very few know to whom they should report a computer security incident. Being prepared and knowing what to do in advance can help to further mitigate the damage. That is why it is very important that an organization advertise its CSIRT both internally and externally. As with emergency services, it is important to find out how to contact a CSIRT before it is needed in an emergency. It is also important to know in advance whom the service can help and what information is needed to ensure that the CSIRT can provide the service requested.

To find out if your organization has a company-supported CSIRT, ask your security officer or system/network administrator, and consult your organization's security policies and practices. Some CSIRTs are members of the Forum of Incident Response and Security Teams (FIRST). See www.first.org/ team-info for a list of FIRST members and their contact information

With millions of organizations now reliant on networks to conduct their businesses, it is a shocking fact that only a few hundred CSIRTs exist around the world today. Many of these CSIRTs continue to cite annual increases of 200 percent or 300 percent in the numbers of computer security incidents reported to them. They are struggling to keep pace with the number of incoming reports. Even with general improvements in the field of network security, a dramatic increase in the number of CSIRTs is urgently needed. More advocates are needed to help organizations understand the risks associated with the failure to detect and appropriately respond to computer security incidents.◆

About the Author

Moira J. West-Brown is a senior member of the technical staff within the CERT® Coordination Center at the Software Engineering Institute. She leads a group that aids in forming new CSIRTs world wide. Active in CSIRT internationally, she has developed a variety of materials on operational and collaborative CSIRT issues. She was elected to the Forum of Incident Response and Security Teams Steering Committee in 1995 and is currently chair. She holds a bachelor's degree in computational science from the University of Hull, United Kingdom.

Open Forum

Security Often Sacrificed for Convenience

By Shawn Hernan
Vulnerability Handling Group, CERT® Coordination Center

When given a choice between a product that is secure and one that is not, nearly everyone will say they would prefer the secure product, all else being equal. But things are not equal. Despite clients' cries for more secure products from vendors, when it comes to writing the check security often gets the short end of the stick.

The Message Clients Send

One e-mail product vendor has been among the market leaders in implementing security features into its products. This vendor, who ships both e-mail servers and e-mail clients, was among the first to add a particular kind of secure authentication to client and server. As the vendor was among the first to do so, there were concerns about interoperability. Would its e-mail client be able to work with other vendors' e-mail servers, and vice-versa? Would the secure authentication scheme prevent interoperation with other vendors' products?

Complicating matters was the fact that the e-mail protocol did not provide for explicit failure messages when an authentication attempt failed. That is, the client was unable to tell if the authentication attempt failed because the password was incorrect, or because the server did not support the same authentication scheme. Here were possible options if the client received a failure message:

- Ask the user for the password again, assuming it was incorrect the first time.
- Try a less secure but more widely implemented authentication scheme, namely plain text passwords.

In other words, the vendor was faced with a tradeoff between interoperability and security by default. The vendor chose security by default and started to ship the client. The default behavior was to stick with the secure authentication scheme, but give the end user a way to configure it so the client could use a less secure authentication scheme.

The effect of this security-conscious choice was that the client would work only with a server from the same vendor, until other vendors implemented the same authentication scheme. The vendor provided documentation with the product to allow an end user to configure the product to work with other vendors' servers. So the issues of security and interoperability were addressed, but security was primary.

Although the end user could configure the product to work with other vendor's servers, the vendor received more than 280 trouble reports from sites that thought the client was broken or that simply did not want to reconfigure the client. The customers wanted interoperability by default.

This market pressure forced the vendor to choose a different set of defaults—the product will now try less secure authentication schemes if the more secure scheme fails. Thus, if a user makes an error in typing a password, the client will try the same incorrect password using all of the authentication schemes including plain text.

This means that if the user makes a typo in entering a password, the slightly incorrect password is sent on the network in plain text. More importantly, if an intruder is able to convince a user to establish a connection to a mail server of the intruder's choice, the intruder can recover the user's password. The consequence of the customers' demands for default interoperability was that they obtained a less secure product.

Having changed the default configuration of the product, we would expect that the vendor would have received trouble reports from other customers complaining about the less secure configuration. But they received only one such report. The message sent to this vendor was loud and clear—default interoperability is more important than default security.

Standardization

Many organizations are under pressure to standardize on one set of applications, operating systems, servers, firewalls, and routers. Standardization can reduce your costs, but also reduces your resistance to catastrophic outages during widespread security events like the Melissa macro virus or the Love Letter visual basic script.

Biological analogies are useful here. Genetic diversity increases the ability of the population to survive in the face of a virulent parasite or disease. Likewise with technology, if your entire organization is comprised of a single platform then your risk of catastrophic loss is higher.

Despite the risks, many organizations are standardizing on small sets of platforms and applications in an effort to save money (sometimes without actually evaluating the total costs of ownership) without accounting for the risks of catastrophic failure.

Again, the message to vendors and system integrators is clear: *sameness* is more important than security.

The User Experience and Mobile Code

Many Web sites use ActiveX, JavaScript, Java, or dynamic HTML to enhance their pages often strictly for aesthetic reasons. But this use of mobile code has sometimes become part of the functionality of the site. Many electronic commerce sites, for example, require the use of JavaScript or ActiveX to complete the transaction. This has led to a serious quandary: Whenever a problem is discovered in any of the mobile code technologies, it is not practical to disable that technology.

Many Web sites, for example, are still vulnerable to the "Cross-site Scripting" attack described in CERT Advisory CA-2000-02, yet have not removed the offending code from their Web sites. Thus, users of that site may be vulnerable if they have decided to trust it. The nature of the vulnerability is that malicious code can be injected from a trusted site into your browser.

Sites are competing on functionality and appearance, and that's how they're being evaluated. In my experience, clients are unwilling to forgo mobile code technology, despite the risks it presents, even when alternatives are available. Again, the message is loud and clear—security is less important than functionality or even appearance.

Conclusion

Security is not only for security products like firewalls and encryption software. The great majority of the problems we see are a result of flaws in ordinary programs. Things like mail servers, spreadsheets, word processors, help programs, Web servers, and all the things we use everyday are the same things that intruders use to gain unauthorized access to your systems.

Security products certainly help, but they are not a substitute for secure programs and protocols. Unless you behave like security really matters—and it does—then you will not get it. And you will not be secure.◆

About the Author

Shawn Hernan is a member of the technical staff at the CERT® Coordination Center where he leads the Vulnerability Handling Group. Prior to joining CERT®/CC, Shawn worked for the Systems and Networks division of the University of Pittsburgh for seven years where he developed databases and network applications, and shared in the system administration of the centralized computing facilities and the large campus network.

Network Security Web Sites

www.disa.mil/line/disalin5.html
This is the site by the Defense Information Systems Agency for Center for Information System Security.

www.vtcif.telstra.com.au/info/security.html
The Computer and Network Security Reference Index's links include frequently asked questions on topics such as Internet firewalls, computer security, and Web security; online document archive relating to network and computer security; and newsgroups.

www.alw.nih.gov/Security
This page features general information about computer security. Its links include advisories of groups around the world on security vulnerabilities and methods to remove or reduce those dangers; articles on computer and network security; and electronic magazines, newsletters, and news sites devoted to this topic.

http://computingcentral.msn.com/topics/safecomputing
This site includes a Safe Computing Forum and talks about how to use firewalls as a protection from computer viruses and hackers.

www.andrew.cmu.edu/~zu22/html/security/security.html
This is a 21-page listing of network security resources.

www.fish.com/satan
See this site for information about the Security Administrator's Tool for Analyzing Networks.

http://netsecurity.about.com/compute/netsecurityi/msub25.htm?rnk=r1&terms=kevin+mitnick
Devoted to articles on computer hacker Kevin Mitnick, including a long article he wrote from the federal detention center.

www.alw.nih.gov/Security/security-docs.html
This site contains miscellaneous documents about various computer security issues that are loosely organized by subject area.

www.gocsi.com
Computer Security Institute's site, with links to articles on topics such as "10 Risks of PKI: Bruce Schneir Debunks the Hype."

www.p-and-e.com/pubs_nstissc.htm
Various security publications listed by the National Security Telecommunications and Information Systems Security Committee.

www.mountainwave.com
This is the site for *Computer Security News Daily*. The lengthy article links include government and business news, the Internet, hackers, products, and the law.

www.dtic.mil/dodsi/bulletin.html
Access this site for publications by the *Security Awareness Bulletin*, a publicationof the Department of Defense Security Institute. The most recent editions, however, are September and December 1997.