Tipps und Tricks zur Informatiksicherheit

Tipps und Tricks um Rechner vor fremden Attacken wirkungsvoll zu schützen und was Sie tun können um das Risiko eines Virenbefalls stark zu vermindern. Eine hundertprozentige Sicherheit wird es vermutlich nie geben, jedoch kann mit den richtigen Restriktionen das Restrisiko auf ein Minimum reduziert werden.
- Unbedingt eine AntiViren Software installieren. Eine Liste von Herstellern ist unter der Rubrik Unix & Linux und Windows zu finden. Viele Hersteller halten sogenannte zeitbegrenzte Testversion auf ihren Webseiten zum Download bereit. Somit kann jeder Anwender für sich entscheiden, welche Software ihm am besten zusagt.

- Antiviren Software ist abhängig von der Aktualität der Virentabelle. Es ist ratsam von Zeit zu Zeit die Virenliste von dem jeweiligen Hersteller aus dem Internet runter zuladen!

- Niemals Programme vom Internet laden von denen der Ursprung nicht bekannt ist.

- Ã–ffnen Sie keine Attachments, deren Art Sie nicht kennen oder die Herkunft nicht eindeutig ist. Um ein Virus nicht versehentlich zu aktivieren, empfehlen wir Mails mit unbekanntem Absender oder zweideutigem Inhalt sofort und unwiderruflich zu löschen!

- Bevor Dateianhänge eingehender E-Mails geöffnet werden, diese zunächst in einem Verzeichnis speichern und nochmal mittels eines Virenscanners überprüfen und gegebenfalls löschen.

- Informieren Sie sich über Sicherheitslücken in Ihrer Internet-Software, einschliesslich des Betriebssystems. Installieren Sie regelmässig entsprechende Updates, Bug-Fixes oder Patches etc.
- Gehen Sie nie ins Internet, wenn Sie als Benutzer im LAN mit Administrator-Rechten angemeldet sind. Richten Sie dafür einen Benutzer mit drastisch eingeschränkten Rechten ein, ansonsten Tür und Tor geöffnet sein könnten.
- Es ist empfehlenswert, den Arbeitsspeicher von Zeit zu Zeit, auf resistente Programme zu überprüfen. Antispywareprogramme übernehmen diese Aufgaben. Es sollte jedoch darauf geachtet werden, dass auch diese regelmässig Upgedatet werden.
- Die "Fenster-Funktion" in Outlook ausschalten und beim Surfen im Internet durch entsprechende Einstellungen des Browsers sogenannte "aktive Inhalte" (Java Scripting oder Aktive Scripting) nicht zuzulassen. Solche Inhalte wie bewegte Bilder und interaktive Angebote können bei der Ãœbertragung eines Computervirus eine entscheidende Rolle spielen. Wer jedoch nicht auf alle Funktionen der neuen Webtechnologie verzichten möchte, sollte zumindest ActiveX unterbinden wobei manchmal auch Einschränkungen beim Besuch von Webseiten gegeben ist.
- Im Bios das System dahingehend anzuweisen, dass beim Start des Systemes nicht mehr zunächst von einem Diskettenlaufwerk gebootet wird. Hin und wieder werden Disketten im Laufwerk "vergessen" welche beim hochfahren des Rechners zuerst gelesen würden. Somit wird verhindert, dass von einer virenverseuchten Diskette gebootet und das System mit einem Bootsektorvirus infiziert wird
- Eine Bootdiskette erstellen, die garantiert virenfrei ist. So eine Diskette kann bei einem evtl. späteren Virenbefall eine grosse Hilfe sein. Oftmals übernimmt diese Arbeit auch die installierte AntiViren Software. Unbedingt die Diskette mechanisch mit Schreibschutz versehen. Softwarebasierender Schreibschutz wird durch sehr viele Viren einfach umgangen.
- Da einige sehr schädliche Viren auch versuchen die Festplatte unter Hilfename bereits installierter Programme zu formatieren, hilft in vielen Fällen ein ganz einfacher Trick, dem Virus derartige Funktionen zu verwehren: Die Dateien Debug.exe, Format.com und Deltree.exe in mit einer Zahl zu versehen, die Dateiendung aber so zu belassen. Die Funktionen der genannten Programme werden bei Aufruf nicht beeinträchtigt.
- Die Server müssen von Zeit zu Zeit durch ein unabhängiges Serverkontrollmonitoring auf Sicherheitslücken gescannt und überwacht werden. Um versuchte Einbrüche in das Netz zu erkennen müssen so genannte Portscanns eben auch als solche erkannt werden. Sicherheitsrevisionen und Test-Hack-Attacken gehören ebenso zum Kontrollinstrument wie auch das sensibilisieren der Benutzer.
- Um die Sicherheit der Unternehmensinformatik zu erhöhen, braucht es viel Zeit und Engagement um die Benutzer regelmässig über Sicherheitsaspekte zu unterrichten und klare Anwenderrichtlinien auszuarbeiten. So sollten etwa Mitarbeiter in regelmässigen Abständen darauf hingewiesen werden, dass sie niemandem, weder telefonisch noch direkt über die Informatikumgebung Auskunft zu geben haben und dass sie erst recht niemandem ihr Passwort verraten sollten.
Ein Passwort ist der Schlüssel, mit dem sich im Internet viele Türen öffnen lassen, deshalb fängt die Online-Sicherheit schon bei der Wahl des richtigen Passworts an. Die meisten Menschen gehen sehr leichtfertig mit ihren Passwörtern um, weil sie erstens zu gutgläubig sind und zweitens nicht erahnen können welchen Ã„rger man sich einhandeln kann, wenn

jemand anderer sich unter ihrem Namen Zutritt zu vertraulichen oder kostenpflichtigen Informationen in Firmennetzen oder im Internet verschafft. Die meisten Hackerattacken werden laut Sicherheitsberatern von den eigenen Mitarbeitern durchgeführt und nicht wie immer propagiert von externen Ã‚Â«bösen BubenÃ‚Â».
Doch nicht nur die Treuherzigkeit vieler Anwender kann zum Sicherheitsrisiko werden, auch gewisse Praktiken sind hoch gefährlich. So ist es vor allem bei KMUs gang und gäbe, dass Kollegen untereinander die Passwörter tauschen. Passwörter haben in einem solchen Szenario eigentlich überhaupt keine Funktion mehr, sondern stören nur. Entsprechend ist die Moral dem ganzen Thema Computer-Sicherheit gegenüber.
Oft sind Passwörter aber auch einfach zu erraten. Steht das Passwort im Lexikon, sollte es nicht verwendet werden, denn Einbruch-Tools haben ganze Lexika geladen und probieren die Wörter in Sekundenschnelle als Zugangsbegriffe durch. Ungünstig sind aber auch die Anfangbuchstaben der Wörter in einem Satz. Oft können sich die Benutzer nämlich die Sätze nicht merken und schreiben sie deshalb auf. Bei einer Ã‚Â«Wer sucht, der findetÃ‚Â»-Aktion wurden Passwörter auf der Rückseite von Tastaturen gefunden oder waren auf den Bildschirmrand geschrieben. Nachfolgen ein paar Regeln im Umgang mit Passwörtern:
- Schreiben Sie ihr Passwort niemals auf und achten Sie beim Eingeben des Passworts, dass Ihnen niemand über die Schulter schaut.
- Ã„ndern Sie auf jeden Fall Ihr Passwort sofort, sobald Sie sich ausspioniert fühlen und informieren sie auch immer Ihren Vorgesetzten.
- Wenn Sie glauben, dass jemand anderer Ihr Passwort verwendet, dann informieren Sie umgehend den Systemadministrator, er kann vielleicht dem Bösewicht eine Falle stellen.
- Passworte sollten keine persönlichen Gegebenheiten wiederspiegeln wie, Vornamen, Nachnamen, Firmennamen, Telefonnummern, Autokennzeichen, Automarken oder Strassennamen etc.
- Das Passwort muss mindestens sechs, besser aber acht Zeichen lang sein und aus einer Mischung von Buchstaben und Zahlen sowie aus Gross- und Kleinschreibung bestehen.
- Am besten eignen sich geografische Namen wie Ortschaften, die per Zufall in einem Atlas nachgeschlagen und durch eine Nummer ergänzt werden. Beispielskombination mit der Ortschaft Ascona: aScoNA25 oder AS2cOna5