Computersicherheit

Qualifizierter Selbstschutz : 11 Schritte zum sicheren Rechner. Dieser Text erklärt, wie Sie Ihren eigenen Computer gegen Angriffe aus dem Netz und gegen Datenverlust absichern.

Ein sicherer Computer ist die Voraussetzung für sicheres Arbeiten im Internet. Die Aufgabe, die eigenen Dateien und den eigenen Rechner zu schützen, ist nicht delegierbar. Ohne qualifizierten Selbstschutz gibt man sich einer Illusion hin. Man muss sich selbst um die eigene Sicherheit kümmern, und man muss vorbeugen. Bildlich gesagt: Wenn es brennt, muss man wissen, wo der Feuerlöscher ist, den man sich vorher beschafft haben muss . Und für den Abschluß einer Feuerversicherung ist es dann definitiv zu spät!

Sicherheit umfasst verschiede Aspekte: den Schutz der eigenen Daten vor Verlust, vor Veränderung und vor unbemerktem Zugriff durch Fremde. Die Sicherung der eigenen Arbeitsfähigkeit - das jederzeitige Funktionieren des Computers - und schließlich den Schutz des eigenen Rechners vor Mißbrauch.

Das Wichtigste sind die eigenen Daten, die auf dem Rechner gespeichert sind. Sie sind bei einem Totalverlust (durch Crash, Diebstahl, Feuer oder anderes) nicht mehr rekonstruierbar, wenn keine Vorsorge getroffen wurde. Hard- und Software wiederzubeschaffen, ist eine Zeit- und Geldfrage.

Was kann Ihnen passieren?

Sie müssen sich gegen verschiedene Szenarien absichern, z.B.:

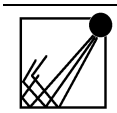
- ✓ Datenverlust durch Schäden (z.B. Festplattencrash)
- ✓ Kompletter Verlust des Computers / Speichermediums (z.B. durch Brand, Diebstahl, Beschlagnahme - in letzteren Fällen hätten Fremde Zugriff auf die eigenen Daten)
- ✓ Krimineller Angriff aus dem Netz / Online-Durchsuchung

Methoden von Angriffen

Neben dem physichen Zugriff auf den Computer sind es vor allem E-Mails mit Schadsoftware (in Anhängen, aber auch in der Mail selbst), infizierte Webseiten und infizierte Dateien (vor allem PDFs), die Angriffe ermöglichen.
Einen detallierten Überblick bietet der
"Gefährdungskatalog 5: Vorsätzliche Handlungen"
https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/g/g05/g05.html .
aus dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html .

Ziele von Angriffen

- ✓ Überwachung des Computers und seiner Nutzer
- ✓ mißbräuchliche Nutzung des Rechners (z.B. für Spam-Versand / Speicherung von Dateien)
- ✓ Ausspähen verwertbarer Daten (z.B. Kontoinformationen)
- ✓ Erpressung (Verschlüsselung von Daten, Entschlüsselung gegen Geld)
- ✓ Ausspähung (Gegenrecherche)



Albrecht Ude
Lehderstraße 53 — 13086 Berlin — Germany
www.ude.de — albrecht@ude.de

07.12.2011

11 Schritte zum sicheren Computer

In einer Stellungnahme zur "Online-Durchsuchung" für das Bundesverfassungsgericht hat Dirk Fox (Secorvo Security Consulting GmbH) beschrieben, wie Computer gegen Angriffe aus dem Netz abgesichert werden können:
Stellungnahme zur "Online-Durchsuchung" - Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07 / von Dirk Fox, Secorvo Security Consulting GmbH
Version 1.1, Stand 29. September 2007
http://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-onlinedurchsuchung.pdf .

Dirk Fox schlägt sieben Maßnahmen vor, denen ich vier weitere anfüge.

1. Patchen des Betriebssystems und der Programme

Jedes Betriebssystem hat Lücken ("Exploits"), die für Angriffe genutzt werden können. Um die Lücken zu schließen, veröffentlichen die Hersteller Sicherheitsupdates ("Patches", Flicken).Installieren Sie diese regelmäßig. Alle modernen Betriebssysteme können Sie so konfigurieren, dass das entweder automatisch passiert oder sie jeweils benachrichtigt werden und dann entscheiden können.

Das gleiche gilt für alle Programme, die Sie einsetzen, um fremde Daten und Dateien zu öffnen, also vor allem den Webbrowser, das Mailprogramm und den PDF-Viewer. Jedes dieser Programm hat Fehler und Lücken. Spielen Sie Patches und Updates regelmäßig ein, sorgen Sie mindestens dafür dass Sie automatisch benachrichtigt werden.

2. Restriktive Konfiguration des Systems

Nutzen Sie den Administrator-Account (der umfassende Rechte hat) nur, um den Rechner (offline) zu konfigurieren und Programme zu installieren.
Um ins Netz zu gehen, nutzen Sie einen Account mit eingeschränkten Nutzerrechten. Sollte ein Angreifer diesen kapern, könnte er dennoch keine Programme installieren o.ä.

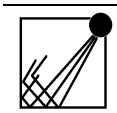
Sichern Sie jeden Account durch ein starkes Password. Hilfreich dabei ist der Passwordcheck des schweizer Datenschutzbeauftragten
https://passwortcheck.datenschutz.ch/check.php .
(Anmerkung: Geben Sie dort nie ein echtes Password ein, sondern eine Zeichenkette, die strukturell gleich ist, also z.B. statt "`aBc123`" etwa "`dEf456`".)

Ebenso wichtig: Das Entscheidende an einem Passwort ist seine Länge:
http://recherche-info.de/2011/12/02/vergesst-passworter-nehmt-pass-satze/ .

3. Restriktive Konfiguration des Browsers

Konfigurieren Sie Ihrenn Webbrowser restriktiv! Unterbinden Sie das Ausführen aller "aktiven Inhalte" wie Java, Javascript etc.
Für den Firefox-Webbrowser gibt es viele kleine Zusatzprogramme ("Addons"), mit denen man die eigene Sicherheit erhöhen kann:
http://www.mozilla.org/de/firefox/new/ ,
https://addons.mozilla.org/de/firefox/ .

Sammlung datenschützender Firefox Erweiterungen (Privacyfoundation)



Albrecht Ude
Lehderstraße 53 — 13086 Berlin — Germany
www.ude.de — albrecht@ude.de

07.12.2011

http://www.privacyfoundation.de/service/firefox_erweiterungen/ .

Firefox-Erweiterungen für Rechercheure:
http://recherche-info.de/internet-recherche-linkliste/firefox-erweiterungen-fuer-rechercheure/ ,

4. Nutzung eines Virenscanners

Setzen Sie stets ein Antivirenprogramm ein und aktualisieren Sie es regelmäßig. Ein Antivirenprogramm, dessen Signaturdatei (anhand derer es Viren erkennt) über einen Monat alt ist, bietet keinen ausreichenden Schutz mehr.
Da auch Virenscanner Lücken haben können, sollten Sie gelegentlich das Programm wechseln. Verwenden Sie auch ein Programm gegen Spionageprogamme ("Spyware").
Konfigurieren Sie den Virenscanner so, dass alle Dateien geprüft werden, und schalten Sie ihn niemals aus.

Gute Programme finden Sie z.B. im Software-Archiv des Heise-Verlages
http://www.heise.de/software/ .

5. Sicherheitssensibler Umgang mit E-Mails

Konfigurieren Sie Ihr Mailprogramm so, dass E-Mails (zunächst) nur als reiner Text dargestellt werden. Unterbinden Sie den Empfang von E-Mails im HTML-, im DOC- oder im RTF-Format. Damit verhindern Sie das Ausführen von Schadcode und Spionage durch das Nachladen von Dateien.
Wo möglich, lesen Sie E-Mails nur offline, so dass keine Dateien unbemerkt aus dem Netz geladen werden können.
Gehen Sie besonders vorsichtig mit Downloads und Dateianhängen von Mails (Attachments) um. Löschen Sie unverlangte oder nicht beschriebene Anhänge unverzüglich (ggfs. beim Absender nachfragen)
Öffnen Sie Dateien in Mailanhängen mit Viewern (die keinen Programmcode ausführen können) statt mit den Programmen (z.B. Word, Acrobat) selbst.

Word Viewer - Anzeigen, Drucken und Kopieren von Word-Dokumenten ohne Word-Installation.
http://www.microsoft.com/downloads/de-de/details.aspx?familyid=3657CE88-7CFA-457A-9AEC-F4F827F20CAC&displaylang=de .

Website mit diversen freien PDF-Readern:
http://pdfreaders.org/ .

Online Sicherheitscheck für Mailprogramme vom Heise-Verlag
http://www.heise.de/security/dienste/Emailcheck-2109.html .

Eine Empfehlung: Das Open-source Mailprogramm Thunderbird, für dass es zahlreiche Addons gibt:
https://www.mozilla.org/de/thunderbird/ .
https://addons.mozilla.org/de/firefox/ .
Dies Mailprogramm ermöglicht die Einbindung von sicherheitsrelavanten Programmen und Verschlüsselungswerkzeugen.

Albrecht Ude
Lehderstraße 53 — 13086 Berlin — Germany
www.ude.de — albrecht@ude.de

6. Scharfe Einstellung der Personal Firewall

Eine Firewall überwacht alle Außenkontakte Ihres Rechners; sie kontrolliert, welche Programme Daten senden oder empfangen dürfen. Mittlerweile sind Firewalls eine Komponente jedes Betriebssystems.
Konfigurieren Sie die Firewall scharf: Kein Außenkontakt ist erlaubt, außer jenen, die Sie explizit gestatten (z.B. Webbrowser und Mailprogramm).

Umfangreicher Eintrag zu Firewalls im Wiki des Hackerboard:
http://wiki.hackerboard.de/index.php/Firewall .

7. Einsatz einer Virtuellen Maschine

Eine Virtuelle Maschine (VM) ist eine Kopie der Konfiguration des Computers im Arbeitsspeicher - sozusagen ein Rechner im Sandkasten. Die Virtuelle Maschine wird jedesmal neu aufgebaut, wenn der Computer neu gestartet wird. Das bedeutet, dass alle Schadprogramme nur so lange wirksam sind, solange dieselbe VM läuft. Bei jedem Neustart des Systems wird schädliche Software entfernt.

Wikipedia-Eintrag mit Links auf Produkte:
http://de.wikipedia.org/wiki/Virtuelle_Maschine .

8. Regelmäßig Backups machen

Legen Sie regelmäßig - am Besten am Ende jedes Arbeitstages - Sicherheitskopien an. Speichern Sie diese nicht nur auf Ihrer Festplatte, sondern auch auf einem externen Medium, z.B. auf einer externen Festplatte.
Es ist sinnvoll, Backups an einem anderen Ort aufzubewahren als dort, wo sich Ihr Computer befindet. Externe Festplatten bieten sich auch an, um Images, Backups und sensible Dateien in einem Bankschließfach oder an einem anderen sicheren Ort zu verwahren.
Neben Backups lohnen

- ✓ Klarkopien der eigenen Daten auf externem Medium
- ✓ Mirrors der eigenen Festplatte auf externem Medium

Wikipedia-Eintrag:
http://de.wikipedia.org/wiki/Backup .

9. Image-Programme

Image-Programme ermöglichen es, alle Dateien eines Mediums (also hier: einer Festplatte bzw. Partition) in einer einzigen Datei zu speichern und zu komprimieren - das Image ist also kleiner als das so gesicherte Medium.
Alle modernen Betriebssysteme haben dieses Feature.
Images sind de facto eine Zeitmaschine. Wenn Sie neue Programme probehalber installieren, erstellen Sie vorher ein Image. Wenn die Programme nicht gefallen, wird nicht deinstalliert (was oft nur mangelhaft funktioniert), sondern das Image eingespielt. Das ist wie ein Zeitsprung, als hätten Sie das Programm nie installiert.

Wikipedia-Eintrag:
http://de.wikipedia.org/wiki/Image_(Informatik) .

10. Speichermedien verschlüsseln

Verschlüsseln Sie Ihre Speichermedien, vor allem die interne Festplatte. Dies ist besonders wichtig bei Laptops und transportablen Geräten, damit im Fall des Diebstahls oder der Beschlagnahme niemand Zugriff auf Ihre Daten hat.
Nutzen Sie das Open-Source-Programm Truecrypt, um die gesamte Festplatte und externe Festplatten zu verschlüsseln:
http://www.truecrypt.org/ .

11. Bleiben Sie informiert und kritisch

Egal, welche Programme Sie einsetzen: Informieren Sie sich regelmäßig über Sicherheitslücken und Sicherheitsfragen. Dabei helfen einige Newsletter und Websites:

Täglicher Newsletter des Heise-Verlages
http://www.heise.de/newsletter .

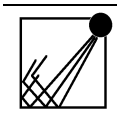
Wöchentlicher Newsletter "Heise Security Summary"
http://www.heise.de/bin/newsletter/listinfo/heisec-summary .

Vierzehntägiger Newsletter "Sicher Informiert" des BSI für Bürger
http://www.bsi-fuer-buerger.de/newsletter/index.htm .

Das Infoportal des Bundesamtes für Sicherheit in der Informationstechnik für "normale" Nutzer
http://www.bsi-fuer-buerger.de/ .

heise Security – News, Dienste und Foren zum Thema Computer-Sicherheit
http://www.heise.de/security/ .

Diese Zusammenstellung ist (bei weitem) nicht vollständig, sondern stellt lediglich eine erste Annäherung an das Thema dar.
Ich bin an Ergänzungen und Korrekturen sehr interessiert und freue ich über jede Mail:
albrecht@ude.de .



Albrecht Ude
Lehderstraße 53 — 13086 Berlin — Germany
www.ude.de — albrecht@ude.de

07.12.2011