Ethical Hacking "Anti-Hacker"

When the word hacking is mentioned, people immediately think of the Pentagon. It is, in fact, true that the US Ministry of Defense has repeatedly been the preferred goal of ambitious computer pirates. However, the real threat to modern society is not a nuclear war triggered off by mistake. What has become a true trouble-maker for business and society is hacking in the form of unauthorized intrusion into private data spheres.

People who professionally deal with encroachments on internal networks are often just taken aback at what they must see. Politically motivated attacks of cyber criminals - stories the media love to spread - are rather an exception. In many cases - more than one would think of - unwanted intrusions into computers of businesses and local or government administrations are committed by their own staff. A recently uncovered case where a staff member of a big trading company sent his female co-workers pornographic material via email is not at all an exception. The problem is that such occurrences usually are not considered to be a form of hacking. This, however, is hacking as well because in such cases the perpetrator made unauthorized access and illegally acquired the names of his victims.

It is estimated that in Europe approximately fifty percent of all cases of network abuse are aimed at the companies’ own staff. In the US, this figure is even higher. Besides the internal network abuse there are cases of real espionage. The French subsidiary of a computer company tried to intrude into the networks of its US headquarters with the intention to spy out profitable businesses and snatch them away. Internet vandalism is another phenomenon that has become more and more widespread: in these cases private web sites or sites of companies or institutions are marred - sometimes with a political background.

All forms of hacking whether they are obvious or concealed cause enormous economic damage. Exact statistical data are, for good reasons, not available. The companies affected rather prefer to remain quiet about hacker attacks and the costly remedying of their consequences for fear of image loss. According to a anonymously carried out survey, conducted among 563 companies, three out of four respondents admitted that they have suffered financial losses due to security insufficiencies. It is estimated that the yearly costs world wide amount to 10 billion US dollars.

One of the most effective remedies against network break-ins is the homeopathic method: thus hackers are beaten with their own weapons. This has been the method of the IERS-Security-Team for quite some time now. Their computer specialists emulate hacker attack strategies in order to test the network security of companies and government agencies. The ”ethical” hackers use the same tools as common hackers when intruding into protected private spheres. Experience shows that they are often successful because the tested systems are vulnerable or – and this is a widespread phenomenon – because the security staff is not properly qualified or simply too careless.

What a hacker does can be compared with the attempt to break into a house. In most cases the front door is locked, but a back door or a window is wide open due to the landlord’s carelessness. Preferably hackers try to outwit those machines which shield the internal network from the outside world, namely firewalls that have been installed for the protection against unwelcome intruders. If ethical hackers want their work to be efficient and carried out under realistic conditions, the first thing they have to do is get information about the current hacker tools. The sources of information are underground bulletins on the Internet and the hackers‘ own web sites which always serve as a treasury for new tools. Additional information are obtained at various meetings and get-togethers. IBM possesses an impressive array of hacker tools as well as comprehensive documentation about system vulnerabilities which are available to the security experts for analysis and consultation purposes.

The aim of ethical hackers is to detect vulnerabilities. After they have been determined, a detailed report is written and presented to the company. Then the security manager of the respective company has to make sure that the security holes are closed. Ethical hackers only test a system in consent with the management of a company. IBM has selected experts. Therefore, it is not possible that a person does security checks who before has acquired his knowledge as a ”real” hacker. In order to make sure that the testing itself does not pose a risk, IBM acts on the principle not to penetrate any further into a system after an attack has been successful, as there would be a risk of real hackers following them doing harm to data and system.

The world of hackers churns out new tools nearly every day. Therefore, a one-time check of a network offers only temporary protection which is insufficient. Big companies like banks, insurance companies, airlines, car manufacturers and large trading companies have their systems already checked routinely. State-of-the-art technology allows even intrusion detection in real time: special sensors compare incoming data with typical data sequences of attacks and recognize, if the tool of a hacker is in action, which immediately raises alarm. This method requires knowledge about the hacker tools as well as having those tools at our disposal (knowledge-based method). The software of these sensors must be regularly updated so that they remain effective.

Ethical hackers do quite well if assigned unusual and special tasks. Recently a banking house which fell victim to cyber blackmailers engaged a security expert team to handle this very critical situation. Anonymous callers claimed to have intruded the bank’s customer database. If the company did not pay a ransom, so they threatened, the case would be made public. The crux was that no intrusion had taken place. Yet, the bank could only prevent harm by hiring computer specialists who proved that their system had not been touched. Such modern threats require quick reaction. Many large companies, however, lack the necessary security policy.

In the future, it should even be more difficult to access critical information from a computer. Researchers at the IBM-Laboratory located in Rueschlikon, Switzerland, are presently working on a technique that detects intrusions in real time, without supplying so-called ”signature files”, beforehand, as is done when employing the ”knowledge-based” method. There the software of the sensors compares running activities with activity profiles of known risk events. The decisive advantage of the new method is that there is no lagging behind the hackers‘ methods, on the contrary, this new technique unfolds preventive security. This ”behavior-based” technology - already available as a prototype – allows to recognize unusual features of a running procedure within a certain system, and thus indicates the attempt of an unauthorized person accessing the system. In order to understand how protective software works you have to be aware that a computer program while running executes a number of system calls each consisting of certain data sequences. ”Open a file”, ”start a new process”, etc. are examples for such system calls. The data sequences produced by a program differ and are dependent on how a program is started and to which interaction the user has to react.

Researchers from IBM work these days with an algorithm that had been developed for the DNA-analysis by their US colleagues and which is known under the project name ”Teiresias”. This algorithm enables us to determine recurring partial sequences or patterns of a data flow and to separate sequences with particular characteristics. What looks like child’s play is enormously useful. With the help of those patterns typical for a program it is possible to check each execution in real time whether it consists of those typical characteristic sequences or whether it contains data sequences that have never been encountered by the system before. If the latter applies, it can be presumed that a hacker manipulates the execution of a program and in this case the protective software will send an alarm to the systems’ administrator. The security mechanism Teiresias can be implemented in any company, it works no matter who uses a certain application and it is independent from the purpose of its use.

Published in the Zurich-based weekly paper Schweizerische Handelszeitung No. 19 of 12th May 1999