Grundschutz

1. Überblick

In diesem Dokument wird beschrieben, welche Programme auf den Rechnern der Hochschule Fulda mindestens installiert sein sollten und wie diese Programme konfiguriert werden müssen, damit eine gewisse "Basissicherheit" vorhanden ist. Da auch die beste Sicherheitsmaßnahme keinen Schutz bietet, wenn die Benutzer und Benutzerinnen den Schutz umgehen oder die Maßnahmen nicht ernst nehmen, gibt es auch einige Hinweise zur Verhaltensweise der Benutzer und Benutzerinnen.

In den Einstellungshinweisen ab Kapitel 2 bedeutet "Start > ... > ...", dass Sie mit dem Eintrag *Start* in der Menüzeile (im Allgemeinen am linken unteren Rand des Bildschirms) beginnen und dann mit einem Eintrag des Menüs, einem Karteikartenreiter oder einem anderen Element weitermachen, das die entsprechende Beschriftung aufweist.

Seitenanfang

2. Notwendige und hilfreiche Programme (technischer Schutz)

Damit Sie mit dem Rechner überhaupt arbeiten können, benötigt er ein **Betriebssystem**. Das Betriebssystem muss immer auf dem aktuellen Stand sein, damit alle bekannten Sicherheits-löcher" gestopft" werden. Falls das Betriebssystem ein "**Automatisches *Update***" zur Verfügung stellt, sollte diese Eigenschaft aktiviert werden, da die Sicherheitslöcher dann so schnell wie möglich geschlossen werden. Die aktuellen *Windows*-Betriebssysteme von *Microsoft* bieten diese Funktion. Bei *Windows 10* können Sie die automatische Aktualisierung des Systems eigentlich nicht verhindern, sodass Sie nichts machen müssen. Falls Sie trotzdem manuell eine Suche nach *Updates* starten wollen, klicken Sie bei *Windows 10* mit der rechten Maustaste auf "Start" und danach auf "Einstellungen". Klicken Sie dann auf "Updates und Sicherheit" und anschließend auf "Nach Updates suchen", um eine Suche nach aktuellen Versionen zu starten.

Der Zugriff auf den Rechner aus dem *Internet* bzw. von Programmen des Rechners auf das *Internet* sollte überwacht und gesteuert werden. Diese Aufgabe übernimmt eine ***Firewall***. Obwohl alle Rechner der Hochschule Fulda durch eine zentrale *Firewall* geschützt werden, sollte trotzdem auf jedem Rechner eine lokale *Firewall* eingerichtet werden, um auch einen Schutz vor Rechnern innerhalb des Hochschulnetzes (*Intranet*) zu gewährleisten, die vielleicht schlecht gepflegt werden und deshalb mit Schad-Software (Viren, Würmern, Trojanern, usw.) verseucht sind. Außerdem kann die lokale *Firewall* unter Umständen verhindern, dass sich Schad-Software

von einem verseuchten Rechner auf andere Rechner der Hochschule ausbreitet. Unter *Windows* können Sie beispielsweise die **Windows-Firewall** verwenden, die standardmäßig in den neueren *Windows*-Betriebssystemen enthalten ist. Klicken Sie mit der linken Maustaste auf "Start" und wählen Sie dann "Windows-Sicherheit" (am Ende der Programmliste), wenn Sie *Windows 10* benutzen. Dort sollte für "Firewall & Netzwerkschutz" der Satz "Keine Aktion erforderlich." stehen. Falls Aktionen erforderlich sein sollten, klicken Sie auf "Firewall & Netzwerkschutz" und dann nacheinander auf "Domänennetzwerk", "Privates Netzwerk" und "Öffentliches Netzwerk" und schalten dort den Schalter "Windows Defender Firewall" auf "Ein". **Auf portablen Rechnern (*Notebooks*) muss unbedingt eine *Firewall* eingerichtet werden!**

Jeder Rechner muss vor Schad-Software (Viren, Würmern, Trojanern, usw.) durch ein ***Antiviren*-Programm** geschützt werden. Die Hochschule Fulda benutzt hierfür das Programm **Sophos Intercept**, das auf allen Hochschulrechnern eingesetzt werden muss. Überprüfen Sie alle formatierten Anhänge (Word, Excel, PDF, ...) von *E-Mails* auf Schad-Software, bevor Sie die Anhänge mit den entsprechenden Programmen öffnen. Weitere Hinweise (auch für private Rechner) finden Sie auf der Seite *Virenschutz (Sophos)* des Rechenzentrums.

Natürlich wollen Sie Ihren Rechner nicht nur schützen sondern auch nutzen. Die erforderlichen Sicherheitseinstellungen für Ihr ***E-Mail*-Programm** können Sie dem separaten Dokument *E-Mail* und die Einstellungen für Ihren ***Web-Browser*** dem Dokument *Web-Browser* entnehmen, da die Anzahl der verschiedenen Produkte den Rahmen dieses Dokuments sprengen würde. Sie können diese Dokumente auch über die Navigationsleiste öffnen. Die Sicherheitseinstellungen für Ihre anderen Programme sollten Sie in der *Hilfe* des Programms oder im *Internet* recherchieren.

Denken Sie daran, alle Programme automatisch oder zumindest regelmäßig zu aktualisieren, damit Sie Schad-Software und *Hackern* die Arbeit so schwer wie möglich machen.

Seitenanfang

3. Passwörter und Zwei-Faktor-Authentisierungen

Wählen Sie ein gutes Passwort und halten Sie es geheim. Im Dokument Passwörter wird beschrieben, wie Sie ein gutes Passwort bilden und wie Sie es ändern können. Beachten Sie bitte unbedingt die folgenden Hinweise.

1. Geben Sie Ihr Passwort niemals an andere Personen weiter, da Sie ggf. dafür verantwortlich gemacht werden, wenn Ihr Benutzerkonto (*Account*) von anderen Personen missbraucht wird.
2. Schreiben Sie Ihr Passwort nicht auf oder bewahren Sie es zumindest weit weg von Ihrem Computer und ohne erkennbaren Bezug zu Ihrem Benutzerkonto auf (niemals im selben Raum).
3. Speichern Sie Ihre Passwörter niemals in Dateien oder Programmen, um sich die Arbeit "zu erleichtern", da sie sonst von Schad-Software gelesen und missbraucht werden können.
4. Ändern Sie sofort Ihr Passwort, wenn es in fremde Hände geraten ist oder Sie den Verdacht haben, dass es unautorisierten Personen bekannt geworden ist.
5. Benutzen Sie verschiedene Passwörter für verschiedene Rechner oder Tätigkeiten.
6. Verwenden Sie Ihren Benutzernamen und Ihr Passwort niemals für Preisausschreiben oder Ähnliches.
7. Verwenden Sie niemals ein Passwort auf irgendeiner *Internet*-Seite, das Ihrem eigenen Passwort ähnelt oder sogar entspricht, da Sie damit einem potenziellen "Hacker" eine Einbruchsmöglichkeit in Ihren Rechner bieten, wenn diese Angaben im Klartext gespeichert werden.

8. Wenn Sie Ihr Passwort vergessen haben sollten, können Sie sich im Rechenzentrum ein neues Passwort aushändigen lassen. Die Überprüfung Ihrer Identität kann vor Ort mithilfe eines Lichtbildausweises oder über eine Videokonferenz erfolgen.
9. Schützen Sie das Hochfahren Ihres Rechners (den sogenannten *Boot*-Vorgang) durch ein Passwort (das sogenannte "BIOS-Passwort", siehe Abschnitte "Funktionen" und "Sicherheit" in der deutschen Erklärung zum BIOS oder besser erklärt im Abschnitt "Configuration" in der englischen Erklärung zum BIOS), wenn Sie auf dem Rechner personenbezogene oder andere sensitive Daten speichern. Dieser Schutz muss auch dann wirksam sein, wenn ein *Eindringling* den Rechner mit einer eigenen CDROM, DVD, einem *Memory Stick* oder etwas Ähnlichem starten will. Falls der Rechner nicht über einen derartigen BIOS-Kennwortschutz verfügt, dürfen personenbezogene Daten nur verschlüsselt auf der Festplatte gespeichert werden.

Der Zugriff auf einige Funktionen einiger Anwendungen (z. B. im **H**ochschul-**Or**ganisations-System für **St**udium und **L**ehre ("horstl")) wird für einige Personen (z. B. Beschäftigte und Lehrbeauftragte) durch eine **Zwei-Faktor-Authentisierung** (oft auch "Zwei-Faktor-Authentifizierung" genannt) geschützt, sodass sich diese Personen neben dem Passwort durch einen zweiten Faktor rechtsgültig identifizieren müssen. Das System kann die Identität der Personen dann über die beiden Faktoren überprüfen (authentifizieren) und ihnen die Privilegien (Rechte) gewähren, die der nachgewiesenen Identität zustehen (Autorisierung). Die Web-Seite zur Zwei-Faktor-Authentifizierung des Rechenzentrums beschreibt, welche Verfahren unterstützt werden und wie sie ggf. eingerichtet werden können. Weitere Informationen zur Zwei-Faktor-Authentisierung finden Sie auch bei Wikipedia. Beachten Sie bitte unbedingt die folgenden Hinweise.

1. Geben Sie Ihren zweiten Faktor (*Smartphone mit registrierter App* oder *Hardware-Token zur Erzeugung eines Einmal-Passworts*) niemals an andere Personen weiter, da Sie ggf. dafür verantwortlich gemacht werden, wenn Ihr Benutzerkonto (*Account*) von anderen Personen missbraucht wird.
2. Falls Sie ein *Hardware-Token* benutzen, ist es verboten, den *Hardware-Token* zusammen mit dem Endgerät (z. B. Notebook) in derselben Tasche zu transportieren.
3. Der Verlust des zweiten Faktors oder ein Verdacht auf Missbrauch des zweiten Faktors **muss unverzüglich** dem oder der IT-Sicherheitsbeauftragten des Rechenzentrums gemeldet werden.

Seitenanfang

4. Persönliche Verhaltensweise

Geben Sie niemals persönliche Daten im *Internet* an, wenn es nicht unbedingt sein muss. Erfinden Sie ggf. Namen und Adressen, wenn Sie sich bei Web-Anbietern registrieren, in Foren diskutieren oder in *Chat*-Räumen unterhalten wollen. Beachten Sie bitte außerdem die folgenden Hinweise.

1. Ändern Sie niemals Ihr Passwort, die Konfiguration des Betriebssystems oder eines Programms auf Wunsch einer anderen (unbekannten) Person, die sich telefonisch bei Ihnen meldet. Laden Sie auch niemals auf Wunsch einer anderen Person Software aus dem *Internet* herunter, um sie dann zu installieren. Rufen Sie niemals bestimmte Web-Seiten auf und geben Sie auch niemals irgendwelche Kommandos ein, wenn Ihnen eine unbekannte Person dazu rät.
2. Geben Sie niemals sensible oder interne Informationen per Telefon weiter.
3. Kennzeichnen Sie portable Datenträger (CDROM, DVD, *Memory-Stick*, usw.) mit sensiblen Daten und verschließen Sie sie, wenn Sie den Raum verlassen.

4. Sorgen Sie für eine geeignete Entsorgung sensibler Dokumente und Datenträger, die zurzeit vertrauliche Daten enthalten oder in der Vergangenheit enthalten haben.
5. Benutzen Sie niemals CDROMs, DVDs usw. aus unbekannten Quellen (liegen einfach irgendwo öffentlich "herum") auf einem Rechner der Hochschule, da durch die *Autostart*-Funktion automatisch Schad-Software auf dem Rechner installiert werden könnte.
6. Öffnen Sie niemals *E-Mail*-Anhänge, wenn Sie die *E-Mail* nicht erwartet haben und bevor Sie den Anhang auf Schad-Software untersucht haben. Denken Sie daran, dass der Absender gefälscht sein kann.
7. Leiten Sie niemals eine *E-Mail* nur deshalb weiter, weil es in der *E-Mail* verlangt wird. Tragen Sie nicht zur Verbreitung von Schad-Software oder *Spam-E-Mail* bei.
8. Verschicken Sie sensible Informationen nicht per *E-Mail* oder nur in verschlüsselter Form.
9. Schützen Sie Ihren Rechner durch einen passwort-geschützten Bildschirmschoner oder melden Sie sich ab, wenn Sie den Raum verlassen.
10. Sorgen Sie dafür, dass auf Ihrem Rechner immer die aktuelle Antiviren- und Anti-Spy-Software installiert ist und benutzen Sie eine aktuelle *Firewall*.
11. Deaktivieren oder entfernen Sie auf keinen Fall die Antiviren-Software oder die *Firewall* ohne Erlaubnis des Rechenzentrums.
12. Niemand darf Software herunterladen oder benutzen, die die Umgehung von Schutzmechanismen ermöglicht. **Ausnahme:** Systemadministratoren und Systemadministratorinnen zur Überprüfung und Wahrung der Sicherheit der Systeme.
13. Niemand darf an seinen Arbeitsplatzrechner ohne Zustimmung des Rechenzentrums eigene Netzwerkzugänge anschließen.
14. Studierende haben keinen Anspruch auf Datensicherung und -wiederherstellung, sodass sie wichtige Daten ggf. selbst sichern müssen.
15. Achten Sie auf sicherheitsrelevante Vorfälle und melden Sie sie.

Seitenanfang

5. Maßnahmen bei Virenbefall

Falls Sie vermuten oder sogar wissen, dass Ihr Rechner von einem oder mehreren Schad-Programmen (Viren, Würmern, Trojanern, ...) befallen ist, sollten Sie folgende Maßnahmen treffen.

1. **Trennen Sie den infizierten Rechner so schnell wie möglich vom Hochschulnetz**, um weitere Schäden durch Verbreitung der Schad-Software auf andere Systeme zu vermeiden. Das betroffene System sollte **möglichst nicht vom Stromnetz getrennt** und auch **nicht heruntergefahren werden**, damit ggf. später forensische Analysen durchgeführt werden können, um die Schad-Software und die verursachten Schäden zu untersuchen und damit Maßnahmen zur Eindämmung von Folgeschäden getroffen werden können.
    - Wenn der Rechner mit einem **Netzwerkkabel** mit dem Hochschulnetz verbunden ist, sollte das Kabel abgezogen werden. Das Kabel ist mit einem Häkchen versehen, das manchmal unter einer Plastikabdeckung versteckt ist und vor dem Abziehen heruntergedrückt werden muss.
    - Wenn der Rechner über das **Funknetz (WLAN)** mit dem Hochschulnetz verbunden ist, sollten Sie versuchen, das Netz über den WLAN-Schalter oder den berührungssensitiven Bildschirm (*Touchscreen*) auszuschalten. Falls die Schad-Software dies verhindert, sollten Sie versuchen, das Gerät auszuschalten, indem

Sie den Ein-/Ausschaltknopf mehrere Sekunden herunterdrücken. Trennen Sie in diesem Fall das Gerät auch vom Stromnetz, falls es damit verbunden ist und entfernen Sie die Batterie, falls dies möglich ist.

Informieren Sie danach bitte sofort den *Helpdesk* des Rechenzentrums und die Person, die für die Administration des Rechners zuständig ist.

2. Melden Sie den Vorfall auch an Ihren IT-Sicherheitsbeauftragten bzw. Ihre IT-Sicherheitsbeauftragte, der bzw. die Ihnen ggf. bei der *Säuberung* Ihres Rechners behilflich ist bzw. Ihnen mitteilt, wer Ihnen helfen kann, die Schad-Software von Ihrem Rechner zu entfernen. Abhängig von der Art der Infektion ist es unter Umständen notwendig, den Rechner neu zu installieren und die Daten von einer Datensicherung zurückzuspielen, da nur so sichergestellt werden kann, dass die Schad-Software vollständig entfernt worden ist.
3. Falls eine Neuinstallation nicht notwendig ist und Sie die Schad-Software selbst entfernen wollen, benötigen Sie eine sogenannte Rettungs-CD, die ein *boot*-fähiges Betriebssystem und eine Antiviren-Software enthält (z. B. Desinfec't). Sie müssen die CD/DVD bzw. den *Memory-Stick* auf einem anderen Rechner erstellen und Ihren Rechner dann von diesem Medium starten, damit Sie eine "virenfreie" Umgebung haben. Anschließend können Sie Ihre Festplatte mit dem Antiviren-Programm untersuchen und die Schad-Software entfernen. Falls kein Virus gefunden wird, kann Ihr Rechner trotzdem mit Schad-Software verseucht sein, die das Antiviren-Programm nur nicht findet. Kontaktieren Sie in diesem Fall unbedingt das Rechenzentrum, bevor Sie Ihren Rechner wieder an das Hochschulnetz anschließen.
4. Damit Ihr Rechner nicht sofort erneut mit Schad-Software verseucht wird, sollten Sie unbedingt die Software Ihres Rechners aktualisieren und sofern noch nicht geschehen, ein Antiviren-Programm und eine lokale *Firewall* installieren. Hinweise hierzu finden Sie im Kapitel 2 dieses Dokuments.
5. Das Rechenzentrum und die lokalen Systemadministratoren und Systemadministratorinnen sind verpflichtet, den Betrieb und die Sicherheit des Hochschulnetzes zu gewährleisten und führen ggf. folgende Aktionen durch, wenn Gefahr im Verzug ist:
    - Falls es erforderlich ist, sperren sie die IP-Adresse an der nächstmöglichen Stelle.
    - Falls der befallene Rechner über das Funknetz (WLAN) im Hochschulnetz ist, sperren sie das Benutzerkonto und unterbrechen die Verbindung.
    - Sie benachrichtigen den Benutzer bzw. die Benutzerin oder den zuständigen Administrator bzw. die zuständige Administratorin über den Fehler.

Seitenanfang

6. Systemadministration

Systemadministratoren und Systemadministratorinnen haben eine besondere Verantwortung und sollten dafür sorgen, dass in ihrem Verantwortungsbereich die IT-Sicherheitsrichtlinie umgesetzt und eingehalten wird. Zusätzlich sollten sie folgende Hinweise beachten.

1. Die Benutzerkonten sollten so angelegt werden, dass nur gute Passwörter benutzt werden können und dass das Benutzerkonto gesperrt wird, falls ein Passwort mehrfach falsch eingegeben wird (wenn das System diese Möglichkeiten bietet).
2. Ändern Sie Standard-Passwörter von Telefonanlagen, Rechnern, Netzkomponenten usw. und sperren Sie ggf. Standard-Benutzer (Gast-*Accounts*), um die Systeme zu schützen.
3. Es sollten regelmäßige Datensicherungen durchgeführt werden und die Datensicherungsmedien sollten ggf. in feuer- und einbruchsicheren Schränken aufbewahrt werden, soweit

es für den Datenbestand erforderlich ist. Falls personenbezogene oder andere sensible Daten extern gelagert werden, sollten sie verschlüsselt gespeichert werden.

4. Ändern oder sperren Sie die Rechnerzugangsberechtigung, wenn eine Person die Hochschule verlässt oder einen neuen Aufgabenbereich erhält. Die erforderlichen Daten müssen vom *Student Service Center (SSC)* für Studierende und von der Personalabteilung für Bedienstete an das Rechenzentrum gemeldet werden, das die Daten umgehend an alle Systemadministratoren und Systemadministratorinnen weiterleitet.
5. Falls ein Systemadministrator oder eine Systemadministratorin die Hochschule verlässt, **müssen** sofort alle System-Passwörter geändert werden und ggf. müssen die Passwort-Dateien bzw. -Datenbanken nach neuen *Accounts* mit Privilegien durchsucht werden, um die Sicherheit der Systeme zu gewährleisten. Unter UNIX-ähnlichen Betriebssystemen muss ggf. auch nach Programmen mit Privilegien (SUID- oder SGID-Bit gesetzt) gesucht werden, die nicht zum normalen Betriebssystem gehören.
6. Temporäre Benutzerkonten sollten deaktiviert werden, wenn das Projekt beendet wurde, für das sie eingerichtet worden sind.
7. Benutzer und Benutzerinnen dürfen ihr Benutzerkonto nicht telefonisch deaktivieren oder aktivieren lassen. Eine Deaktivierung oder Aktivierung kann nur schriftlich oder persönlich veranlasst werden. Soweit die Person nicht bekannt ist, muss die Identität vorher überprüft werden. Die Überprüfung kann vor Ort mithilfe eines Lichtbildausweises oder über eine Videokonferenz erfolgen. Bei schriftlichen Anträgen sollte auch geklärt werden, ob der Antrag tatsächlich von der Person gestellt worden ist.
8. Systemadministratoren und Systemadministratorinnen sollten Software herunterladen und benutzen, die die Überprüfung und Wahrung der Sicherheit der Systeme ermöglicht (z. B. *Password Cracker* zur Überprüfung von guten und schlechten Passwörtern, falls das System einen Zugriff auf die Passwörter zulässt).

Seitenanfang

7. Funknetze (WLAN) / *Server*

Für den Betrieb von Funknetzen (WLAN) und *Server* gelten die folgenden Bestimmungen.

1. Die Fachbereiche und zentralen Einrichtungen dürfen eigene Funknetze, die einen Zugang auf die allgemeine Rechnerinfrastruktur erlauben, nur mit Zustimmung des Rechenzentrums betreiben. Isolierte Funknetze für die Ausbildung dürfen nach Bedarf eingerichtet und betrieben werden.
2. Der Netzzugang zu produktiven Funknetzen darf nur über eine Benutzerauthentifizierung erfolgen. Ein Zugang über Hardware- oder IP-Adressen ist nicht erlaubt.
3. Der Datenverkehr in Funknetzen muss verschlüsselt sein. Passwörter dürfen auf keinen Fall im Klartext in einem Funknetz übertragen werden. Hinweise zur Einrichtung des WLANs finden Sie auf der Web-Seite WLAN (eduroam) des Rechenzentrums.
4. Die Zugangsdaten (IP-Adresse, Benutzerkonto, Zeit) zu produktiven Funknetzen müssen protokolliert werden.
5. Die Fachbereiche und zentralen Einrichtungen dürfen eigene *Server*, die mit dem Hochschulnetz verbunden sind, nur mit Zustimmung des Rechenzentrums betreiben. Isolierte *Server* in abgeschlossenen Labornetzen für die Ausbildung dürfen nach Bedarf eingerichtet und betrieben werden.
6. In Funknetzen dürfen keine *Server* betrieben werden.

7. Über externe Zugänge dürfen *Server* nur über eine gesicherte VPN-Verbindung verwaltet werden. Hinweise zur Einrichtung der VPN-Software finden Sie auf der Web-Seite VPN Zugang des Rechenzentrums.
8. Die VPN-Zugangs-Software, die Konfigurationsdatei für die VPN-Software sowie die Benutzerkennung und das Passwort für die Einwahl in das Funknetz der Hochschule Fulda dürfen nicht an andere Personen weitergegeben werden.

Seitenanfang

8. Datenverschlüsselung

Es gibt sehr viele Produkte, die die Verschlüsselung von Daten unterstützen. Wenn Sie sensitive Daten als Anlage einer *E-Mail* verschicken wollen, können Sie die Datei oder Dateien beispielsweise mit dem Programm 7-zip komprimieren und verschlüsseln. Das Passwort zum Entschlüsseln können Sie dem Empfänger dann z. B. telefonisch mitteilen. "7-zip" unterstützt auch die Verschlüsselung des Archiv-Verzeichnisses (*header encryption*), sodass eine unbefugte Person noch nicht einmal die Namen der Dateien im Archiv herausfinden kann.

Wenn Sie im täglichen Betrieb auf Ihrer Festplatte arbeiten, wollen Sie die Dateien nicht manuell ver- und entschlüsseln, zumal die Dateien dann für den Zeitraum der Bearbeitung unverschlüsselt auf der Festplatte gespeichert wären. Hierfür benötigen Sie ein Produkt, das die Daten automatisch und für Sie transparent (*on-the-fly*) ver- und entschlüsselt. Diese Produkte lassen sich in zwei Klassen einteilen:

1. Produkte, die Dateien oder alle Dateien in einem Dateiverzeichnis verschlüsseln. In diese Kategorie fällt beispielsweise das Produkt *Encrypting File System (EFS)*, das eine Erweiterung des NTFS-Dateisystems von *Microsoft* ist und damit in jedem modernen *Windows*-Betriebssystem zur Verfügung steht. Da temporäre Dateien in der *Windows*-Welt häufig in anderen Verzeichnissen oder sogar in anderen Partitionen gespeichert werden, kann es passieren, dass die temporären Dateien nach der Bearbeitung unverschlüsselt zur Verfügung stehen (die temporäre Datei wird zwar gelöscht, aber ihr Inhalt wird nicht zerstört, sodass er später wiederhergestellt werden könnte).

2. Produkte, die eine verschlüsselte Partition in einer Datei anlegen (ein sogenannter *Container*) oder eine vollständige Partition der Festplatte verschlüsseln. Sie werden dann noch in Produkte unterschieden, die nur Daten-Partitionen verschlüsseln können und solche, die auch System-Partitionen verschlüsseln können. Falls ein Produkt sowohl Daten- als auch System-Partitionen verschlüsseln kann, kann die gesamte Festplatte verschlüsselt werden. In diese Gruppe gehören z. B. das kommerzielle Produkt SecurStar DriveCrypt sowie das freie Produkt VeraCrypt. Wikipedia stellt in dem Artikel "Comparison of disk encryption software" Eigenschaften, Verfügbarkeit, Aktualität usw. von vielen Festplattenverschlüsselungsprogrammen dar. *Microsoft Windows* bietet für einige Betriebssystemversionen das Programm BitLocker an.

Eine detaillierte Beschreibung zum Einsatz dieser Programme würde den Rahmen dieser Dokumentation sprengen. Weitere Informationen finden Sie z. B. bei Wikipedia 7-zip, Encrypting_File_System, VeraCrypt, BitLocker.

Seitenanfang

9. Aussonderung von Rechnern, Druckern und Datenträgern

Bei der Aussonderung von Rechnern und Datenträgern sollte man daran denken, dass die Daten physikalisch nicht zerstört bzw. überschrieben werden, wenn man die Dateien löscht, sodass sie

später unter Umständen wiederhergestellt werden können. Beachten Sie deshalb unbedingt die folgenden Hinweise.

1. Sorgen Sie dafür, dass sensible Dokumente bzw. Datenträger (CDROM, DVD, *Memory-Stick*, usw.) mit personenbezogenen oder anderen sensiblen Daten nicht wiederherstellbar zerstört werden (z. B. mithilfe eines Schredders, soweit dies möglich ist), bevor sie ausgesondert werden.

2. Sorgen Sie dafür, dass Festplatten ggf. vollständig magnetisiert oder so zerstört werden, dass sie nicht wiederhergestellt werden können, wenn sie personenbezogene oder andere sensible Daten enthalten haben.

3. Denken Sie daran, dass (Netzwerk)-Drucker häufig mit Festplatten ausgestattet sind, auf denen Dateien vor dem Ausdruck zwischengespeichert werden und vergessen Sie deshalb nicht, die Daten auf diesen Festplatten ebenfalls zu zerstören, bevor der Drucker ausgesondert wird.

4. Viele Geräte speichern Konfigurationen in *Flash*-Speichern. Denken Sie daran, die Konfigurationen zu löschen, bevor Sie das Gerät aussondern, da die Kenntnis der Konfiguration unter Umständen einen Angriff auf die IT-Infrastruktur erleichtert.
5. Denken Sie daran, dass unter Umständen auch Multi-Funktionsgeräte, *Scanner*, Fax-Geräte usw. mit Festplatten oder *Flash*-Speichern ausgestattet sind, auf denen Daten zwischengespeichert werden. Löschen Sie diese Daten, bevor Sie das Gerät aussondern.

Seitenanfang

10. Weitere Hinweise

Moderne Kopierer sind im Allgemeinen mit Festplatten ausgestattet, auf denen die Kopien vor dem Ausdruck zwischengespeichert werden. Vergessen Sie nicht die Daten auf den Festplatten zu vernichten, bevor der Kopierer ausgesondert wird. Falls auf dem Kopierer auch personenbezogene oder andere sensible Daten kopiert werden sollen, sollte der Kopierer unbedingt in einem verschlossenen Raum aufgestellt werden und nicht an das Hochschulnetz angeschlossen werden. Die Daten der Festplatte können gelesen werden, wenn ein Rechner mit dem Kopierer verbunden werden kann und das Administrator-Passwort bekannt ist (für viele Kopierer steht das Standard-Passwort zusammen mit der Bedienungsanleitung im *Internet*). Einige Kopierer können mit einem Modul zum sicheren Löschen der Festplatte ausgestattet werden.

Seitenanfang

Letzte Änderung: 29. November 2021 | PDF-Version