Business
Substances
Environment

Information
for the
underwriter

Information and communication technology

apropos

Computer viruses

The concept
Virus strains
Cases of damage
Types of criminal
Legal situation
Preventive measures
Tips for the underwriter

1.7

AssTech
D-80526 München
Germany

The concept

Viruses, worms and other software "bugs" represent a danger to data security.

Just as biological viruses require host cells in order to multiply, computer viruses need a software program to function as host. Not until a virus has established itself as an executable program code in the host program can it duplicate itself and smuggle the duplicates into other programs. As a rule, computer viruses are made up of four program blocks, each with its own function:

1. Check program
2. Reproduction and infection block
3. Identification program
4. Action block and/or damage function

Overwrite viruses attack the host program, replacing program codes with virus codes and thus destroying them; the program can no longer be executed.

Non-overwrite viruses manipulate programs by inserting branch instructions that make it possible to switch between program codes and virus codes. The host program can still be executed, but each time the program is booted the virus code is processed as well.

In contrast to a virus, a worm does not require a host program. It is an autonomous program that spreads through systems and networks by reproducing itself automatically but does not modify either data or programs. Given time, however, a worm can completely paralyse a program's performance.

Like viruses, so-called logic bombs are manipulated programs that are generally used as elements of computer viruses, too. "Detonation" of a bomb can be triggered by certain criteria, e.g. the date, the calling up of certain data, or the number of program starts.

Trojan horses and logic bombs share the feature that they are not visible until they are activated. Trojan horses are concealed program extensions which attempt to manipulate data without being discovered by the normal user.

Virus strains

Although exotic names such as Michelangelo, Israeli and Datacrime have recently been the cause of much – if unwarranted – ado, it would be foolish to underestimate the problem of software viruses.

According to reports by manufacturers of anti-virus software, over 90 % of all known damage was caused by the following viruses:

- Jerusalem (Israeli)
  Activates itself on any Friday, 13th.
- Yankee Doodle
  Plays the melody of the same name at 5:00 pm and attacks special files (e.g. COM.EXE).
- Vacsina
  Automatic update functions which preserve the system date and time valid at the time of infection for the data they infect (i.e. later updates are stored with the old date and time). The infection of new files is marked by a bleep.
- Ghost
  The seconds field in the time display of infected files shows 62 and, depending on the virus variant, the files are periodically overwritten. If a special section (boot sector) of a portable or stationary data medium is infected, a bouncing ball appears on the display.

- Perfume
  After an infected file has been called up for, say, the 80th time, it can be started again only after inputting "4711".
- Black Jack (Autumn Leaves)
  Every autumn this virus is activated and disrupts the display by making the characters drop down the screen like falling leaves.
- Stoned (New Zealand)
  The memory is infected and in turn infects any diskettes addressed by the system. When applications are booted, arbitrary texts and messages are displayed on screen.

There are many different variants of these viruses and they manifest themselves in quite different ways.

To date, more than 1000 types of virus have been identified, only about 10 of which, however, may actually be considered really malignant.

Cases of damage

In 1987 hackers in the USA managed to infiltrate the top security level of the NASA network through a loophole in the operating system. By installing a Trojan horse, they were able to maintain top-priority access authorisations even after the loophole in the operating system had been discovered.

At the beginning of the 1990s computer AIDS hit the headlines. Unidentified persons had sent out about 20,000 copies of a diskette allegedly containing information on AIDS. When the diskette was started, however, it renamed all files on the fixed disk. A message displayed on screen offered to send the victims a diskette to decipher the new names provided they transfer a large amount of money to a particular bank account.

Similar notoriety was achieved by the "Happy Christmas" chain letter, which has been appearing since December 1987. Once activated, the program looks for all the processor's data communications files, simultaneously drawing a Christmas tree on the screen, and then infects the communication partners by reproducing itself. Although the first version of "Happy Christmas" does not destroy any data, the damage caused by blocking communication and memory capacities can be considerable. A second version, which began appearing in spring 1988, does in fact destroy data and must therefore be classified as much more dangerous.

A more recent example of a computer virus is Michelangelo, which was to activate itself on 6 March 1992. The German authorities warned users about this virus, which tries to format the fixed disks in MS-DOS operating systems. It is now known that in Germany only about 100 cases of damage were reported to the authorities, although the real number is likely to have been much higher.

In the former West Germany some 5000 cases of computer crime were recorded in 1990. Experts have put the total damage at more than DM 5 billion.

Types of criminal

The concept of computer misuse can comprise one or more individual, sometimes related, crimes. In principle, these crimes can be divided into two broad groups depending on the criminals' motives.

On the one hand there are those whose prime aim is to enrich themselves either materially or immaterially; theft, fraud and blackmail are the main offences.

On the other hand, there are motives such as revenge and frustration coupled with the desire to harm others. This group of offenders might also be described as "intelligent arsonists".

Experts believe that the number of crimes that go unreported – especially those committed by the second group of criminals – is extremely high. After all, what company that has been harmed by one of its own employees is going to "shout it from the rooftops"?

Industry insiders assume that more than 80% of all software manipulations are done by employees and freelancers of the victim company.

The problem of hacking is not always clearly classifiable. Although hackers feel an allegiance to their own code of honour, once they have cracked a system the temptation to make a name for themselves through manipulation often proves irresistible. It is then but a short step from illegality to full-scale computer crime.

Legal situation

Two aspects of computer crime make the legal situation in this area highly problematical. Firstly, it is almost impossible to track down the offenders, especially in cases where destructive viruses are implanted in a system. Secondly, in many countries, particularly those of the former Soviet bloc, computer crime has not even found its way into the lawbooks.

In Germany the authorities reacted to this new form of crime by extending criminal law. In an effort to combat computer crime, the German Criminal Code was supplemented by § 202a (data espionage), § 263a (computer fraud), § 303a (data tampering) and § 303b (computer sabotage).

This means that in Germany computer saboteurs, spies and defrauders – along with hackers – face criminal prosecution and punishment. As already mentioned, however, the latter hardly ever occurs for want of evidence.

As a rule, crime statistics are not very reliable because of the large number of crimes that go unreported. But the Federal Office of Criminal Investigation in Germany published the following general breakdown of computer crimes for the period 1980–1986:

Fraud	about 33%
Espionage	about 53%
Sabotage	about 10%
Unauthorised access	about 4%

The German government went further in setting up the Federal Office for Security in Information Technology. With the aid of the "KIDS" warning system, government and industry are kept abreast of the latest developments. This work is carried out in coordination with the criminal investigation offices of the respective Länder (federal German states).

Preventive measures

What is true for biological viruses is true for the computer variety too: prevention is better than cure.

Despite the fact that modern data security standards already include measures to deter manipulation, in the special case of software manipulation it is also necessary to observe the following:

Technical measures

- Write protection for disks and diskettes
- Protection facilities (for processors and data media) against unauthorised access
- Access priorities (security tools)
- Continuous data backup (program backup to be used for restart only)
- Automatic callback for data networks with dial-up lines
- Antivirus programs (from reputable and experienced software manufacturers) for constant monitoring of installed software and for checking new software prior to installation

Organisational measures

- Ongoing checks of the trustworthiness of permanent staff and firms/persons under contract
- A clear system of access authorisations
- No alien software (particularly diskettes for promotion, demonstration and entertainment purposes)
- Checks on trustworthiness of software sources
- Virus tests
- Separation of data media according to programs and files where possible
- Detailed list of current data and programs together with documentation (date, source, length)
- Regular clearing-out of old data stocks and programs
- Emergency plan for low-level formatting

This list contains only the main points and is primarily intended for PC users. Other standards would apply in the case of companies with separate IT departments and their own computer centres. Consistent discipline and quality assurance are the most effective means of recognising errors due to negligence and deliberate sabotage before harm is done.

Tips for the underwriter

The insurance industry offers a range of products as cover against IT risks.

In accordance with the General Conditions for Electronics Insurance in Germany only property damage to hardware (including all operating-system programs installed) is indemnified.

Electronics insurers offer only very few models that cover consequential interruptions to business and/or additional costs incurred to keep business operations going.

Data medium insurance provides cover for external data media which do not belong to the hardware, including the data and programs stored on them. As a rule, only property damage is covered, although some insurers have extended the product by what is known as software insurance. This extension covers losses due to the deletion or manipulation of data and programs even where there is no prior damage to the data medium. Thus wilful actions of third parties, sabotage and malice are covered.

Computer misuse insurance is a component of fidelity insurance and provides cover against embezzlement and wilful damage done to the insured by means of data processing devices. Individual persons or groups of persons (e.g. contractual relationship) must be explicitly named. If the perpetrator of the crime is not known or was not named in the policy, no indemnification is payable. On the other hand, it is possible to include unidentified persons in the scope of cover by means of a special policy clause.

Pure financial loss caused by third parties not in the insured's employ can be covered by a data misuse policy.

A separate data liability insurance (or sometimes in the form of an additional clause in a professional indemnity or employers' liability policy) can provide cover for pure financial loss to third parties caused, for example, by violations of the German Data Protection Act.

In Germany, for example, there is also a special form of legal expenses insurance covering data protection. This insurance is available either as a stand-alone policy or as an extension clause to a company's legal expenses policy and covers the costs of legal defence in connection with suits brought under the German Data Protection Act.

Although the products described above are those on offer in Germany, they are also of relevance for international business.

In the case of all-risk covers, particular attention should be paid to elements of electronics insurance given under the named perils, exclusion lists for unnamed perils and sublimits for inclusions. Special consideration should be given to the possible inclusion of electronic equipment, systems and components in the misuse clauses of property insurance policies.

Given the different legal and market frameworks in each country, it is not surprising that the range of electronics insurance products offered varies considerably. Within the European Union it is France and Italy who have played a certain pioneer role.

The underwriter's task of assessing the risk is made more difficult by an inadequate or even non-existent legal framework and very little claims experience in both the national and international markets.

The products mentioned above are just the main ones used in Germany to insure electronics equipment and data; in the final analysis each company must recognise and evaluate its own risks.

Electronics insurance experts are in a position to provide risk analyses. Particularly where worms, viruses and other software "bugs" are involved, the advice of an outside specialist and the tailoring of insurance policies to a company's individual needs are of prime importance.

Postal address·
AssTech
Assekuranz und Technik
Risk Management Service GmbH
D-80526 Munchen
Germany

Office address.
AssTech
Assekuranz und Technik
Risk Management Service GmbH
Sederanger 4–6
D-80538 Mùnchen
Germany

Telephone: ++49-89-3844-585
Telefax ++49-89-3844-586
Telex· 5215247 bav d

Spanish subsidiary:

BEER & AssTech, S A.
RISK MANAGEMENT SERVICE, S.A.
Miniparque Empresarial de La Moraleja

Telephone (++1) 6509142
Telefax. (++1) 6509514