FBI survey finds cybercrime rising

January 24 2006

Nearly nine out of 10 public and private institutions suffered computer security incidents in 2005, but less than 10 percent of those report the incidents to law enforcement, according to a FBI survey.

The 2005 FBI Cyber Crime Survey, which used responses from 2000 organizations in four states, found that 20 percent of organizations reported enduring 20 or more cyber-security attacks in the last year.

Only 9 percent of those who suffered attacks alerted law enforcement, according to the survey, released last week. Many of those who didn't said they believed it wasn't illegal or that there was little law enforcement could do.

Of those who reported to law enforcement, 91 percent said they were satisfied with the response they got.

Ron Teixeira, executive director of the National Cyber Security Alliance, said that small businesses tend not to report cyber crimes to law enforcement for a variety of reasons.

"Small businesses may not know what to do," he said. "They may not know who to call that can help."

He also said that bad publicity is a reason businesses don't report cyber crimes.

"They don't want to be seen as a bad actor," he said. "They're afraid of what may happen."

Paul Kurtz, executive director of the Cyber Security Industry Alliance, agreed.

"An organization may not want to report because of what they fear it might do to their market share and their investors," he said.

Kurtz added that businesses may not report cyber crimes because they assume nothing can be done.

"There's a perception among victims that reporting a crime won't bring any returns," he said, "that there's no chance of prosecution and investigation."

Sixty-four percent of respondents said they incurred a financial loss from a computer security attack. Viruses and worms alone accounted for $12 million of the $32 million total lost funds.

From the survey results, the FBI estimates that cyber crime cost about $67 billion to U.S. companies over the year.

Kurtz noted that these estimated numbers tend to vacillate, in part because the estimators use different criteria.

"We don't have a common methodology for assessing the cost of cyber attacks," Kurtz said. "You can't manage what you can't measure."

According to the survey, viruses and spyware are still the most populous threats to security.

Virus problems were reported by 83 percent of organizations; spyware problems were reported by 79 percent. More than 20 percent said they'd experienced port scans or network or data sabotage.

Attacks came from 36 different countries, according to the survey. The United States produced 36 percent of them, with China accounting for 24 percent more.

However, masking software makes it often unclear where the attack is originating.

Teixeira said that new technologies are creating new potential security threats. Specifically, he cited insecure wireless networks and BlackBerry and PDA viruses as places that can lead to infected networks.

Teixeira said that businesses should work to educate employees on cyber-security.

"It's incredibly important to have a cyber-security policy," he said. "Any employee can become the weakest link in security."

Kurtz said that security should be a priority for all organizations from the start.

"The best defense is thinking about security in the beginning, and not having it be an afterthought," Kurtz said.

"It's not just about technology," he added. "You need to have policies in place as an organization."

Kurtz also said organizations should have a security officer, who is "part of the regular calculus of what a firm does."

Teixeira said consumer education programs will go a long way in making sure people and organizations are proactive and prepared in their security systems.

"The FBI report showed that the small business community doesn't have the resources and the education to put cyber security at the forefront of their priorities," he said.

Teixeira said his organization is trying to key a consumer education campaign, through their Web site, StaySafeOnline.info.

"Part of the problem is that until recently, there hasn't been a coordinated approach to consumer education," he said.

Kurtz, who also recommended StaySafeOnline.info as a tool to educate individuals and businesses, said Congress's role in cyber crime prevention is becoming problematic.

The Senate Committee on Foreign Relations passed along to Senate a motion signing on to the Council of Europe's Convention on Cyber Crime.

However, Kurtz said, two senators are anonymously blocking the chamber from voting on the resolution.

"We need to create the international infrastructure to prosecute cyber criminals," Kurtz said. "We have to create relationships, and have these laws on the books in multiple countries."

Kurtz called the Convention on Cyber Crime "a very solid step that doesn't require the passing of any new laws," and said it was "unexplainable" that two senators would want to block a vote on it.

Copyright 2006 by United Press International

Citation: FBI survey finds cybercrime rising (2006, January 24) retrieved 6 May 2024 from https://phys.org/news/2006-01-fbi-survey-cybercrime.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.