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 auch dem Ansehen der Universität, ganz abgesehen von der Möglichkeit, dass vertrauliche Daten in die falschen Hände gelangen können. Aber Sie sind nicht hilflos: Mit geeigneten Maßnahmen können Sie den „Cybergangstern“ das Leben schwer machen.

- ## Antivirus-Software

  Kein Rechner sollte ohne Antivirusprogramm laufen. Das URZ 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 secure.uni-hd.de/nutzer/virusinst.html. Doch bedenken Sie, dass ein Antivirusprogramm nur vor dem Hersteller bekannten Schadprogrammen schützt. Da ständig neue auftauchen, bringen die Hersteller meist mehrmals täglich Updates heraus. Zur Aktualisierung von Sophos betreibt das URZ einen eigenen Server. Aufgrund des Zeitfensters zwischen Erscheinen eines Virus und Update der Software sollten Sie sich aber nie darauf verlassen, dass eine Antivirussoftware 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 URZ einen Updateserver. Eine Anleitung zu dessen Benutzung finden Sie auf der Seite secure.uni-hd.de/system/wsus.html. 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 (z.B. Firefox) sollten Sie deshalb den im Browser integrierten Updatemechanismus nutzen.

- ## 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 selbst wenn die Software Sie nicht zwingt, Ihr Passwort regelmäßig zu ändern, tun Sie es trotzdem. Verwenden Sie für verschiedene Dienste (z.B. URZ, externe Mailprovider, diverse Netzwerke) jeweils eigene Passwörter. Müssen Sie diese als Gedächtnisstütze aufschreiben, bewahren Sie die Zettel so sicher auf wie Ihr Bargeld!

- ## Firewall

  Eine Firewall schützt, korrekt konfiguriert, 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 Netz nicht durch eine eigene Firewall geschützt (z.B. Institutsfirewall des URZ mindestens Stufe 1, bei Ihrem EDV-/Netzbeauftragten zu erfragen), sollte auf Ihrem Rechner die Personal Firewall aktiv sein. Die Konfiguration sollte so restriktiv wie möglich sein. Erbringt Ihr Rechner keine Netzdienste (wie z.B. freigegebene Laufwerke oder Drucker), sollte die Firewall alle eingehenden Verbindungen abweisen.

- ## 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 Zertifikat aus (*Fortsetzung auf der Rückseite*).

UNSERE EMPFEHLUNGEN FÜR IHRE IT-SICHERHEIT

- ## Verschlüsselung im Netz

  Fortsetzung der Innenseite: 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 kommen, wenn Sie das notwendige Wurzelzertifikat nicht in Ihren Browser importiert haben. Sie können dies unter secure.uni-hd.de/nutzer/zertifikate.html tun. Ältere Dienste wie telnet, ftp, pop oder imap übertragen Ihre Daten im Klartext über das Netz. Bei Nutzung dieser Dienste sollten Sie verschlüsselte Varianten wählen, wie unter secure.uni-hd.de/nutzer/pw.html erklärt.
  VPN: Wenn Sie von zuhause oder von anderswo aus über fremde Netze (auch WLAN, vor allem auch mit „eduroam“) Daten mit dem Universitätsnetz austauschen, sollten Sie zur Verschlüsselung der Daten eine VPN-Verbindung zum URZ herstellen (vpn.uni-hd.de).

- ## Kabellose Netzwerke (WLAN)

  WLANs bieten nicht dieselbe Sicherheit wie kabelgebundene Netzwerke, deshalb ist eine Verschlüsselung der Übertragung notwendig. Nutzen Sie das vom URZ bereitgestellte WLAN „UNI-HEIDELBERG“, dann müssen Sie den VPN-Server des URZ verwenden, damit eine Verschlüsselung gewährleistet ist. Wenn Sie zuhause WLAN nutzen, sollten Sie die beste Verschlüsselung (derzeit WPA2/AES) einstellen.

- ## 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-Absender-Angaben lassen sich sehr leicht fälschen! Klicken Sie nicht aus Neugier auf den Link oder das Attachment einer Spam-Mail, Sie können damit Schaden anrichten.

- ## 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.

- ## Schutz mobiler Geräte

  Wenn Ihr Laptop, Smartphone oder USB-Stick abhanden kommt und sensible Daten enthält, kann das für den „Finder“ sehr vorteilhaft sein. Deshalb sollten mobile Geräte zumindest durch ein Passwort geschützt sein. Bei höheren Sicherheitsanforderungen lesen Sie bitte unsere Seite secure.uni-hd.de/system/crypto.html.

  Unter der Oberfläche moderner Smartphones und Tablets befindet sich ein Betriebssystem ähnlich dem Ihres PCs, also besitzt es auch ebensolche Sicherheits-lücken. 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.

- ## Weitere Information

  Weitere Information zur IT-Sicherheit erhalten Sie von Ihrem EDV-Beauftragten und auf den Internetseiten des Teams Sicherheit secure.uni-hd.de. Unsere E-Mail-Adresse ist: team-sicherheit@urz.uni-heidelberg.de, bei Fragen können Sie sich gerne an uns wenden.

URZ

Universitätsrechenzentrum

www.urz.uni-heidelberg.de

Mit uns können Sie rechnen!

Unsere Empfehlungen für Ihre IT-Sicherheit

Stand: Januar 2012

UNIVERSITÄT HEIDELBERG
Zukunft. Seit 1386.