Pressemitteilung der Universität Hamburg, Arbeitsstelle für wissenschaftliche Weiterbildung vom 24.06.2015

Was jeder über IT-Sicherheit wissen sollte

Schutz vor Hacker- und Insider-Angriffen

Fehlende oder unzureichende Konzepte und Maßnahmen im Bereich der Informationssicherheit können zu erheblichen Schäden für die Wirtschaft führen. Das Echo von den Edward Snowden Enthüllungen ist noch nicht verhallt, als im Juni Angriffe auf die IT des Bundestages bekannt werden, bei denen Daten an bislang unbekannte Hacker abgeflossen sind. Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde bisher auf 14 Rechnern der Trojaner nachgewiesen. Dass auch große Unternehmen nicht gefreit vor diesen Angriffen sind, zeigen z.B. die erfolgreichen Hackerangriffe auf Sony und auf die Kreditkartenunternehmen Visa und Mastercard. Und man muss leider davon ausgehen, dass die Dunkelziffer bei der Cyberkriminalität besonders hoch ist. Zum einen, weil nur ein gewisser Prozentsatz von Hackerangriffen überhaupt erkannt wird, zum anderen weil der Datenklau für die betroffenen Einrichtungen eine peinliche Angelegenheit ist, die möglichst nicht an die Öffentlichkeit gelangen soll.

Allerdings: besser als nachbessern oder gar vertuschen ist die rechtzeitige Vorbeugung. Denn vor Hackerangriffen kann man sich schützen! Es gibt einfache Maßnahmen, um die eigenen Daten und Hardware zu schützen.

Einfache Tipps zum Schutz vor Cyber-Kriminalität

von Dr. Matthias Bonnesen, Universität Hamburg

- **Updates**: Neben Lücken in Software ist auch der Mensch selbst häufig Ursache für die Entwendung von vertraulichen Daten. Als wichtigste Maßnahme, um sich vor solchen Angriffen zu schützen sollten Benutzer von IT-Systemen regelmäßig alle notwendigen Sicherheitsupdates einspielen und einen stets aktualisierten Virenscanner installiert haben.
- **Unbekannter E-Mail-Absender**: E-Mails von unbekannten Absendern sollte generell misstraut werden.

- **Gefälschter Absender**: bei gezielten Angriffen auf Personen kann jedoch die Absenderadresse gefälscht sein. Auch beim Angriff auf den Bundestag wurde die Absenderadresse von Angelika Merkel genutzt.
- **Anhänge** von „ .exe“- Dateien sollten nie ohne Rückfrage des angeblichen Absenders ausgeführt werden. Häufig sind diese Anhänge in Archivdateien (meist .zip) versteckt oder der Angreifer versucht den Anhang durch eine weitere Endung wie .pdf zu tarnen, wie z.B. durch „Rechnung.pdf.exe“. Hier sollte man sich nicht täuschen lassen; es handelt sich um eine ausführbare Datei, die jeglichen Schadcode installieren kann. Schadcode innerhalb einer solchen Archivdatei wird von den Virenscannern des Mailservers häufig nicht erkannt.
- **Links:** Ebenfalls gern genutzt sind Emails, die Links auf präparierte Webseiten enthalten, auf denen sich gefährlicher Schadcode befindet. Deshalb solle man äußerst skeptisch sein, wenn eine Mail Links enthält.
- **Ausführen von Scripten unterbinden:** Generell können Webseiten mit Schadsoftware infiziert sein und auf diese Weise den Rechner befallen. Es besteht jedoch die Möglichkeit, das Ausführen von Scripten zu unterbinden. Hierzu gibt es Plugins für den Browser, wie z.B. „NoScript“. Gelangt man auf eine mit Schadsoftware präparierte Webseite, bleibt der Rechner verschont, da die bösartigen Programme nicht ausgeführt werden. Es besteht die Möglichkeit, für ausgewählte Webseiten Scripte zu erlauben.
- **Persönliche Daten:** Auch sollte man sich davor hüten**, persönliche Daten per Email** weiterzugeben.
- **Vorsicht bei Mails mit** einer Aufforderung zum Antworten, aber ohne persönliche Anrede. Statt eines Namens erfolgt die Anrede mit „Sehr geehrter Kunde, sehr geehrte Kundin“.
- **Daten auf Webseiten eingeben:** Gleichermaßen beliebt sind Links auf Webseiten, wo persönliche Daten eingegeben werden sollen, nicht selten Benutzer- oder sogar Bankdaten. Zu beachten ist, dass in dem Linktext jeder beliebige Text angegeben werden kann, obwohl der Link auf eine ganz andere Seite führt. Hat man einen Link angeklickt, sollte man sich genau ansehen, welche URL (Internet-Adresse) im Browser erscheint. Häufig hat die URL keine Ähnlichkeiten mit dem hinterlegten Linktext, auf den man geklickt hat. Zuweilen werden aber auch bekannte Domains vorgetäuscht. So wird z.B. anstatt „www.sparkasse.de“ eine völlig andere Domain aufgerufen, die nur im Unterverzeichnis den Banknamen aufweist wie z.B. www.betruegerdoamin.com/sparkasse.de/index.php oder der vorgetäuschte Seitenname

befindet sich in der Subdomain: www.sparkasse.de.betruegerdomain.com. Auch in diesen Fällen handelt es sich nicht um die URL einer Bankseite. Hinzu kommt, dass gefälschte Webseiten meist nicht verschlüsselt sind. Befindet man auf der Login-Seite einer echten Bank, erfolgt die Übertragung ausnahmslos verschlüsselt. Deshalb sollte im Browser immer am Anfang der URL https://.. erscheinen, wobei das ‚s' für die verschlüsselte Verbindung steht.

- **Onlinebanking:** Generell sollte man Bankseiten, auf denen man sich einloggt, nicht durch Anklicken von Links besuchen, sondern selber die URL in den Browser eingeben. Wer ganz sicher gehen will, kann ein eigenes, nur für Internetbanking vorgesehenes Betriebssystem nutzen, das den Rechner von CD/DVD oder schreibgeschützen USB-Stick startet und den Zugriff auf die Festplatte komplett verbietet.

Befolgt man diese Hinweise beim beruflichen wie auch beim privaten Umgang mit der IT, so sinkt die Wahrscheinlichkeit, Opfer von Cyberkriminalität zu werden, drastisch.

Professionelles Informationssicherheitsmanagement

Für Unternehmen und Behörden reichen diese einfachen Schutzmaßnahmen nicht aus. Um größere und angreifbarere Serverstrukturen vor Hacker- und Insiderangriffen zu schützen, bieten sich sowohl kryptografische Verfahren als auch Intrusion-, Detection- und Intrusion-Prevention-Systeme an. Zudem ist entsprechend ausgebildetes Personal notwendig. Die Universität führt regelmäßig Weiterbildungsseminare zum Thema IT-Sicherheit in Unternehmen und Behörden durch. Das dreiwöchige Seminar „IT-Security-Management" und die zweitägige Schulung „ISO 27001-Zertifikat auf der Basis des IT-Grundschutzes" richten sich an Personen mit IT-Vorkenntnissen.

Weitere Informationen und Anmeldung:

Dr. Matthias Bonnesen

m.bonnesen@aww.uni-hamburg.de

Tel. 040/42838-9713, -9700

Pressekontakt

Magdalene Asbeck

Universität Hamburg, Arbeitsstelle für wissenschaftliche Weiterbildung

Schlüterstr. 51

20146 Hamburg

Tel.: +49 (0) 40/428 38-9711, -9700 (Infotelefon)
E-Mail: m.asbeck@aww.uni-hamburg.de

Die Arbeitsstelle für wissenschaftliche Weiterbildung der Universität Hamburg wurde 1975 gegründet und gehört zu den renommiertesten und größten Einrichtungen der wissenschaftlichen Weiterbildung in Deutschland. Ein Team von 15 festen und ebenso vielen studentischen Mitarbeiterinnen und Mitarbeitern betreut rund 120 Dozentinnen und Dozenten und ca. 4500 Teilnehmende pro Semester.
Die AWW steht für universitäre Weiterbildung, Kompetenz und Erfahrung auf höchstem Niveau. Sie bietet Berufstätigen wissenschaftlich fundiertes Wissen für ihren Job und Zugang zu aktuellen Forschungsergebnissen, ausgereifte Curricula, Praxisnähe, anerkannte Abschlüsse und Zertifikate. Berufliche Weiterbildungsangebote finden abends und am Wochenende statt oder ortsunabhängig mittels moderiertem E-Learning. Angebote für alle Bürgerinnen und Bürger, die vom universitären Wissensschatz profitieren möchten und auf Qualität Wert legen, sind das Kontaktstudium für ältere Erwachsene und die öffentlichen Vortragsreihen des Allgemeinen Vorlesungswesens an der Universität Hamburg.