Ralph Lehmann
IT-Sicherheitsanalyse
und Beratung

Ralph Lehmann · IT-Sicherheitsanalyse und Beratung · Kochstraße 34 · 04275 Leipzig

Kochstraße 34
04275 Leipzig

Tel.: (03 41) 3 06 99 05
Fax: (03 41) 3 08 10 31
mobil: (01 70) 3 11 37 35

e-mail: info@ralph-lehmann.de
Web: www.ralph-lehmann.de

Sicher OHNE Virenscanner

Absicherung von Windows XP und Windows Vista gegen Schadsoftware

Steuernummer: 231/244/00473
Bankverbindung: Sparkasse Leipzig, BLZ: 860 555 92, Kto-Nr.: 1 895 153 928

1. Einleitung

Stellen Sie sich vor, eines Tages stünde ein netter, Ihnen allerdings völlig unbekannter Herr vor Ihrer Tür und würde Sie bitten, ihm kurzfristig fünfzig Euro zu leihen. Was würden Sie tun?

Sie haben genau zwei Möglichkeiten:

- Obwohl Sie täglich Zeitung lesen und die Nachrichten sehen, ist Ihnen der freundliche Herr nicht als Gauner bekannt. Er steht deshalb nicht auf Ihrer **schwarzen Liste**. Deshalb zücken Sie entschlossen Ihre Geldbörse und händigen dem Herren die gewünschte Summe aus.
- Obwohl Sie intensiv überlegen, können Sie sich nicht erinnern, dass der freundliche Herr zu Ihrem Bekanntenkreis gehört. Er steht deshalb nicht auf Ihrer **weißen Liste**. Sie grüßen daher höflich zum Abschied und schließen die Tür.

Was hat das aber mit der Vermeidung einer Infektion Ihrer/Ihres Computer(s) mit schädlicher Software zu tun?

Das Beispiel soll verdeutlichen, vor welchem prinzipiellen Problem jeder Virenscanner steht – der Nutzung einer so genannten **schwarzen Liste**. Eine solche Liste muss prinzipiell immer veraltet und unvollständig sein. Meist enthält sie außerdem fehlerhafte Einträge, z.B. also gute Bekannte, die irrtümlich auf die Liste geraten sind oder aber Software, welche jahrelang zuverlässig für Sie gearbeitet hat und nun plötzlich einen Fehlalarm auslöst.

2. Schwarze Listen und Ihre Probleme

Einige weitere Beispiele sollen verdeutlichen, warum schwarze Listen meistens nicht zuverlässig funktionieren können:

- Niemand käme auf die Idee, seinen Kindern eine Liste mit potentiell gefährlichen Personen in die Hand zu drücken, das Mitgehen mit **nur** diesen Personen zu verbieten, mit **beliebigen anderen** jedoch zu erlauben.
- Kaum jemand würde im Wald Pilze sammeln und später verspeisen, nur weil sie ihm nicht als giftig bekannt sind.
- Keine Bank würde sich bei der Bewilligung eines Kredits allein darauf verlassen, dass die SCHUFA - Auskunft des Kreditnehmers keine Auffälligkeiten zeigt.

3. Weiße Listen und ihre Vorteile

Weiße Listen haben meist nur wenige Einträge. Sind sie daher übersichtlich und leicht zu handhaben.

- Auch kleine Kinder sind in der Lage, sich eine überschaubare Anzahl vertrauenswürdiger Personen als „sicher" zu merken.
- Der Ansatz „Alles, was nicht als essbar bekannt ist, ist nicht essbar!" sollte Pilzvergiftungen zuverlässig vermeiden.
- Der Kreditnehmer liefert eine weiße Liste mit Sicherheiten. Das Risiko für die Bank wird damit erheblich reduziert.

4. Der Lebenszyklus einer schädlichen Software und warum ein Virenscanner immer veraltet ist

Um zu verstehen, warum der Schutz vor schädlicher Software durch Anwendung einer schwarzen Liste nicht zuverlässig sein **kann**, ist es hilfreich zu wissen, wie die „Karriere" einer solchen Software gewöhnlich verläuft.

a) Die schädliche Software wird gemäß ihrer Bestimmung entworfen, programmiert und getestet.
b) Die Schadsoftware wird verbreitet.
c) Erste Anwender bemerken Unregelmäßigkeiten und melden diese mit einiger Verzögerung an die Hersteller der Virenscanner.
d) Die Hersteller der Virenschutzsoftware analysieren den Schädling und aktualisieren ihre Software.
e) Die Hersteller testen die aktuelle Version ihrer Virenschutzsoftware und stellen diese den Anwendern zur Verfügung.
f) Die Anwender aktualisieren ihre Virenscanner.

Zwischen den Schritten b und f dieser Liste vergeht nicht selten geraume Zeit. Oft haben die Programmierer schädlicher Software diese bei Erreichen von Schritt f bereits so modifiziert, dass der Virenscanner sie auch mit aktuellen Signaturen nicht erkennen kann.

An dieser Stelle soll nicht unerwähnt bleiben, dass die Geschwindigkeit, mit der die Programmierer schädlicher Software ihre Produkte zu modifizieren in der Lage sind, in den letzten Jahren stark gestiegen ist. Dem gegenüber hat sich der Zeitraum von der ersten Endeckung einer schädlichen Software bis zur Aufnahme des entsprechenden „Fingerabdrucks" in die Signaturen der Virenscanner-Hersteller kaum verkürzt. Aus diesem Grund sind heutzutage wesentlich mehr nicht identifizierbare Schädlinge im Umlauf als noch vor einigen Jahren.

5. Warum empfehlen Behörden (z.B. das BSI) Virenscanner?

Aus Sicht einer Behörde oder Organisation, die dem Gemeinwohl verpflichtet ist, stellt die Infektion **einzelner** Computer mit schädlicher Software kein großes Problem dar. Organisationen wie z.B. das Bundesamt für die Sicherheit in der Informationstechnik (BSI) sind vielmehr dafür zuständig, Sorge zu tragen, dass schädliche Software nicht wie eine Epidemie einen **Großteil** der Computer infiziert.

Virenscanner sind trotz aller Mängel geeignet, die seuchenartige Ausbreitung schädlicher Software zu verhindern – allerdings nur dann, wenn sie auf einem Großteil aller verwendeten Computer verwendet werden. Spätestens einige Tage nach dem Auftauchen eines neuen Schädlings erkennt ihn die Mehrheit der verwendeten Scanner. Die schädliche Software kann sich dann nur noch langsam weiter ausbreiten.

Vermutlich muss davon ausgegangen werden, dass das BSI der überwiegenden Mehrheit der Computerbetreiber nicht zutraut, ihre Systeme durch bessere, aber auch weniger simple Sicherungsmaßnahmen vor dem Befall mit schädlicher Software

zu schützen. Die Empfehlungen des BSI sind deshalb folgerichtig, auch wenn sie den **einzelnen** Betreiber nicht zuverlässig vor Schäden schützen können.

6. Wie Computer durch die Anwendung weißer Listen geschützt werden können

Computer werden betrieben, um bestimmte Aufgaben zu erfüllen. In den meisten Fällen ist es ziemlich einfach, eine konkrete Liste dieser Aufgaben zusammenzustellen. Je nach Branche, Unternehmensgröße, Spezialisierung usw. hat diese Liste natürlich andere Inhalte. Deshalb ist die konkrete Auswahl der Software, die zur Bewältigung der Aufgaben benötigt wird, **unternehmensspezifisch**.

Darüber hinaus werden an die Software **unternehmensübergreifend** allgemeine Anforderungen gestellt:

- Der Hersteller und ggf. der Händler der Software sind vertrauenswürdig.
- Der Vertrieb der Software ist gegen Manipulationen abgesichert.
- Der Hersteller der Software behebt entdeckte Fehler zeitnah.

Wenn Sie in der Lage sind, sich bei den in Ihrem Unternehmen anfallenden Aufgaben ausschließlich auf Software zu stützen, die sowohl Ihre **unternehmensspezifischen** als auch die **unternehmensübergreifenden** Anforderungen erfüllt, können Sie Ihre Computer wirksam gegen den Befall mit schädlicher Software schützen. Es ist hierzu ausreichend, Software, die nicht **mindestens** die **unternehmensübergreifenden** Anforderungen erfüllt, nicht auszuführen oder ausführen zu lassen.

Gehen Sie wie folgt vor, um Ihrer Computer durch Anwendung einer **weißen Liste** zu schützen:

a) Stellen Sie eine Liste jener Programme zusammen, die zur Bewältigung Ihrer unternehmensspezifischen Aufgaben am besten geeignet ist.
b) Stellen Sie sicher, dass Ihre Liste nur Programme enthält, die alle unternehmensübergreifenden Anforderungen erfüllt.
c) Verhindern Sie die Ausführung aller Programme, die kein Bestandteil Ihrer weißen Liste sind.

Beachten Sie, dass Ihnen schädliche Software nun nichts mehr anhaben kann, da sie nicht Bestandteil Ihrer weißen Liste sein wird und deshalb weder absichtlich noch versehentlich ausgeführt werden kann.

7. Wie die Ausführung von Software, die nicht Bestandteil Ihrer weißen Liste ist, verhindert werden kann

Die **vollständige** Umsetzung der folgenden Maßnahmen gewährleistet, dass auf Ihren Computern keine unerwünschte Software (Viren, trojanische Pferde usw.) ausgeführt werden kann:

a) Stellen Sie sicher, dass Windows aus vertrauenswürdiger Quelle (z.B. direkt vom Händler) geliefert und ordnungsgemäß lizenziert wird. Beachten Sie, dass einige der folgenden Punkte nicht umsetzbar sind, wenn das Betriebsystem nicht ordnungsgemäß aktiviert bzw. auf Echtheit überprüft werden kann.

b) Stellen Sie sicher, dass die Windows-Firewall oder ein entsprechender Filter auf Ihrem DSL-Router aktiv ist, bevor Sie den Computer mit dem Internet verbinden.
c) Installieren Sie alle empfohlenen Updates für Ihr Betriebsystem und stellen Sie sicher, dass auch zukünftig neu erscheinende Updates regelmäßig installiert werden.
d) Beschaffen Sie die von Ihnen benötigte Anwendungssoftware aus vertrauenswürdiger Quelle. Installieren Sie diese wie vorgesehen in das Programmverzeichnis (z.B. C:\Programme). Konfigurieren Sie die Software wie vom Hersteller empfohlen.
e) Aktualisieren Sie Ihre Anwendungssoftware mit den vom jeweiligen Hersteller empfohlenen Updates und stellen Sie sicher, dass auch zukünftig neu erscheinende Updates regelmäßig installiert werden.
f) Richten Sie für die tägliche Arbeit mit dem Computer für **alle** Benutzer eingeschränkte Benutzerkonten ein. Diese verfügen **nicht** über die Berechtigung, neue und eventuell gefährliche Software in das Programmverzeichnis (z.B. C:\Programme) oder in das Systemverzeichnis (z.B. C:\Windows) zu installieren.
g) Erzwingen Sie mit Hilfe von Systemrichtlinien, dass durch eingeschränkte Benutzer **ausschließlich** Software aus dem Programmverzeichnis (z.B. C:\Programme) und dem Systemverzeichnis (z.B. C:\Windows) ausgeführt werden kann.
h) Stellen Sie sicher, dass sowohl Sie selbst als auch Ihre Mitarbeiter die tägliche Arbeit ausschließlich mit eingeschränkten Benutzerkonten verrichten.

Hinweis: Es ist unmöglich, durch die nachträgliche Abarbeitung der o.g. Schritte sicherzustellen, dass ein Computer frei von schädlicher Software ist. Wenn dieser bisher auf unsichere Weise betrieben wurde, muss die sichere Konfiguration des Computers zwingend mit der Neuinstallation des Betriebsystems beginnen.

8. Zusammenfassung

Computer unter Windows XP und Windows Vista können durch sorgfältige Konfiguration und Umsetzung geeigneter organisatorischer Konzepte zuverlässig vor bösartiger Software wie z.B. Viren und trojanischen Pferden geschützt werden. Der Einsatz spezieller Produkte wie z.B. Virenscanner ist hierzu nicht erforderlich.

Haben Sie weitere Fragen zum Schutz Ihrer Computer oder benötigen Sie Unterstützung bei der Erstellung und Umsetzung der beschriebenen Konzepte? Dann vereinbaren Sie einfach telefonisch einen Beratungstermin. Die Erstberatung erfolgt grundsätzlich **kostenfrei**.

Stand: 21.05.2007

Die jeweils aktuelle Version dieses Dokuments können Sie unter
www.ralph-lehmann.de/Service___Downloads/service___downloads.html

herunterladen.