So viel Schutz muss sein!

So sollten Sie Ihren privaten Rechner mindestens absichern.
Ein Leitfaden für Endanwender.
Bitte unbedingt umsetzen!

Stand: 26.07.2012

Lizenz: CC BY NC SA

antago

Lizenz dieses Dokuments: creative commons

- Sie dürfen:
  - das Werk bzw. den Inhalt vervielfältigen, verbreiten und öffentlich zugänglich machen
  - Abwandlungen und Bearbeitungen des Werkes bzw. Inhaltes anfertigen
- Zu den folgenden Bedingungen:

<u>Namensnennung:</u>
Sie müssen den Namen des Autors/Rechteinhabers in der von ihm festgelegten Weise nennen
(Antago GmbH, Nennung mit Name, Logo und Link auf https://www.antago.info)

<u>Keine kommerzielle Nutzung:</u>
Dieses Werk bzw. dieser Inhalt darf nicht für kommerzielle Zwecke verwendet werden.

<u>Weitergabe unter gleichen Bedingungen:</u>
Wenn Sie das lizenzierte Werk bzw. den lizenzierten Inhalt bearbeiten oder in anderer Weise erkennbar als Grundlage für eigenes Schaffen verwenden, dürfen Sie die daraufhin neu entstandenen Werke bzw. Inhalte nur unter Verwendung von Lizenzbedingungen weitergeben, die mit denen dieses Lizenzvertrages identisch oder vergleichbar sind.

cc BY NC SA

Dürfen wir uns vorstellen?

Antago: Unternehmen und Portfolio

antago

Was bietet Ihnen Antago?

- Die Antago GmbH ist ein europaweit tätiges Unternehmen im Bereich der IT- und Informationssicherheit. Wir sorgen für die strukturierte, bedarfsorientierte Absicherung von Informationen.
- Unabhängig, kompetent und fair bieten wir Ihnen:
  - Security Scans und Penetrationstests
    Kompetente Sicherheitsuntersuchungen inkl. Risikoanalyse und Maßnahmenkatalog
  - Informationssicherheitsmanagmentsysteme (ISMS)
    Analyse und Erarbeitung bedarfsorientierter Sicherheitskonzepte
    (auch gem. IT-Grundschutz / ISO 27001)
  - Risikoanalysen und Sicherheitskonzepte
    Bedarfsorientierte Sicherheit: „So wenig wie möglich, so viel wie nötig!“.
  - Security Awareness
    Sensibilität im Unternehmen schaffen – die Sicherheitslücke Nr. 1 adressieren.
  - Livehackings und Schulungen
    Know-How aus erster Hand.

Einleitung

Was erwartet Sie?

Was erwartet Sie?

- Auf den folgenden Seiten finden Sie einfache Maßnahmen, die Sie als Privatanwender unbedingt ergreifen sollten, um Ihren Rechner und Ihre Daten angemessen abzusichern.
- Alle wichtigen Maßnahmen haben wir mit einem Kasten versehen (☐). Machen Sie einfach einen Haken, wenn Sie sie umgesetzt haben.
- Natürlich kennen wir Ihre Sicherheitsbedürfnisse nicht im Detail – deshalb können wir hier nur den absoluten Basisschutz darstellen, der absolut überall vorhanden sein sollte.
- Bei Firmennetzen und bei besonderen privaten Systemen gilt:
  - Sie benötigen ein maßgeschneidertes, auf Ihre Sicherheitsbedürfnisse abgestimmtes Konzept! Bitte denken Sie in diesem Fall an uns.

Ein paar offene Worte

- Dieses Papier bietet Ihnen eine Hilfestellung und wurde von uns mit großer Sorgfalt erarbeitet. Dennoch gilt:
  - Dieses Papier ist kein Ersatz für den gesunden Menschenverstand.
  - Dieses Papier kann Fehler enthalten.
    Bitte kontaktieren Sie uns, wenn Sie einen Fehler entdecken.
  - Dieses Papier kann unvollständig sein.
    Bitte kontaktieren Sie uns, wenn ein wichtiges Thema fehlt.
  - Dieses Papier veraltet.
    Schauen Sie öfter auf unserer Webseite vorbei.
  - Wir übernehmen keine Gewährleistung für die in diesem Papier aufgeführten Empfehlungen und Softwareprodukte.

Schritt für Schritt – so geht’s!

Antago: Sicherheit ist einfach!

Das Wichtigste zuerst: Datensicherung! (I)

- Die wichtigste Sicherheitsmaßnahme ist und bleibt die Datensicherung!
- Ihr PC/Laptop/iPhone/Handy/... wird ganz sicher irgendwann kaputt gehen und Ihre Urlaubsfotos und -videos, Ihre Briefe, e-Mails und Steuererklärungen mit ins digitale Grab nehmen.
- In aller Regel geschieht dies zum denkbar ungünstigsten Zeitpunkt.

- Sichern Sie deshalb wichtige Daten zeitnah nach bedeutenden Änderungen. Ggf. ist das sogar mehrmals am Tag sinnvoll (z.B. wenn Sie gerade an einer wichtigen Arbeit schreiben).
- Sichern Sie nicht nur Ihre Daten, sondern führen Sie auch in regelmäßigen Abständen eine komplette Sicherung Ihrer Systeme durch (Vollbackup!). Damit sichern Sie die Daten, die installierten Programme, das Betriebssystem und alle Konfigurationsdateien. So stellen Sie sicher, dass Sie nichts Wichtiges übersehen und dass Sie im Falle eines Falles schnell und relativ mühelos wieder arbeitsfähig sind.
- Sichern Sie ausnahmslos alle Systeme, auf denen sich wichtige Daten befinden (könnten)! Vergessen Sie nicht Ihre kleinen digitalen Helfer wie iPhone, Handy, Laptop und Co.!

Das Wichtigste zuerst: Datensicherung! (II)

- Führen Sie Datensicherungen auf einem speziell dafür angeschafften Datenträger durch.
  - Verwenden Sie nicht die lokale Festplatte zur Datensicherung.
  - Verwenden Sie keine USB-Sticks für die Datensicherung – diese Medien sind chronisch unzuverlässig. Verwenden Sie z.B. eine externe USB-Festplatte.
- Heben Sie nicht nur eine Sicherung Ihrer Daten auf, sondern mehrere Generationen davon. Falls im Falle eines Falles eine Sicherung defekt ist, sind die Daten dennoch nicht verloren.
- Testen Sie, ob die Datensicherung auch wirklich funktioniert (das ist leider seltener der Fall als Sie annehmen...).
- Für ganz Vorsichtige oder für wirklich wertvolle Daten gilt:
  - Lagern Sie eine Kopie der Datensicherung außerhalb Ihres Hauses.
  - Verschlüsseln Sie Ihre Datensicherung, wenn Sie vertrauliche Daten besitzen.

Sichere Passwörter – so geht's ganz einfach!

- Unsichere Passwörter wie z.B. „123456“, „pAssw0rt“, „Liebe123“ etc. können von Bösewichtern leicht erraten werden – oft mit fatalen Folgen!
- Aber auch das ist wahr: Zu komplizierte Passwörter werden schnell vergessen.
- Wie baut man sich ein sicheres Passwort, an das man sich garantiert erinnert? Hier eine ganz einfache aber wirkungsvolle Anleitung:
  - Denken Sie sich einen Satz aus, z.B. „Am 24.12. ist Weihnachten.“
  - Stellen Sie nun die Anfangsbuchstaben der Wörter, die Ziffern und Satzzeichen hintereinander (bei unserem Beispiel: A24.12.iW.)
- Das Passwort ist sehr sicher, aber Sie werden es garantiert nicht vergessen - der Satz bleibt im Gedächtnis!
- Wenn Sie sich viele Passwörter merken müssen, können Sie einen Passwort-Safe verwenden. Diese Programme heben Ihre Passwörter sicher auf und sie müssen sich nur ein Passwort (das für den Safe) merken. Am Ende des Vortrags finden Sie einen Link zum Herunterladen eines Passwort-Safes.

Windows absichern!

- Nicht als Administrator arbeiten!
  Arbeiten Sie nicht als Administrator auf Ihrem PC, wenn es nicht unbedingt sein muss (das ist nur ganz selten der Fall). Legen Sie sich ein eigenes Benutzerkonto mit eingeschränkten Rechten an und verwenden Sie dieses. Wenn etwas schief gehen sollte, bleibt der Schaden begrenzt.
- Updates, Updates, Updates!
  Führen Sie in regelmäßigen Abständen ein Update von Windows durch. Aktivieren Sie am besten die automatischen Windows-Updates. Erkannte Sicherheitsmängel in Windows werden dadurch behoben.
- Personal Firewall nutzen!
  Verwenden Sie die Firewall von Windows (die ist wirklich gut)! Wenn Ihr Betriebssystem keine eigene Firewall besitzt, so installieren Sie eine (beliebige andere und einigermaßen bekannte) Personal Firewall aus dem Netz. Die gibt es für Privatanwender kostenfrei (Wo? Siehe letzte Seite).

Oft vergessen: Bitte gesamte Software aktuell halten!

- Über die Windows Updates wird nur die Software von Microsoft aktuell gehalten - Lücken in anderen Programmen werden nicht gestopft. Angreifer wissen das und attackieren Systeme zunehmend über diesen Weg.
- Sorgen Sie deshalb unbedingt dafür, dass auch jene Software auf Ihrem Rechner aktuell bleibt, die nicht von Microsoft stammt (Java, Acrobat Reader, Open- bzw. LibreOffice, Thunderbird, Firefox, ...):
  - Informieren Sie sich, wie Ihre Anwendungssoftware mit Updates versorgt werden kann.
  - Wenn Software über die Funktion für automatische Updates verfügt, aktivieren Sie sie.
  - Prüfen Sie in regelmäßigen Abständen, ob die Software auf Ihrem Rechner noch aktuell ist. Auf der letzten Seite finden Sie den Link zu einem Tool, mit dem Sie die Aktualität Ihrer gesamten Software leicht prüfen können.
  - Führen Sie in regelmäßigen Abständen (alle ein bis drei Monate) ggf. per Hand ein Update durch.
- <u>Es gilt also auch hier:</u> Updates, Updates, Updates!

Achten Sie besonders auf Ihren Browser!

- Webbrowser sind besonders gefährdet, weil sie beliebige Inhalte aus dem Internet herunterladen und interpretieren.
- Mittlerweile hat sich eine ganze kriminelle Industrie auf die Lücken in Browsern spezialisiert und verdient Geld, indem sie Systeme über die Webbrowser mit Adware (Software, die unerwünscht Werbeeinblendungen generiert) bzw. Spyware (Software, die den Benutzer ausspioniert) infiziert. Diese lästige bzw. hoch gefährliche Form der Software wird verwundbaren Browsern auf speziell dafür präparierten Webseiten untergeschoben.

- Achten Sie deshalb unbedingt darauf, dass Ihr Webbrowser auf dem neuesten Stand ist. Verwenden Sie insbesondere nicht mehr den Internet Explorer 6, sondern entweder den aktuellsten Internet Explorer oder einen alternativen Browser (z.B. den Mozilla Firefox) in der aktuellsten Version!
- Denken Sie an die Plugins in Ihrem Webbrowser – Lücken in diesen Programmen stellen ein Einfallstor dar, weil sie ein Bestandteil des Browsers sind. Eine traurige Berühmtheit ist übrigens seit längerem der Flashplayer von Adobe...

- <u>Es gilt auch hier wieder einmal:</u> Updates, Updates, Updates!

Vorsicht vor fremden Programmen!

- Installieren Sie keine Programme, die Ihnen im Netz angeboten bzw. aufgedrängt werden (z.B. durch eingeblendete Werbung oder Gewinnspielen auf Webseiten).
- Installieren Sie keine Programme, über die Sie sich nicht (z.B. durch eine kurze Google-Recherche) informiert haben.
- Beherzigen Sie immer die folgenden Grundsätze:
  - Nicht aktiv danach gesucht? Wird nicht installiert!
  - Nicht darüber informiert? Wird nicht installiert!
- Diese Empfehlungen gelten vor allem für Antivirus-Programme. Es werden mittlerweile eine ganze Menge gefälschte Antivirus-Programme im Netz angeboten. Installieren Sie nur eine Antivirus-Software eines namhaften Herstellers!

Rechner vor Schadsoftware schützen! (I)

- Installieren Sie eine Antivirus-Software. Die gibt es von vielen namhaften Herstellern für Privatanwender kostenfrei zum Herunterladen (Wo? Siehe letzte Seite).
- Lassen Sie die Anti-Virus-Software permanent im Hintergrund laufen, damit Schädlinge umgehend entdeckt, bekämpft und entsorgt werden können.
- Führen Sie regelmäßig ein Update des Virenscanners durch. Am besten soll das der Virenscanner selbst erledigen (Automatische Updates gibt es bei jedem guten Virenscanner!).

Rechner vor Schadsoftware schützen! (II)

- Schalten Sie die e-Mail-Filterung Ihres Mailkontos ein. Die allermeisten Viren, Trojaner und SPAM-Mails werden so entsorgt, noch bevor sie auf Ihren Rechner gelangen (das spart Zeit und Nerven).
- Klicken Sie nicht auf Mail-Anhänge (Attachments), die Sie von unbekannten Absendern erhalten – auch wenn die Begründung dafür noch so gut (oder abenteuerlich) sein sollte. Diese Attachments sind alle böse, hinterhältig und gemein oder bestenfalls unglaublich unwichtig.
- Seien Sie besonders misstrauisch bei Anhängen, die ausführbare Programme enthalten (*.exe, *.com, *.vbs, *.bat, *.scr, *.pif, ...).

Lästige Werbemails (SPAM) vermeiden!

- Geben Sie Ihre Mailadresse nicht leichtfertig weiter und veröffentlichen Sie Ihre Mailadresse nicht auf Webseiten.
  Spammer suchen hier gezielt nach Opfern.
- Viele Webseiten verlangen bei einer Registrierung die Eingabe einer Mailadresse. Geben Sie hier nicht Ihre eigentliche Adresse an, sondern legen Sie sich für diese Fälle eine spezielle Mailadresse zu (z.B. „ihr.name_spamfalle@irgendein-mailprovider.com“).
- Kaufen Sie keine in SPAMs beworbenen Produkte.
  Sie ernähren sonst die SPAM-Versender.
- Antworten Sie niemals auf SPAM und klicken Sie niemals auf Links in SPAM-Mails („Wenn Sie keine Mails mehr erhalten wollen, klicken Sie hier!“). Sonst weiß der SPAM-Versender, dass Sie seine Mail gelesen haben und Sie erhalten nur noch mehr SPAM.

Seien Sie verschlüsselt unterwegs!

- Verwenden Sie – wann immer dies möglich ist – beim Arbeiten im Internet Protokolle, die Ihre Daten verschlüsselt übertragen.
- Protokolle mit Verschlüsselung erkennt man am zusätzlichen „S“ im Namen (POP3S statt POP3 , IMAPS statt IMAP, SMTPS statt SMTP, HTTPS statt HTTP, ...) und sorgen dafür, das sensible Informationen (wie z.B. Ihre Passwörter) sicher über das Internet übertragen werden.
- Fragen Sie Ihren Provider nach der Möglichkeit, verschlüsselte Protokolle beim Versenden und Abholen von e-Mails (POP3S / IMAPS und SMTPS) zu verwenden! Ein guter Provider wird Ihnen diese Protokolle zur Verfügung stellen.
- Versenden Sie keine sensiblen Daten (PINs, TANs, Passwörter, Kreditkarten-Nummern etc.) unverschlüsselt - also z.B. niemals per Mail oder beim Besuch einer normalen Webseite (http://...).

Wireless LAN sichern!

- Verschlüsseln Sie Ihr Wireless LAN richtig
  - Betreiben Sie niemals Ihr Wireless LAN unverschlüsselt.
  - Benutzen Sie nicht die veraltete Verschlüsselung „WEP“.
  - Nutzen Sie die Verschlüsselung „WPA2“ oder zumindest „WPA“.
  - Kaufen Sie notfalls ein Gerät, das WPA2 bzw. WPA unterstützt!
- Wechseln Sie den voreingestellten Namen des Wireless-Netzes.
- Auch bei Wireless LAN gilt: Gutes Passwort wählen!
  Wählen Sie als Netzwerk-Passwort keine leicht zu erratenden Namen oder Zeichenketten (wie z.B. „12345678“, „qwertzuiop“ oder „geheimnisvoll“) - böse Menschen erraten diese Passwörter leicht.
- Setzen Sie keine MAC-Filter ein.
  Diese Filter machen nur Arbeit und lassen sich sehr leicht umgehen.

DSL-Router sichern

- Setzen Sie ein eigenes Passwort für die Konfigurationsoberfläche Ihres Routers. Verwenden Sie dabei keine einfachen Passwörter (wie „start“, „12345“ oder „geheim“) - diese werden leicht erraten.
- Kontrollieren Sie die Einstellungen des Routers:
  Ist die Fernwartung wirklich deaktiviert?
- Kontrollieren Sie die Einstellungen des Routers:
  Sind wirklich keine Maschinen für den Zugriff von außen freigegeben? Das Feature nennt sich meistens „DMZ-Host“ oder „Server im internen Netz“ o.ä..
  Hier dürfen keine Rechner oder IP-Adressen eingetragen sein.
- Wenn Sie einen Zugriff von außen erlauben müssen oder wollen, dann bitte nur für einige wenige und sorgfältig ausgewählte Ports.
- Wenn Sie nicht wissen, was ein Port, eine IP-Adresse oder Fernwartung ist:
  Finger weg! Fragen Sie jemanden, der sich auskennt.

Datenträger säubern!

- Bevor Sie ein gebrauchtes elektronisches Gerät (Rechner, Laptop, Digitalkamera, USB-Stick, iPod, Blackberry, Handy, Drucker, ...) verschenken, verkaufen oder verleihen, sollten Sie die Datenträger in diesen Geräten gründlich löschen.
- Ein einfaches Löschen bzw. ein einfaches Formatieren reicht nicht aus. Einfach gelöschte Daten oder einfach formatierte Datenträger können umgehend wieder lesbar gemacht werden.
- Verwenden Sie entsprechende Programme, die Daten gründlich (durch – ggf. mehrfaches - Überschreiben) löschen.
- Diese Programme gibt es kostenlos im Netz (siehe letzte Seite).

Mobile Geräte schützen!

- Mobilen Geräte (Laptops, mobile Festplatten, Smartphones usw.) können verloren/geklaut werden. Fremde besitzt dann Ihr Gerät und – was meistens noch schlimmer ist - Ihre Daten!

- Verschlüsseln Sie die Datenträger von mobilen Geräten, wenn auf ihnen persönliche oder vertrauliche Informationen gespeichert sind. Das geht sehr einfach und Programme zum Verschlüsseln von Festplatten, Laptops und USB-Sticks gibt es kostenlos im Netz (siehe letzte Seite).

- Nicht alle mobilen Geräte unterstützen die Verschlüsselung der lokalen Daten.
  Achten Sie beim Kauf eines Gerätes auf dieses wichtige Feature.
  Fragen Sie nach und bestehen Sie vor dem Kauf auf eine Antwort!

- Bei Laptops gilt: BIOS-Passwort und Festplattenkennwort setzen!
  Dadurch können Fremde gefundene oder gestohlene Geräte nicht verwenden.

- Bringen Sie an allen mobilen Geräten einen Aufkleber mit (anonymen) Kontaktdaten an und versprechen auf dem Aufkleber einen großzügigen Finderlohn.
  Verlorene und geklaute Geräte kommen dann häufig zum Besitzer zurück... (vor allem, wenn sie aufgrund der Sicherheitsmaßnahmen vom Finder oder Dieb nicht benutzt oder verkauft werden können).

Eigene Daten schützen!

- Zu Schluss einige kurze Worte über das Schützen eigener Daten – hier wird aktuell viel zu viel falsch gemacht!

- Veröffentlichen Sie nur solche Daten über sich im Netz (z.B. auf Facebook, Twitter, der eigenen Homepage, Foren usw.), die Sie auch auf Plakatwände in der Innenstadt Ihres Wohnorts (zusammen mit Ihrer Anschrift) schreiben würden.
- Legen Sie Ihre Accounts in sozialen Netzen etc. nur unter einem Pseudonym an.
- Prüfen Sie vor der Weitergabe von Daten, Fotos, Filmen etc. genau, was Sie gerade tun. Hier gilt: Einmal veröffentlicht – für immer außerhalb Ihrer Kontrolle.
- Seien Sie vorsichtig, mit wem Sie Gespräche über welche Themen über die Webcam führen. Ihr Gegenüber kann Sprache und Bild unbemerkt aufnehmen. Diese Aufnahmen können ggf. gegen Sie verwendet werden. Dies gilt vor allem für sexuelle Inhalte.
- Sprechen Sie mit Ihren Kindern über diese Themen.

Fazit

Können Sie jetzt beruhigt sein?

Jetzt können Sie beruhigt sein!?

- Die Empfehlungen der letzten Seiten sind für den normalen Endanwender in aller Regel völlig ausreichend.
- Ihr Computer ist nach der Umsetzung der Maßnahmen zwar kein Fort Knox. Er ist aber so sicher, dass sich jene Angreifer, die an ihrem Computer Interesse haben, die Zähne ausbeißen werden.
- Wenn Sie ein Unternehmen absichern wollen oder wenn Sie ein erhöhtes Sicherheitsbedürfnis haben (weil z.B. auf Ihrem Rechner besonders vertrauliche Daten gespeichert sind), so müssen Sie sehr wahrscheinlich weitere, auf Ihre Bedürfnisse abgestimmte Sicherheitsvorkehrungen treffen.
- An dieser Stelle ist das Wissen und die Erfahrung von Spezialisten gefragt, die ein passendes Sicherheitskonzept erstellen.
- Denken Sie dabei bitte an die Antago GmbH!

Programme und Webseiten

Weiterführende Links

Programme für Ihre Sicherheit: Hier kostenlos!

- Für Privatanwender kostenloser Virenscanner:
  z.B. der Avira AntiVir Personal Edition: http://www.free-av.de/
- Kostenloser alternativer Browser:
  z.B. Mozilla Firefox: http://www.mozilla-europe.org/de/
- Sicheres Löschen von Datenträgern:
  z.B. Eraser: http://www.heidi.ie/eraser/
- Verschlüsseln von Datenträgern:
  z.B. Truecrypt: http://www.truecrypt.org
- Sämtliche Software auf Aktualität prüfen:
  z.B. Software-Up-To-Date: http://www.software-uptodate.de oder
  Secunia PSI: http://secunia.com/products/consumer/psi/ oder
  Heise: http://www.heise.de/security/dienste/Update-Check-877012.html
- Passwort-Safe zur sicheren Aufbewahrung von Passworten:
  z.B. KeePass: http://www.keepass.info

Weitere Infos für Endanwender

- Von allgemeinen Infos bis zu ganz konkreten Anleitungen:
  http://www.bsi-fuer-buerger.de/
- Test des Webbrowsers auf Sicherheitslücken beim heise-Verlag:
  http://www.heise.de/security/dienste/browsercheck/
- Online-Überprüfung auf Sicherheitslücken vom Landesbeauftragten für den Datenschutz Niedersachsen und dem heise-Verlag:
  http://www.heise.de/security/dienste/Netzwerkcheck-2114.html
- Klicksafe – umfangreiches Portal für Internetsicherheit
  https://www.klicksafe.de/

So kontaktieren Sie uns

Antago: Replacing Luck.

Unsere Kontaktdaten – wir freuen uns auf Sie!

- Sie haben Fragen? Sie benötigen weitere Informationen oder ein unverbindliches Angebot? Wir freuen uns auf Sie!

  - Antago GmbH
    Robert Bosch Str. 7
    D 64293 Darmstadt

    Internet: https://www.antago.info
    Phone: +49 6151 428568 0
    Fax: +49 6151 428568 1
    E-Mail: sicherheit[at]antago.info

antago