, dass wir nicht nur jede Menge Geld sparen, sondern auch noch das bessere Konzept haben.

Datensicherung

Zu einem Sicherheitskonzept gehört auch eine Strategie, im Bedarfsfall ohne großen Aufwand das System wiederherzustellen und damit Daten zu retten und natürlich viel Arbeit zu sparen. Es bietet sich an, regelmäßig mit einem der zunehmend komfortabler gewordenen Image-Programmen regelmäßig auf anderen Datenträgern Images zu ziehen. Hierzu hat unser Mitglied deoroller einen gesonderten Beitrag verfasst, der in den nächsten Tagen hier erscheinen wird.

Anmerkung:
Dieser Beitrag richtet sich vor allem an die weniger erfahrenen User. Fortgeschrittenen sei der Vortrag von Volker Birk empfohlen:
http://www.ulm.ccc.de/chaos-seminar/wind...y/recording.htm

(Update)
Leider ist obige Seite zur Zeit nicht erreichbar. Unser Mitglied Cidre hat die Thesen des Vortrages hier zusammengefasst:
http://www.dedies-board.de/wbb2/thread.php?threadid=133