

Make 2003 more secure

Contributed by Linux
Tuesday, 08 August 2006

The challenges to info-tech security will surely be daunting, and companies' efforts to stay safe will have to keep increasing.

With holiday cookies and sweets still being shared around offices everywhere, security is the least of concerns these days as most businesses are thinking merry, not wary. So what better time to examine the year ahead for what to expect in terms of computer security? First, 2003 will surely pose some pretty daunting challenges to chief security officers and the organizations they protect. At the same time, improvements in software and technology will elevate computer security to another level. Here's a quick rundown of what to expect:

The challenges to info-tech security will surely be daunting, and companies' efforts to stay safe will have to keep increasing.

With holiday cookies and sweets still being shared around offices everywhere, security is the least of concerns these days as most businesses are thinking merry, not wary. So what better time to examine the year ahead for what to expect in terms of computer security? First, 2003 will surely pose some pretty daunting challenges to chief security officers and the organizations they protect. At the same time, improvements in software and technology will elevate computer security to another level. Here's a quick rundown of what to expect:

Spam becomes an even bigger headache

According to e-mail security-service provider Message Labs, spam's growth rate will continue to be faster than that of legitimate e-mail--and in terms of sheer volume, spam will eclipse the legit stuff. That will make the spam torrent more burdensome and harder to control. Companies that haven't invested in antispy software will need to do so, pronto, or have their employees waste more and more time simply hitting the delete key.

Part of the bargain will be businesses accepting the fact that some messages will get tossed out with the trash, as antispy programs are hardly perfect. Still, it's better than being up to your eyeballs in smutty missives and come-ons for investment scams from randomly generated e-mail addresses.

Instant messaging succumbs to spam, too

Once a relative haven, instant messaging has recently become a target for spammers seeking new outlets. According to e-mail consultancy Ferris Research, IM spammers works off lists of addresses freely traded on the Internet. They usually send a message to someone on live IM asking them to visit a Web site that sells smut, bogus software, or often legitimate products being marketed in unfortunate ways.

Since no IM spam-screening software is yet available, an IM user on the wrong list could spend a good chunk of time refusing invitations from IM spammers. That coverage hole will force many corporations to consider moving their IM users onto private messaging systems not accessible to the public Internet.

Hardware, hardware, hardware

Security isn't shrink-wrapped anymore. Eighty percent of the licenses for expensive, high-grade firewall programs come on specially configured pieces of hardware designed to run this software. That's way up from a few years ago. And its only the start.

From VPN servers to IDSs to newer pieces of software designed to spot behavioral aberrations that point to a security breach, more and more products are moving from a piece of self-contained software that an IT consultant or your own systems administrator installs to a specialized piece of equipment built with security in mind. The upside? These systems are generally easier and cheaper to install and launch in a network. The downside? Less flexibility for companies with special software needs.

Safe computing outside the corporate perimeter. Employees logging into corporate networks from home PCs over public broadband connections are now commonplace. As a result, security software and hardware that once did a fine job of guarding sensitive systems looks increasingly vulnerable. That's because all these remote networks, be they employees or partners, are no longer snugly inside the "official" data-security perimeter.

Also, persistent worm-virus outbreaks, such as Nimda, explain why more and more corporations are going through the considerable hassle of putting security software--firewall, intrusion detection systems, antivirus software--on every desktop machine. Companies with end-to-end protection remain in the minority, but they won't be for long as it becomes easier to link up fleets of desktops with central control consoles that not only talk to the big, heavy-duty security appliances but also to the thousands of small programs guarding the road warriors' machines.

Identity theft goes berserk online. Call in the copycats. When well-organized ID thieves convinced a clerk at a Long Island (N.Y.) software company to give them access to tens of thousands of credit reports using his company's password, they illustrated how the Net makes the part of ID theft that was hard until now--accumulating the information--much easier. With widely available credit reports such an integral part of American business, it's hard to imagine how the credit agencies can quickly and simply limit access to the reports without impeding the flow of commerce.

With easy access to credit reports available to thousands of people throughout the U.S., expect blockbuster ID thefts in 2003 and beyond. Whereas credit-card numbers were traded freely on the Internet in the past, now the bad guys will trade entire personal dossiers. And fixing the problem will be much harder because it's pretty easy to screen out someone who has picked up one of your credit-card numbers but much harder when it comes to a rogue who has that, your bank-account number, your social security number, and the last five addresses you have called home.

Of course, this little list is just the beginning. I haven't even touched on still-early trends such as merging physical and online security: Companies are starting to look at guarding these assets in coordination because often computer-security breaches start with physical breaches.

Likewise, more and more businesses are installing software that tracks theft of sensitive, high-end intellectual property. Once ham-fisted, the second generation of these systems works much better, according to Gartner security analyst John Pescatore.

All told, computer security remains one of the more dynamic areas of the moribund IT sector. And it'll get only more interesting in the coming year.