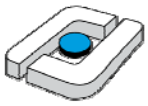

Hochschule Osnabrück
University of Applied Sciences

IT-Sicherheitsrichtlinie der Hochschule Osnabrück

Inhaltsverzeichnis

1. Inhalt und Ziel dieser Richtlinie

Ziel dieser Richtlinie ist es, das Personal und die Studierenden der Hochschule Osnabrück für die Belange der Sicherheit der Informationstechnologie (IT) zu sensibilisieren, um eine störungsfreie und sichere IT-Nutzung zu gewährleisten. Das unsachgemäße Verhalten der eigenen IT-Nutzer ist nachweislich Grundlage des überwiegenden Teils von Sicherheitsvorfällen. Daher ist die Verbesserung der IT-Sicherheitskenntnisse und die Erhöhung der Eigenverantwortung jedes IT-Nutzers eine wirksame Maßnahme zur Erhöhung der IT-Sicherheit.

In dieser Richtlinie werden Grundregeln und Empfehlungen für eine sichere und ordnungsgemäße Nutzung der IT-Infrastruktur der Hochschule Osnabrück definiert. Die Wissenschaftsfreiheit wird von den Regelungen und Empfehlungen nicht eingeschränkt.

2. Geltungsbereich und gesetzliche Grundlagen

Diese Richtlinie gilt für die Nutzung der zentralen und dezentralen IT-Infrastruktur der Hochschule Osnabrück (Fakultäten, Labore, Rechnerpools, Institute, zentrale Geschäftsbereiche und zentrale Einrichtungen), bestehend aus Rechnern und anderen Systemen zur rechnergestützten Informationsverarbeitung. Es wird empfohlen, die Regelungen und Empfehlungen auch bei der privaten IT-Nutzung zu berücksichtigen.

Die Richtlinie basiert auf dem Bundesdatenschutzgesetz (BDSG), dem Niedersächsischen Landesdatenschutzgesetz (NLDG), den damit in Verbindung stehenden Verordnungen sowie dem Urheberrechtsgesetz in Bezug auf den disziplinierten und sorgfältigen Umgang mit Daten.

3. Vorgaben und Empfehlungen für IT-Nutzer

Die in den folgenden Abschnitten

- Internet, WWW und E-Mail
- Viren und andere schädliche Software
- Nutzerkennungen und Passwörter
- Schutz sensibler Daten
- PC-Pools und Softwarelizenzen

aufgeführten Regelungen und Empfehlungen gelten für sämtliche IT-Nutzer der Hochschule Osnabrück (Professorinnen und Professoren, wissenschaftliche und künstlerische Mitarbeiterinnen und Mitarbeiter, Lehrkräfte für besondere Aufgaben, Mitarbeiterinnen und Mitarbeiter in Technik und Verwaltung und die Studierenden). Sie bilden die Grundlage für eine sichere und störungsfreie IT-Nutzung.

3.1. Internet, WWW und E-Mail

Das Internet ist ein weltumspannendes Netz mit Millionen von Rechnern. Es ist ein offenes Netz, das für jeden zugänglich ist.

Genutzt wird das Internet als schnelles, effizientes Medium zur Informationsrecherche, zur Übertragung von E-Mails und zur Abwicklung vielfältiger Geschäfte.

Gerade die Offenheit und die zunehmende geschäftliche Nutzung machen das Internet attraktiv für Kriminelle, die versuchen, Systeme mit Schadsoftware zu infizieren und für kriminelle Zwecke zu nutzen. Die Gefährdungen reichen vom Abhören privater Informationen und Passwörtern (Datenklau, Identitätsdiebstahl) bis zur Internet-Blockade ganzer Unternehmen oder Organisationen.

Zum Schutz der Daten der Hochschule Osnabrück sind daher folgende Regelungen bei der E-Mail-Nutzung und dem „Surfen“ im Internet zu beachten.

E1 Die Übertragung sensibler Informationen (z.B. per E-Mail) ist nur in verschlüsselter Form zulässig!

E-Mails sind Postkarten, keine Briefe!

E-Mails werden unverschlüsselt übertragen und auf vielen Rechnern zwischengespeichert. E-Mails sind daher mit Postkarten vergleichbar: Sie können an vielen Orten mitgelesen werden.

E-Mails an hochschulinterne Adressaten werden oft auch über das Internet weitergeleitet. Daher gilt unabhängig davon, ob E-Mails intern verschickt werden:

Versenden Sie nie vertrauliche oder personenbezogene Daten unverschlüsselt per E-Mail.

Einfache Maßnahmen

- zur Verschlüsselung von E-Mails (1.+2.) und

- zum sicheren Zugriff auf zentral abgelegte Daten (3.).

1. Nutzung der ZIP-Verschlüsselung

Die meisten Komprimierungsprogramme erlauben die Angabe eines Passworts. Das kostenfreie Programm 7-Zip (http://www.heise.de /software/download/7_zip/13139) kann sogar AES verschlüsseln. Aber auch die Basis ZIP-Verschlüsselung ist nicht einfach zu knacken, wenn ein hinreichend langes (≥12 Zeichen) und zufälliges Passwort verwendet wird. In der Gruppe, die die Unterlagen austauschen will, (z.B. Berufungskommission) muss dann einmalig ein sicheres Passwort festgelegt werden.

2. Nutzung einer dedizierten Verschlüsselung, wie z.B. AxCrypt

In der Handhabung bequemer als die ZIP-Verschlüsselung ist AxCrypt (http://www.heise.de/software/download/axcrypt/31828, Freeware). Es bietet eine sichere AES-Verschlüsselung, kann Passwörter speichern und integriert sich in den Windows-Explorer, so dass mit der rechten Maustaste direkt verschlüsselt und entschlüsselt werden kann. Dabei können nicht nur einzelne

Dateien, sondern direkt ganze Folder verschlüsselt werden. Nachteile: Installation erforderlich, nur für Windows verfügbar.

3. Zentrale Dokumentenablage mit verschlüsseltem Zugriff

Die Gruppe, die auf sensible Daten zugreifen will, legt diese zentral geschützt ab (z.B. geschützte StudIP-Veranstaltung mit eingeschränkten Zugriffrechten) und greift ausschließlich per https auf die Daten (z.B. die StudIP-Veranstaltung) zu (siehe auch D4).

E2 Kein Öffnen von E-Mail-Anhängen ohne vorhergehende Plausibilitätsprüfung!

E-Mail Absender ist leicht fälschbar

E-Mails sind einer der häufigsten Übertragungswege von Viren. Daneben können E-Mail-Inhalte und -Absender sehr leicht gefälscht werden. Begegnen Sie deshalb empfangenen E-Mails immer mit gesundem Misstrauen. Prüfen Sie, z.B. anhand der Formulierung, ob es plausibel ist, dass die E-Mail tatsächlich vom angegebenen Absender stammt.

Ausführbare Anhänge löschen

Ganz besondere Vorsicht gilt ausführbaren Anhängen. Diese sollten Sie grundsätzlich NICHT öffnen, sondern direkt löschen. Öffnen Sie ausführbare Anhänge nur, nachdem Sie sich zuvor explizit – z.B. durch einen Anruf beim Absender – von deren Vertrauenswürdigkeit überzeugt haben. Dies gilt insbesondere auch für komprimierte oder verschlüsselte ausführbare Anhänge.

E3 Kein Versand ausführbarer Anhänge per E-Mail!

Automatische Filterung

Aufgrund ihrer Gefährlichkeit werden E-Mails mit ausführbaren Anhängen von vielen Unternehmen direkt gefiltert. Sie erreichen ihren Adressaten erst gar nicht. Falls die E-Mail ihren Adressaten erreicht, sollte dieser sie nicht ungeprüft öffnen (siehe E2).

Verzichten Sie daher auf den Versand ausführbarer Anhänge.

E4 Misstrauen Sie Internet-Links in E-Mails

Phishing

Links in E-Mails werden häufig genutzt, um Anwender auf nicht vertrauenswürdige Web-Seiten zu führen. Bekanntestes Beispiel ist das Phishing, bei dem man über einen Link auf eine Bankseite gelangt, die zwar optisch der Originalseite gleicht, sich jedoch auf dem Webserver eines Internet-Kriminellen befindet.

Drive-by-Downloads

Bereits das Klicken auf den Link in der E-Mail kann ausreichen, um ihren Rechner mit Schadsoftware zu verseuchen und für den Angreifer zugänglich zu machen (sog. Drive-by-Downloads oder Heap-Overflows).

Genau wie bei den Anhängen (siehe E2), sollten Sie auch E-Mail-Links nur betätigen, nachdem Sie sich von der Vertrauenswürdigkeit der E-Mail überzeugt haben.

E5 Automatisches Nachladen von Inhalten aus dem Internet deaktivieren!

Anzeige der E-Mail kann zur Verseuchung führen

In E-Mails können Links eingebettet sein, die automatisch Daten aus dem Internet nachladen. Bei der HTML-Anzeige einer solchen E-Mail, werden automatisch z.B. Bilder aus dem Internet geladen und mit der E-Mail angezeigt. Diese Funktion ist höchst sicherheitskritisch, da z.B. auch Schadsoftware von Servern Internet-Krimineller automatisch ausgeführt werden könnte. In diesem Fall reicht die HTML-Anzeige der E-Mail, um Ihren Rechner zu verseuchen und für den Angreifer zugänglich zu machen.

Konfigurieren Sie Ihr E-Mail-Programm daher so, dass bei der Anzeige von E-Mails Inhalte aus dem Internet nicht automatisch nachgeladen werden.[1][2]

Als weitere Vorsichtmaßnahmen können Sie das Vorschaufenster abschalten, damit E-Mails nicht automatisch geöffnet und angezeigt werden.

E6 Kein Versand von E-Mails mit anstößigen Inhalten

Kein Surfen auf Seiten mit anstößigen Inhalten

Kein Speichern von anstößigen Inhalten

Anstößige Inhalte sind u.a.

- Inhalte, die gegen Ethik und den guten Geschmack verstoßen oder eine Personen belästigen,
- illegale, rassistische, gewalttätige, sittenwidrige oder pornografische Inhalte.

E7 Kein Download von Software aus dem Internet

Die in der HS Osnabrück eingesetzte Software ist lizenziert und geprüft. Im Internet bereitgestellte Software ist nur bedingt vertrauenswürdig. Ihr Einsatz kann schädliche Folgen für die IT der Hochschule nach sich ziehen.

Laden und installieren Sie daher keine Software aus dem Internet zur Vermeidung von Lizenzproblemen und zum Schutz der Hochschul- Rechner und -Netze.

Falls Sie eine neue/andere Software installieren wollen, wenden Sie sich an ihren Systemadministrator.

---

[1] In MS Outlook: Extras -> Optionen -> Sicherheit -> „Bilder und andere externe Inhalte in HTML-E-Mail blocken“ aktivieren

[2] In GroupWise: Werkzeuge -> Optionen -> Umgebung -> Layouts „Standardlayout & Schriftart beim Lesen" -> „Einfacher Text“ und Werkzeuge -> Optionen -> Umgebung -> Standardaktionen „Externe HTML-Bilder" -> „Warnung immer anzeigen“

Empfehlungen

E8 E-Mails der Hochschule Osnabrück

Wenn Sie Ihre E-Mail-Adresse der Hochschule Osnabrück verwenden, repräsentieren Sie damit als Hochschulmitglied die Hochschule Osnabrück. Achten Sie daher auf Inhalt und Aufmachung Ihrer E-Mail. Hier einige Hinweise:

- Achten Sie auf Ausdruck, Höflichkeit und Korrektheit.
- Wählen Sie Anrede, Betreff und Grußformel zielgerichtet.
- Eine Signatur mit Telefonnummer und ggf. Adresse erleichtert dem Empfänger die Rückantwort.
- Lesen Sie vor dem Absenden die E-Mail noch einmal aus Sicht des Empfängers.

E9 Vorsicht beim Surfen im Internet!

Im Internet lauern viele Gefahren:

- Falls Ihre Systemsoftware nicht auf dem neuesten Stand aktualisiert ist, kann bereits der Aufruf von Seiten zu einer Infektion ihres Rechners führen, die ihr Virenscanner ggf. nicht erkennt (Drive-by-Downloads). Da Seiten vieler Webserver gehackt wurden, betrifft dies nicht nur sog. „Schmuddelseiten“.
- Bilder können Schadsoftware enthalten, die bereits beim Anzeigen des Bildes ausgeführt wird.
- In vielen Seiten ist zur Steigerung der Funktionalität Software eingebettet, die beim Laden der Seite ausgeführt wird (Java, JavaScript, ActiveX).

Surfen Sie daher nur auf vertrauenswürdigen Seiten.

Jedermann kann im Internet Inhalte bereitstellen, anonym und unzensiert. Begegnen Sie daher Informationen auf Ihnen unbekannten Seite mit gesundem Misstrauen.

E10 Nutzung von Firefox mit NoScript-Plugin

Besser nicht den MSIE nutzen

Der Microsoft Internet Explorer (MSIE) ist der am meisten genutzte Browser und damit das attraktivste Angriffsziel für Angreifer.

Der Firefox-Browser (www.mozilla-europe.org/de/firefox) erlaubt bessere Sicherheitseinstellungen als der MSIE. Die Ausführung aktiver Inhalte kann im Browser nur global erlaubt oder verboten werden. Beim Verbieten aktiver Inhalte lassen sich jedoch viele Seiten nicht mehr problemlos darstellen. Andererseits führt ein globales Erlauben aktiver Inhalte zu einem Sicherheitsrisiko. Das Firefox-Plugin NoScript (http://noscript.net) ermöglicht es, aktive Inhalte seitenbasiert per Mausklick freizugeben. Beim Surfen im Internet kann so die Ausführung aktiver Inhalte zunächst generell geblockt und für vertrauenswürdige Seiten gezielt zugelassen werden.

NoScript: Freigabe aktiver Inhalte per Mausklick

E11 Begrenzen Sie die Größe Ihrer E-Mails

E-Mail Bomben sind große unerwünschte Mails, die zur Überflutung von Mailservern und damit ggf. zum Blockieren des Mailsystems führen können.

Um der Gefahr von E-Mail-Bomben vorzubeugen, haben viele Unternehmen ihre maximale Größe von E-Mails beschränkt auf z.B. 10 MByte.

< 10 MByte

Durch den Verzicht auf übergroße E-Mails stellen Sie sicher, dass Ihre Mails den Empfänger erreichen.

3.2. Viren und andere schädliche Software

Viren, Makro-Viren, Würmer, Trojanische Pferde oder Hoaxes werden unter dem Begriff Schadsoftware zusammengefasst. Schadsoftware wird in den allermeisten Fällen über das Internet (E-Mails, WWW) verbreitet. Aber auch mobile (USB-Stick/-Festplatte, Memory Card, DVD) Datenträger bieten die Gefahr der Infektion.

Die Schadenswirkung reicht von Popup-Fenstern, die ihnen lediglich die Zeit stehlen, über das Löschen von Daten, dem Abgriff eingetippter Nutzerkennungen/Passworte/ PINs (durch sog. Keylogger) bis zur kompletten Fernsteuermöglichkeit ihres PCs über das Internet durch Angreifer. Eine entsprechende Schadsoftware ist häufig in der Lage, sich selbst weiter zu verbreiten und sich so in Ihr System einzunisten und zu verstecken, dass die Infektion später kaum erkannt werden kann. Aufgrund der Leistungsfähigkeit moderner Rechner bemerken Sie es in der Regel auch nicht, wenn ein Angreifer über die eingeschleuste Hintertür parallel seine Software auf Ihrem PC ausführt. Ihr Rechner wird in diesem Fall ggf. zum Bestandteil eines Botnetzes (eines Netzes vieler von einem Angreifer ferngesteuerter Rechner) und für kriminelle Aktivitäten missbraucht.

Für PCs mit Internetzugang ist daher ein Virenscanner, der dem Befall mit Schadsoftware vorbeugt, unbedingt erforderlich. Da täglich neue Schadprogramme entwickelt werden, muss der Virenscanner regelmäßig aktualisiert werden.

In der Hochschule Osnabrück ist jeder PC standardmäßig mit dem Virenscanner SOPHOS ausgestattet, der sich automatisch regelmäßig über das Internet aktualisiert.

Ein Virenbefall zieht beträchtliche Wiederherstellungs- und Desinfektionsaufwände und ggf. eine Rufschädigung der Hochschule nach sich. Daher sind trotz Virenscanner einige Regeln zu beachten.

V1 Bei Virenalarm durch Sophos:

1. Ruhe bewahren

2. Systemadministrator informieren

3. PC NICHT ausschalten, ggf. Netzwerk-Stecker ziehen

4. Die Desinfektion NICHT selbst durchführen

Falls Sophos eine Virenbefall meldet, informieren Sie umgehend ihren Systemadministrator (siehe Kapitel 6), der dann die Schritte zur Desinfektion einleitet.

Starten Sie die Desinfektion nicht selbst, da ihr Systemadministrator den Befall sonst ggf. nicht dokumentieren und weiterverfolgen kann. Schalten Sie den PC nicht ab, da sich manche Viren erst beim Neustart einrichten.

Als vorbeugende Maßnahme um eine weitere Verbreitung vorzubeugen, ziehen Sie den Stecker, der Ihren PC mit dem Netzwerk verbindet:

Netzwerkstecker:  Buchse am PC: 

V2 Prüfen Sie Funktion und Aktualität ihres Virenscanners

Die korrekte Funktion Ihres Sophos-Virenscanners erkennen Sie am Symbol rechts unten in der Taskleiste. Funktioniert Ihr Virenscanner nicht wie erwartet, ändert sich das Symbol zu einem roten Kreuz .

= ok

= Fehler!

Melden Sie die Fehlfunktion Ihrem Systemadministrator (siehe Kapitel 6).

V3 Melden Sie ungewöhnliche Verhaltensweisen Ihres Rechners!

Da es nach dem Auftreten einer neuen Schadsoftware immer eine gewisse Zeit dauert, bis der Hersteller seinen Virenscanner so angepasst hat, dass dieser die neue Schadsoftware erkennt, bietet ein Virenscanner keine 100%-ige Sicherheit. Es kann trotz Virenscanner zu einem Befall kommen!

Lange Lade-/ Startzeiten

Ungewöhnliche Festplattenaktivität

Hohe Sytemlast

Ein Hinweis für einen möglichen Befall ist, dass sich Ihr System ungewöhnlich verhält. Ungewöhnliche Verhaltensweisen sind z.B.

- außergewöhnlich lange Lade-/Start- oder Rechenzeiten von Programmen,
- unbegründete Festplattenaktivitäten oder
- eine unbegründete hohe Systemlast.

Wenn sich Ihr System nicht wie gewohnt verhält, melden Sie dies ihrem Systemadministrator (siehe Kapitel 6).

3.3. Nutzerkennungen und Passwörter

Passwörter in Verbindung mit Nutzerkennungen sind der am häufigsten verwendete Schutzmechanismus für den Zugriff auf Systeme, Anwendungen und Daten. Sie dienen u.a.

- zum Schutz Ihrer E-Mails vor fremden Zugriff,
- zu Ihrem PC-Login,
- zur Anmeldung bei Intranet-Applikationen (StudIP, myHS, SAP etc.),
- zur Anmeldung bei Internet-Applikationen (z.B. Shops, Auktionen, Fahrkarten),
- zum Schutz der Konfiguration von Netzkomponenten (z.B. DSL-Router).

Unsichere oder ausgespähte Passwörter bieten Angreifern eine erste Einstiegsmöglichkeit in das System. Von diesem Einstiegspunkt aus erweitern Angreifer gezielt ihre Berechtigungen und greifen dann über das Netz andere Rechner, wie z.B. Serversysteme, an.

Jeder Hochschulmitglied hat eine Nutzerkennung und ein Passwort. Auch Externe können zeitlich befristet eine Zugangsberechtigung (Nutzerkennung / Passwort) erhalten.

Einem Angreifer reicht die Nutzerkennung und das Passwort *eines einzelnen* Anwenders, um ins System zu gelangen. Daher ist es so wichtig, dass jeder einzelne Anwender/PC-Nutzer sichere Passwörter verwendet und diese angemessen schützt.

Das Ermitteln fremder Nutzerkennungen und Passwörter wird als Identitätsdiebstahl bezeichnet, da der Passwort-Dieb in Ihrem Namen handeln kann, sobald er Ihr Passwort kennt.

N1 Verwenden Sie sichere Passwörter!

- Keine Kombinationen aus Namen, Geburtstagen o.ä.

- Mindestlänge 8 Zeichen

Gerne werden Telefonnummern, Geburtstage, Namen, Tastenfolgen (asdf) oder Kombinationen dieser als Passwort verwendet. Zur Erhöhung der Sicherheit werden darüber hinaus oft einzelne Zeichen durch Sonderzeichen ersetzt (z.B. a durch @ oder S durch $), Zahlen ein- oder angefügt oder Worte rückwärts geschrieben. Solche Passwörter bieten jedoch nur eine begrenzte Sicherheit, da sie durch Wörterbuch-Angriffe mit frei zugänglichen Tools relativ schnell automatisiert ermittelt werden können.

Wörterbuch-angriffe

Sind Passwörter zu kurz, können sie relativ schnell durch automatisiertes Testen aller möglichen Zeichenkombinationen einer bestimmten Länge ermittelt werden. Daher sollten Passwörter mindestens 8 Zeichen lang sein, besser länger. Mit jedem zusätzlichem Zeichen wird das Passwort sicherer.

Mindestlänge 8 Zeichen

Wirklich zufällig gewählte Passwörter bieten einen guten Schutz -

Gut: zufällige

sind jedoch schwer zu merken.

Passwörter

Ein mögliches Verfahren, Passwörter zu bilden, die zufälliger sind und an die man sich trotzdem recht gut erinnern kann, ist es, die Anfangsbuchstaben der Worte eines frei gewählten deutschen Satzes als Passwort zu nutzen.

Anfangsbuch-staben eines Satzes als Passwort

Beispiel: Als Mitglied der Hochschule Osnabrück sollte ich nur sichere Passwörter verwenden. -> Passwort „AMdHSOSsinsPv“

N2 Halten Sie ihre Passwörter geheim!

- Passwörter nicht an Kollegen oder Freunde weitergeben

- Passwörter nicht am Telefon nennen

- Passwörter sicher verwahren

- Passwörter nicht in E-Mails versenden

- Passwörter nicht auf ungeschützten Internet-Seiten eingeben

Behandeln Sie Passwörter mit der gleichen Sorgfalt wie Ihren Haustürschlüssel oder Ihre Kreditkarte. Wenn jemand anderes Ihr Passwort für missbräuchliche Zwecke einsetzt, fällt der Schaden auf Sie zurück!

Passwort = Haustür-schlüssel

Geben Sie Passwörter nicht weiter, auch nicht am Telefon, auch nicht, wenn der Anrufer überzeugende Gründe aufführt, weshalb Ihr Passwort gerade jetzt benötigt wird.

Social-Engineering

Wenn Sie ein Passwort unbedingt aufschreiben wollen, verwahren Sie die Abschrift an einem Ort, an dem Sie auch andere wertvolle Dinge aufbewahren, die Sie vor dem Zugriff anderer schützen wollen. Beispiele sind ihre Geldbörse oder ein abgeschlossener Schrank, zu dem nur Sie den Schlüssel haben.

Sichere Verwahrung

Achten Sie bei der Nutzung von Passwörtern im Internet darauf, dass die Verbindung verschlüsselt ist, bevor Sie ein Passwort eingeben. Die verschlüsselte Verbindung erkennen Sie daran, dass die Internet-Adresse nicht mit „http://“, sondern mit „https://“ beginnt. Falls sie mit „http://“ beginnt, fügen Sie einfach ein „s“ hinter „http“ in die Adresse ein und laden die Seite dann neu.

Verschlüsse-lung mit https

Melden Sie sich von personalisierten Webseiten immer ab. Ansonsten erleichtern Sie es einem Angreifer, ihre Sitzung zu übernehmen.

Abmelden

N3 Wechseln Sie ihr Passwort bei Verdacht auf Kompromittierung

Wenn die Gefahr besteht oder Sie den Verdacht haben, dass jemand anderes Ihr Passwort kennt, dann wechseln Sie Ihr Passwort umgehend!

Dies ist z.B. dann der Fall, wenn Sie vermuten, dass jemand anderes unter ihrer Zugangskennung arbeitet (veränderte Daten,

Login-Zeiten) oder wenn Sie Ihr Passwort notiert und die Abschrift verloren haben sollten.

N4 Nutzen Sie verschiedene Passwörter für verschiedene Einsatzzwecke!

Nutzen Sie Ihr Hochschul-Passwort nicht im Internet!

Personalisierte Anwendungen im Internet (z.B. Auktionen, Shops, etc.) erfordern eine Anmeldung mit Nutzerkennung und Passwort. Nutzerkennung und Passwort sind auf dem Server der Internet-Firma (ggf. verschlüsselt) gespeichert. Daher sollten Sie davon ausgehen, dass die Internet-Firma ihre Nutzerkennung und Ihr Passwort kennt. Des Weiteren hängt die Vertraulichkeit Ihres Passworts davon ab, wie gut die Internet-Firma ihre Server (auf denen die Passwörter gespeichert sind) schützt. Oft genug gibt es Einbrüche in Firmen-Servern, nach denen Nutzerkennungen und Passwörter im Internet veröffentlicht wurden.

Hacker dringt in Firmen-server ein und stiehlt Passwörter

Sie wollen, dass ihre Zugangskennungen nicht von der Sicherheit irgendwelcher Internet-Firmen abhängen? Sie wollen, dass der Betreiber einer Internet-Anwendung nicht unter Ihrem Namen andere (Internet-) Anwendungen oder Ihr Hochschul-Account nutzt? Dann sollten Sie für unterschiedliche Einsatzzwecke verschiedene Passwörter (und am Besten auch verschiedene Nutzerkennungen) wählen. Dabei sollten Sie darauf achten, dass aus dem einen Passwort nicht ein anderes in einfacher Weise ableitbar ist. (z.B. Dkei2Jebay → Dkei3Jamazon → Dkei4Jpostbank)

N5 Serverseitige Prüfung der Passwortsicherheit

Mit der Einführung von OSCA werden viele Abläufe und Daten gebündelt und Studierenden sowie Mitarbeitern über Standard-browser zugänglich gemacht. Über das Internet ist so ein Zugriff auf zentrale Datenbanken mit kritischen personenbezogenen Daten möglich. Im Vergleich zum aktuellen Zustand steigt durch OSCA sowohl der Schutzbedarf als auch die Angriffsfläche.

OSCA → erhöhter Schutzbedarf

Um einen sicheren Zugangsschutz zu gewährleisten überprüft daher die Hochschule in regelmäßigen Zeitabständen mit gängigen Passwort-Cracking-Tools die Sicherheit der verwendeten Passwörter.

HS prüft PW-Dateien

Wenn dabei Ihr Passwort geknackt wird, werden Sie informiert und gebeten ein sicheres Passwort zu wählen. Falls dies mehrfach passiert, wird Ihr Zugang gesperrt.

3.4. Schutz sensibler Daten

Gibt es bei uns an der Hochschule überhaupt sensible Daten? Durchaus! Hier einige Beispiele:

- personenbezogene Daten von Studierenden, wie z.B. nicht anonymisierte Klausur- bzw. Prüfungsergebnisse,
- die Zuordnung von Matrikelnummer zum Namen bei Studierenden,
- personenbezogene Daten von Mitarbeitern,
- Bewerbungsunterlagen,
- Passwortdateien (diese sind selbst in verschlüsselter Form als sensibel zu betrachten),
- Daten aus der Finanzbuchhaltung.

Bei der Frage, ob Daten sensibel sind oder nicht, fragen Sie sich am besten selbst, ob eine Veröffentlichung der Daten irgendwelche negativen Folgen für die Hochschule Osnabrück haben könnte. Falls ja, sind die Daten als sensibel anzusehen.

Gefährdet sind sensible Daten insbesondere auf mobilen Geräten und bei der Übertragung über unsichere Netze wie dem Internet.

Mobile Geräte sind in Mode, seien es Laptops, Netbooks, PDAs, Handys oder auch USB-Sticks. Alle mobilen Geräte haben einen gemeinsamen Nachteil: Sie sind relativ leicht zu entwenden. Dabei ist der Verlust des eigentlichen Geräts schon ärgerlich genug. Ein weitaus gravierenderer Schaden kann jedoch entstehen, wenn auf dem Gerät gespeicherte sensible Daten in fremde Hände gelangen.

Um die Daten auszulesen, benötigt ein versierter Angreifer vielfach keine Nutzerkennung. Z.B. kann bei Laptops, Netbooks und einigen Netzwerkdruckern die Festplatte ausgebaut und direkt gelesen werden.

Ähnlich unsicher ist die Übertragung von Daten über das Internet oder über Funknetze wie WLANs.

Damit sensible Daten in solchen Fällen nicht in falsche Hände gelangen, sind einige Regeln zu beachten:

D1 Schützen Sie sensible Daten auf mobilen Geräten:

Falls eine Speicherung nötig ist, sind die Daten zu verschlüsseln!

Am besten ist es, grundsätzlich keine sensiblen Daten auf mobilen Geräten zu speichern.

Falls sensible Daten auf mobilen Geräten gespeichert werden, dann sind diese zu verschlüsseln. Hierzu gibt es frei verfügbare Programme, wie z.B. TrueCrypt (http://www.truecrypt.org). Ihr Systemadministrator (siehe Kapitel 6) unterstützt Sie gerne bei der Installation und Nutzung.

Verschlüsselungssoftware

Notebooks der Verwaltung werden so ausgeliefert, dass Laufwerk D automatisch verschlüsselt ist.

D2 Kein Versand sensibler Daten per E-Mail!

Falls sensible Daten per E-Mail versendet werden sollen, sind diese zu verschlüsseln. Vorschläge, wie dies geschehen kann, sind in Regel E1 angegeben.

D3 Drucken von sensiblen Daten

Falls Sie sensible Daten auf Netzwerkdruckern in anderen Räumen oder im Flur ausdrucken, verwenden Sie nach Möglichkeit die passwortgeschützte Druckermailbox. Den eigentlichen Ausdruck führen Sie durch wenn Sie persönlich am Drucker sind.

Lassen Sie gedruckte sensible Daten nicht unbeaufsichtigt liegen. Nehmen Sie Drucke unverzüglich aus dem Ausgabefach.

D4 Zugriff auf sensible Daten im Internet nur über HTTPS

Falls Sie über das Internet auf sensible Daten zugreifen oder sensible Daten eingeben, achten Sie darauf, dass die Verbindung verschlüsselt ist. Eine verschlüsselte Verbindung erkennen Sie daran, dass die Internet-Adresse mit „https://“ beginnt (siehe auch Regel N2).

https://

D5 Datenlöschung bei der Nutzung mobiler Datenträger

Häufig werden sensible Daten zum Transport auf mobilen Datenträgern (CDs, USB-Sticks, etc.) gespeichert.

Vor der Wiederverwendung bzw. Entsorgung der Datenträger sind die sensiblen Daten so zu löschen, dass sie nicht rekonstruierbar sind.

USB-Sticks mit der Software „Eraser“ löschen

Ein einfaches Löschen bzw. Formattieren des Datenträgers reicht hierzu nicht aus, da die Daten dann mit wenig Aufwand wieder rekonstruiert werden können.

Ein sicheres Löschen ist mit speziellen Löschprogrammen möglich.

CD zer-schneiden

Bei read-only Datenträgern (z.B. CD) eignet sich eine physikalische Zerstörung des Datenträgers.

Bei der zentralen IT steht eine Tonne zur Aufnahme von Daten-trägern (auch Laufwerken), die sicher entsorgt werden sollen.

Regelungen für die Hochschul-Verwaltung

DV1 Zentrale Datenhaltung

Daten sind zentral auf Netzlaufwerken zu speichern, da sie sonst nicht der Datensicherung unterliegen.

3.5. PC-Pools und Softwarelizenzen

Die Hochschule bietet als Serviceleistung für Studierende mehrere PC-Pools mit Rechnern und Zugang zur Hochschul-IT an. Aufgrund der Nutzung durch immer wieder wechselnde Personen sind für PC-Pools besondere Regeln erforderlich, um deren Verfügbarkeit sicherzustellen und Missbrauch zu vermeiden. Da die Verfügbarkeit und Funktionsfähigkeit der PC-Pools im ureigensten Interesse der Studierenden liegt, sind alle Studierenden aufgerufen, diese Regelungen einzuhalten und Abweichungen zu melden.

P1 Es ist untersagt, in PC-Pools

- Speisen oder Getränke einzunehmen oder

- zu rauchen.

Schonen Sie die Geräte, fahren Sie die PC's nach Gebrauch herunter und schalten Sie die diese aus. Sie helfen damit auch Energie zu sparen.

P2 Nehmen Sie an Poolrechnern keine bleibenden Änderungen vor!

Dies betrifft sowohl Software- und Konfigurationsänderungen als auch Änderungen an der Hardware und Verkabelung.

Des Weiteren stellt die Hochschule Studierenden verschiedene Software bereit. Teilweise ist die bereitgestellte Software lizenziert (z.B. bestimmte CAD- oder Computeralgebra-Software).

P3 Kopieren Sie keine lizenzierte Software auf andere Rechner!

Falls Sie Software kopieren wollen, überprüfen Sie zunächst durch Ansprache des jeweiligen Betreuers, dass die Lizenzbedingungen ein Kopieren erlauben.

Durch das unerlaubte Kopieren lizenzierter Software machen Sie sich strafbar! Kopieren Sie lizenzierte Software auch nicht auf andere Hochschul-Rechner.

P4 Verstöße gegen die obigen Regeln werden sanktioniert!

Nutzer, die gegen die obigen Regeln nicht einhalten, können von der Nutzung einzelner oder sämtlicher PC-Pools ausgeschlossen werden.

Diebstahl wird angezeigt. Bei Sachbeschädigung wird ein Schadenersatzanspruch geltend gemacht.

4. Organisatorische Regelungen

Nachstehend werden für bestimmte Personengruppen der Hochschule Osnabrück grundlegende Verantwortlichkeiten mit IT-Bezug aufgeführt.

4.1. Vorgesetzte

Vorgesetzte sind dafür verantwortlich, ihre Mitarbeiter auf diese IT-Sicherheitsrichtlinie hinzuweisen und sie für IT-Sicherheitsbelange zu sensibilisieren.

4.2. Administratoren

Administratoren sind für die IT-Sicherheit der von ihnen betreuten IT-Systeme verantwortlich. Umzusetzende Sicherheitsmaßnahmen sind im IT-Sicherheitskonzept der Hochschule Osnabrück beschrieben.

4.3. Revisoren

Die Revision evaluiert die getroffenen Maßnahmen und deckt Handlungsbedarf auf.

4.4. Datenschutzbeauftragter

Der Datenschutzbeauftragte ist zu beteiligen

- bei der Einführung neuer Programme, die personenbezogene Daten verarbeiten,
- beim Austausch personenbezogener Daten mit Dritten (außerhalb der Hochschule Osnabrück) und
- bei der Verarbeitung personenbezogene Daten durch Dritte.

In seiner Verantwortung liegt es sicherzustellen, dass die Anforderungen des BDSG und NLDG angemessen berücksichtigt werden.

4.5. Weitere organisatorische Regelungen

O1 Eigenverantwortlicher sicherer und datenschutzkonformer Umgang mit Informationen

Egal ob Studierender, Lehrender oder Mitarbeiter: Tragen Sie zu einem sicheren und datenschutzgerechten Umgang mit Informationen bei!

Informationssicherheit kann nur begrenzt „von oben herab“ sichergestellt werden - trotz zentraler Konzepte und Analysen. Es hängt entscheidend davon ab, ob Sie mitmachen!

Fallen Ihnen Schwachstellen, organisatorische Mängel, Gefährdungen oder unangemessene Schutzmaßnahmen auf, dann teilen Sie es dem IT-Sicherheits- und Datenschutzbeauftragten der Hochschule mit. Schon zahlreiche Mängel konnten dadurch abgestellt werden.

O2 Meldung von Sicherheitsvorfällen

Sicherheitsvorfälle in der Verwaltung sind dem IT Helpdesk zu melden. Sicherheitsvorfälle in den Fakultäten und dem Institut für Musik sind den zugehörigen IT-Ansprechpartnern zu melden.

O3 Zutrittsberechtigungen für Mitarbeiter von Fremdfirmen

Zutrittsberechtigungen für Mitarbeiter von Fremdfirmen sind auf die minimal erforderliche Anzahl zu beschränken. Vergabe und Rückgabe der Berechtigungen sind schriftlich festzuhalten.

Im Rahmen der vertraglichen Beauftragung der Firma ist sicherzustellen, dass die zutrittsberechtigten Mitarbeiter zur Nichteinsichtnahme und Geheimhaltung von Unterlagen der Hochschule verpflichtet sind. Weist die Fremdfirma eine entsprechende Bestätigung nicht schriftlich nach, so sind die zutrittsberechtigten Mitarbeiter der Fremdfirma durch die Hochschule zu belehren und zu verpflichten.

O4 Auftragsdatenverarbeitung

Eine Verarbeitung personenbezogener Daten im Auftrag ist immer dann gegeben, wenn die Hochschule personenbezogene Daten an Dritte zur Verarbeitung weitergibt. Ein Beispiel ist die Weitergabe von Studierendendaten zum Druck von Diplomzeugnissen.

Die Hochschule ist dabei verantwortlich für den angemessenen Schutz ihrer personenbezogenen Daten bei der Verarbeitung durch den Dritten (das beauftragte Unternehmen, denen personenbezogene Daten überlassen werden).

Der Dritte ist deshalb durch die Hochschule vertraglich auf die Einhaltung der Anforderungen des Landes- und Bundesdatenschutzgesetzes zu verpflichten (NDSG, §6). Die Hochschule bleibt verantwortlich, dass der Dritte angemessene Schutzmaßnahmen gemäß NDSG §7 vorsieht und hat sich dessen zu vergewissern.

5. Datenschutz

Beim Datenschutz geht es um den Schutz personenbezogener Daten, um das Recht auf informationelle Selbstbestimmung zu gewährleisten: Jede Person soll selbst über die Preisgabe und Verwendung ihrer Daten bestimmen können.

Die Hochschule Osnabrück verarbeitet eine Vielzahl personenbezogener Daten, wie insbesondere Studierenden- und Mitarbeiterdaten. Diese Daten sind gemäß den Vorgaben des Niedersächsischen Datenschutzgesetztes (NDSG) und des Bundesdatenschutzgesetzes (BDSG) zu schützen.

Die nachstehenden Regeln geben wichtige Grundsätze und Vorgaben des NDSG und BDSG wieder.

DS1 Personenbezogene Daten nur für Hochschulzwecke erheben

Personenbezogene Daten dürfen erhoben werden, wenn ihre Kenntnis zur Erfüllung der Aufgaben der Hochschule erforderlich ist. Die Daten sind grundsätzlich beim Betroffenen zu erheben. Der Betroffene ist über den Zweck der Erhebung aufzuklären.

Sollen personenbezogene Daten zu einem anderen Zweck erhoben werden, bedarf dies der Einwilligung der Betroffenen. Die Einwilligung ist freiwillig und bedarf grundsätzlich der Schriftform. Den Betroffenen ist der Erhebungszweck mitzuteilen.

DS2 Personenbezogene Daten nur im unbedingt erforderlichen Umfang erheben!

Es gilt der Grundsatz der Datensparsamkeit: Personenbezogene Daten sind am besten geschützt, wenn Sie erst gar nicht gespeichert werden.

Personenbezogene Daten sollen nur erhoben werden, wenn dies unbedingt notwendig ist. Dann nur die minimal zur Erfüllung des Zwecks erforderlichen Daten erheben.

Der Grundsatz der Datensparsamkeit verlangt auch die Löschung personenbezogener Daten, sobald diese nicht mehr benötigt werden.

Aufgrund zahlreicher bekannter Datenschutzvorfälle und der starken Vernetzung kommt der Datensparsamkeit eine ganz besondere Bedeutung zu.

DS3 Personenbezogene Daten nur zum vorgegebenen Zweck einsetzen!

Personenbezogene Daten unterliegen der Zweckbindung. Sie dürfen nur zu dem Zweck verwendet werden, zu dem Sie erhoben wurden. Eine Änderung des Verwendungszwecks bedarf der Zustimmung der Betroffenen.

DS4 Gehen Sie mit personenbezogenen Daten vertraulich um!

Mitarbeiter öffentlicher Stellen und ihrer Auftragnehmer sind auf das Datengeheimnis verpflichtet, d.h. zum vertraulichen Umgang mit personenbezogenen Daten. Diese Verpflichtung gilt nach Beendigung der Tätigkeit weiter.

DS5 Organisatorische und Technische Maßnahmen

Die §§ 9 und 10 BDSG und § 7 des NDSG geben organisatorische und technische Anforderungen vor, die bei der Verarbeitung personenbezogener Daten sicherzustellen sind. Wichtige dieser Anforderungen sind nachstehend angegeben:

Zugangs- und Zugriffskontrolle: Es ist sicherzustellen, dass Unbefugte nicht auf personenbezogene Daten zugreifen können und Mitglieder nur auf die personenbezogenen Daten zugreifen können, für die sie zugriffsberechtigt sind. Dies gilt sowohl bei der Erhebung, der Verarbeitung und bei der Übermittlung von personenbezogenen Daten.

Datenträgerkontrolle: Es ist sicherzustellen, dass Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

Eingabekontrolle: Es muss überprüfbar und feststellbar sein, von wem zu welcher Zeit welche personenbezogenen Daten eingegeben wurden.

Übermittlungskontrolle: Es muss überprüfbar und feststellbar sein, von wem zu welcher Zeit welche personenbezogenen Daten übermittelt wurden.

6. Ansprechpartner

Nachstehend sind die IT-Ansprechpartner/Systemadministratoren für die Organisationseinheiten der Hochschule Osnabrück aufgelistet.

IT Helpdesk	First Level Support für Zentrale IT helpme@hs-osnabrueck.de	0541 969 7100
Zentrale IT (2nd Level Support)		
	O.Jury@hs-osnabrueck.de	0541 969 3250
	P.Krikowski@hs-osnabrueck.de	0541 969 3594
Ansprechpartner in den Fakultäten und Departments		
IuI	J.Hoff@hs-osnabrueck.de	0541 969 3686
WiSo	E.Henze@hs-osnabrueck.de	0541 969 2007
	F.Huckriede@hs-osnabrueck.de	0541 969 2974
AuL	F.Reekers@hs-osnabrueck.de	0541 969 5165
MKT	M.Malachinski@hs-osnabrueck.de	0591 80098 215
	M.Schroeter@hs-osnabrueck.de	0591 80098 279
	M.Schoening@hs-osnabrueck.de	0591 80098 446
Bibliothek	O.Meyer@hs-osnabrueck.de	0541 969 3227
Beauftragter für Datenschutz und IT-Sicherheit		
	A.Scheerhorn@hs-osnabrueck.de	0541 969 3540