The Importance Of Antivirus

Posted on October 17, 2019

Antivirus Protection and Information Security

It is ethically important to acquire and install cryptographic means of information protection without fail for an organization that uses information systems in which confidential information is to be processed, in the case when the use of such systems is regulated by law. Everyone who uses an antivirus program is faced with the phenomenon of updating the anti-virus database. Antivirus programs work on the principle of malicious code detection, using data from antivirus signatures stored in virus databases. Every day in the world, there are tens of thousands of new malicious programs. And most often, the only thing that protects the user's computer from all these threats is a working anti-virus program. As a rule, the virus databases of leading products contain a huge number of records; for example, the virus collection of antivirus is more than 10 million records, but the number of records does not always determine the quality of virus detection (Sukhai 128).

Antivirus signatures often contain outdated records about viruses of a decade ago. For example, the new antivirus companies did a great job and reduced the virus database to 3 million records, leaving, however, only the most urgent and dangerous threats. This significantly speeds up the work of the antivirus and reduces the load on the user's system. When virologists of an antivirus company discover a new virus, they decode it and identify areas of malicious code, fragments of which are then added to antivirus signatures, using which the antivirus can detect viruses in infected files. Every day, the laboratory analyzes and adds more than 15 thousand records to its viral databases (Sukhai 128). That is why it is necessary to update the antivirus; otherwise, a new (completely fresh) virus simply cannot be detected by the antivirus. Moreover, anti-virus programs are also developing – new methods for detecting malware, new functions are being created, and the protection of the antivirus itself is improving. It is also important to use a licensed protection program, as most often, pirated versions of well-known antivirus software do not have the ability to update automatically, which makes these programs useless for protecting the user.

As stated earlier, antivirus software serves to diagnose, treat and prevent computer viruses. Diagnostics detect viruses and notify the user of the computer. Having found the virus, the antivirus software can prompt the user to cure the infected file, put it in quarantine or delete it. The prevention consists of the fact that the anti-virus program is launched together with the operating system, and viruses are checked in every program or file launched, i.e., it cleans the computer constantly (Kshetri n.p.).

Computer Viruses, Software Piracy, and Cyber Risk

To date, there is a huge variety of computer viruses in the world. According to Symantec, in 2008, the total number of viruses exceeded 1 million copies. It is for the definition of a particular type of virus that anti-virus programs have a signature database to check the scanned files. And when suspicion is detected, the program notifies the user. Antivirus programs have three modes of scanning for the presence of malicious software: minimal, medium (optimal), and maximum (paranoid). Paranoid security level provides the maximum degree of protection but usually consumes a large number of computer resources. The optimal level provides a sufficient level of protection, and it is recommended for daily work. The minimum level of protection usually includes a check on the signature database; that is, the antivirus provides information only if it is really a 100% virus (Griffin 136–53).

The problem of piracy arose even when the software was distributed only on physical media. At that time, the main negative effect of unlicensed software was the loss of revenue by the development companies, which adversely affected the development of their software products. Unlike developed countries, states on the territory of the former Soviet Union were much more vulnerable to piracy due to the weakness of distribution networks of licensed software, low purchasing power, and a lack of respect for both private property in general and intellectual property in particular.

With the onset of the Internet era, the problem of pirated software has only intensified – and has intensified many times. Firstly, access to unlicensed and counterfeit programs has been simplified – it’s easy to find and, without leaving home, download the key generator or activator to almost any paid program, and often, the programs themselves have pre-compromised security. Secondly, there are completely new types of threats associated with the use of pirated software in a networked environment. Of the four types of risks – legal, financial, technical, and reputational – associated with the use of unlicensed software for PC users constantly connected to the global network, financial and technical ones have increased especially (Kshetri n.p.).

Collective Responsibility for Secure Digital Systems

The danger of using pirated and counterfeit software is the loss of money and time to solve problems, as well as the risk of loss of computer security, including passwords and confidential information, such as cookies containing information about visited sites and user preferences. Infection with viruses often occurs even at the stage of finding hacked programs, and the loss of time occurs when security systems are compromised. Often, pirated versions are deprived of Internet functionality; they cannot be automatically updated; that is, they have a reduced level of protection, not to mention malicious code purposely built by pirates.

A joint study conducted by Microsoft and Group-IB last year showed that when pirated software is

downloaded from the Internet, a user with a probability of 92% risks the security of the computer and personal data, including the details of access to the Internet banking systems. Another joint analysis conducted in 2011 on unlicensed copies of Windows 7, Vista, and XP revealed that 6% of downloaded pirate distributions contain viruses and Trojans, and most such software can be used to steal passwords and personal data. In this case, the antivirus is not always able to detect malicious software before installing the system (Griffin 136–53).

To ensure the security of users, active joint actions are required from the state, its legislative institutions, law enforcement agencies, large IT companies, and specialized associations that protect intellectual property rights and consumers' rights to purchase a quality product. Therefore, Microsoft decided to consolidate the efforts of all stakeholders and opened the International Center for Combating Cybercrime in November last year. Its creation will not only protect people around the world from serious criminal groups using the Internet for the implementation of economic crimes but will also promote the development of a civilized software market based on fair competition.

Works Cited

Griffin, Ronald C. Cybercrime. *Journal of International Commercial Law and Technology*, vol. 7, no. 2, 2012, pp. 136–53.

Kshetri, Nir. The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, 2010, doi:10.1007/978-3-642-11522-6.

Sukhai, Nataliya B. Hacking and Cybercrime. *Proceedings of the 1st Annual Conference on Information Security Curriculum Development – InfoSecCD '04*, 2004, p. 128, doi:10.1145/1059524.1059553.