itEXPERsT
Your Data Guard

5 Schritte zur IT-Sicherheit -

Wie Sie Ihre Computer gegen Hackerangriffe absichern

Einleitung

Die Absicherung von IT-Systemen ist ein komplexes und ständig aktuelles Thema, das keinesfalls auf die leichte Schulter genommen werden sollte. Hacker sind oftmals äußerst einfallsreiche und kreative Personen, ständig wechselt die Bedrohungslage. Regelmäßig werden Sicherheitslücken in Hard- und Software entdeckt, die die Betreiber der Computer in prekäre Situationen bringen.
(Mehr Infos und Beispiele auf: http://itexperst.com/b/news/vorfaelle)

Einfache und effektive Maßnahmen

Seit 2012 gibt es eine Liste mit einigen **erstaunlich einfachen** und **trotzdem effektiven Maßnahmen**, für die eine australische Forschergruppe den **nationalen US-Sicherheitspreis** des SANS-Institutes erhielt. Die Australier analysierten sämtliche zivilen und militärischen Computereinbrüche. Ihr Ziel war es, einfache und wirksame Maßnahmen zu entdecken, um Angriffe ins Leere laufen zu lassen, also mit möglichst geringen Mitteln eine möglichst breite Abdeckung der Maßnahmen gegen Cybereinbrüche zu erreichen.

Top-Effizient
Werden diese einfachen Maßnahmen umgesetzt, laufen **85%** aller Angriffe ins Leere!

Die empfohlenen Maßnahmen sind einfach und top-effizient! Werden Sie umgesetzt, laufen 85 % aller Angriffe ins Leere! Zusätzlich **kostet** die Umsetzung **nur einen Bruchteil** des Betrages, der für alle Sicherungsmaßnahmen aufgewendet werden müsste.

itEXPERsT hat mit den Erkenntnissen aus der australischen Studie und den eigenen, umfangreichen Erfahrungen 5 wertvolle Tipps für Sie zusammengestellt.

Tipp 1

Sicherheitsupdates für Betriebssysteme installieren

Jede Software, jedes Programm altert und zeigt Schwächen. In der Software wie auch im Betriebssystem werden immer wieder Sicherheitslücken entdeckt. **Durch ein regelmäßiges Sicherheitsupdate werden solche Sicherheitslücken zeitnah geschlossen.**

Hacker können innerhalb kürzester Zeit Schadsoftware entwerfen, die diese Sicherheitslücken ausnützt. Schlimmstenfalls greift ein Hacker auf Ihren Computer zu, kann jedes beliebige Programm darauf starten und Ihr System übernehmen. Dann nützt der Hacker Ihren Computer wie sein eigenes System, um z.B. Schadsoftware zu verschicken, andere Systeme anzugreifen oder schwerwiegenden Missbrauch zu betreiben.

Viele Betriebssysteme bieten bereits eine **automatische Installation** solcher Sicherheitsupdates an. Wichtig ist hier, diese sehr **zeitnah** durchzuführen. **Empfohlen werden Zeiträume bis zu 48 Stunden**, in denen die Updates eingespielt werden sollten.

Mit schlechtem Beispiel voran?
96 % aller britischen Unternehmen haben keine ausreichenden IT-Sicherheitsmaßnahmen! (http://itexperst.at/?p=6165)

Tipp 2

Sicherheitsupdates für alle Anwendungen installieren

Was für das Betriebssystem gilt, ist auch für die Anwendungen zu beachten! **Spielen Sie innerhalb von 48 Stunden Sicherheitsupdates aller Anwendungsprogramme ein.** Oft wird hierbei bestimmte Software leicht übersehen, wie z.B. Flash oder Java. Gerade diese beiden Programme werden gerne über Sicherheitslücken ausgenutzt, da oft veraltete Versionen eingesetzt werden.

Folgen der Nachlässigkeit

Hacker legen die Hälfte der weltweiten Finanztransaktionen lahm. Neben dem erschreckend hohen Anteil an Cyberangriffen wurde herausgefunden, dass das Hauptziel in der gezielten Destabilisierung der Märkte lag.

Hacker legen die Hälfte der weltweiten Finanztrans-
aktionen lahm. (Mehr dazu auf: http://itexperst.at/?p=5554)

Tipp 3

Dem Benutzer die Administratorrechte entziehen

Wenn eine Schadsoftware wie z.B. **ein Virus oder ein trojanisches Pferd (Trojaner)** einen Computer befällt, werden - unter einem normalen Anwenderkonto installiert - maximal die Benutzerdaten des Anwenders ausgelesen.

Wird jedoch **oft mit dem Administratorkonto gearbeitet, nistet sich die Schadsoftware direkt** unter diesem Administratorkonto **auf dem Rechner ein. Der Hacker übernimmt das gesamte Netzwerk.** Das ist **der schlimmste Fall für ein Unternehmen**, weil davon ausgegangen werden muss, dass die gesamte Infrastruktur befallen ist. Jeder PC, jeder Server wird verseucht, auf alle Daten wird zugegriffen. Es ist dies das **Worst-Case-Szenario** für die IT-Sicherheit und **die Schadensbehebung ist äußerst kostenintensiv.**

Lassen Sie es lieber nicht so weit kommen!
Durchschnittlicher Schaden bei einem Hackerangriff:
70.000 € bei Kleinunternehmen.
(Mehr dazu auf: http://itexperst.at/?p=5449)

Tipp 4

Whitelisting von Anwendungen

Dürfen nur bekannte Programme ausgeführt werden, ist es für Cyberkriminelle schwieriger, die Kontrolle über ein Computersystem zu erlangen. Bei der **Whitelist** handelt es sich um eine **Liste**, in **der** die **zulässigen und bekannten Programme** verzeichnet sind.

Versagt der Virenschutz, z.B. wenn unbekannte Schadsoftware auf dem Computer eingeschleust wurde, verhindert ein Wächter die Ausführung der unbekannten Schadsoftware.

Bei Windows 7 und Windows Server 2008 ist dieses Whitelisting eingebaut, es nennt sich **Applocker**. Das **Blockieren von unbekannter Software** ist möglich.

> *Es kann jeden treffen:*
>
> *Die CME-Gruppe, größte Finanz- und Derivatbörse in Chicago, USA, hat bekannt gegeben, dass ein Angriff im Juli dieses Jahres private Kundeninformationen gefährdete.*

Einbruch bei der CME-Gruppe
(Mehr Info auf: http://itexperst.at/?p=6261)

Tipp 5

Führen Sie Penetrationstests durch

Wissen Sie, ob alle Sicherungsmaßnahmen zu Ihrer Zufriedenheit durchgeführt wurden? Gibt es noch irgendwo Sicherheitslücken in Ihren Systemen?

Haben Sie alle Möglichkeiten und Maßnahmen für Laien ausgeschöpft, sind Sie zwar schon wesentlich sicherer, doch **zur absoluten IT-Sicherheit benötigen Sie** einen Experten – am besten **itEXPERsT!**

Bedenken Sie die Folgen einer mangelhaften IT-Sicherheit!
Angenommen, ein Hacker bricht in Ihren Computer zur Verwaltung der Benutzerrechte (Domaincontroller) ein ...
Angenommen, ein Hacker verschafft sich Zugang zu Ihren Kundendaten und missbraucht diese für illegale Geschäfte ...
Wie massiv ist Ihr Schaden? Der finanzielle, der emotionale, der zukünftige ...
(Vertrauensverlust Ihrer Kunden, Haftungsproblematik etc.)

Gehen Sie kein Risiko ein!

Alle Ihre Systeme werden von uns getestet, um mögliche Einbruchswege aufzuzeigen. Ihr IT-Netzwerk wird auf alle bekannten Sicherheitslücken überprüft. **Das höchste Niveau an IT-Sicherheit** für Ihr Unternehmen! – Zu hoch für herkömmliche Hacker.

Dipl. Ing. Christian Perst, Hackerabwehr und Datendetektiv,
SANS zertifizierter Incident Handler und digitaler Forensiker,
Gerichtlich zertifizierter Sachverständiger

10 gute Gründe, itEXPERsT zu beauftragen

1. Sie haben wichtige Kundendaten in Ihren Systemen gespeichert, für die **Sie haften.** Sie wissen, dass das Sicherheitsrisiko im IT-Bereich ohne entsprechende Maßnahmen nahezu explosionsartig steigt.
2. **Sie können es sich nicht leisten**, wenn **Ihre Systeme** für Stunden oder auch Tage **zum Erliegen** kommen.
3. **Sie sind zu intelligent**, um sich auf ein **unkalkulierbares Sicherheitsrisiko** einzulassen.
4. **Sie wollen** für Ihre Daten und deren Sicherheit **nur das Beste/den Besten.**
5. Sie haben noch nie einen sogenannten Penetrationstest durchführen lassen und haben somit keine Ahnung, ob **Ihr System wirklich sicher ist**.
6. Sie wollen Viren, Trojanern und Hackern **immer einen Schritt voraus sein.**
7. **Sie sind** lieber **vorher klüger** als nachher.
8. **Sie schätzen** Menschen und Unternehmen mit **sozialer Verantwortung.**
9. **Sie wollen keinesfalls als Katastrophenmeldung** und Opfer unter den News aufscheinen.
10. Sie beauftragen ausschließlich Leute, die **engagiert**, **erfahren**, **äußerst gründlich** und **absolut zuverlässig** sind und nicht eher ruhen, bevor Sie nicht zu **100% zufrieden** mit dem Ergebnis sind!

Der Kontakt

Dipl. Ing. Christian Perst

SANS zertifizierter Incident Handler und digitaler Forensiker
Gerichtlich zertifizierter Sachverständiger

Rupert-Gugg-Str. 53
A-5280 Braunau

tel.: +43 / 77 22 / 98 200
mobil: +43 / 699 / 18 19 94 63
E-Mail: christian.perst@itEXPERsT.at
www.itEXPERsT.at

itEXPERsT – EXPERsT YOUR IT!

Version 1.3, Stand 12.02.2015