As more companies open their networks to partners, customers, and suppliers, they simultaneously render themselves vulnerable to increased cyber security risks, including viruses, denial-of-service attacks, and web site spoofs. Although this vulnerability may raise a few eyebrows, it isn't necessarily alarming.

However, downtime related to security breaches is on the rise, and downtime is alarming. After all, an increase in breach-inflicted downtime arguably suggests a parallel increase in either the frequency or severity of threats to your company's e-business systems.

Two years ago, half of the respondents to the Global Security Survey survived the year without experiencing downtime related to security breaches. In contrast, only 26 percent of the 4,900 executives, security professionals, and technology managers who responded to last year's survey managed to avoid breach-inflicted downtime. (The Global Security Survey is conducted annually by InformationWeek Research and PricewaterhouseCoopers. You can find results from the year 2000 survey in “It's Time To Clamp Down,” July 10, 2000, at www.informationweek.com/794/security.htm.)

As a network administrator, you don't need to be told that downtime, whatever its cause, results in both productivity and financial losses. (See “Did You Know?” on p. 28.) Productivity and financial losses, however, represent only some of the potential costs of attacks on your e-business. Bored teenagers, disgruntled workers, political hacktivists, and anyone else with a passive or malicious interest in targeting your company can cost it not only money but also time, secrets, pride, and customers' respect. (For evidence of how hack attacks can affect your company, see “Hack Attacks” on p. 33.)

The question to which these reported security breaches give rise is this: Why can't organizations adequately protect their e-business systems?

SECURING E-BUSINESS IS DIFFICULT

The simple answer to this question sounds like an excuse, but nevertheless it is true: Securing an e-business is difficult—really difficult—and it is difficult for several reasons. For one thing, a successful approach to e-security requires input not only from IT and security managers but also from business managers. Sometimes getting these people to agree can be difficult.

For another thing, adequately securing your company's e-business is inherently difficult because no one product from any single vendor can protect your e-business from every angle. Consequently, you're faced with several difficult questions:

- What categories of products comprise a complete security solution?
- Of these categories, which products should you choose?
- How can you know whether or not the security products you choose will work well together?
- How can you easily manage these varied products?

To spare you the trouble of finding answers to these questions, Novell investigated these questions and, based on the answers, developed the Net Security solution. The Net Security solution is Novell's strategy to help you find and deploy security products that meet your company's specific security needs. To this end, the Net Security solution does the following:

- Identifies the nine elements of a complete security solution
- Defines the purpose each element serves
- Lists one or more Novell or Novell-partner products that not only serve the purpose of each element but also work well with the other products included in the Net Security solution
- Lists only products that are integrated with NDS eDirectory, the foundation of the Net Security solution

The Net Security solution thus helps you define your company's security needs and locate the solution or solutions that meet those needs. In other words, through its Net Security solution, Novell simplifies the task of securing your company's e-business system.

NINE PIECES TO THE SECURITY PUZZLE

Novell used information from industry analysts and security experts, including IDC, Gartner, PricewaterhouseCoopers, and Giga Information Group, to determine that a complete security solution is comprised of nine elements, each of which serves a specific purpose. (See Figure 1 on p. 26.)
The Net Security solution includes one or more Novell or Novell-partner products within each of nine product categories that represent the elements of a complete security solution.

- **Firewall.** This element secures customer, partner, and employee Internet access.

- **Authentication and Authorization.** Working together, these elements confirm user identity and grant access accordingly.

- **Single Sign-on.** This element increases security on your company's network by enabling fast and secure access to multiple applications with a single password.

- **Virtual Private Network.** This element enables remote users and branch offices to securely connect to your company's network.

- **Intruder Detection.** This element prevents unauthorized access to your company's network.

- **Certificate Management.** This element automates security management functions.

- **Secure Business Communications.** This element enables effective collaboration across one or more N et products that define a networking environment that blurs the boundaries between the Internet, intranets, and extranets, as well as corporate, public, and wired-to-wireless networks.

- **Intruder Detection.** This element prevents unauthorized access to your company's network.

- **Net Control.** This element automates security management functions.

**Figure 1.** The N et Security solution includes one or more N ovell or N ovell-partner products within each of nine product categories that represent the elements of a complete security solution.

**KEEP IT TOGETHER**

For each of the nine elements, the N et Security solution positions one or two N ovell or N ovell-partner products that solve the specific security problems of that element. The remainder of this article discusses these problems and solutions.

A s you might imagine, however, none of the products that comprise the N et Security solution can, on its own, address the fundamental problem with the difficulty of securing an e-business. Securing an e-business can be overwhelmingly complex, and complexity can yield ironic results. For example, a highly complex security solution can heighten the margin for human error, which in turn can increase the likelihood of security holes. In other words, increased complexity can result in reduced security.

**N DS eDirectory 8.5**

The N et Security solution combats this potential complexity problem at its foundation with N DS eDirectory. N DS eDirectory—in conjunction with N DS-enabled N et Security products—simplifies the task of securing your company's e-business systems by providing a central repository for security information (such as users' identity information and access rights).

As you probably already know, N DS eDirectory is well-suited for e-business. N DS eDirectory supports Lightweight Directory Access Protocol version 3 (LDAP v3), the Internet standard for accessing directory information. Equally important in an e-business context, N DS eDirectory is cross-platform, running on all the leading platforms including Solaris, Windows 2000, Windows NT, Linux, TRU 64 U N I X, and, of course, N et-W are 5.

In addition, N DS eDirectory is fault tolerant and highly reliable, which means it provides nonstop service for your e-business applications (and in turn reduces downtime). Finally, N DS eDirectory is highly scalable, so you can easily handle the dramatic increase in the number of users and applications that e-business necessarily brings.

N DS eDirectory further simplifies the complexity of securing your company's e-business systems by offering a single point of management for all N et Security products (as well as all other LDAP v3-enabled security products). A s a N ovell likes to say, N DS eDirectory is the glue that holds together the varied pieces of the N et Security solution. (For more information about N DS eDirectory, visit www.novell.com/products/nds or read "N DS eDirectory: What's in a Name?" N ovell Connection, July 2000, pp. 6–18. You can download this article from www. ncmag.com/past.)

**OPEN SECURITY**

A bout seven years ago, companies began tentatively connecting to the Internet. These companies approached the task with extreme caution and erected what amounted to impenetrable walls to keep the bad guys (which basically meant anyone on the Internet) out of the company's infrastructure.

Recently, this traditional view of the purpose of firewalls has changed. In the context of e-business, firewalls must exact what you may call open security. Today's firewalls must be as good at letting people in as they are at keeping people out. Firewalls must enable customers, partners, suppliers, and employees who are temporarily or permanently beyond the borders of the LAN and WAN to access selected portions of the network with ease. Simultaneously, firewalls need to ensure that no one except these authorized users can access the corporate network—period.

**N ovell BorderManager Firewall Services 3.6**

N ovell confronts the challenge of providing open security with N ovell BorderManager Firewall Services, the security...
Did You Know?

Cyber crime is costly, and at least one survey has the statistics to prove it:

Of the 643 companies included in the 2000 Computer Crime and Security Survey, 42 percent were willing to divulge the financial losses they suffered as a result of cyber attacks. The reported total of losses came to U.S. $265,589,940—that's more than double the combined annual total from the '97, '98, and '99 surveys. (For more information about this survey, conducted by the Computer Security Institute in conjunction with the U.S. Federal Bureau of Investigation, see www.gocsi.com/prelea_000321.htm.)

Minimize Risky e-Business

Arguably the most basic problem with security in a digital world has to do with verifying that someone is who he or she claims to be. A common approach to authentication— that is, verifying a claimed digital identity—is to request a password. However, passwords pose at least one problem: People with malicious intent and time to spare can crack a password— no matter how long and seemingly random that password is. Consequently, vendors have come up with password alternatives such as token- and biometric-based authentication methods.

Novell Modular Authentication Service Packages

Novell Modular Authentication Service packages enable you to deploy and manage several authentication methods— including password, token, smart card, and biometric methods. Depending on the Novell Modular Authentication Service package you choose, you can use one of these methods alone, or you can combine them to create various login sequences.

For example, the Novell Modular Authentication Service Starter Pack (which is available as a free download for NetWare servers) enables you to include one Novell-developed authentication method in each login sequence you create. (For more information about Novell-developed authentication methods, see "What's New?" on p. 36.)

Novell Modular Authentication Service Enterprise Edition 2.0 includes biometric methods (in the form of software modules) developed by both Novell and third-party partners. For more information, see "What's New?" on p. 36 or visit www.novell.com/products/NMAS.

PASSWORD PROBLEMS? FORGET ABOUT 'EM!


- Change passwords frequently.
- Use different passwords for different systems.
- Don't create easy passwords or passwords that are real words.
- Don't post passwords in easy-to-find locations.

You know he's right, of course. However, Mitnick's advice is much easier to say than it is to enforce. As a network administrator, you have to hold the line on the use of passwords. The good news is that you can enforce standards and rules to prevent people from using passwords that are easy to guess or crack.

FEATURE: Minimize Risky e-Business

Foundation of BorderManager Enterprise Edition 3.6. (For a list of the enhancements in this recently released version of BorderManager, see "What's New?" on p. 36.) Certified by the International Computer Security Association, BorderManager Firewall Services enables you to protect your company's confidential data using the following components:

- Packet-Filtering Firewall. The packet-filtering firewall enables you to filter TCP/IP packets, thus controlling access to Internet hosts based on the source and destination host's name or IP address.
- Circuit-Level Gateways. The circuit-level gateways enable you to grant users access to the Internet and to TCP/IP intranet servers without enabling TCP/IP on users' workstations.
- Application-Level Gateways. The application-level gateways enable you to control which ports and addresses users can access. You can also control which files users can access on these ports and addresses.

For more information about BorderManager Firewall Services, visit www.novell.com/products/bordermanager/firewall.

Cyber crime is costly, and at least one survey has the statistics to prove it:

Of the 643 companies included in the 2000 Computer Crime and Security Survey, 42 percent were willing to divulge the financial losses they suffered as a result of cyber attacks. The reported total of losses came to U.S. $265,589,940—that's more than double the combined annual total from the '97, '98, and '99 surveys. (For more information about this survey, conducted by the Computer Security Institute in conjunction with the U.S. Federal Bureau of Investigation, see www.gocsi.com/prelea_000321.htm.)

DID YOU KNOW?

Cyber crime is costly, and at least one survey has the statistics to prove it:

Of the 643 companies included in the 2000 Computer Crime and Security Survey, 42 percent were willing to divulge the financial losses they suffered as a result of cyber attacks. The reported total of losses came to U.S. $265,589,940—that's more than double the combined annual total from the '97, '98, and '99 surveys. (For more information about this survey, conducted by the Computer Security Institute in conjunction with the U.S. Federal Bureau of Investigation, see www.gocsi.com/prelea_000321.htm.)

Graded authentication enables you to control access to your company's network and directory resources based on assigned clearance levels, resources grades, and login sequences. (See Figure 2 on p. 30.) Basically, Novell Modular Authentication Service grants access to graded resources only when both the clearance level and login sequence match the resource's grade.

For example, you may assign a particular NetWare volume a Biometric & Password & Token grade. Novell Modular Authentication Service thereafter grants access to this volume only when both of the following are true:

- The user has a Biometric & Password & Token clearance level.
- The user uses the required login sequence, which (as you can guess) includes a biometric, password, and token authentication method.

Novell Modular Authentication Service Enterprise Edition 2.0 includes authentication methods (in the form of software modules) developed by both Novell and third-party partners. For more information, see "What's New?" on p. 36 or visit www.novell.com/products/NMAS.
administrator, you know only too well the difficulty of explaining password basics to hundreds or thousands of users. And if explaining basic password policies is difficult, enforcing them is nearly impossible.

Consequently, having different passwords for different systems is only theoretically more secure than having a single password for multiple systems. After all, if users avoid the pains of creating and remembering passwords by inventing simple ones or writing down good ones, your security system is seriously flawed.

**Novell Single Sign-on 2.0**

With Novell Single Sign-on 2.0, you get the best of both worlds: Users are free from the nearly impossible task of remembering a growing number of passwords, and you can confidently require the use of different passwords for different systems. Novell Single Sign-on enables users to access web sites, Windows applications, client-server applications, custom in-house applications, and IBM mainframes using only their NDS username and password.

To work this magic, Novell Single Sign-on uses Novell International Cryptographic Infrastructure (which is included with Novell Single Sign-on) to encrypt users’ secrets. These secrets—which are typically passwords, but can also be X.509 certificates, tokens, or even biometric information—are stored in SecretStore. (SecretStore is Novell-patented technology that stores encrypted usernames and passwords as a hidden attribute of the NDS User object.) After users authenticate to the network, their workstation automatically accesses SecretStore, which provides the credentials needed to authenticate to other systems.

For more information about Novell Single Sign-on 2.0, see www.novell.com/products/sso or read “Novell Single Sign-on 2.0: Forget Multiple Passwords,” Novell Connection, Oct. 2000, pp. 40–44. (You can download this article from www.ncmag.com/past.)

**A LITTLE PRIVACY, PLEASE**

You need an inexpensive way to connect remote users and branch offices to each other and to your company’s network so they can access internal files and applications. Of course, the Internet is an easy way to provide this access, but the Internet is notoriously (and inherently) insecure.

Virtual Private Network (VPN) solutions address this problem. A VPN is an encrypted tunnel for private communications over a public IP network, typically the Internet. VPN devices at both ends of a desired connection establish this tunnel before each communication session and encrypt the data packets they exchange.

VPNs are secure alternatives to the modem banks you may maintain for remote users or to the private leased lines you may lease for branch-office connectivity. In fact, VPNs are arguably more secure than costly WAN lines and telephone lines. After all, data sent over telephone and private lines is unencrypted. Consequently, if someone taps into these lines (which is possible, contrary to popular belief), the data are there for the taking. In contrast, if someone taps into an encrypted VPN tunnel, the data within are encrypted and, therefore, undecipherable.

Visit our advertiser,
CyberStateU at
www.CyberStateU.com
An even greater benefit of VPNs is that they save companies money—a lot of money. Specific amounts are difficult to quantify, but most estimates range from 60 percent to 80 percent savings. (For more information about saving money with VPNs, see “Virtual Private Networks: Making a Public Network Private,” Novell Connection, Feb. 1998, pp. 6–21. You can download this article from www.ncmag.com/past.)

**BorderManager VPN Services 3.6**

As a component of the BorderManager Enterprise Edition 3.6, BorderManager VPN Services is a firewall-based VPN solution. Using BorderManager VPN Services, you can provide remote offices, mobile users, partners, and suppliers secure access to your company’s confidential data over the Internet or other public backbones. Between the centralized management and the single sign-on services it provides, BorderManager VPN Services significantly reduces administrative costs. In this way, BorderManager VPN Services delivers the 80 percent savings that represent the high-end of the VPN potential-savings spectrum.

For more information about BorderManager VPN Services, visit www.novell.com/products/bordermanager/vpns. You can also find more information about VPNs in general and about an earlier version of BorderManager VPN Services in “Virtual Private Networks: Making a Public Network Private,” Novell Connection.

**AUTHORIZATION**

Figure 2. Novell Modular Authentication Services Enterprise Edition 2.0 supports graded authentication, which enables you to control access to network and directory resources based on assigned clearance levels, resource grades, and login sequences.

**ANTIVIRUS SOFTWARE: WHEN YOU HATE TO HEAR ILOVEYOU**

Of the 643 companies included in the 2000 Computer Crime and Security Survey, 85 percent detected viruses within a 12-month period. The Computer Crime and Security Survey is conducted annually by the Computer Security Institute and the U.S. Federal Bureau of Investigation. (For more information about the survey, see www.goci.com/prelea_000321.htm.)

Computer viruses can disrupt the flow of e-business activity, and when they do, they’re more than just irritating—they’re costly. According to McAfee, a provider of antivirus solutions, virus infections cost companies more than U.S. $12.1 billion in 1999. This amount is more than double the combined total of previous years. The total for 2000 probably goes far beyond the 1999 total, given the fact that the ILOVEYOU bug alone cost companies an estimated U.S. $6.7 billion within only the first five days of its spread. (See Example 1 in “Hack Attacks” on p. 33.)

**NetShield for NetWare**

NetShield for NetWare, from Network Associates, is designed to protect your company’s NetWare servers (and the four million other NetWare servers running worldwide). NetShield for NetWare automatically cleans, quarantines, or deletes the infected file, depending on how you have configured NetShield for NetWare.

For more information about NetShield for NetWare, visit www.mcafeeb2b.com/products/netshieldnw/default.asp.

**CERTS CONTROL**

Information exchanges over the Internet are inherently insecure—that’s the sad truth of the matter. Consequently, companies that want to exchange information with customers and other companies over the Internet need a way to ensure that these exchanges are secure, trustworthy, and legally binding. A Public-Key Infrastructure (PKI) meets these needs.

PKI refers to the technology, cryptographic framework, and services required to generate, store, and manage public-private key pairs. A PKI provides a way to associate these public-private key pairs with the entities (such as servers or users) for which these key pairs were generated. The resulting collection of information is called a digital certificate.

A PKI manages the generation, signing, and revocation of such certificates and also performs transparent key and certificate management for end users. All of these services are necessary for establishing the trust companies need to exchange information over the Internet.

**Entrust/PKI 5.0**

Entrust/PKI 5.0 is a cost-effective and easy-to-use product that enables you to easily create and manage industry-standard certificates. These certificates in turn enable you to use digital signatures and encryption (among other things) to establish and maintain secure information exchanges with employees, customers, partners, suppliers, and any other entity with which your company does business.

For more information about Entrust/PKI 5.0, visit www.entrust.com/entrust/index.htm.

**E-WORDS—KEEP ‘EM CLEAN!**

Before the term e-business was coined, you were probably already engaged in at least one activity now included under the
e-business header: exchanging e-mail. In an e-business context, e-mail messages are equally as or even more vital to business communications than phone calls.

Unfortunately, e-mail messages can be intercepted and, if not properly secured, they can be read or even changed before reaching their intended recipient. When the recipient receives a message, there is no way that he or she can know that the message is really from the claimed sender and that the message is intact.

**Novell GroupWise 5.5 Enhancement Pack**

Among several other collaborative tools, GroupWise 5.5 Enhancement Pack includes an easy-to-use messaging system that protects your company’s network from the types of security breaches that some e-mail systems invite. The GroupWise messaging system secures business communications—from desktop to destination—by supporting industry-standard PKI certificates, such as those generated by Entrust/ PKI 5.0. By using these certificates, users can encrypt and sign their messages, thus ensuring the integrity of these messages.

Of course, GroupWise is far more than just a messaging system. For in-depth information about the latest GroupWise version, see “GroupWise 6: A Reliable and Secure Mail Carrier” on p. 6.

**WHO’S THERE? DETECTING INTRUDERS**

Nearly 20 percent of the respondents to the 2000 Computer Crime and Security Survey detected unauthorized access to or misuse of their web site connections. Of these respondents, 64 percent had their company’s web site defaced, and 60 percent suffered denial-of-service attacks. (See www.gocsi.com/prelea_000321.htm.)

When intruders attack your company’s web site, the result can be a harmless and embarrassing nuisance or a costly blow to the flow of your e-business activities, as evidenced by several of last year’s widely publicized attacks. (See “Hack Attacks.”)

BINDVIEW BV-CONTROL FOR NETWARE AND NDS

BindView bv-Control for NetWare and NDS is a complete security and systems management solution that, among many other capabilities, enables you to configure and report on intrusion-detection issues. From a Windows 2000 workstation, bv-Control allows you to assess your network’s relative level of security.

Using this comprehensive security assessment, you can find and fix security risks and easily apply security policies designed to curtail future risks. In fact, bv-Control enables you to enforce security policies throughout your enterprise with just a few clicks of your mouse.

For more information about BindView bv-Control for NetWare and NDS, visit www.bindview.com.

**CONTROLLING NET ACCESS**

Partners, customers, and suppliers who access your company’s web servers don’t directly log in to your company’s network, which raises this question: How do you determine that these external users truly are who they claim to be, and beyond that, how do you determine what resources they have rights to see and use? Controlling access to web servers is tricky business, particularly because web servers frequently have weak access control functions and may not be directory enabled.

**Novell iChain 1.5**

Novell iChain 1.5 addresses this problem by front-ending any web server and enabling you to take a policy-based approach to managing the authentication and authorization of web site users. (See Figure 3.) As an extranet access control solution, Novell iChain is a security and management platform for authenticating and authorizing users who are trying to access protected information on your company’s web site.

Novell iChain 1.5 runs on appliances based on Novell’s award-winning Internet Caching System (ICS) software. You purchase a Novell ICS appliance (running ICS 1.3) from the ICS appliance vendor of your choice. Using Novell iChain and NDS, do an over-the-wire upgrade to enhance the ICS software and add the Novell iChain functionality.

The result is the Novell iChain Internet Caching System server. The Novell iChain Internet Caching System server is logically positioned between your company’s web servers and the Internet and runs only in reverse proxy mode, both protecting and accelerating your company’s web servers. (See Figure 3.) The Novell iChain Internet Caching System server provides single sign-on to secure access to all of the applications you want to make available to users through your company’s web site.

The Novell iChain Internet Caching System server also protects data integrity by employing Secure Sockets Layer (SSL) sessions between browsers and the proxy and using HTTPS between the proxy and the web servers.

The Novell iChain Internet Caching System server interfaces with several other Novell iChain components, including the Novell iChain Authentication service and the Novell iChain Authorization service. The Novell iChain Authentication service enables users to authenticate to and authorize users who are trying to access protected information on your company’s web site.

To control access after authentication, the Novell iChain Authorization service
Hack Attacks

EXAMPLE 1
Within days of its release in early May, the infamous ILOVEYOU virus had spread to tens of millions of computers. The virus clogged e-mail systems everywhere by replicating and redelivering itself each time an unsuspecting user opened the enticing but sadly infected message. Estimated cost to businesses: U.S. $6.7 billion dollars in the first five days alone. (See www.informationweek.com/794/security.htm.)

EXAMPLE 2
During the first quarter of 2000, a flood of denial-of-service attacks downed seven of the Internet’s busiest sites, namely Yahoo!, Buy.com, ZDNet, eBay, CNN.com, Amazon.com, and E-Trade. Some of the web sites were completely inaccessible for three hours. Yahoo! took the first hit—and it was hit hard. The attack rendered the Yahoo! portal essentially inaccessible for three hours, with availability during these hours ranging from 0 to only 10 percent. (See “Cyberterrorists Crash Web Party,” InternetWeek, Feb. 10, 2000, at www.internetwk.com/story/NW20000210S0001. See also www.gocsi.com/prelea_000321.htm, where you’ll find excerpts from the 2000 Computer Crime and Security Survey, which is conducted jointly by the Computer Security Institute and the U.S. Federal Bureau of Investigation (FBI). Some of this information is from the complete report, which is available free of charge upon request.)

EXAMPLE 3
On February 14, 2000, in the same week that denial-of-service attacks downed seven of the Internet’s busiest sites, a lesser known, less costly, but arguably more embarrassing spur-of-the-moment security prank occurred: During an online presidential interview on CNN, a computer security consultant assumed then-President Clinton’s chat-room name and put a few words into the president’s mouth. To the approximately 400 users who had logged on to chat with the president on Valentine’s Day 2000, Clinton appeared to say, “Personally, I would like to see more porn on the Internet.” (See “Online Clinton Imposter Called for More E-Porn,” Feb. 16, 2000, at www.newsbytes.com/news/00/143951.html.)

EXAMPLE 4
On Wednesday, October 25, Microsoft discovered that hackers had broken into its internal network. The hackers reportedly accessed Microsoft’s system using a QAZ Trojan attack, which enabled them to transmit hidden code by way of what appeared to be a normal e-mail attachment. The code executed on the company’s server and enabled the hackers to record passwords to source code for future versions of Windows and Office. The hackers then continued on page 34.

Visit our advertisers

Atlantis Software (www.atlantissoftware.com),

AdRem Software (www.adremsoft.com),

and GroupLink (www.grouplink.com)
continued from page 33

EXAMPLE 5

Nine days after discovering the QAZ Trojan attack, Microsoft discovered a second, presumably unrelated intrusion into its corporate network. This time, the hacker, using the alias Dimirri, gained access to Microsoft’s Events page and uploaded a file called “Hack the Planet,” claiming to have then downloaded an encrypted file containing Microsoft usernames and passwords. Only five days later, Dimitri hacked Microsoft’s Events page a second time, this time defacing the page with a snide message reading, “Patching your systems is very hard huh?” (See http://www.msnbc.com/news/486630.asp. You can also find an image of Dimitri’s message at www.attrition.org/mirror/attrition/2000/11/07/events.microsoft.com.)

EXAMPLE 6

If you visited the Yankees’ web site the morning after the World Series, you were greeted by the message “Yankees Suck!!!” along with the picture of a naked man moaning you and the rest of the world. In this case, hackers reportedly attacked the Internet Service Provider’s (ISP) servers and redirected browsers to the page bar- ring (pardon the pun) the anti-Yankees message. (See “Hackers Pitch Strikes to Site’s Security,” eweek, Nov. 6, 2000, at www.zdnet.com/eweek/stories/general/0,11011,2650244,00.html.)

EXAMPLE 7

Late September, an IKEA customer requested a catalog from the furniture dealer’s web site and in response received an error message. The error message included the path to a consumer database, which the user used to open the door to the names, addresses, phone numbers, and e-mail addresses of approximately 150,000 IKEA customers. (See “Seeking Cyberspace Safeguards,” Computer Reseller News, Sept. 29, 2000, at www.channelweb.com/components/search/Article.asp?ArticleID=20288.)

EXAMPLE 8

Western Union had to down its web site in early October after discovering that a hacker copied credit- and debit-card data from as many as 15,700 customers. (See “Seeking Cyberspace Safeguards,” Computer Reseller News, Sept. 29, 2000, at www.channelweb.com/components/search/Article.asp?ArticleID=20288.)

EXAMPLE 9

On November 6, Computer Reseller News reported that either pro-Palestinian or pro-Israeli groups had hacked more than 30 web sites. The report added that the U.S. FBI’s National Infrastructure Protection Center (NIPC) warned U.S. companies that attacks at any point could be directed toward them. (See “MidEast Conflict’s IT Impact,” Computer Reseller News, Nov. 3, 2000, at www.channelweb.com/components/search/Article.asp?ArticleID=21280.)

EXAMPLE 10

The night before heading to a polling station to vote, at least one U.S. citizen was making a last ditch effort to urge his fellow Americans to vote his way. The nameless and relatively articulate hacker (compared to the script kiddies usually guilty of web-site defacement) left a 1,000-word statement on the op.org site that half-heartedly supported Gore as essentially the lesser of the two evils. (See www.msnbc.com/news/486630.asp. You can also find an image of the pro-Gore rant at www.attrition.org/mirror/attrition/2000/11/06/www.gop.org/mirror.html.)

consults rules you create and store in NDS eDirectory. You can apply these rules to Novell iChain Community objects (objects Novell iChain adds to the NDS schema), as well as container, User, and Group objects.

For more information about Novell iChain 1.5, see “What’s New?” on p. 36. You can also visit www.novell.com/products/iChain and www.novell.com/consulting/bso/access.

Netegrity SiteMinder

A Netegrity product, SiteMinder also addresses the problem of authenticating and authorizing web site users. SiteMinder is a scalable and reliable platform for securely managing and personalizing large e-commerce portals for global 2000 corporations and their affiliates, business-to-business trading marketplaces, and service providers.

For more information about Netegrity SiteMinder, visit www.netegrity.com.

STAGING SECURITY

Of course, few companies will want to deploy a complete security solution all at once. Fortunately, the Net Security solution is modular, enabling you to deploy the products that meet your specific needs as those needs arise. Further, you have the assurance that the Net Security products you choose today will work well with the Net Security products you deploy tomorrow.

Ultimately, the Net Security solution is designed first and foremost to simplify the complexity of securing an e-business. With the Net Security strategy and the products positioned with the Net Security solution, you’ll be able to secure your e-business (and thus reduce the downtime associated with security breaches). (For more information about the Net Security solution, visit www.novell.com/solutions.)

Linda Kennard works for Niche Associates, an agency that specializes in writing and editing technical documents.