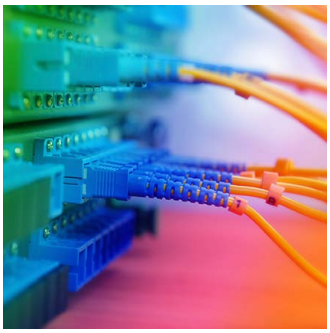

# PC-Grundsicherung

## Auf Nummer Sicher

Wer mit seinem PC im Internet surft, setzt sich mehr oder weniger auch der Gefahr aus, Ziel eines Angreifers zu werden - wer im Internet mit einem ungesicherten PC surft, verliert mit Sicherheit binnen kürzester Zeit die Kontrolle über sein eigenes System.

Tom Liston, ein Sicherheitsspezialist, konnte dies eindrucksvoll demonstrieren, indem er zum Test mit einem "ungepflegten" Windows-System, das heißt, einem System ohne aktuelle Updates und aktuellen Virenscanner, per Web-Browser im Internet surfte. Nur eine typische Sitzung im Internet reichte aus, um über 3 MB an Schadsoftware auf dem System zu installieren – selbstverständlich ohne, dass der "normale" Benutzer davon etwas gemerkt hätte. Eine Nachahmung des Selbstversuches von Tom Liston ist selbstverständlich nicht zu empfehlen.

Schon das Befolgen einiger weniger Grundregeln beim Betrieb von PCs und Notebooks verringert die Gefahr, dass Dritte auf interne Daten zugreifen oder das System schädigen können, beträchtlich. Jede Sicherungsmaßnahme bedeutet zwar einen mehr oder weniger großen Komfortverlust, jedoch wiegt dies weniger schwer, denkt man an das Desaster, das durch eine gelungene Angreiferattacke entsteht.

**Bei der Verarbeitung personenbezogener Daten sind alle an der Hochschule verpflichtet, Maßnahmen zur Grundsicherung von Computern umzusetzen.**

Die Informationen zur PC-Grundsicherung sind in drei Kategorien eingeteilt. Die Basissicherung kann jeder Computerbenutzer ohne besondere Vorkenntnisse selber an dem Gerät vornehmen. Die meisten Hinweise beinhalten Einstellungen, die einmalig am PC vorgenommen werden müssen.
Ebenso sind alle Computernutzer dazu angehalten, die Regeln zur organisatorischen Sicherung zu befolgen, die sich vor allem auf den Umgang mit dem Gerät beziehen. Arbeitsplätze, an denen sensible Daten verarbeitet werden, sollten zudem eine erweiterte Sicherung erfahren.

Zur **Basissicherung** von Computern gehören:

- das Arbeiten mit mehreren passwortgeschützten Benutzeraccounts
- die regelmäßige Durchführung von Windows-Updates
- die Installation von Antivirensoftware
- eine regelmäßige Sicherung der Datenbestände und
- Web-Surfen mir Sicherheitsbewusstsein.

Die **organisatorischen Sicherung** von Computern und digitalen Daten beinhaltet:

- Diebstahlschutz: Lasern von Geräten
- die Beachtung von Hinweisen Hinweise zur Zugänglichkeit der Geräte
- der verantwortungsbewusste Umgang mit Chipkarten
- die ordnungsgemäße Wartung und Entsorgung von Geräten und Datenträgern und
- das Einhalten von Bestimmungen zur Privatnutzung von Geräten und Diensten.

Zur **erweiterten Sicherung** von PCs gehören:

- Datei-, Ordner- und Festplattenverschlüsselung
- die Überprüfung von Sicherheitslücken

### Aus Tom Liston: Follow the Bouncing Malware*

**Das Ergebnis nur EINES Besuchs einer Website mit einem ungepflegten PC führte zur unbemerkten Installation folgender Schadprogramme:**

hp2.exe (16,384 bytes) tvmupdater4bp5.exe (195,072 bytes) AtPartners.dll (96,256 bytes) SplWbr.dll (454,656 bytes -- entpackt drei Dateien mit 892,288 bytes) ezbdlLs.dll (151,040 bytes -- entpackt vier Dateien mit 314,880 bytes) hp1.exe (49,152 bytes) mm20.ocx (61,440 bytes) 8-24.exe (40,960 bytes) MediaMotor25.exe (9,056 bytes) ast_4_mm.exe (129,152 bytes) IeBHOs.dll (129,536 bytes) cpr_mm2.exe (270,415 bytes) ab1.exe (500,869 bytes) tvm_bundle.exe (53,738 bytes) und natürlich cpr_mm2.exe (270,415 bytes) nochmal...

**Die Gesamtsumme**
Heruntergeladen: 15 Dateien mit 2.428.141 Byte Installiert: 20 Dateien, die 3.029.613 Byte auf der Platte belegen.
*ins deutsche übersetzt von heise Security (siehe Linkliste).

- IT-Sicherheits-Scans für Server und Subnetze.

Auch wenn Sie geeignete Sicherungsmaßnahmen treffen, verbleibt dennoch ein Restrisiko. Beispielsweise vergeht immer eine gewisse Zeit zwischen dem Bekanntwerden einer Schwachstelle und deren Behebung durch den Hersteller.

Zur Überprüfung Ihres bisherigen Umgangs mit Computern und digitalen Daten in Hinblick auf Sicherheitslücken stellen wir Ihnen eine Checkliste (direkt hier unten zu finden) bereit.

## Downloads

Eine Checkliste und eine Zusammenfassung zur PC-Grundsicherung als PDF-Dokument ist in der Überarbeitung.

## Linkliste

Heise: Schädlingen auf der Spur:
http://www.heise.de/security/Schaedlingen-auf-der-Spur--/artikel/49687/0

Bild: iStockphoto.com/kynny

# PC-Grundsicherung - Basissicherung

## Auf Nummer Sicher - Teil I

Basissicherung kann jeder Computerbenutzer ohne besondere Vorkenntnisse selber an dem Gerät vornehmen. Die meisten Hinweise beinhalten Einstellungen, die einmalig am PC vorgenommen werden müssen.
Ebenso sind alle Computernutzer dazu angehalten, die Regeln zur organisatorischen Sicherung zu befolgen, die sich vor allem auf den Umgang mit dem Gerät beziehen. Arbeitsplätze, an denen sensible Daten verarbeitet werden, sollten zudem eine erweiterte Sicherung erfahren.

Die Basissicherung von Computern beinhaltet

- das Arbeiten mit mehreren passwortgeschützten Benutzerkonten
- die regelmäßige Durchführung von Windows-Updates
- die Installation von Antivirensoftware
- eine regelmäßige Sicherung der Datenbestände und
- Web-Surfen mit Sicherheitsbewusstsein.

## Arbeiten mit mehreren passwortgeschützten Benutzerkonten

Alle Zugänge zu Systemen der Ruhr-Universität Bochum sind grundsätzlich durch Passwörter zu schützen. Benutzerberechtigungen (Accounts) sind personengebunden zu vergeben. „Lehrstuhlpasswörter“ oder Benutzerberechtigungen, die von mehreren Personen genutzt werden, sind zu vermeiden. Das hat vor allem den Grund, dass nur so Passwörter regelmäßig geändert und Zugänge nach dem Ausscheiden von Mitarbeitern auch zeitnah wieder entzogen werden können. Dabei sollten auch die Zugriffsrechte des jeweiligen Benutzers angemessen eingestellt sein.

Da alle Nutzer des RUB Intranets im wahrsten Sinne des Wortes an einem Strang hängen, sind nicht allein die kompromittierten Systeme von Hackereinbrüchen betroffen. Diese werden in der Regel als Sprungbrett zum Attackieren benachbarter Systeme verwendet. Solche Attacken starten vielfach mit dem Versuch, die Passwörter anderer Accounts des befallenen Systems sowie benachbarter Systeme zu knacken. Diese Vorgehensweise führt häufig zum Erfolg, da erfahrungsgemäß Accounts mit denselben Passworten auch auf anderen Systemen verwendet werden. Verwenden Sie daher sichere Passwörter, um Einbrüche in Ihr System zu erschweren. Die Sicherheit von Passwörtern erhöhen Sie, wenn Sie folgende Regeln befolgen:

- Nutzen Sie keine gebräuchlichen Begriffe, nebeneinander liegende Tastenfolgen oder Begrifflichkeiten, die mit Ihren persönlichen Daten zusammenhängen. Verwenden Sie keine nebeneinanderliegende Tastenfolgen wie „qwert“ oder triviale Zahlenfolgen „123456“.
- Ein Passwort sollte mindestens aus 8 Zeichen bestehen.
- Kombinieren Sie Zahlen, Buchstaben und Sonderzeichen sowie Groß-und Kleinschreibung. Vermeiden Sie bitte Umlaute.
- Bauen Sie sich Eselsbrücken und formen Sie z.B. Sätze zu Passwörtern um: **D**iese **K**ombination **i**st **ein r**elativ **s**icheres **P**ass**w**ort = DKi1rsPw
- Verwenden Sie im Internet, beispielsweise beim Einkaufen, niemals denselben Account und dasselbe Passwort, das auch Ihr System schützt. Sie können nicht einschätzen wie andere Systembetreiber mit Ihren Zugangsdaten umgehen. Verwenden Sie ebenso für solche Zwecke niemals Ihre RUB-LoginID oder das zugehörige Passwort.
- Es kann sinnvoll sein, sich Passwörter zu notieren. Diese sollten dann aber unbedingt sicher und für Dritte unzugänglich aufbewahrt werden.
- Ihre Passwörter sollten Sie in regelmäßigen Abständen ändern.

nach oben

## Regelmäßige Durchführung von Windows-Updates

Zum Schutz gegen Angriffe ist es unerlässlich, Sicherheitsupdates (Patches) des Betriebssystems und der

### Benutzerkonten

Der Administrator eines Rechners verfügt über umfassende Rechte, die ihm u.a. die Möglichkeit einräumen, Änderungen an Systemdateien vorzunehmen. Vor schwerwiegenden Folgen bei z.B. Hackereinbrüchen können Sie Ihren Computer schützen, indem Sie mehrere Benutzerkonten anlegen: Arbeiten Sie insbesondere im Internet nur mit einem Benutzerkonto mit eingeschränkten Rechten. Nutzen Sie einen Adminstrator-Account nur, wenn Sie Software installieren oder deinstallieren möchten.

Sollten Sie sich beim Surfen im Netz trotz Vorsicht Schadcode einfangen, so kann dieser zunächst nur mit den eingeschränkten Rechten des aktiven Benutzerkontos tätig werden und keine Schäden im Betriebssystem anrichten. Dennoch sind in diesem Fall natürlich alle Datenbestände in Gefahr, auf die der aktive Benutzeraccount Zugriff hat.

Anwendungsprogramme zu installieren. Die meisten Betriebssysteme bieten den Benutzerinnen und Benutzern Hilfen an, um sie auf einem aktuellen Stand zu halten.

**Windows Server Update Services (WSUS)**
Ein vollautomatisches Verfahren zur regelmäßigen Aktualisierung von Windows Systemen bietet der zentrale WSUS-Server der RUB: Der WSUS-Server aktualisiert das Windows Betriebssysteme, Office- und einige weitere Microsoft-Produkte. Die Aktualisierung kann vollständig automatisiert werden, so dass hierfür kein Benutzereingriff mehr erforderlich ist. Ein weiterer Vorteil dieses Verfahrens besteht darin, dass die komplette Aktualisierung im Intranet der RUB abgewickelt wird. Die Nutzung dieses Verfahrens wird für alle Systeme der Ruhr-Universität dringend empfohlen.
Der WSUS-Server ist von Netzwerken außerhalb der RUB nur über einen VPN-Tunnel erreichbar.
Besteht keine Möglichkeit den WSUS-Server zu nutzen, so kann man auf die üblichen von Microsoft vorgesehenen Verfahren zum Systemupdate zurückgreifen. Ausführliche Informationen zum Thema Updates finden Sie hier.

**Aktualisierung zusätzlicher Softwareprodukte**
Das Aktualisieren weiterer installierter Programme wie zum Beispiel alternativer Web-Browser oder Mediaplayer darf nicht vergessen werden. Es empfiehlt sich eine Liste dieser Anwendungen anzulegen.
Inzwischen gibt es Tools, die bei der Aktualisierung zusätzlicher Softwareprodukte Hilfestellung leisten. Beispielsweise überprüft der Personal Software Inspector der Firma Secunia ein System auf veraltete Programme und warnt, wenn aktuelle Sicherheitsupdate zu installieren sind. Der Personal Software Inspector (PSI) ist für persönlichen Gebrauch kostenlos erhältlich. Für die Verwendung an der Ruhr-Universität ist eine Campus-Lizenz erworben worden. Sie können sich im Servicecenter von IT.SERVICES zum Stand der Secunia Lizenz informieren.
Weitere Informationen unter Updates.

nach oben

## Installation von Antivirensoftware

Ein Antivirus-Toolkit und eine Firewall sind neben der Installation von Systemupdates und der Beherzigung von Verhaltensregeln die besten Maßnahmen zum Schutz gegen Computerviren und Angriffen aus dem Internet. Die Ruhr-Universität Bochum hat eine Campus-Lizenz der Firewall- und Antivirensoftware von Sophos zentral finanziert. Studierende und Einrichtungen der Ruhr-Universität können die Software kostenlos nutzen.
Damit ein Antivirus-Programm zuverlässig funktioniert, muss es regelmäßig gepflegt werden. Das heißt, dass die Virendefinitionsdateien, aufgrund derer das Programm einen Virus identifiziert, regelmäßig aktualisiert werden müssen. Die Ruhr-Universität betreibt zentral einen entsprechenden Upate-Server.

Die Software, sowie Anleitungen zur Konfiguration sind über IT.SERVICES erhältlich.

nach oben

## Regelmäßige Sicherung der Datenbestände

Um Datenverluste bei Systemausfällen oder anderen Problemfällen zu begrenzen, sollten regelmäßige Datensicherungen (Backups) durchgeführt werden. Hierbei werden die Daten eines Computersystems vollständig oder teilweise auf externe Speichermedien kopiert.

IT.SERVICES bietet gegen eine geringe Gebühr einen zentralen Backup-Dienst für Server und Arbeitsplätze an der RUB an. Studierende können den kostenlosen Fileservice für Studierende nutzen.

Den Mitarbeiterinnen und Mitarbeitern an der Ruhr-Universität steht außerdem im Rahmen des Ressourcenverbundes NRW ein Archiv-Dienst an der RWTH Aachen zur Verfügung. Hier können Daten mit direktem Bezug zu Forschung und Lehre langfristig gesichert werden.
Die Aufbewahrungsfrist der Daten ist zunächst einmal unbegrenzt, vorausgesetzt der Account an der RWTH Aachen wird regelmäßig verlängert. Es handelt sich allerdings nicht um einen Archivierungsdienst im Sinne gesetzlicher Anforderungen zur Erfüllung von Aufbewahrungsfristen.
Zur Nutzung des Datenarchivs der RWTH Aachen kann im Servicecenter von IT.SERVICES ein Nutzerkennzeichen des Ressourcenverbunds beantragt werden. Die Datensicherung erfolgt über eine Tivoli Klientensoftware. Eine detaillierte Anleitung findet sich auf den Seiten der RWTH Aachen.

nach oben

## Web-Surfen mit Sicherheitsbewusstsein

Die weitaus meisten Arbeiten im Internet werden mit Hilfe eines Webbrowsers erledigt. Gängige Web-Browser sind zum Beispiel der Internet Explorer, Firefox und Chrome. Webbrowser sind das ideale Werkzeug zum Suchen, Anzeigen und Herunterladen von Informationen aus dem Internet. Mittels des Webbrowsers lädt ein Internetnutzer Informationen, die ein Webserver bereitstellt, auf seinen PC herunter.
Zusammen mit den statischen Texten, die im Browserfenster angezeigt werden, können dabei auch kleine Programme (Javaapplets oder ActiveX Controls) oder Skripte (Javascript, VBscript) geladen werden, die auf dem Arbeitsplatz des Internetnutzers zumeist automatisch ausgeführt werden. Unterschiedliche Sicherheitskonzepte sollen dafür sorgen, dass diese Programmstücke keinen Schaden im Dateisystem des Nutzers anrichten können. Allerdings ergeben sich immer wieder Schwachstellen in den Sicherheitsvorkehrungen, die es Dritten erlauben, den PC zu kompromittieren. Wurde vor wenigen Jahren noch der größte Teil des Schadcodes über E-Mailanhänge an den Endnutzer verteilt, so werden inzwischen die meisten Trojaner über Sicherheitslücken in Webbrowsern auf die Endsysteme verbracht.

Der Symantec Threat Report von 2016 zeigt, dass von 3172 Webseiten eine mit Malware verseucht ist.

**Es ist daher grundsätzlich davon abzuraten, dass ein System, auf dem sicherheitskritische Anwendungen laufen, auch zum Surfen im Internet verwendet wird.**

Durch Sicherheitseinstellungen in den Browsern lässt sich die Gefahr mindern, dass sich Schadcode über Browserschwachstellen auf dem System ausbreiten kann. Ausführliche Anleitungen dazu werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben.

BSI Browsercheck: http://www.bsi-fuer-buerger.de/Browsercheck

nach oben

## Sie benötigen Hilfestellung?

Falls Sie mit den Maßnahmen zur Sicherung Ihres PCs nicht alleine zurecht kommen, hilft Ihnen das Servicecenter von IT.SERVICES gerne weiter.

## Downloads

Eine Checkliste und eine Zusammenfassung zur PC-Grundsicherung als PDF-Dokument ist in der Überarbeitung.

## PC-Grundsicherung


- zurück zur Übersicht
- zu Teil II - organisatorische Sicherung
- zu Teil III - erweiterte Sicherung

# PC-Grundsicherung - Organisatorische Sicherung

## Auf Nummer Sicher - Teil II

Die Informationen zur PC-Grundsicherung haben wir in drei Kategorien eingeteilt. Die Basissicherung kann jeder Computerbenutzer ohne besondere Vorkenntnisse selber an seinem Gerät vornehmen. Der Großteil der Hinweise beinhalten Einstellungen, die einmalig am PC vorgenommen werden müssen.
Ebenso sind alle Computernutzer dazu angehalten, die Regeln zur organisatorischen Sicherung zu befolgen, die sich vor allem auf den Umgang mit dem Gerät beziehen. Arbeitsplätze, an denen sensible Daten verarbeitet werden, sollten eine erweitere Sicherung erfahren.

Zur organisatorischen Sicherung von Computern gehören

- Diebstahlschutz: Lasern von Geräten
- die Beachtung von Hinweisen zur Zugänglichkeit der Geräte
- der verantwortungsbewusste Umgang mit Chipkarten
- die ordnungsgemäße Wartung und Entsorgung von Geräten und Datenträgern und
- das Einhalten von Bestimmungen zur Privatnutzung von Geräten und Diensten.

## Diebstahlschutz: Lasern von Geräten

Ein Beitrag zum Diebstahlschutz ist das Lasern der Geräte mit dem Label der Ruhr-Universität. Eine solche Lasergravur bringt das Druckzentrum der Hochschule an. Vereinbaren Sie einen Termin mit dem Druckzentrum, dann können Sie die Geräte in der Regel nach kurzer Wartezeit direkt wieder mit- und in Gebrauch nehmen.

Den Internetauftritt des Druckzentrums finden Sie unter:
http://www.druckzentrum.ruhr-uni-bochum.de

Öffnungszeiten und Kontakt zum Druckzentrum:
Montag - Donnerstag von 8.00 - 16.30
Freitag von 8.00 - 15.00
Raum: UV 01/44
Tel.: 0234 / 32-24134
Fax.: 0234 / 32-14782

## Zugänglichkeit der Geräte

IT-Arbeitsplätze sind in der Regel vernetzt und eröffnen so den Zugang zum Intranet der Ruhr-Universität. Auf IT-Arbeitsplätzen und Servern befinden sich schutzwürdige Informationen wie Forschungsergebnisse oder personenbezogene Daten. Achten Sie daher darauf, wer Zugang zu den Systemen hat:

- Kontrollierter Umgang mit Schlüsseln:
  Zutritt zu den Räumen (Büros, Serverräume), in denen die Systeme stehen, sollten nur diejenige Personen haben, die dort auch Aufgaben zu erledigen haben.
- Schließen Sie die Räume in Abwesenheit ab.
- Stellen Sie sicher, dass sich Besucher (z.B. auch Wartungspersonal) nur in Ihrem oder im Beisein eines anderen Mitarbeiters im Büro oder Serverraum aufhalten.
- Fahren Sie IT-Arbeitsplätze nach Erledigung der Arbeiten herunter. Sperren Sie den Zugriff auf das System auch beim kurzzeitigen Verlassen des Arbeitsplatzes: Windowstaste-L (ab Windows XP), Ctrl-Alt-Entf – Sperren. Ein Bildschirmschoner ist zu verwenden und sollte so eingestellt sein, dass man bei Wiederinbetriebnahme das Passwort eingeben muss.
- Sichern Sie die Rechner gegen Diebstähle, etwa durch Anbringen eines Kensington-Schlosses (siehe auch oben).
- Stellen Sie den Rechner und Monitor so auf, dass niemand versehentlich Einsicht in Ihren Bildschirm nehmen kann.
- Lassen Sie keine Authentifizerungsmerkmale (z.B. Chipkarten, Passworte) ungeschützt am Arbeitsplatz herumliegen.
- Besondere Vorsicht ist bei mobilen Systemen geboten. Achten Sie stets auf eine sichere Aufbewahrung, schützen Sie das System gegen Einsichtnahme Dritter, verwenden Sie verschlüsselte Datenübertragungswege und ggfs. auch eine Datenträgerverschlüsselung.

nach oben

## Verantwortungsbewusster Umgang mit Chipkarten

Für den Zugang zu VSPL und anderen sicherheitsrelevanten Systemen werden an der Ruhr-Universität Chipkarten (RUBCard) anstelle von LoginID und Passwort verwendet. Die Zwei-Faktor-Authentifizierung der Chipkarte (etwas, was man weiß: "die PIN"; etwas, was man hat: "die RUBCard") ist wesentlich sicherer als eine Authentifizierung durch LoginID und Passwort. Weitere Informationen zur RUBCard finden Sie auf den Webseiten der Ausgabestelle.
Sicherheitsrelevante Vorgänge mit der Chipkarte werden signiert. Die elektronische Signatur kommt dabei innerhalb der Ruhr-Universität ihrer Unterschrift gleich.
Ihr Umgang mit der Karte sollte dieser wichtigen Funktion angemessen sein. Entscheidend für die Sicherheit ist der Umgang mit der Karte selbst, der Umgang mit der PIN und das Verhalten am Arbeitsplatz. Welchem anderen Menschen würden Sie erlauben, dass er Ihre Unterschrift verwendet?

Beachten Sie bitte:

- Ihre Chipkarte darf deshalb ausschließlich von Ihnen selbst genutzt werden. Eine Weitergabe ist nicht erlaubt. (Um dennoch bestimmte berechtigte organisatorische Regelungen zuzulassen sehen die Anwendungssysteme (z.B. VSPL) eine Vertretungsregelung vor, mit der eine von Ihnen beauftragte Person Arbeiten mit dem System erledigen kann.)
- Bewahren Sie die Karte so auf, dass niemand Sie unbemerkt entnehmen oder „ausleihen“ kann.
- Ziehen Sie beim Verlassen des Arbeitsplatzes die Karte aus dem Kartenleser und nehmen sie mit. Lassen Sie also die Karte (auch nicht für kurze Zeit) unbeobachtet im Kartenleser stecken.

Für die PIN gelten im Wesentlichen die Regeln, wie sie auch für Passwörter gelten (s.o) - keine simplen Ziffernfolgen, nicht das eigene Geburtsdatum etc. Sie bestehen aus 5 Stellen, sollten aber ebenso nirgends aufgeschrieben zu finden sein und möglichst nicht anderen leicht abzufangenden gefährdeten Kennungen entsprechen.

Einen Verlust der Karte müssen Sie unverzüglich bei der Ausgabestelle der RUBCard melden, damit Missbrauch verhindert werden kann. Die Karte und das darauf befindliche Zertifikat werden dann gesperrt. Im Regelfall erhalten Sie unverzüglich eine neue Chipkarte. Finden Sie Ihre alte Karte vor Ausgabe einer neuen wieder, wird ein neues Zertifikat aufgebracht.

nach oben

## Bestimmungen zur Privatnutzung von Geräten und Diensten

Zur privaten Nutzung der IT-Einrichtungen der Ruhr-Universität sagt die „Ordnung für die Nutzung der von der Ruhr-Universität Bochum angebotenen Datendienste“ in §5 aus:

"Die Nutzung des Dienstleistungsangebots ist grundsätzlich den Zwecken von Forschung, Lehre und Studium, sowie der Aus- und Weiterbildung und der Erfüllung sonstiger Aufgaben der Ruhr-Universität Bochum vorbehalten.Eine private Nutzung ist nur zulässig, soweit dadurch dienstliche Belange nicht tangiert werden. Eine kommerzielle Nutzung des Dienstleistungsangebots ist grundsätzlich unzulässig, soweit sie nicht Zwecken von Forschung und Lehre dient oder im Rahmen einer genehmigungsfreien oder allgemein genehmigten Nebentätigkeit im Sinne der Hochschulnebentätigkeitsverordnung NW erfolgt."

Im Rahmen der privaten Nutzung der IT-Dienste der RUB ist die gleiche Obacht anzuwenden wie bei deren dienstlicher Nutzung. Private PCs und Notebooks sollten grundsätzlich nicht direkt über eine freie Netzsteckdose ans Instituts-Netzwerk (LAN) angeschlossen werden, sondern über einen sogenannten HIRN-Port. HIRN-Ports verfügen netzseitig über zusätzliche Sicherungsvorkehrungen, die die Ausbreitung von Schadcode im Intranet erschweren. Bei Bedarf kann das das Network Operation Center (NOC) der RUB Netzdosen aus dem Instituts-LAN zu HIRN-Ports umkonfigurieren.

Einige - jedoch nicht alle!! - über Campusverträge für die RUB lizenzierte Softwareprodukte, sowie eine Reihe weiterer Produkte mit Forschung-und-Lehre-Lizenz, dürfen von den Mitarbeiterinnen und Mitarbeitern der RUB auch auf ihrem heimischen PC/Notebook installiert und genutzt werden. Hinweise hierzu finden Sie auf den Webseiten von IT.SERVICES zur Softwarebeschaffung. Softwareprodukte speziell für Studierende dürfen von diesen ebenfalls auf dem privaten PC/Notebook installiert und genutzt werden. Beachten Sie bitte die jeweiligen Lizenzbedingungen und fragen Sie im Zweifelsfall im Servicecenter von IT.SERVICES nach.

Die Aktualisierungsdienste Sophos-Antivirus und WSUS dürfen Sie auch zur Aktualisierung der Software auf Ihrem heimischen PC/Notebook nutzen.

nach oben

## Downloads

Eine Checkliste und eine Zusammenfassung zur PC-Grundsicherung als PDF-Dokument ist in der Überarbeitung.

## PC-Grundsicherung


- zurück zur Übersicht
- zu Teil I - Basissicherung
- zu Teil III - erweiterte Sicherung

# PC-Grundsicherung - erweiterte Sicherung

## Auf Nummer Sicher - Teil III

Die Informationen zur PC-Grundsicherung sind in drei Kategorien eingeteilt. Die Basissicherung kann jeder Computerbenutzer ohne besondere Vorkenntnisse selber an seinem Gerät vornehmen. Der Großteil der Hinweise beinhalten Einstellungen, die einmalig am PC vorgenommen werden müssen.
Ebenso sind alle Computernutzer dazu angehalten, die Regeln zur organisatorischen Sicherung zu befolgen, die sich vor allem auf den Umgang mit dem Gerät beziehen. Arbeitsplätze, an denen sensible Daten verarbeitet werden, sollten eine erweitere Sicherung erfahren.

Zur erweiterten Sicherung von PCs gehören:

- Datei-, Ordner- und Festplattenverschlüsselung
- die Überprüfung von Sicherheitslücken
- IT-Sicherheits-Scans für Server und Subnetze

## Datei-, Ordner- und Festplattenverschlüsselung

Daten lassen sich vor der Einsichtnahme durch unberechtigte Dritte schützen, indem sie verschlüsselt auf Datenträgern (z.B. Festplatten oder USB-Sticks) abgelegt werden. Informationen, die mit einem nach dem Stand der Technik sicheren Verschlüsselungsverfahren gesichert sind, können nicht in falsche Hände geraten, z.B. wenn ein System entwendet wird oder bei einem Hardwaredefekt die Festplatte getauscht werden muss. (Auch defekte Datenträger sind mit Spezialtechniken noch lesbar.)
Es gibt vielfältige Verschlüsselungsverfahren, mit denen Inhalte einzelner Dateien oder Verzeichnisse, aber auch ganzer Datenträger gesichert werden können. Eine kurze Übersicht dazu, mit zahlreichen Empfehlungen, ist beim BSI für Bürger zu finden.
Aber: Die Daten sind in der Regel nur bei ausgeschaltetem Gerät geschützt. Wird bei Systemstart das Passwort (oder Zertifikat, biometrische Merkmal …) zur Entschlüsselung eingegeben, so sind die Daten im laufenden System wie unverschlüsselte Daten verfügbar.

Im Folgenden werden einige Möglichkeiten zur Verschlüsselung kurz vorgestellt.

**Dateien oder Ordner verschlüsseln:**
In den gängigen Office-Produkten kann man Dateien meist verschlüsselt abspeichern. Diese Variante ist jedoch nicht sehr sicher, da mittlerweile Programme angeboten werden, die diese einfache Verschlüsselung aufheben können. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät Nutzern, für die Verschlüsselung von Dateien und E-Mailanhängen das Programm Gpg4win zu nutzen. Weitere Informationen über Gpg4win erhalten Sie auf den Internetseiten des BSI.

Die meisten Versionen des Windows Betriebssystems (außer Home-Edition) bieten mit dem Encrypted File System (EFS) die Möglichkeit, Dateien und Verzeichnisse auf NTFS-Laufwerken zu verschlüsseln. Dies lässt sich durch Rechtsklick auf die Datei oder den Ordner und Aufruf des Kontextmenüs Eigenschaften-> Erweitert -> „Inhalte verschlüsseln“ erreichen. Das Verschlüsseln erfolgt mit einem von Windows automatisch erzeugten und im Zertifikatsspeicher des Benutzers abgelegten Zertifikats. Dies sollte man auf jeden Fall sichern, siehe BSI für Bürger.
Die Entschlüsselung erfolgt bei Zugriff auf die Daten transparent (automatisch), daher ist der Schutz der EFS-Verschlüselung so stark wie das Passwort des Benutzerkontos: Ein Dritter, der sich unbefugt unter dem Benutzerkonto anmelden kann, hat Zugriff auf die Daten.
Achtung: Kopiert man eine EFS verschlüsselte Datei oder verschlüsselten Ordner auf ein FAT-Laufwerk, so geht die Verschlüsselung auf dem Ziellaufwerk verloren.
Technisch Interessierte finden eine ausführliche Beschreibung des EFS beim BSI oder im MS Technet.

Auch durch Datenkompressionsprogramme, wie zum Beispiel die Open-Source-Anwendung 7-Zip , lässt sich eine Verschlüsselung durch Setzen eines Passwortes erzwingen. Ohne Wissen des Passwortes kann nicht mehr auf die komprimierten Daten zugegriffen werden. Diese Methode ist jedoch nur sinnvoll für kleine Datenmengen, da die De- und Komprimierung sonst zuviel Zeit in Anspruch nehmen.

**Festplattenbereiche, Partitionen oder das Gesamtsystem verschlüsseln:**
Gerade bei mobilen Geräten ist es sinnvoll, das gesamte System (Daten und Betriebssystem) zu verschlüsseln. Auf dem Markt sind viele kommerzielle Produkte zu diesem Zweck verfügbar, z.B. Sophos Safeguard.

Die meisten Windows Betriebssysteme bieten mit dem MS Bitlocker Drive Encryption eine bereits integrierte Lösung an. In der Standardvariante nutzt MS Bitlocker eine Hardwareerweiterung, die in vielen Notebooks zu finden ist, das Trusted Platform Module (TPM). Eine Kurzanleitung zur Standardkonfiguration findet man wieder bei BSI für Bürger.
Der MS Bitlocker kann aber auch ohne TPM genutzt werden. Eine Anleitung findet man hier.

Bei jeglicher Art von Verschlüsselung muss sichergestellt werden, dass kein Passwort oder Sicherheitsschlüssel/Zertifikat verloren geht. Das ist meist gleichbedeutend damit, das Passwort unter gesicherten Bedingungen (z.B. im verschlossenen Umschlag im Tresor) zusätzlich aufzubewahren.

nach oben

## Überprüfung auf Sicherheitslücken

Microsoft stellt Windows-Nutzern kostenlos den "Baseline Security Analyzer" zur Verfügung. Das Tool untersucht das Windows-System auf Sicherheitslücken. Die Bedienung ist selbsterklärend. Das Protokoll listet detailliert die Gegenstände der Überprüfung, Ergebnisdetails und Vorgehensweisen zur Behebung auf.
Auf der Technet Site von Microsoft finden Sie den Baseline Security Analyzer.

nach oben

## IT-Sicherheits-Scans für Server und Subnetze

Um größtmögliche Netz- und Datensicherheit im Intranet der Ruhr-Universität zu erreichen, müssen die angeschlossenen Endgeräte und Server regelmäßig mit den aktuellen Sicherheitskorrekturen versorgt und die darauf installierten Dienste gegen mögliche Schwachstellen abgesichert werden. Leider reicht es häufig nicht hin, die aktuellen Betriebssystem-Updates einzuspielen. Immer wieder treten Schwachstellen in Applikationen auf, für die es keine Sicherheitskorrekturen gibt, oder es treten unbeabsichtigt Konfigurationsfehler auf.
Die Stabsstelle Informationssicherheit bietet die Überprüfung von Windows-, Linux- oder Unix-Servern auf bekannte Sicherheitslücken und Schwachstellen an. Als Ergebnis eines solchen Scans wird ein Protokoll erzeugt, das potentielle Schwachstellen des Servers auflistet und Empfehlungen für die erforderlichen Maßnahmen gibt.
Die Überprüfungen werden mit dem bekannten Netzwerk- und Sicherheitsscanner Nessus in der erweiterten professionellen Version durchgeführt. Dies garantiert den Zugriff auf die aktuellsten Sicherheitstests.

**Was wird überprüft**
Ein Standard-Scan beinhaltet Tests auf bekannte Sicherheitslücken in den Diensten, die auf dem Server laufen. Ein erweiterter Scan beinhaltet zusätzlich einen Test auf Betriebssystemschwachstellen.

**Wer kann einen Sicherheitsscan veranlassen**
Die Beauftragung eines Sicherheitsscans erfolgt ausschließlich durch Netzbetreuer, die dem Network Operation Center (NOC) als Ansprechpartner für ein IP-Subnetz der Ruhr-Universität Bochum benannt worden sind. Die IP-Nummer des zu testenden Servers muss zu dem IP-Subnetz der Ruhr-Universität gehören, für das der Netzbetreuer zuständig ist. Das Ergebnis des Scans erhält der Netzbetreuer in Form einer HTML-Datei bzw. als Papierausdruck.
Bei Interesse können sich Netzbetreuer per Email oder telefonisch an die Stabsstelle Informationssicherheit wenden.

Brigitte Wojcieszynski
Tel.: 0234 / 32-23409
Sekretariat: 0234 / 32-24001
Mail: itsb@rub.de

nach oben

## Sie benötigen Hilfestellung?

Falls Sie mit den Maßnahmen zur Sicherung Ihres PCs nicht alleine zurecht kommen, hilft Ihnen das Servicecenter von IT.SERVICES gerne weiter. Auf den Seiten von IT.SERVICES finden Sie weitere Informationen.

## Downloads

Eine Checkliste und eine Zusammenfassung der PC-Grundsicherung im PDF-Format befindet sich in der Überarbeitung.

## PC-Grundsicherung


- zurück zur Übersicht
- zu Teil I - Basissicherung
- zu Teil II - organisatorische Sicherung