

Cybercrime Costly for Companies

By Jen Woods

Whether or not corporate cybercrime is escalating is unclear, but one thing is certain: companies are experiencing increased financial and operational losses from electronic crimes, according to a recent survey.

CSO Magazine's third annual E-Crime Watch Survey was conducted in conjunction with Carnegie Mellon University's CERT Coordination Center, the United States Secret Service, and the Microsoft Corporation between July 2005 and June 2006. Survey questions focused on a wide range of security issues, including intellectual property theft, denial of service attacks, malicious code (such as worms and viruses), phishing, spam, website defacement, spyware, and theft of consumer records.

Three-quarters of the 434 security executives surveyed said they had at least one security incident in the last year. The respondents reported an average of about three security incidents per year.

The survey shows that companies are better equipped to prevent corporate computer security breaches, since the average number of computer security incidents per company declined compared to numbers for the two previous years. About 69% of respondents said they thought their companies were better prepared to prevent cybercrime this year than they were last year. At the same time, 56% said they were more concerned about security threats than they were a year ago.

The average number of security events reported per respondent decreased from 86 for 2005 to 34 for 2006. In addition, 20% of respondents reported decreases in security events, compared with 13% last year. However, a larger number, about 36%, of this year's respondents reported increases in their numbers of security breaches.

There is no question that financial losses associated with cybercrimes are on the rise. About 40% of respondents reported financial impacts from security problems, with the average loss being 740,000 dollars, compared with an average loss of 507,000 dollars last year.

In addition to financial burdens, companies experienced operational losses. In fact, most companies, about 63%, experienced operational losses, such as system downtime and lost productivity.

continued on back

Also, according to the survey, more security executives were able to quantify the financial impact of cybercrimes. Last year, more than 60% of respondents said they did not know what their total financial losses to e-crime were. This year, only 30% were unable to estimate their total losses.

E-crimes are committed both inside and outside of companies, and each year the percentages of crimes committed by each group fluctuate. This year, intruders from outside of companies committed about 58% of electronic crimes, almost twice as many as company employees, who committed about 27%.

However, insider attacks are increasingly becoming a threat. Of the companies that experienced security problems, the majority, 55%, reported at least one insider offense, compared with 39% last year.

Few companies, only 28%, worked with law enforcement or took the criminals to court. Most respondents said they were not able to take action because there was not enough evidence or the financial impacts of the crimes did not warrant prosecution.

The most common types of e-crime incidents, according to 72% of respondents, were automated attacks such as viruses, malicious code, and worms. Other common offenses included unauthorized access to or use of information systems or networks, implementation of spyware, and production of illegal spam emails.

Targeted attacks, while not the most common, are increasing. 36% of respondents reported theft of proprietary information such as customer records, 33% reported system sabotage, and 30% reported intellectual property theft.

Companies surveyed had an average of 3,800 employees. On average, companies spent about 414,000 dollars on IT security in the last year, and they spent almost as much on "physical security," including hardware, software, and video surveillance equipment.

The most effective security technologies and techniques reported were stateful firewalls, electronic access control systems, and password complexity.

On the Net

CSO Magazine

www.csoonline.com/index.html

Software Engineering Institute's CERT Program

www.cert.org

United States Secret Service

www.secretservice.gov