Goldene Regeln IT-Sicherheit

Der Schutz der IT-Systeme und Daten der Hochschule kann nicht ausschließlich durch zentrale Maßnahmen des RZ gewährleistet werden. Gerade in einem Netzwerk, auf das täglich auch viele private Rechner zugreifen, ist es notwendig, dass alle Nutzer einige Regeln einhalten, um Schaden von sich und anderen abzuwenden.

Es ist erwiesen, dass ein Großteil erfolgreicher Angriffe möglich war, weil viele Rechner schlecht konfiguriert waren. Die hier beschriebenen Maßnahmen schaffen eine ausreichende Grundsicherheit gegen aktuelle Bedrohungen und sollten von allen Nutzern umgesetzt werden.

1 Betriebssystem aktuell halten

Halten Sie Ihr Betriebssystem stets aktuell, indem Sie verfügbare Updates zeitnah einspielen, da bekannte Schwachstellen für automatisierte Angriffe gegen verwundbare Systeme ausgenutzt werden.

Alle modernen Betriebssysteme bieten neben einem manuellen Update auch die Möglichkeit den Updatevorgang zu automatisieren. Das Betriebssystem nimmt regelmäßig über das Internet Verbindung mit dem eingestellten Update-Server auf, prüft das Vorhandensein neuer Updates und installiert diese dann auch selbstständig.

Für Windows 2000/XP/2003 Server kann der Windowsupdateserver (WUS) des Rechenzentrums verwendet werden:

http://www.rz.uni-wuerzburg.de/dienste/arbeitsplaetze/support/installation/windowsupdate/

2 Virenscanner einsetzen und aktuell halten

Schützen Sie Ihren Rechner vor der Infizierung mit Schadsoftware wie Viren, Würmern und Trojanischen Pferden durch die Nutzung eines Virenscanners. Die bloße Installation einer derartigen Software ist allerdings für einen wirksamen Schutz nicht ausreichend. Entscheidend sind die Aktualität und die richtige Konfiguration der wichtigsten Funktionen des Programms.

Wenn sie nicht standardmäßig aktiviert sind, sollten Sie folgende Einstellungen immer vornehmen:

- Zugriffsscan ständig aktiv
- wöchentlicher Komplettscan des Systems durchführen
- automatisches Updates aktivieren

Das RZ stellt für alle Mitarbeiter und Studierenden der Hochschule das Anti-Virus von Spohos zur Verfügung. Dieser Virenscanner sollte auf allen Rechnern der Hochschule eingesetzt werden und darf von allen Nutzern auch auf privaten Rechnern eingesetzt werden, solange sie Angehörige der Hochschule sind.

Informationen zur Nutzung des Sophos Anti-Virus finden Sie unter:

http://www.rz.uni-wuerzburg.de/dienste/arbeitsplaetze/support/installation/virenscanner/

3 Anwendungsprogramme richtig konfigurieren und aktuell halten

Hierzu gehören insbesondere Office-Programme (MS-Office, Openoffice, Acrobat, …), Internetbrowser und Mailprogramme, aber auch Programme zum Chatten oder zum Abspielen von Multimediainhalten (Windows Mediaplayer, Realplayer, Winamp, …). Durch gezielt manipulierte Webseiten und Dateien ist das Bedrohungspotential hier mittlerweile genauso hoch wie bei Serverdiensten, die Anwendungen werden aber im Gegensatz zu diesen bei einem Betriebssystemupdate nicht mit aktualisiert.

4 Sichere Passwörter verwenden

Alle Benutzerkonten eines Systems müssen mit einem Passwort versehen sein, da der Rechner sonst leicht über das Netzwerk angreifbar ist. Insbesondere wird bei vielen Standardinstallationen von Windows XP kein Administratorkennwort gesetzt! Passwörter sollten einige Mindestanforderungen bzgl. Länge und Komplexität erfüllen, damit sie nicht durch einfaches (evtl. automatisiertes) Durchprobieren erraten werden können:
http://www.rz.uni-wuerzburg.de/dienste/benvw/anlaufstellen/beratung/regeln_fuer_passwoerter/

5 Nicht mit Administratorrechten arbeiten

Sie sollten im Normalfall lokal nicht mit Administratorrechten arbeiten sondern lediglich mit den eingeschränkten Rechten eines normalen Benutzers. Bei allen modernen Betriebssystemen können Benutzerkonten mit verschiedenen Rechten versehen werden. Einen unbegrenzten Zugriff auf alle Funktionen des Betriebssystems erhalten Benutzerkonten der Kategorie "Administrator" bzw. "root". Bei Konten der Kategorie "Benutzer" bzw. "eingeschränkt" sind die Rechte dagegen limitiert.

Administratorrechte sind notwendig, um Konfigurationen vorzunehmen oder zu ändern. Die Arbeit mit Administratorrechten ermöglicht es vielen Schadprogramme erst ihre schädigende Wirkung voll entfalten zu können. Ein erfolgreicher Angreifer verfügt so automatisch ebenfalls über Administratorrechte.
Nicht benötigte Benutzerkonten sollten deaktivert oder gelöscht werden.

Falls Sie unter Windows mit eingeschränkten Rechten arbeiten, können Sie einzelne Anwendungen mit Administratorrechten laufen lassen, indem Sie im Programm-Menue oder im Explorer das entsprechende Programm mit der rechten Maustaste anwählen und den Menuepunkt „Ausführen als..“ anwählen.

6 Software und Daten aus sicheren Quellen verwenden

Software aus nicht vertrauenswürdigen Quellen (z.B. P2P-Tauschbörsen oder inoffizielle Webseiten) enthält häufig Schadsoftware wie Viren, Würmer, Trojaner und Rootkits. Beim Öffnen bzw. Ausführen der entsprechende Datei(en) wird die Schadsoftware aktiv, vielfach ohne dass der Nutzer dieses bemerkt. Dabei ist es unerheblich, ob es sich um eine manipulierte Anwendung oder um manipulierte Daten für eine verwundbare Anwendung handelt.

Nutzen Sie deshalb ausschließlich Originalsoftware/-daten und beziehen Sie diese möglichst direkt vom Hersteller bzw. von einer vertrauenswürdigen Quelle.

Installieren Sie nur wirklich benötigte Software.

7 Rechner vor unberechtigtem Zugriff schützen

Lassen Sie Ihren Rechner nicht unbeobachtet, wenn Sie angemeldet sind. Loggen Sie sich aus, sperren Sie den Zugriff oder aktivieren Sie einen Bildschirmschoner mit sicherem Passwort, wenn Sie Ihren Arbeitsplatz verlassen, auch wenn es sich nur um eine vermeintlich kurze Zeitspanne handelt.

Schalten Sie Ihren Rechner aus, wenn Sie Ihren Arbeitsplatz für längere Zeit verlassen, wie zum Beispiel zum Feierabend.

8 Keine zweifelhaften Mails bearbeiten oder beantworten

Führen Sie grundsätzlich keine Software aus, die Ihnen als Mailanhang zugesandt wird. Deaktivieren Sie im Mailprogramm die automatische Anzeige bzw. das Ausführen von Mailanhängen. Misstrauen Sie Mails, die die Aufforderung enthalten, Software zu installieren oder Passwörter, Kreditkartennummern, PINs, TANs oder ähnliches zu übermitteln. Antworten Sie nicht auf Mails mit unerwünschtem oder zweifelhaftem Inhalt, auch nicht, um die Versendung dieser Mails abzubestellen. Virenbefallene Mails täuschen in der Regel vertraute Absendeadressen vor. Misstrauen Sie unerwarteten Mails und insbesondere ihren Dateianhängen. Deaktivieren Sie nach Möglichkeit die HTML-Ansicht von E-Mails und nutzen Sie stattdessen die Textansicht. Prüfen sie alle auf den Rechner geladenen Dateien mit einem Virenscanner.

9 Sensible Informationen nicht leichtfertig preisgeben

Seien Sie misstrauisch, wenn Sie jemand wegen eines (vermeintlichen) Problems kontaktiert, und von Ihnen sensible Daten wie Passwörter oder Konfigurationseinstellungen wissen möchte. Die IT-Verantwortlichen der Hochschule und externe Dienstanbieter werden Sie nicht nach Ihrem Passwort fragen.
Lassen Sie sich im Zweifelsfall den Namen des IT-Verantwortlichen nennen und rufen Sie Ihn unter der Telefonnummer aus dem Adressbuch bzw. Informationssystem der Hochschule zurück.

10 Nicht benötigte Dienste deaktivieren

Entfernen Sie nicht benötigte Dienste und Anwendungsprogramme oder installieren Sie diese erst gar nicht. Falls Dienste/Programme nicht permanent benötigt werden (Chat-Client, …), dann sollten diese manuell gestartet und nach Gebrauch wieder deaktiviert/beendet werden.

11 Daten/System sichern

Die sorgfältige Anwendung der Goldenen Regeln verbessert die Sicherheit Ihres Systems und der darauf gespeicherten Daten. Ein absolut sicherer Schutz gegen Angriffe, Anwenderfehler oder Hardwareschäden ist leider nicht möglich. Da Dateien im Schadensfall auch verändert werden können, sollte eine Datensicherung auch eine Wiederherstellung zu einem weiter zurückliegenden Zeitpunkt erlauben. Um Datenträgerfehlern vorzubeugen sollten Backups (evtl. rotierend) auf verschiedenen Datenträgern gesichert werden.

Das zentrale Backup des Rechenzentrums sichert die Netzlaufwerke im Novellnetz, den zentralen Mailserver und die Serversysteme des Rechenzentrums. Lokale Laufwerke Ihres Rechners werden vom zentralen Backup nicht erfasst.