

So viel Schutz muss sein!

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

Stand: 01.04.2011



Dürfen wir uns vorstellen?

- Die Antago GmbH ist ein europaweit tätiges Unternehmen im Bereich der IT- und Informationssicherheit. Wir sorgen für die strukturierte, bedarfsorientierte Absicherung Ihrer Informationen.
- Unabhängig, kompetent und fair erhalten Sie von uns:
 - ✓ Security Scans
Sicherheitsüberprüfungen von Systemen, Netzen und Applikationen
 - ✓ Informationssicherheitsmanagementsysteme (ISMS)
Analyse und Erarbeitung bedarfsorientierter Sicherheitskonzepte
(auch gem. IT-Grundschutz / ISO 27001)
 - ✓ IT-Forensik
Gerichtsfeste Beweissicherung und Analyse von IT-Sicherheitsvorfällen
 - ✓ Security Awareness
Sensibilisierungsmaßnahmen für Ihre Mitarbeiter
 - ✓ Praxisnahe Schulungen
KnowHow aus erster Hand für Techniker und Geschäftsleitung



Wir sind KEIN...

...Systemhaus

- Wir haben kein Interesse daran, Ihnen Hard- oder Software zu verkaufen.

...Reseller/Integrator

- Wir sind unabhängig von Herstellern.

...fremdfinanziertes Unternehmen

- Wir sind unabhängig von Geldgebern.

...Tochterunternehmen

- Wir sind an keinen Konzern gebunden.





Was erwartet Sie?

- Auf den folgenden Seiten sehen Sie alle Maßnahmen, die Sie als Privatanwender unbedingt ergreifen sollten, um sich sicher im Internet zu bewegen.
- Alle Maßnahmen die Sie unbedingt umsetzen sollten, haben wir mit einem Kasten versehen (). Machen Sie einen Haken, wenn Sie sie umgesetzt haben.
- Schauen Sie öfters auf unserer Webseite vorbei – dieses Dokument wird bei Bedarf von uns aktualisiert.
- Natürlich kennen wir Ihre Sicherheitsbedürfnisse nicht im Detail – deshalb können wir hier nur den absoluten Basisschutz darstellen, der nun wirklich 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.





Einige 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 Fehler finden.
 - ➔ Dieses Papier kann unvollständig sein. Bitte kontaktieren Sie uns, wenn ein wichtiges Thema fehlt.
 - ➔ Wir übernehmen keine Gewährleistung für die in diesem Papier aufgeführten Empfehlungen und Software-Produkte.

Soviel Schutz muss sein: Datensicherung!

- Die wichtigste Sicherheitsmaßnahme ist die Datensicherung!
- Ihre Festplatte wird ganz sicher irgendwann kaputt gehen und Ihre Urlaubsfotos und -videos, Ihre Briefe, e-Mails und Steuererklärungen mit ins digitale Grab nehmen.
- Führen Sie deshalb unbedingt in regelmäßigen und sinnvollen Abständen eine Datensicherung durch.
- Sichern Sie den gesamten Rechner ohne Ausnahme, sonst übersehen Sie vielleicht wichtige Daten.
- Vergessen Sie nicht, auch die Daten Ihres Handy (Ihres PDA, Ihres Notebook etc.) zu sichern! Auch diese Daten sind wertvoll!

Wie sieht eine vernünftige Datensicherung aus?

- Sichern Sie alle (wirklich **ALLE!**) Daten (Betriebssystem, Programme, Konfigurationen, Anwendungsdaten) von allen (wirklich **ALLEN!**) Systemen (PC, Laptop, Handy, PDA, ...).
- Sichern Sie Ihre Daten zeitnah, nachdem wichtige Änderungen vorgenommen wurden – ggf. sogar mehrmals am Tag (z.B. wenn Sie gerade an einer wichtigen Arbeit schreiben).
- Heben Sie nicht nur eine gesicherte Version Ihrer Daten auf, sondern mehrere Generationen der Datensicherung.
- Testen Sie, ob die Datensicherung auch wirklich funktioniert (das ist leider seltener als Sie annehmen...).
- Lagern Sie eine Kopie der Datensicherung außerhalb Ihres Hauses.
- Verschlüsseln Sie Ihre Datensicherung, wenn Sie vertrauliche Daten besitzen.

So viel Schutz muss sein: Sichere Passwörter!

- Passwörter müssen unbedingt so gewählt werden, dass sie von Bösewichtern nicht erraten werden können!
- Wie baut man ein sicheres Passwort, an das man sich garantiert erinnert? Hier eine 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 sich garantiert an das Passwort erinnern - der Satz bleibt im Gedächtnis!
- Das ist selbstverständlich:
Denken Sie sich einen eigenen Satz aus!
Das Passwort „A24.12.iW.“ ist ja jetzt bekannt wie der sprichwörtliche bunte Hund... :)

Soviel Schutz muss sein: Windows absichern!

Nicht als Administrator arbeiten!

Arbeiten Sie nicht als Administrator auf Ihrem PC, wenn es nicht unbedingt sein muss. 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 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).

Soviel Schutz muss sein: Gesamte Software updaten!

- Über die Windows Updates wird nur die Software von Microsoft aktuell gehalten - Lücken in anderen Programmen werden nicht gestopft. Angreifer wissen dies und attackieren Systeme zunehmend über diesen Weg.
- Sorgen Sie deshalb unbedingt dafür, dass auch jene Software, die nicht von Microsoft stammt mit Updates versorgt wird.
- Denken Sie dabei auch an die Plugins in Ihrem Webbrowser – Lücken in diesen Plugins stellen ein Einfallstor dar, weil sie ein Bestandteil des Browsers sind. Eine traurige Berühmtheit ist übrigens aktuell der Flashplayer von Adobe...
- Also auch hier gilt: **Updates, Updates, Updates!**
- Auf der letzten Seite finden Sie den Link zu einem Tool, mit dem Sie die Aktualität Ihrer gesamten Software prüfen können.

Soviel Schutz muss sein: Auf den Browser achten!

- Webbrowser sind besonders gefährdet, weil sie beliebige Inhalte aus dem Internet herunterladen und interpretieren.
 - Mittlerweile hat sich eine ganze 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: **Updates, Updates, Updates!**
 - Verwenden Sie nicht mehr den Internet Explorer 6, sondern entweder den aktuellsten Internet Explorer oder einen alternativen Browser (z.B. den Mozilla Firefox) – natürlich auch hier nur die aktuellste Version!



So viel Schutz muss sein: Viren & Co. fernhalten!

- Schalten Sie die e-Mail-Filterung Ihres Mailkontos ein. Sehr viele Viren, Trojaner und SPAM-Mails werden so entsorgt, noch bevor sie auf Ihren Rechner gelangen.
- Klicken Sie niemals auf Mail-Anhänge (Attachments), die Sie von unbekanntem Absendern erhalten. Diese Attachments sind alle böse, hinterhältig und gemein oder bestenfalls unglaublich unwichtig.
- Seien Sie besonders misstrauisch bei Anhängen, die ausführbare Programme enthalten (*.exe, *.vbs, *.bat, *.scr, *.pif, ...).



So viel Schutz muss sein: Viren & Co. entsorgen!

- Installieren Sie sich eine Anti-Virus-Software.
Die gibt es von vielen Herstellern für Privatanwender kostenfrei im Netz. (Wo? Siehe letzte Seite).



ACHTUNG!

Es sind viele gefälschte Antivirus-Programme im Netz unterwegs. Installieren Sie nur eine Antivirus-Software eines namhaften Herstellers! Vor dem Installieren gilt: Informieren!

- Lassen Sie die Anti-Virus-Software permanent im Hintergrund laufen, damit Schädlinge umgehend entdeckt und bekämpft werden können.
- Führen Sie regelmäßig ein Update des Virenschanners durch. Am besten soll das der Virenschanner selbst erledigen (Automatische Updates gibt es bei jedem guten Virenschanner!).

So viel Schutz muss sein: 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.

So viel Schutz muss sein: 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, dass 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://...).

So viel Schutz muss sein: Wireless LAN sichern!

- Verschlüsseln Sie Ihr Wireless LAN richtig:
Betreiben Sie niemals Ihr Wireless LAN unverschlüsselt.
Benutzen Sie nicht die veraltete Verschlüsselung „WEP“ – die ist absolut nutzlos. Nutzen Sie die Verschlüsselung „WPA“, möglichst aber „WPA2“.
- Kaufen Sie notfalls einen neuen Accesspoint, der WPA oder WPA2 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.
Wie man sichere Passwörter generiert, wissen Sie ja schon!
- Setzen Sie keine MAC-Filter ein.
Diese Filter machen nur Arbeit und lassen sich sehr leicht umgehen.

So viel Schutz muss sein: DSL-Router sichern!

- Setzen Sie ein Passwort für die Konfigurationsoberfläche Ihres Routers. Verwenden Sie dabei keine Standard-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 was Fernwartung ist: Finger weg! Fragen Sie jemanden, der sich auskennt.

So viel Schutz muss sein: Datenträger säubern!

- Bevor Sie ein gebrauchtes elektronisches Gerät (Rechner, Laptop, Digitalkamera, USB-Stick, iPod, Blackberry, Handy, Drucker,) verschenken, verkaufen oder verleihen, müssen 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).

So viel Schutz muss sein: Mobile Geräte sichern!

- Mobilen Geräte (Laptops, mobile Festplatten, PDAs usw.) können geklaut werden. Der Dieb besitzt dann das Gerät und – was meistens noch schlimmer ist: Ihre Daten!
- Die Datenträger von mobilen Geräten sollten deshalb immer verschlüsselt werden, wenn auf ihnen vertrauliche Informationen gespeichert sind. 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 lokal gespeicherten Daten. Achten Sie beim Kauf eines solchen 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 und einen Aufkleber mit Kontaktdaten und dem Versprechen von Finderlohn anbringen.
Geklaute Laptops kommen dann häufig zum Besitzer zurück...

Jetzt können Sie beruhigt sein!?

- Die Empfehlungen der letzten Seiten sind für den normalen Endanwender in aller Regel völlig ausreichend.
- Ihr Computer ist jetzt immer noch 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 gesteigertes 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!**

Firewall, Virens Scanner, Browser: Hier kostenlos!

- **Für Privatenwender kostenloser Virens Scanner**
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>

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/portscan/test/>



**Vielen Dank
für Ihre Aufmerksamkeit!**



