CYBERTERRORISM: ARE WE LEAVING THE KEYS OUT?

By Kevin Cunningham, Vice President of Marketing and Founder
Waveset Technologies, Inc.

In a post-Sept. 11 world, the security community is being asked to address a growing list of sobering scenarios that range from the newly plausible to the truly frightening. One of the much-discussed issues is cyberterrorism -- the possibility that a motivated cell of political or religious fanatics could hack into vital military, government or commercial computers from remote locations and bring the free world's defense and communications systems to its knees.

If you work for a high-risk organization -- a government agency, defense contractor, transportation organization, financial institution, communications/media company, or other high-profile firm -- chances are, you've thought about these possibilities.

Like many of the once-unthinkable scenarios, it's a disturbing notion. However -- and fortunately -- it remains a scenario more fit for a Tom Clancy novel than for a pragmatic security professional. Here's why.

Web site hacking and cracking has largely been confined to consumer sectors with high online profiles. It's the news site that's hacked with a bogus news story that sets off a fraudulent stock-price run-up. Or it's the retail site that finds its customer files compromised by thieves seeking credit card numbers. The work of other hackers (including so-called "hacktivists") could be largely characterized as joyriding, vandalism, or graffiti -- unauthorized entry into proprietary systems and the resultant posting of malicious messages.

Fortunately, these kinds of stunts -- while disruptive, illegal, and expensive -- are rarely catastrophic. And, as intrusion detection systems continue to improve in sophistication, they become more difficult to accomplish.

THE REAL THREAT

Unfortunately, the far more significant threats lie inside -- not outside -- the organization. Due to a variety of circumstances, including loosely aligned business processes and un-enforced security policies, many companies unwittingly "leave the keys out" to their protected networks, databases, and applications. Outside hackers aren't the primary threat -- the greater danger stems from people who at one time or another have had legitimate access to information, or who are using legitimate accounts to mask illegitimate activities.

To use a terrorism-based analogy, consider the events of Sept. 11. Hijackers did not elude perimeter security and storm airplanes from the tarmac. Instead, they were credentialed, ticketed passengers with authorized access to commercial airliners which they then turned around and used as weapons of mass destruction.

It's largely the same situation with computer networks. Media accounts focus on fictitious scenarios of hackers tapping into U.S. systems from remote terrorist camps. However, in reality, most espionage, theft, and damage to computer systems is performed by insiders -- or hackers masquerading as insiders -- using legitimate credentials to slip in easily and, often, unnoticed. How are they

able to do this? Largely because corporations lack the visibility into and control over the systems required to keep it from happening.

SO, WHAT ARE THE REAL RISKS?

These insider-driven scenarios might not fall under popular definitions of cyberterrorism. But the fact is, they represent far greater exposure and risk for public- and private-sector organizations. Consider a terrorist -- armed with proper ID and password -- connecting to a financial institution site to siphon off or launder money that funds terrorist activities in the U.S. Or a cell tapping into personnel files for identity-theft purposes. This stealthier form of cyberterrorism is based not on system disablement, but on data and monetary theft -- the means to an end for the terrorist and his activities.

How much money are we talking about? In its latest survey, the Computer Security Institute found that *reported* financial losses from computer crime and security breaches in 2002 totaled about $455 million. However, only forty percent of the survey's 503 respondents agreed to quantify their losses, meaning the price tag is certainly much higher.

Just as importantly, these vulnerabilities are not limited to terrorist opportunists. Unfortunately, they are far more likely to be the province of authorized insiders: disgruntled employees or recently terminated ex-employees, embezzlers, former contractors and consultants, or others bent on revenge. In fact,

a recent study by the American Society of Industrial Security found that vengeful employees are now the biggest security worry for 90% of US bosses.

However, it's not always who you think. While an IT administrator might have the most sophisticated systems access, a business user with detailed knowledge about your customers, data, and business processes, can wreak far greater damage in identifying and stealing/deleting sensitive information. For example, a records administrator could compromise patient privacy at a healthcare facility. Or a bank officer could access account balances to initiate the unauthorized transfer of funds. In one key stroke, users in these types of situations can wreak corporate-wide havoc without ever leaving their chair.

Gartner estimates that more than 70 percent of unauthorized access to information systems is committed by employees, as are more than 95 percent of intrusions that result in significant financial losses. [1] What's more, according to The Hurwitz Group, for every in-house attack reported, there could be as many as 50 that are either unreported -- or undetected.[2]

And this brand of risk affects not only high-profile federal agencies or Fortune 500 companies. It also affects lower-profile infrastructure targets. You might consider a railroad a stodgy "old-economy" kind of enterprise. But the repercussions of computer network sabotage are enormous. One authorized user

[1] "Security in a World Without Secrets," Gartner, R. Hunter, February 2002

[2] "Case study of insider sabotage," *CSI Journal*, Vol. XVI, No. 3, Nov. 3, 2000

could send dozens or hundreds of trains on collision courses, causing widespread loss of life, hundreds of millions of dollars in property losses, and untold complications to the nation's supply chain.

If you're thinking that you haven't heard much about these kinds of issues -- well, you're right. With the average cost-per-incident of cyber theft reaching $2 million, not too many companies are interested in disclosing their losses. Disclosure often results in bad PR, loss of investor confidence, litigation -- and, quite possibly, invites copycats.

RENEGADE KEYS

The fact is, many companies and government agencies have what I call "Tootsie Pop" security -- it's hard on the outside, but soft and mushy on the inside. As I mentioned earlier, firewalls, VPNs, and other perimeter security strategies continue to improve in their ability to repel unwanted intruders. However, it's a different story on the inside where most organizations tend to relax and let their guard down. And that leads to significant vulnerabilities and exposures. A few key examples:

1. Dormant accounts

A close colleague of mine was a former senior IT administrator at a major healthcare organization. In his role, he had super-user access privileges to more than 4,000 separate clinical, diagnostic, financial, and administrative systems. He eventually left the company to help launch a start-up that, like many in recent months, died on the vine. Fortunately, he had remained on good terms with his former employer and ultimately returned to the same firm where he reclaimed his original position. He jokingly told me that he was immediately productive on his first day back at his old job -- because almost all of his former user accounts were still active. In the two-year hiatus, no one had shut off his authorized access -- a common oversight leading to the proliferation of "orphaned" accounts, or "back door entries" into the enterprise. Luckily, my colleague is the honest type, and would never take advantage of such security vulnerability. Unfortunately, this is not always the case – and the news is full of examples to prove it.

IDC estimates that as many as 30-60 percent of access profiles in large corporations are no longer valid.[3] META Group describes these accounts as magnet for hackers and intruders. "We estimate that released/former employees typically continue to have access to network resources for several weeks after departing. This presents an obvious security threat and, in many countries, is a breach of applicable privacy regulations."[4]

2. Unchanged Passwords

It's a similar story in many companies. Most operating systems, applications, and other network elements ship with a pre-configured administrative ID and password. In my experience, as many as half of those default accounts remain unchanged by the deploying companies. That's like buying a newly constructed house and not changing the lockset on the front door -- virtually anyone has the standard key.

3. Un-enforced Security Policies

In some cases, it's the easy things that get overlooked. Sure, you've probably written tight policies that cover all aspects of security -- but does your organization consistently enforce those policies? For example, do you require -- and audit – that users rotate their passwords on a regular basis? Do you ensure that passwords use mandatory non-alpha characters, have minimum lengths, and refrain from common

[3] "Old IDs Never Die; They Just Cause Trouble," *Computerworld*, July 31, 2000

[4] META Group; METABit: "Off the Books, But Not the Systems," Mark Bouchard, March 27, 2002

words? How can you tell these policies are adhered to? The fact is, most companies have no way of telling.

4. Lax Control over Access Privileges

Too often, administrators grant permissions in a very *ad hoc* manner. In a previous position with another company, I remember asking our SAP administrator for an account so that I could access some key corporate financial information. He didn't know me, but by simply asking, I was given access. Should I have had that level of access? Who knows? Nobody stopped to ask an important question. More importantly, who knew to delete my account when I left the company? Bet you dollars to donuts my SAP account still exists.

5. Lack of Visibility into Privileges

Most organizations lack a comprehensive and integrated view of user access privileges across the enterprise. This often leads to conflicting and potentially risky access combinations such as a user who has privileges on both purchasing and accounts payable applications.

INDUSTRY REGULATION

In sum, it's practices like these that leave many corporate and government networks vulnerable to the stealthier, less showy kinds of hacking and cyberterrorism.

But there are non-terror-related issues that require consideration as well: government-mandated regulatory issues. For financial services firms, Gramm-

Leach-Bliley (GLB) establishes very specific limits on the accessibility and privacy of customer financial information. In the healthcare industry, the Health Insurance Portability and Accountability Act (HIPAA) prescribes similarly stringent requirements to protect the confidentiality of patient records. Both legislative initiatives are expressly intended to shore up weak internal security situations that affect the public sector. Dormant accounts, default passwords, and lax security policies are inherently incompatible with HIPAA/GLB compliance.

SO, HOW DID WE GET IN THIS MESS?

The reasonable question for anyone responsible for managing security issues is, well, how did we get into such a mess? Simple -- we in the IT community are victims of our own success. Ten or 20 years ago, the size and number of enterprise applications or inter-networked systems was manageable. It was a fairly easy exercise to manage identities -- to assign and manage user accounts.

Today, several years after the advent of the Web, it's a radically different story. It's not uncommon for a large enterprise to have thousands of different systems to administer – both inside and outside the physical confines of their organization. At the same time, the number and diversity of user communities has changed considerably – evolving from an elite set of technical users to a broader, more distributed population of line-of-business users, partners, suppliers, and even customers. Managing the accounts and associated identities for thousands of users

across thousands of systems? It's a low-value time drain that until recently never rose to the top of the priority list -- but it's an issue we ignore at our own peril.

Gone are the days of mainframes when IT departments could tightly control change processes and manage user administration centrally. Servers have since propagated across the enterprise to support distributed client/server applications. Web, e-business, and extranet applications have compounded the challenges further. Yes, the productivity gains and new revenues are undeniably compelling -- but we've lost IT control of user management.

So, today, we have a hodgepodge of legacy, client/server, and Web applications with new systems coming online every week. Absent a centralized, consistent interface/system/process for managing identities, most companies resign themselves to two alternatives: throwing bodies at the problem (which becomes increasingly unfeasible as the scale and scope of IT systems grow) or ignoring it altogether.

HOW CAN WE SOLVE THE PROBLEM?

If it sounds like an intractable problem, fear not. While there is no silver bullet, there are a variety of sensible, pragmatic steps you can take to increase your security, limit the incidence of and damage from cyberterrorism, and improve your overall productivity at the same time.

1. Define Security Policies

Create a policy manual (or, perhaps, emulate/adapt an existing one) that defines and describes the proper processes and procedures for securing your network and computing environments. For example, what are your company's password requirements? How often must they be changed? How many characters should they be? What characters are required? Which ones are forbidden? You should also tightly define what level/title/role in your company can access what information. For example, a physician in the southeast might only be able to access patient records in that region. Or an accounts payable clerk may be prevented from also accessing the inventory order system.

2. Establish "Need-to-Know" Access Rules

Given the overwhelming volume of users, applications, and systems, it can be very tempting to simply provide blanket access privileges for groups of "similar" users. After all, rather than face a continuing stream of requests for authorization changes, it's easy and fast for time-strapped IT managers to simply grant full access rights to data. Of course, this leaves networks and systems dramatically exposed to vulnerabilities -- an ideal scenario for a hacker or terrorist. Once you've implemented a need-to-know hierarchy for data, don't be shy about asking requesters what they need access to, and why.

3. Implement Centralized Visibility and Control over User Access

This goes to the root of perhaps the greatest vulnerability that you can reduce or eliminate most easily. No longer can you get by with "islands of

administration" having different interfaces, management consoles, and processes. New software tools can provide *unified* administration over a virtually unlimited number of systems, applications, and users to automate routine, yet complex, operations that ensure consistent security policy enforcement.

4. Leverage a Distributed Architecture Model

Even though you're unifying the management and administration of users, it's crucial that you resist the allure of *centralizing* user-account data, which can be difficult to implement, and lead to a single point of failure and penetration – resulting in reliability *and* security issues. A repository of IDs and passwords is simply too tempting of a target. Instead, adopt a philosophy of centralized management but local enforcement, leaving critical identity information where it more safely resides on the native platforms.

5. Automate the Access: Easy-On, Easy-Off

Once you've achieved centralized visibility into and control over user data, you're in a better position to more easily manage user accounts. Now, for example, you can manage from a single point-of-identity to provide user access to multiple systems and applications across an organization. Hiring a new employee? You can activate user accounts for all the systems she needs to access in a single action. More importantly, the reverse is true when you need to terminate employee (or partner) access to accounts with a single, immediate transaction.

6. Audit Policies and Procedures

Best practices for identity management also extend to establishing strict risk assessment procedures and audit trails. Review what users are accessing which systems and databases – and understand why. Also review who's granting and approving the privileges. In other words, set up checks and balances so that no single individual has total autonomy over the granting or revocation of access privileges.

CONCLUSION

In the final analysis, protection from cyberterrorism boils down to the right combination of people, processes, and technology. We need to educate our IT staff and employees about security and their roles in enforcing it. We need to carefully implement and follow "best-practices" security processes and review and modify those processes on a regular basis. And we need to deploy the right technology to assist all of these efforts and shore up vulnerabilities that may exist.

Classic media-driven cyberterrorism scenarios that portray wide-scale disablement of computer and military systems are disturbing, but fortunately, remain fairly remote as firewalls and other perimeter security measures continue to improve.

Stealthier intrusions -- using legitimate access methods or inside operations -- remain a higher probability. Here, the goals are data and identity theft, fraud, and embezzlement for both terrorist purposes and more common motivations such as

greed or revenge. Regardless of the motivation, however, companies and government agencies can take numerous common-sense steps to reduce their exposure and any potential damage by carefully managing user IDs and passwords -- and ensuring they don't "leave the keys out."

ABOUT THE AUTHOR

Kevin Cunningham is a founder and senior executive at Waveset Technologies where he is responsible for the company's market positioning, product definition, and outbound communications. He helped start Waveset after more than 15 years in the software industry where he focused on bringing innovative technologies to market. Before co-founding Waveset, Kevin led product marketing efforts at UniSQL, Inc. and Tivoli Systems Inc., where he oversaw the definition, positioning, and promotion of the company's award-winning systems management solutions.