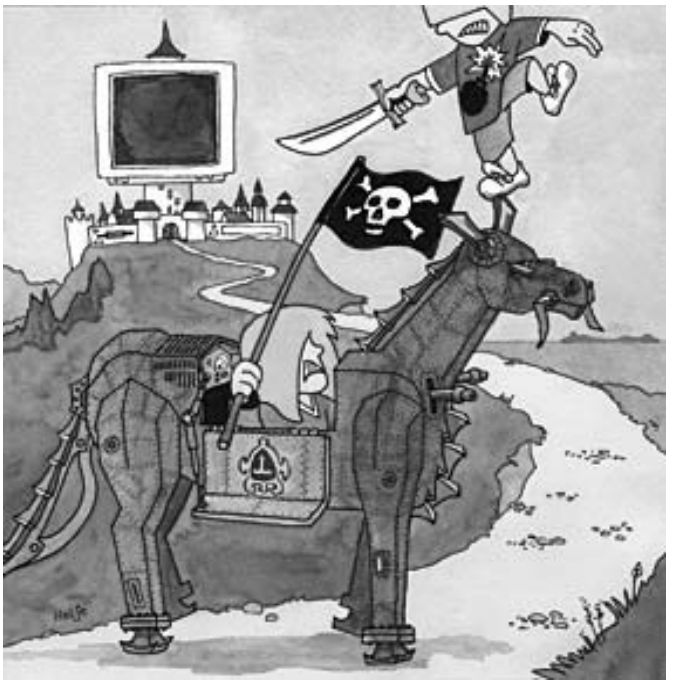
INHALT



ZUM THEMA

IT-Sicherheit

Eine sichere Informationstechnik ist eine der wesentlichen Voraussetzungen für eine prosperierende Wirtschaft und eine Gesellschaft, die Computersysteme in ihren Alltag integriert hat. Mehr noch: Die Sicherheit vieler anderer technischer Systeme kann heute nur mithilfe informationstechnischer Komponenten in diesen Systemen gewährleistet werden. Diese IT-Sicherheit bedeutet jedoch mittlerweile zweierlei: Einerseits muss die Technik selbst zuverlässig und sicher funktionieren, andererseits darf aufgrund der weltweiten Vernetzung über das Internet das einzelne Computersystem nicht gefährdet sein. Der erste Aspekt – Verlässlichkeit der Technik – wurde bereits im Heft 3/1992 von LOG IN untersucht. Der zweite Aspekt – Sicherheit unter den Gesichtspunkten des Internets – wird im vorliegenden Heft vorgestellt, diskutiert und mit Vorschlägen für den Unterricht ergänzt.

Das Titelbild zum Thema wurde von Jens-Helge Dahmen, Berlin, für LOG IN gestaltet.

IT-Unsicherheit

In einer aktuellen Nachricht des Bürger-CERT, an dem u.a. das Bundesamt für Sicherheit in der Informationstechnik (BSI) beteiligt ist, steht es klipp und klar geschrieben: „Nachdem Microsoft an seinem Patch-Day vergangene Woche Lücken in Word und Excel geschlossen hat, weist nun ein weiteres Office-Produkt eine sicherheitskritische Lücke auf. Diese macht es Angreifern möglich, das Präsentationsprogramm PowerPoint als Einfallstor für Viren, Würmer und Trojanische Pferde zu nutzen. Öffnet ein Nutzer eine präparierte PowerPoint-Datei, die ihm beispielsweise per E-Mail zugesandt wurde, können vertrauliche Daten, wie z.B. seine Passwörter, ausspioniert werden. Es sind bereits PowerPoint-Dateien im Internet unterwegs, die die Schwachstelle aktiv nutzen."

Und in einem nahezu zur selben Zeit versandten Bericht heißt es: „Hacker nutzen derzeit eine Sicherheitslücke, um sich Administratorenrechte auf Linux-Rechnern zu verschaffen […]. Das Sicherheitsleck betrifft alle 2.6er-Kernel-Versionen. Nutzer sollten schnellstmöglich die von den jeweiligen Herstellern aktualisierten Kernel-Pakete installieren."

Meldungen dieser Art, lassen jeden Computer-Besitzer gleichermaßen daran zweifeln, ob er überhaupt noch „Herr im Hause" seines Computers ist und was er sich einhandelt, wenn er sich der großen weiten Welt, dem World Wide Web öffnet.

Noch vor wenigen Jahren hatte die Gefährdung von Computersystemen nur zwei Hauptursachen: menschliche Irrtümer bei der Konstruktion der Computersysteme und menschliche Dummheit bei der Bedienung dieser Systeme. Nicht erst seit dem GAU in Tschernobyl standen auch die Sicherheits- und Verlässlichkeitsaspekte bei der Computertechnik zur Debatte. Bereits 1968 wurde in der ersten NATO-Konferenz zum Software-Engineering darüber diskutiert, wie Fehler beim Schreiben von Software minimiert werden können. Denn eins ist klar: Im Allgemeinen kann nicht die Anwesenheit von Fehlern in informationstechnischen Systemen nachgewiesen werden, sondern es kann nur bewiesen werden, dass der gerade erkannte und hoffentlich ohne Nebeneffekte beseitigte Fehler nicht mehr existiert. (Dieses Phänomen stand übrigens bereits im LOG-IN-Heft 3/1992 im Mittelpunkt des Themas.)

Mit der zunehmenden Vernetzung von Computern vor allem über das Internet sind allerdings auch neue Quellen der Sicherheitsgefährdungen entstanden (was nicht bedeutet, dass menschliche Irrtümer und menschliche Dummheit nicht weiterhin eine wesentliche Rolle spielen). Insbesondere die Existenz von so genannten Monokulturen bei Betriebssystemen und Standardsoftware ist eine der Hauptursachen der starken Gefährdung. Aufgrund der Dominanz eines einzelnen Produkts am Markt sind die in diesem Produkt bekannten Schwachstellen hauptsächlich verbreitet und bewirken bei ihrer Ausnutzung besonders hohe Schäden. Das bedeutet aber nicht, dass andere Produkte weniger Sicherheitslücken in sich tragen. Nach Feststellungen des BSI weist die Anzahl der bekannten Sicherheitslücken ein Verhältnis von 50:50 zwischen dem marktführenden Produkt und den anderen Betriebssystemen auf. Vor allem bilden finanzielle Interessen heutzutage die ausschlaggebende Antriebskraft, unter Kenntnis dieser Schwachstellen gezielt Computersysteme zu missbrauchen.

Eine sichere Informationstechnik ist eine der wesentlichen Voraussetzungen für eine prosperierende Wirtschaft und eine Gesellschaft, die Computersysteme in ihren Alltag integriert hat. Ähnlich wie kleinen Kindern die Gefahren des Straßenverkehrs bewusst sein müssen, damit sie sich ungefährdet im Straßenverkehr bewegen können, so muss auch allen Nutzerinnen und Nutzern von Computersystemen von vornherein deutlich sein, welchen Angriffen sie weltweit ausgesetzt sind, um sie rechtzeitig und nachhaltig abwehren zu können.

Doch IT-Sicherheit ist mehr als die Verhinderung von Viren und Würmern, und sie ist auch kein statischer Zustand, sondern ein ständiger Prozess. IT-Sicherheit beginnt beispielsweise mit regelmäßiger Datensicherung. Sie umfasst aber auch den aktiven Schutz der eigenen personenbezogenen Daten und der Daten anderer – beispielsweise durch entsprechende Verschlüsselung und entsprechendem Passwortschutz.

IT-Sicherheit ist aber auch nicht mehr auf den eigenen Computer beschränkt. Sie betrifft ebenso den weltweiten Datenaustausch, d.h. jede E-Mail und vor allem die Anhänge, die mit E-Mails versandt werden. Und sie betrifft das unkontrollierte Surfen im Internet. Denn allein das Öffnen einer Webseite kann bewirken, dass einschlägige Schadprogramme unbemerkt heruntergeladen werden.

Eine weit verbreitete Ansicht ist, dass IT-Sicherheitsmaßnahmen zwangsläufig mit kostenintensiven Investitionen in die Technik und nicht erreichbarem Expertenwissen verknüpft sind. Klar ist zwar, dass es eine hundertprozentige IT-Sicherheit nicht gibt. Aber die „IT-Unsicherheit" kann durchaus minimiert werden, und zwar dann, wenn aufgeklärte und mündige Computer-Nutzerinnen und -Nutzer ein entsprechendes Bewusstsein dafür haben. Die meisten Angriffe auf die Sicherheit können nur aufgrund von Unkenntnis und mangelndem Problembewusstsein der Anwender gelingen – eine weitere Aufgabe der informatischen Bildung, genau diesem Unwissen entgegenzuwirken!

Bernhard Koerber
Helmut Witten