Unsere Empfehlungen für Ihre IT-Sicherheit

Warum ist Sicherheit wichtig?

Nicht so sehr klassische „Hacker“, sondern immer mehr professionelle kriminelle Banden bedrohen heute die Datensicherheit. Letztlich geht es dabei um Geld. Dies kann Zugangsdaten zum Online-Banking betreffen, aber auch die Vermietung Ihres Computers, falls dieser kompromittiert wurde, zur Versendung von Spam-Mails, Verteilung von Schadsoftware oder für Angriffe auf fremde Server. Dies schadet nicht nur Ihnen, sondern auch dem Ansehen der Universität, ganz abgesehen von der Möglichkeit, dass vertrauliche Daten auf Ihrem Computer in die falschen Hände gelangen könnten. Aber Sie sind nicht hilflos: Mit geeigneten Maßnahmen können Sie den „Cybergangstern“ das Leben schwer machen.

Antivirus-Software

Kein Rechner sollte ohne Antivirus-Programm laufen. Das HRZ besitzt eine Campuslizenz für Sophos, das von allen Universitätsmitgliedern auch zu Hause verwendet werden darf. Es ist für alle gängigen Betriebssysteme verfügbar. Eine Anleitung zur Installation finden Sie unter www.uni-giessen.de/cms/fbz/svc/hrz/svc/software/antivir.

Doch bedenken Sie, dass ein Antivirusprogramm nur vor bereits bekannten Schadprogrammen schützt. Da ständig neue Schadprogramme auftauchen, bringen die Hersteller der Antivirus-Software meist mehrmals täglich Updates heraus. Zur Aktualisierung von Sophos betreibt das HRZ einen eigenen Server. Aufgrund des Zeitfensters zwischen dem Erscheinen eines Virus und dem Update der Antivirus-Software sollten Sie sich aber nie darauf verlassen, dass eine Antivirus-Software Ihren Rechner zu 100% schützt.

Updates gegen Sicherheitslücken

In vielen Fällen werden Rechner gekapert, indem bestehende Fehler in Programmen von Hackern für deren Zwecke genutzt werden. Deshalb ist es wichtig, die Fehlerkorrekturen der Programmhersteller zeitnah einzuspielen. Für Microsoft-Produkte wie Windows und MS-Office betreibt das HRZ einen Updateserver. Informationen und eine Anleitung zur Nutzung finden Sie auf der Seite www.uni-giessen.de/cms/fbz/svc/hrz/svc/software/wssus.

Für andere Betriebssysteme und Anwendungen benutzen Sie den entsprechenden Dienst des Herstellers. Da derzeit Webbrowser und deren Hilfsprogramme (z.B. Flash, Adobe Reader, Java) beliebte Opfer sind, sollten Sie diese immer auf dem aktuellsten Stand halten. Bedenken Sie, dass alle Browser in gewissen Versionen kritische Sicherheitslücken enthielten. Falls vorhanden sollten Sie deshalb den im Browser (z.B. Firefox) oder Mailprogramm (z.B. Thunderbird) integrierten Updatemechanismus nutzen.

Firewall

Eine Firewall, korrekt konfiguriert, schützt Ihren Rechner vor unerwünschter oder sogar gefährlicher Kontaktaufnahme über das Netz. Die Firewall kann ein dediziertes Gerät im Netz sein, oder eine „Personal Firewall“, die auf Ihrem Rechner läuft. Alle modernen Betriebssysteme (Windows ab XP, Mac OS X, Linux) bringen eine solche Personal Firewall schon mit. Ist Ihr (Instituts-)Netz nicht schon durch eine eigene Firewall geschützt, sollte auf Ihrem Rechner die Personal Firewall aktiv sein. Die Konfiguration sollte so restriktiv wie möglich sein. Erbringt Ihr Rechner keine Dienste im Netz (wie z.B. freigegebene Laufwerke oder Drucker), sollte die Firewall alle eingehenden Verbindungen abweisen.

Zugang zu Ihrem Rechner vor Ort

Wer auf Ihren Rechner Zugriff hat, kann darauf Unheil anrichten. Denken Sie deshalb immer daran, Ihr Arbeitszimmer selbst bei kurzer Abwesenheit abzuschließen, einen Bildschirmschoner mit Passwortschutz einzustellen und Ihren Rechner zu sperren.

Umgang mit Passwörtern

Viele Angriffe gelingen, weil es leicht war, ein Passwort zu erraten. Wählen Sie deshalb Ihre Passwörter sorgfältig. Sie sollten mindestens sechs Zeichen lang sein. Die Maximallänge variiert je nach Anwendung, meist liegt sie bei acht bis zwölf Zeichen. Verwenden Sie eine Mischung von Groß-und Kleinbuchstaben, Ziffern und Sonderzeichen und möglichst kein „normales“ Wort. Teilen Sie Ihr Passwort niemandem mit. Auch ein Administrator benötigt es nicht und wird Sie daher auch nie dazu auffordern, es ihm per Mail zuzusenden oder es in ein dubioses Web-Formular einzugeben. Auch wenn Sie nicht dazu gezwungen werden, Ihr Passwort regelmäßig zu ändern, tun Sie es trotzdem. Verwenden Sie für verschiedene Dienste (z.B. HRZ, externe Mailprovider, App-Shops, diverse Netzwerke) jeweils eigene Passwörter. Sollten Sie dafür eine Gedächtnisstütze benötigen, so ist die Nutzung eines entsprechenden Programms (z.B. Password Safe, KeePass) eher zu empfehlen, als das Aufschreiben auf einem Zettel.

Unverlangt zugesandte Dokumente

Alle Dateien, die Ihnen unverlangt zukommen, müssen als potentiell gefährlich betrachtet werden. Gefahren lauern in aktiven Inhalten (z.B. Makros, Javascript) oder der Ausnutzung von Programmfehlern in zugehörigen Anwendungen. Fragen Sie im Zweifelsfall vor dem Öffnen der Datei beim Absender nach, ob mit der Datei alles seine Richtigkeit hat. E-Mail-Absenderangaben lassen sich sehr leicht fälschen! Klicken Sie nicht aus Neugier auf den Link oder das Attachment einer Spam-Mail. Sie können damit Schaden, nicht nur am eigenen Rechner, anrichten.

Kabellose Netzwerke (WLAN)

WLANs bieten nicht dieselbe Sicherheit wie kabelgebundene Netzwerke, deshalb ist eine Verschlüsselung der Übertragung notwendig. Nutzen Sie das an der JLU vom HRZ bereitgestellte WLAN „eduroam“, so ist die Datenverschlüsselung implizit gegeben. Wenn Sie dagegen „ugifula“ verwenden, müssen Sie zusätzlich eine VPN-Verbindung aufbauen, damit Ihre Daten verschlüsselt werden. Wenn Sie zuhause WLAN nutzen, sollten Sie die beste Verschlüsselung (derzeit WPA2/AES) einstellen.

Verschlüsselung im Netz

Die Verschlüsselung von Daten bei der Übertragung über das Netz verhindert, dass sensible Informationen (wie z.B. Passwörter) von Unbefugten mitgelesen werden können. Beim Zugriff auf Netzdienste per Webbrowser ist dazu die SSL-Verschlüsselung Standard. Sie erkennen dies daran, dass die URL mit „https:“ beginnt und Ihr Browser ein geschlossenes Schlosssymbol anzeigt. Um sicher zu stellen, dass Sie mit dem richtigen Server verbunden sind, und nicht mit einer illegalen Kopie, weist der Server sich mit einem Zertifikat aus, das Sie sich durch Klicken auf das Schlosssymbol anzeigen lassen können. Passt dieses nicht zur aufgerufenen URL oder kann nicht verifiziert werden, bringt der Browser eine Warnmeldung: Bitte nicht ungelesen wegklicken, sondern der Ursache nachgehen! Eine Warnmeldung, vor allem bei Smartphones, kann bei Zugriff auf Server der Universität auftreten, wenn Sie das notwendige Wurzelzertifikat (Deutsche Telekom Root CA 2) nicht in Ihren Browser importiert haben. Sie können dies tun unter

www.uni-giessen.de/cms/fbz/svc/hrz/svc/ident/zertifikat/ca_certs

Ältere Dienste wie telnet, ftp, pop oder imap übertragen Ihre Daten im Klartext über das Netz. Bei Nutzung dieser Dienste sollten Sie die verschlüsselten Varianten bzw. Ports wählen (ssh, sftp, pops, imaps).

VPN

Wenn Sie von zuhause oder von anderswo aus über fremde Netze Daten mit dem Universitätsnetz austauschen, sollten Sie zur Verschlüsselung der Daten eine VPN-Verbindung zum HRZ herstellen (vpn.uni-giessen.de). Dies gilt auch bei der Nutzung von WLAN, auch „eduroam“, bei einer fremden Institution.

Schutz mobiler Geräte

Wenn Ihr Laptop, Smartphone, Tablet oder USB-Stick abhandenkommt und sensible Daten enthält, kann das für den „Finder“ sehr vorteilhaft sein. Deshalb sollten mobile Geräte zumindest durch ein Passwort geschützt sein. Unter der Oberfläche moderner Smartphones und Tablets befindet sich ein Betriebssystem ähnlich dem Ihres PCs, also besitzt es auch ebensolche Sicherheitslücken. Entsprechend gelten hier dieselben Regeln wie bei einem PC, z.B. was Updates betrifft. Über Lücken, die sich zum „Jailbreak“ nutzen lassen, kann auch Ihr Smartphone angegriffen werden.

Cloud

Es ist sehr einfach und bequem, Daten bei Anbietern von Online-Speicher wie Dropbox, Skydrive, iCloud oder ähnlichen zu lagern und dann mit beliebigen mobilen Endgeräten darauf zuzugreifen. Bedenken Sie aber, dass Sie Ihre Daten dabei aus der Hand geben und oft keine Einflussmöglichkeiten haben, wo Ihre Daten lagern und wer darauf Zugriff hat. Sensible Daten sollten Sie daher nicht in der Cloud speichern. Das HRZ stellt verschiedene Arten von Speichermöglichkeiten bereit, bei denen die Daten sicher JLU-intern gespeichert werden. Diese Angebote werden für eine noch bequemere Nutzung weiterentwickelt. Für dienstliche Daten ist eine Richtlinie zur Speicherung von Daten in Abhängigkeit ihres Schutzbedarfs in Vorbereitung.

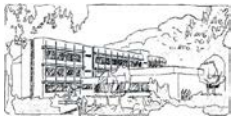
Weitere Informationen

Weiter Informationen zur IT-Sicherheit erhalten Sie auf den Internetseiten des IT-Sicherheitsbeauftragten

http://www.uni-giessen.de/cms/fbz/svc/hrz/svc/sicherheit

Die zugehörige E-Mail-Adresse ist: itsicherheit@uni-giessen.de,
bei Fragen können Sie sich gerne an ihn wenden.

Impressum: Herausgeber: Hochschulrechenzentrum,
Verantwortlich i.S.d.P.: Dr. Michael Kost
Stand: 06.08.2013



HRZ
HOCHSCHULRECHENZENTRUM
Universität Gießen

JLU Gießen > HRZ > IT-Sicherheit

Hochschulrechenzentrum

der Justus-Liebig-Universität Gießen

Unsere Empfehlungen für Ihre IT-Sicherheit

Hochschulrechenzentrum

Heinrich-Buff-Ring 44
D 35392 Gießen

Tel.: 0641-99-13100
Fax: 0641-99-13019

http://www.uni-giessen.de/cms/hrz/