Hacking Cum Laude

With the rapid growth of electronic commerce, companies feel exposed to new risks. Hackers encroach protected communication systems, manipulate business operations and compromise customer data. Yet, there is a remedy for it: by making use of the hackers' own weapons, anti-hackers preventively uncover exposures. The know-how of these experts is useful in so many fields. Their future looks bright as a wide field of career opportunities open up.

Movie pictures in the eighties evoked scenes where irresponsible hackers triggered off a nuclear war. Only ten years later reality has outpaced fiction. According to British sources, pro-Serbian hackers attacked 170 banks, internet providers, editing houses, radio and TV stations worldwide during the Kosovo war. With virus-infested emails, the Belgrade "cyber-soldiers" and their accomplices in other eastern countries took revenge for the bombardment by NATO countries. The successfully attacked computer systems crashed or refused their legitimate users access for several hours. In extreme cases, databases were completely deleted. For the first time the world experienced cyber-terrorism on a large scale. Their originators did not have to throw real bombs – yet, their attacks hit the very heart of the first world.

The Spectrum Covers Anything from Annoyance to Blackmailing

Politically motivated attacks from cyber criminals are spectacular exceptions. Hacking, the unauthorized intrusion into private data spheres, has become a real disruptive factor for industry and commerce. In many cases - more than one would imagine - intrusions into computers of businesses and local or government administrations are committed by their own staff. In a recently uncovered case a member of the staff of a large trading company sent his female co-workers pornographic material via email. Unfortunately, this is not an exception. In fact, 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 hacker attacks on networks are committed by the company's or organization's own staff. 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. One cyber attacker, for example, expressed his protest against the German Government's policy of supervision. He marred the web site of the Cologne Federal Office responsible for defending the constitution with caricatures of politicians. According to a recent report of the American Institute of Computer Security, every fifth home page owner had cause to complain about unauthorized visitors or downright misuse of their web sites within the past twelve months.

Using All Tricks

Hackers use all the tricks and sometimes cause enormous damage. They “bombard”, for example, their victims’ systems with e-mails (mail bombing) until it crashes. Another method is smuggling a program (sniffer) into somebody else’s network system in order to sniff out their data (such as passwords or protected information). There is another spying technique, (spoofing) where the hacker sets up fake web sites with the aim to elicit confidential data (like bank pin codes) from the unsuspicious user.
All forms of hacking whether they are obvious or concealed cause enormous damage. Exact statistical data are not available. Affected companies prefer to keep quiet about hacker attacks and the costly remedying of their consequences for fear of image loss. According to an anonymously carried out survey among 563 companies, however, three out of four respondents admitted that they have suffered financial losses due to security insufficiency. The annual loss world-wide is estimated to amount to 10 billion US dollar. Cyber-crime becomes increasingly a matter for the courts. According to a survey carried out in the US, the number of those who take legal action against hackers has nearly doubled within three years.

Homeopathic Method

One very effective remedy against network break-ins is the homeopathic method: hackers are beaten with their own weapons. This has been the method of the Emergency Response Service Team - founded in 1988 - 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 personnel 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. Their sources of information are underground bulletins on the Internet and approximately 2000 web sites on which insiders exchange knowledge about newly-developed hacker tools. Additional information can be 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 report is written and presented to the company or organization. Then the security manager of the respective company has to make sure that the security holes are closed. Ethical hackers test a system only in consent with the management of a company. IBM has selected experts for these tasks. 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 is a risk of real hackers following them doing harm to data and systems.

Know-how - Tried and Tested in the Business World

Those who don't care may suffer. Such was the experience of a Saudi-Arabian Oil company whose managers thought to have done enough for network security by applying some cheap security solution. One day the IBM ERS team received an alarm: one of the company's main servers which controls thirty hosts had been penetrated by a hacker. The company's business operation was massively disturbed, and – as the IBM specialists were to find out when doing detailed analysis – the so-called log files had been swept off the storage disc. These files are actually a protocol of each single activity performed by the server and may be helpful in tracking down unwelcome visitors. At the company's premises in Saudi Arabia, the IBM-experts finally succeeded in analyzing the log files with the help of data remnants of the deleted C-drive, thus enabling the company to find the perpetrator.
There was no little surprise: none else than a member of the oil company's security team was found guilty of having paralyzed their computer system. It appeared that he had tried to do a security scan and lost control over the system. Later, however, he admitted that he had acted provocatively. The detailed detective work necessary to solve this task confirms once again that the threat to a network often emanates from the company's own personnel.

Difficult Task

Thanks to their great experience, ethical hackers do quite well if assigned unusual and special tasks. Recently a bank who fell victim to cyber blackmailers engaged the IBM Security Team to help them solve a particularly 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 secured computer system had not been touched.
Such modern threats require quick reactions. Airlines, for example, have integrated firm procedures into their disaster instruction plans in case of a hacker attack. In many large companies, however, such guidelines are still missing. Network security needs to generate a fast and intelligent response in case of an emergency. To get back to the above mentioned oil company: it was in fact utterly irresponsible of their managers to keep the company's networks running after the hacker attack has become obvious. The affected server should immediately have been disconnected and replaced by a back-up in order to keep the attacker in the dark about his being discovered. If a person in a crucial situation responds inadequately or wrongly, he may be the one who causes the biggest harm.

Preventive Protection

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 (RTID): 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 (knowledge-based method). The software of these sensors must be regularly updated (signature files) so that they remain effective. RTID is employed for the protection of intranet and Internet, but also for protecting an extranet which, for example, is used by airlines to communicate with their alliance partners.

Sensor Systems for Banks

US companies know and appreciate RTID technology already. European enterprises are just about to discover its value. Presently, IBM is installing an RTID sensor system at a bank in Barcelona, Spain, after having checked their system thoroughly. All practical experience tells that the configuration of those sensors requires quite a lot of technical know-how in order to be really effective. For it is the fine tuning that finally ensures that unwelcome intruders - and only them – be discovered by the automatic security mechanism. The first experiences which we are gathering in Barcelona confirm the efficiency of the system. The continuous monitoring of the system is performed by the banks own security people as well as by IBM experts from the Network Operation Center who are 24 hours, 7 days a week at the customers' disposal. 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.
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 mechanisms. 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.

Analogy to the DNS-analysis

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 in which 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. The tests which have been performed with this prototype have proved the effectiveness of this software.

Network Security – Carriers Promising a Bright Future

Total security – so any serious security expert will tell – can't be realized in networking not even with the most sophisticated protecting mechanism. The development of security systems is always a "work in progress". Network security, however, is not only a technical component, equally important is the staff that handles the system. A new occupational field has opened up in the past years which is still growing and gaining importance. In large companies where network security is vital, a hierarchy of security experts has evolved. The top of the pyramid is formed by the security officer who is usually part of the management.
Many of the jobs in the field of security require a master's degree (computer science, mathematics, physics). The leading security experts must understand the risk structure of a system and develop long-term solutions in the field of security. It is usually a computer scientist holding a Ph.D. who fills such a post. The senior technical analyst also has an academic background in computer science. He has specialized in network intrusions or computer viruses which qualifies him as a specialist for emergency situations. Besides his profound knowledge of various operating systems he is well-experienced in dealing with network breaches.
Another field of activity is product development. This person develops, for example, software against viruses and protective tools (firewalls) to prevent network intrusions. The technical administrator may either be holder of a master's degree or may have a bachelor's degree with a technical background. He has a solid knowledge about his network surrounding and is able to handle emergency cases. Practically no technical basis is required from the helpdesk analyst. He answers the customers' calls when they have problems regarding network security. With the help of a questionnaire, he compiles the information necessary for the security expert to allow a first assessment about the nature of the individual problem.

Excellent Prospects

Experts in network security have excellent prospects for their careers. As the demand exceeds the present supply, wages are usually quite respectable. Those, however, who have just completed their studies or practical training are not yet considered to be well-versed experts. What they lack is experience. They have to get familiar with networks in their natural environment, implement and run them. It is only "on the job" where you acquire indispensable knowledge through experience. The commitment to life-long learning is rewarded by a job that has the touch of pioneering spirit and is seasoned with a pinch of adventure.

Published in the Zurich-based monthly journal io**management** No.11/1999. Publisher: ETH-Zentrum für Unternehmenwissenschaften BWI