APRIL 2013
VOL. 15 | NO. 03

INFORMATION SECURITY®

MANAGING IDENTITIES IN HYBRID WORLDS

Secure access for a mobile workforce requires gaining control of IAM.

BOTNET TAKEDOWNS: A DRAMATIC DEFENSE, BUT DOES IT CHANGE THE GAME

ADDRESS IPv6 BEFORE YOUR SECURITY TIMES OUT

TechTarget

Security Transitions: Let's Act On What We Know Is True

Building security into software and renewed attention to identity management. BY ROBERT RICHARDSON

AS GARY MCGRAW mentions in his [In]Security column this month, the continuing flow of news about sophisticated, international cybercrime—so prominent in the media recently—might finally have gotten to us. In a good way. A lot of words have been squandered in proclaiming the death of antivirus scanning, the collapse of the endpoint, and the inability of traditional intrusion detection systems to serve any good purpose against advanced threats; and yet, we have seen no paradigm shift in the trenches where it counts.

McGraw's primary solution, one that I've always been inclined to favor, lies in developing more security capable software. I don't know that game-changing shifts in the resilience of software should be expected anytime in the near future though. Our education columnists Doug Jacobson and Julie Rursch note that college classes in software development generally give security issues a cold shoulder, saying that "…In our software classes, we focus on getting students to program and to learn the aspects of the language. Seldom do we ask them to consider security and rarely, are their programs graded on it."

Still, while we may not get the next generation of programmers trained for security, we still generally concede that the old approaches won't get the job done either. I can't help but recall that our recent reader survey found that one in five of enterprise respondents indicated that within five years, they'd no longer be committed to using static signature scanning. There was similar chatter in the halls at the recent RSA conference in San Francisco: scanning doesn't cut it. I don't know anyone who's actually

jettisoned endpoint scanning, but it does feel to me as if practitioners have at least moved to a point where they're willing to concede that just throwing more antivirus software onto the desktop is not going to stop anything other than the most basic of attacks.

Guest columnist David Sherry, at least, believes that the role of the CISO is changing to recognize the new degree of risk within the enterprise. Sherry notes, and I think many observers would agree that there is a new level of maturity in both the security industry and the CISO function. Does that maturity mean our organizations will take a rational view of what defenses were in place should a breach occur, or is the guy who's gutsy enough to stop wasting time on scanning software likely to wind up looking for a new career when an intrusion is discovered?

So what changes in security technology or approach could actually make a difference? In addition to better software coding, one potential game changer in security is a renewed attention to identity management. Peter Gregory notes, "Organizations in this situation are not in control of their asset management policies." What isn't necessarily a revolution in security, on the other hand, is the rollout of IPv6. It doesn't really bring new capabilities, Fernando Gont argues, "There are no security features in IPv6 that were not readily available for IPv4."

I think many observers would agree that there is a new level of maturity in both the security industry and the CISO function.

Finally, in a nod to the ongoing changing of the sophistication of attacks, this issue offers a look at the current state of botnets. I mention this piece partly because of its author, our newly arrived features writer and editor Kathleen Richards. She's hit the ground running and her handiwork is embedded throughout this month's issue. I'll let the article speak for itself, but for the moment let it suffice to say that there's a lot going on with botnets.

Oh, and we're not going to stop botnets with static virus scanners. It's really time to stop just saying this sort of thing and actually, start acting like we know it's true. ■

Chinese Hackers, "Active Defense" and Other Bad Ideas

Hacking back won't work in cyberwarfare. The only way forward is to build software and systems with fewer vulnerabilities. BY GARY MCGRAW

IN FEBRUARY, the security firm Mandiant confirmed, with plenty of hard evidence, what we've known for a long time: Chinese cyberespionage is rampant and worrisome. From the Aurora attacks in 2009 through the spectacular RSA token hack of 2011 to the ironically, self-described attacks on the computer systems at *The New York Times* in 2012, state-sponsored cyberespionage has been constant news for years.

Every revelation comes with a renewed beating of the cyberwar drums. Many otherwise sane people have discussed the idea of going on the offensive and "hacking back" by booby-trapping honeypot data or setting loose malicious software. Distressingly, this sort of cyberoffense is being repackaged—and camouflaged—in a clever and, ironically, Newspeak way under the rubric "active defense."

Let's get this straight up front: active defense is irresponsible. We will never vanquish a cyberenemy by going on the offensive—unless we involve our impressive kinetic capabilities. The problem is: we all live in glass houses and should avoid rock throwing.

The only alternative is doing some heavy lifting and investing in security engineering, software security, and building security in. We have to build our cyberhouses out of something other than glass. Leveraged properly, security engineering can serve as a real deterrent in our otherwise steady slide towards cyberwar.

CYBERESPIONAGE IS NOT CYBERWAR

The Mandiant report is well worth the time it takes to read it. Chock full of data gathered over multiple engagements (141), the report makes a solid, evidence-based

argument: many cyberespionage attacks have been perpetrated by the Chinese. (Note that Mandiant tracks other hacker collectives including the Russians and the Eastern Europeans, but China is the easiest to vilify because of the well-publicized attacks attributed to the Chinese since 2009.)

That Mandiant chose to publish its evidence is commendable. When the "Chinese Hackers Infiltrate New York Times Computers" story was first reported by *The New York Times* in January, Mandiant pointed the finger at the Chinese military. At the time, the Chinese Defense Ministry issued this statement: "It is unprofessional and groundless to accuse the Chinese military of launching cyberattacks without any conclusive evidence." The Chinese asked for evidence, and they got it.

If a forensic computer security firm like Mandiant can triangulate one particular set of espionage attacks to the Chinese military, why can't we do the same thing during a cyberwar incident and go after our enemies with impunity?

The answer may surprise you.

Remember, the attacks that Mandiant forensically "reversed" in painstaking detail started in 2006, with the longest single intrusion lasting for four years and 10 months. The forensic effort likely took weeks, or months.

There is time for this kind of careful analysis in a cyberespionage incident involving information extraction. That helps with the thorniest issue in cyberattacks: the problem of attribution. Mandiant gathered lots of evidence, and it took great care to untangle tricky and misleading paths—ironically, using low-skill Facebook logins along the way.

A cyberwar attack is likely to unfold over minutes, seconds or split seconds.

Here's the bad news. A cyberwar will not unfold over years, months or even days. A cyberwar attack is likely to unfold over minutes, seconds or split seconds. Cyberwar will happen at super-human speed. Of course, cyberespionage and APT attacks may well help to set the stage for a cyberwar attack, but we'll ignore that for now.

Imagine a cyberattack against the power grid. By hacking in and controlling about 50,000 smart meters, intentionally causing a 300-megawatt stability problem in the grid is well within the realm of possibility. Properly carried out, a stability problem like this could destroy key transformers in the grid, causing permanent damage that would take months, or years to repair.

During the fog of war, an attack like this could unfold in seconds, and determining who is perpetrating it, may not be possible. Forensics takes time on the Internet, and

there is simply no time to game the attribution problem in most realistic cyberwar scenarios.

In the end, it's clear that cyberespionage, though reprehensible and certainly worthy of response, is not the same as cyberwar.

It's critical to emphasize that attribution through forensics is vastly different from active attribution during an actual attack. Time frames are diverse enough that war and espionage must be teased apart.

ACTIVE DEFENSE IS IRRESPONSIBLE

Any active defense strategy is going to involve the use of a security hole that is exploited on the original attacker's system. If you want your "hack back" to succeed, you have to have something to hack.

Washington is all a buzz about "active defense," mostly without thinking through what it really means, or just how ridiculous it is philosophically. Policymakers are not technologists so we have to be patient with them; but unfortunately, many technologists are hucksters and that is just a crying shame.

In order for active defense to work, somebody needs to find a security hole (most likely in software) and develop an exploit for that hole. Then, get this, they need to keep the hole secret so that the exploit they just developed continues to work.

I'm not talking about a configuration error on the attacker's server, or a network firewall problem, or some failure to patch. I'm talking about a real software vulnerability.

Imagine a situation in which a booby-trapped active-defense file is placed in a honey pot for an attacker to take—we're sticking with espionage here. The active-defense file is designed to exploit a hole in whatever software is used to process the file. So, the attacker extracts the file and uses some program to read it. A successful "hack back" requires some vulnerability in the reader program. Maybe it's Adobe Reader, Microsoft Windows or even the Java interpreter, but it's vulnerable; and the vulnerability is a vaulted zero-day exploit known only by the active attackers.

Now imagine that the attacker is smart enough to capture and isolate the "hack back" code. Ye olde zero-day exploit now belongs to the enemy. Oops! If you throw a rock at your enemy, do not be surprised to find it thrown right back at you. There is a reason that the Romans designed spears to be thrown once.

In the end, there is this truism: the only way forward in computer security is to build systems with fewer vulnerabilities. Finding a vulnerability and packaging it up into a "hack back" system hurts everybody—including the purveyor (or purchaser) of active defense. Finding a vulnerability, *and then fixing it*, is obviously the right thing to do.

Another issue is figuring out whom to "hack back." This is the attribution problem, which only a long,

painstaking forensic investigation can solve with any authority. Almost all attacks on the network involve using a number of third-party "stooge" servers as a front and, sometimes, a platform for an attack. Without solving the attribution problem, those who "hack back" run the risk of "being Gandalfed."

Why not hide behind a common enemy of the nation-state? Or a corporation you're attacking? Attackers have been doing it for decades.

Finally, if active defense does not involve "hacking back" and getting outside of your own network, but rather simple intrusion detection, then we should call a spade a spade and cut the Doublespeak. If active defense is just intrusion detection and monitoring of self in real time, then it's the same old, same old warmed over with a new sexy name. Yawn.

WHAT IS WASHINGTON TO DO?

Sadly, the government's approach to cybersecurity is as anemic as it is bureaucratic. FISMA checklists may help drag slow-moving agencies into the '90s, but they are certainly not cutting new ice. Compared to setting up and watching perimeter defenses (which is exactly what operational network security does), active defense sounds way cooler. Plus, the Department of Homeland Security only recently started figuring out where the government is connected to the Net, so they are easily distracted.

President Obama's leadership on the issue is appreciated, but at the same time underwhelming. More specifically, his latest executive order is vague and it does not address how to build secure infrastructures. It talks about Frameworks and asks NIST to create more paperwork. That's too bad. We need more specific and actionable leadership here.

Driven by the realization that firewalls, basically, don't work; and that the perimeter has dissolved as we embrace the cloud; people looking for the answer, who don't know any better, may well embrace active defense, warts and all. That would be a shame because we're sitting here in our glass houses talking about rock throwing again. That won't end well for anybody. ■

GARY MCGRAW, *Ph.D., is CTO of software security consulting firm Cigital. He is a globally recognized authority on software security and the author of eight best-selling books on this topic. Send comments on his column to feedback@infosecuritymag.com.*

CISOs: From No Seat to Multiple Hats

Roll up your sleeves. The CISO role in many enterprises is expanding beyond security risk mitigation to risk management, privacy and regulations, and compliance. BY DAVID J. SHERRY

IF YOU HAVE WORKED in information security for the past 15 years, you have witnessed a maturation in the mission of security that is quite remarkable. In its infancy, security was oftentimes viewed as the troglodytes at the end of the corridor, who focused on analyzing packet streams, firewall logs and anti-virus anomalies. Some of the fear that hovered over security practitioners was simply the result of the role that they played, and their secretive and covert way of performing their duties. Still, security practitioners diligently performed their tasks, and sought and gained increasing relevance.

Fast forward to the current day, and you will see a new view of security in many enterprises: security is evolving towards a broader focus in risk management. The responsibility of traditional information security has not decreased in importance or duty, but the mindset and role has certainly become more risk-based in nature for security leaders and many current CISOs. And this is appropriate, as information security management at its core is the mitigation, transference, reduction and elimination of risk to the enterprise.

Many CISOs' responsibilities now include privacy and its related functions and regulations; compliance with federal and local mandates and external entities; and a deeper penetration into legal arenas. And this makes sense, as a seasoned and trained security executive would have the right qualifications to take on this wider scope. As privacy and compliance continue to gain importance in the success of an enterprise, and with some hesitancy of adding senior headcount, assigning responsibilities to the CISO is a sound business model.

Aside from the demands on time and prioritization, such a move is seen as an extremely positive transition for the security profession. A security professional oftentimes brings a different skillset and experience to the table, identifying both the risks and their solutions in a way that may not have been seen in the former structure. A move to include risk management with security has also enabled the mission of security to take some additional spotlight, which has become an unexpected fringe benefit to taking this broadening role. An experienced CISO or similar security leader can share solutions that are more holistic in nature, and support the establishment of processes that can satisfy different risk and compliance concerns in several different areas. This can only be seen as a positive for information security.

DEFINING THE NEW SECURITY AND RISK FUNCTION

The biggest challenge is sometimes the scope. The increasing responsibilities can sometimes impact the focus that is necessary in the day-to-day security function. There could also be some pushback from the IT security function itself, as some of the technical operations may not see the need for the risk-based methodology. Also, establishing the credibility of a newly expanded function is something that must be overcome confidently and quickly. The function needs to be implemented iteratively, beginning with a board-level mandate, wide publicity, seed financing to establish base-level solutions and the celebration of documented success. It is also important that the CISO establishes the powerful tool of a high-level and cross-functional committee of enterprise leadership that meets regularly on all things security, risk, privacy and compliance. Having this group be both a sounding board and an approval authority, will have a positive impact on how the expanded security and risk function sees their role, and how they fit into the overall risk management posture.

An experienced CISO or similar security leader can share solutions that are more holistic in nature.

There are obvious economies of scale with combining the functions as well. Partnerships with audit, legal and risk can be developed or deepened, and common solutions and needs can be identified and addressed. Having a more holistic approach, with several key function heads on the governing body, will also bring more spotlight on the original security function, and aid in validating their mission. Security can now be observed chairing and leading the decision-making process in several key areas, which would have been unheard of only a short time

ago. Finally, in the area of incident response, what was traditionally handled in the IT world is now shared and communicated to a wider audience. This has enabled the old mantra of "it's a technology problem" to be reduced or eliminated, and allowed the security and risk function to now be seen as contributors to the success of the enterprise.

Security has reached a new juncture in its maturation as a discipline, one where an expanded role with more impact can now be achieved. It wasn't very long ago that security was looking for a seat at the table. Now its practitioners are not only sitting there, they may be wearing more than one hat. Now is the time to embrace this evolution. Security practitioners has worked hard to establish relevance in the enterprise, and the recognition that a company would want the security function to take on increasing responsibilities is a humbling and exciting one. It validates the actions and thinking that has been developing as a security community, and establishes the function as a business one in addition to a technology one.

It's an exciting time to be in security and in a CISO role. I would imagine that if we have a similar conversation in two or three years, we would be looking back with pride at our expanding security discipline, and embracing the next wave of challenges. Put on those hats! ■

DAVID J. SHERRY *is the chief information security officer at Brown University, with university-wide responsibility and authority regarding matters of information security and privacy. He leads the Information Security Group, charged with the development and maintenance of Brown's information technology security strategy, IT policies and best practices, security training and awareness programs, as well as ongoing risk assessment and compliance tasks. Send comments on this column to feedback@infosecuritymag.com.*

Why Information Security Education Isn't Making the Grade

It isn't just the industry that gets poor marks in security.

BY DOUG JACOBSON AND JULIE A. RURSCH

AT LEAST WE'RE CONSISTENT. When it comes to information security in industry or education, we are not taking a holistic approach. Information security is a bolt-on feature.

Business executives on down to the IT staff continue to treat security as a separate issue, handled by IT specialists. Rarely do software or system engineers approach the design of a product with the intent to include security from the start.

It is no different in security education: we don't educate our computer engineers and computer scientists to take a holistic approach to security. We teach information security in a separate class or, if students are lucky, classes; and these courses are usually electives. Is it any wonder when these individuals leave our hallowed halls to enter the workforce, they treat information security in the same vein?

Why do we do such a poor job in information security education? It is the approach we take to teaching computer engineering, software engineering and computer science. We design a curriculum to help students learn to use logic. That part is good. We have them take sciences and math to learn about the physical world, as well as the ordered reasoning needed to complete advanced math courses. Students must also take the humanities to make them well-rounded individuals with a cursory understanding of the world outside of "geekdom."

But, when we teach our primary courses, those which set our students apart from others in their knowledge base, we don't take a holistic approach to their education. We start students in introductory courses that break

things into small pieces, which are easier for them relate to and understand. Good for us, we help them get started. But, it's in the second through fourth years of undergraduate education in computer engineering, software engineering and computer science that it falls apart.

> We silo information security, instead of incorporating it into every class we teach.

The field is so vast and we have so many different areas to specialize in, we allow students to focus on the details of a language, building hardware, or learning algorithms. We silo information security, instead of incorporating it into every class we teach. As educators, we spend a lot of time focusing on getting students to cover all the basics. We treat security in any area as a topic that is added on at the end of the semester, if we have time; we don't allocate a lot of time in lectures or in labs on it.

In our software classes, we focus on getting students to program and to learn the aspects of the language. Seldom do we ask them to consider security and rarely, are their programs graded on it. Why else would things like buffer overflows and SQL injections work? Even error or data input checking is a task relegated to the end of the semester, when topics fly by fast and furious so we can "get the material covered." With our cursory approach to these important topics, is it any wonder that students pay little attention to them?

SECURITY ACROSS THE CURRICULUM

Some students specialize in information assurance or information security as part of their majors, and they need specific courses that focus on security topics. But, for the general computer student population, we need to take a more holistic approach to teaching security: it needs to be part of every course and included from the first day.

In this way, we believe that we could take a page from our colleagues in the English department, who have over the course of the past 10 years or so, pushed through a concept of "writing across the curriculum." The point these faculty made was that English 101 and 102, or their equivalents at various universities, had historically been taught as the two basic courses that every freshman endured. And, then the computer engineering, computer science, and software engineering students could forget about writing.

That, as we all know, is not true. Technical reports, as well as documentation, are an essential part of work in the computing field. At many major universities, computer science students are now required to take additional English courses that occur throughout their four-year career and complement their technical courses. In

one example, the technical instructor provides the content, but the English faculty member helps the students write concise summaries and complete the final report for the course.

We believe "security across the curriculum" would be a wiser approach for information security education. It would incorporate security as a topic from the beginning of every course, and we would continue to refer to it as we teach students about the basic concepts in each course. This would then carry over to their work as design engineers or programmers. When sitting down to work on a new project, we always start at the beginning and lay out the landscape. We should include security as part of the design plan. And, the security of the project should be considered at every revision and stage.

So, let's change the kind of consistency that information security education is known for. We need to endorse "security across the curriculum" in which students learn in every course how important security is to a project. If we teach students to take a holistic approach, it will only follow that they can take this same perspective when they reach the business world. ■

DOUG JACOBSON *is a professor in the department of electrical and computer engineering at Iowa State University and director of the Information Assurance Center, which was one of the original seven NSA-certified centers of academic excellence in information assurance education.*

JULIE A. RURSCH *is a lecturer in the department of electrical and computer engineering at Iowa State University and director of the Iowa State University Information Systems Security Laboratory, which provides security training, testing and outreach to support business and industry. Send comments on this column to feedback@infosecuritymag.com.*

MANAGING IDENTITIES IN HYBRID WORLDS

Are you losing control of access management as SaaS and mobile devices take hold? To achieve better operational consistency and scale, consider a centralized IAM system.

By Peter H. Gregory

YOU WOULD THINK that managing identities and access rights in an organization would be settled, solved and routine by now. But the ebb and flow of disruptive technologies such as cloud-based systems, mobile apps and bring-your-own devices (BYOD) have made it as elusive as ever.

Identity and access management (IAM) is the business and technology concerned with effective management of all users' access to an organization's assets and facilities. It is difficult to fund IAM projects because they consume resources without actually adding business functionality. IAM is a part of the organization's plumbing; you take it for granted until you turn on the hot water and nothing happens.

Many organizations do not realize that their IAM is out of control until one of the following occurs:

- Security incident caused by an insider with excessive privileges
- Security incident caused by a former employee who still has access rights

- An external auditor or regulator discovers lapses in IAM processes resulting in too many people having access to too many roles and systems

This is a growth pain—a rite of passage—that practically every organization experiences. Only when the pain becomes great—when the organization experiences an incident or some lapse– is it willing to face the music and fix the problem. This may not be that different from waking up in a bed-bug infested bed; at first the bites aren't so bad, but eventually you can't deny the infestation.

By understanding the symptoms of a troubled identity management program, an organization can quickly identify and seek to remedy the issues before an identity-related incident can take its toll.

THE IAM PROBLEM DEFINED

There's no mincing words: organizations in this situation are not in control of their access management policies. Typical scenarios that many enterprises face include ineffective onboarding, accumulation of privileges, failure to terminate user access, and departments that take on their own access management when they start using cloud and SaaS solutions.

Many organizations lack a detailed onboarding policy that specifies which job titles are permitted to have access to systems, roles and resources. As a consequence, access requests for new employees often sound like this: "New employee Rachel needs access to System A like Jody, System B like Phillip, and System C like Alexis. " Requestors don't really know what new employees need, but they're pretty sure that if their access were similar to existing em-

Many organizations lack a detailed onboarding policy that specifies which job titles are permitted to have access to systems, roles and resources.

ployees, then new employees would be able to get their jobs done. The problem with this approach is that existing employees might have far more access privileges than they actually need, often as
a result of job "movers," who accumulate privileges.

Employees who stay on for more than a couple of years often move from position to position as their skills grow and the organization's needs change. The result is known as accumulation of privileges: seasoned employees have access to systems, roles and resources needed for their current job, as well as positions they have held in the past. But organizations that become aware of this problem are often unable to effectively deal with it. When employees transfer from one job to another; rarely do they make a clean break in which their old, job-specific

roles can be removed. Usually, employees who have transferred to a new position still have responsibilities in their former position, perhaps until a new person is hired, a new hire or another transfer is trained, or they have completed some projects. Organizations often forget that those older privileges need to be removed.

When employees leave the organization, their access to all internal and external systems and facilities is revoked immediately. This is particularly critical when workers are being terminated, a circumstance in which the consequences of IT errors can be devastating. It is even more complicated in organizations that utilize systems and applications where each has its own isolated access management systems.

The proliferation of compelling Web-based applications and services has resulted in organizations whose departments have begun to use SaaS and other cloud-based services. Employees often manage access to these services within their own departments. The problem here is that the employees, who manage access to these unsupported services, are usually not aware of corporate IT's access policies or processes. Moreover, users' access to these services is not tied to centralized access services such as Microsoft Active Directory, IdentityMinder or SiteMinder. When employees transfer or leave the organization, their access to these unsupported systems will generally persist for months, or even years. Situations like this can go undetected for years until an incident occurs.

ESTABLISHING IAM BUSINESS RULES

As organizations grow and encounter IAM problems, IT and management generally reach a consensus that business rules must be established. Controls must be effective and reliable if organizations are to regain control of their access management programs. The following is a blueprint for IAM business processes:

- **Corporate HR manages the who-works-here system of record.** Human resources is the organization responsible for tracking the full-time and part-time employees in the organization. To be effective, HR must also manage the temporary workers including contractors, consultants, interns and temps. This must also include personnel in external service organizations who access the organization's systems and resources. The information about personnel resides in the HR information system, or HRIS.

- **Employee HR data must flow from the HRIS to a central directory service.** As the official system of "who-works-here" record, key transactions from the HRIS flow to the organization's centralized access directory, through a workflow system.

- **A centralized directory service that can scale.** Simplicity and scale are the drivers that compel many organizations to rely on a single authentication service,

whether it's a pure directory service such as Active Directory, LDAP or a cloud-based service such as SafeNet. While the compromise of a user's centralized credentials means an attacker can reach more applications and systems, consider the alternative: separate credentials for each application. This leads to users choosing poor passwords or writing them down. The overhead of having multiple access control systems to manage adds complexity and introduces more opportunities for errors.

A centralized access management system will have visibility into all of the access rights that any given subject has.

- **Automated provisioning to streamline user account setup.** The process of setting up user accounts manually is time consuming and prone to error, and may even be subject to abuse. When properly controlled by workflow, additions and changes to user accounts can be automatically fulfilled.

- **An IAM system that offers a built-in access matrix.** Typically, too daunting to implement manually, an IAM system can have an access matrix that pairs a subject's job title—and possibly other salient facts such as work location, business unit ID, and so on—to each role in a system. The intersection of job title and role can result in the following potential outcomes:

  - **Birthright:** Access is provisioned automatically
  - **Allowed:** Access is provisioned on request
  - **Reviewed:** Access is provisioned when designated approvers consent
  - **Exception.** Access is not provisioned unless executives approve
  - **Prohibited:** Access is not provisioned under any circumstances

- **A workflow system to manage access requests.** Rather than blindly allowing all access requests to be fulfilled automatically even when they obey access matrix rules, many organizations may opt for one or more levels of review, and require approval of each access request. Depending on risk, sensitivity of data, or the "quality of fit" in the access request, a workflow system can require approval of resource owners, infosec staff, and others as needed.

- **Define rules for segregation of duties, and implement them electronically.** A centralized access management system will have visibility into all of the access rights that any given subject has. Any new request

should examine the request access and compare it with all access rights currently held by the subject, to see whether any "toxic combinations" of access rights would result. One example is if an employee in the accounting department has the dual roles of payment request and approval, which normally must be held by separate people.

- **Detailed recordkeeping is a basic requirement.** Every element about an access request—review, approval and provisioning—must be documented in a way that makes it easy to research requests and approvals to see who was involved.

- **Reviews and audits need to continue even with IAM systems in place.** It is still necessary to periodically review users' access rights. The primary reason is to determine whether every person in a certain role still requires access to those roles. These periodic reviews should include the master access matrix, workflow and approval rules, and rules for segregation of duties. Another reason for periodic reviews is to verify that approvals were made properly. It's also a good idea to make sure that the basic worker termination process is working by comparing HR records of existing workers.

Any organization operating a comprehensive controls framework such as COBIT needs to determine which of those controls will be implemented in the IAM system, and which ones will be external to it.

OPERATING MULTIPLE IAM ENVIRONMENTS

Disruptive growth via mergers and acquisitions may result in organizations having an IAM system for some of their applications and manual processes for others, or multiple IAM systems.

Many of today's IAM tools include the means for acquiring access rights info straight out of target systems—some easier, some less so.

To achieve better operational consistency and scale, most organizations will try to get back to having a single IAM platform for all of their principle systems and applications. Migrating authentication/authorization, or even just the workflow and provisioning, can be a tricky affair.

However, many of today's IAM tools include the means for acquiring access rights info straight out of target systems—some easier, some less so. Many IAM vendors include these features to make it easier for an organization to bootstrap its first IAM platform, but this

also makes it easy to switch from one IAM system to another, or to combine a mixed environment into a single, monolithic system.

SELECTING AND OPERATING THE SYSTEM

If your organization intends to implement a centralized authentication and authorization system—SiteMinder, instead of an internal Active Directory, for example—then evaluating internal and cloud-based applications with centralized and cloud-based authentication/authorization systems is essential.

During IAM system evaluation, an on-site proof-of-concept may be useful, but generally the scope is limited, so you need to carefully select applications for IAM system testing. Most organizations that implement IAM systems will have applications that IT chooses not to pipe-in to automatic provisioning.

Organizations that undertake the initiative to acquire IAM systems need to understand how authentication, data flows, workflows and account provisioning will work in their own environments. It may be necessary to survey all in-scope systems to determine the viability of integrating authentication and account provisioning. Each system will have its own integration issues, which you should identify beforehand. ■

PETER H. GREGORY, *CISA, CISSP, DRCE is an information security manager, computer security specialist, and writer. He is a 30-year IT veteran, having worn every hat and coat in the IT closet. Send comments on this column to feedback@infosecuritymag.com.*

BOTNET TAKEDOWNS: A DRAMATIC DEFENSE, BUT DOES IT CHANGE THE GAME?

Multilayered defense and user education are the best strategies against botnets.

By Kathleen Richards

BOTNETS REMAIN a major challenge for infosec professionals. Companies such as Microsoft and Symantec have proclaimed success using legal and technical countermeasures to disrupt a few of the Internet's more egregious botnets, but we're not likely to shrug ourselves free of this scourge anytime soon. The growing sophistication of the malware used to propagate bots—seen, for example in 2012's peer-to-peer ZeroAccess bot—combined with creative monetization schemes, make botnets resurface almost as quickly as they are knocked down.

After a CrowdStrike dismantling in March 2012, the Kelihos 3 botnet, reestablished itself within 20 minutes of a significant takedown. There are steps security pros can take to help keep bots off their networks, but the infections and cyberattacks that botnets are sometimes used to launch, remain hard-to-detect malware threats for websites and increasingly, mobile devices.

As much as anything, botnets are about the money. Consider the ZeroAccess bot. First identified in 2011, ZeroAccess ranked at the top of security researchers' malware threat lists in Q4 2012. The peer-to-peer bot

network is estimated to have 200,000 "supernodes" controlling 10 times that number of zombie computers at any given time, according to Kindsight Security Labs.

ZeroAcess exemplifies what security researchers say is a growing problem for Google's AdWords, Microsoft's Bing Ads (formerly Adcenter) and online advertisers—automated monetization schemes known as malvertising and pay-per-click ad fraud. Botnet masters can infect and partially control millions of zombie computers, which, unknown to end users, click on ads hosted on legitimate and fraudulent websites in an effort to game pay-per-click advertising on online search engines.

"From a malvertising perspective, we see an increasing trend of ads whose destinations are modified by the bots to other sites, which probably paid the bot masters for that service," said Ziv Mador, the director of security research for the SpiderLabs team at Trustwave.

"Every 15 minutes [ZeroAccess] will contact the Command and Control [C&C] site and get a list of ads to click on and it continues to do that throughout the day, 24/7," said Brendan Ziolo, vice president of marketing at Kindsight, which estimates that the ZeroAccess bot is earning about $1 million per day. "They are basically getting paid to click on ads hosted on people's websites. Potentially, they are actually operating these websites that are clicking on the ad," he said. "On an individual bot basis, it is tiny, but when you add it up to the full size of the botnet itself, it can become quite significant."

Nor is click fraud, the only scheme out there for making botnets profitable. In the case of Bitcoin mining, the network of bots, literally, create money out of computer processing cycles. The workings of Bitcoin, perhaps the most widely used alternative non-state-issued currency in the world, are beyond the scope of this article, but currency within the system is given value by its scarcity; and in this system, the scarcity is created by requiring that money be processed by computationally intensive procedures. Having a great deal of computational power enables you to create Bitcoin value more quickly.

> **"We see an increasing trend of ads whose destinations are modified by the bots to other sites, which probably paid the bot masters for that service."**
>
> *— Ziv Mador, director of security research, Trustwave*

Harnessing that power from computers owned by others means you are able to do it at no cost. It's the sort of application a botnet creator might dream of.

Kindsight offers botnet detection and remediation services to Internet service providers. The company's

Network Intrusion Detection System uses an offline sensor, which is deployed at aggregation points on service provider networks. It analyzes network traffic using signature-based intrusion detection technology that hones in on the protocols used in C&C and peer-to-peer communications, according to Kevin McNamee, the security architect and director of Kindsight Security Labs. The C&C protocols are far less likely to change than the malware itself, which is modified and repackaged continually to outpace antivirus software—to the tune of about 15,000 distinct versions of the ZeroAccess bot in the lab's malware sample database.

Last year, two versions of the ZeroAccess bot consistently ranked as active, high-level threats, according to Kindsight's analysis of data collected from its service provider deployments.

The newer version, Botnet.ZeroAccess2, which emerged in Q2 2012 and uses an UDP-based C&C protocol, ranked as the top high-level threat in the second half of the year. Botnet.ZeroAccess1, which uses an encrypted P2P protocol, according to Kindsight's data, dropped to 12th by Q4 2012 and appears to be "winding down."

At the RSA Conference 2013 in February, Kindsight introduced a Botnet Security Service to address what it said is a growing problem. According to company data, malware generated by various botnets accounted for four out of the top five home network infections in 2012: Win32.Bot.ZeroAccess, Win32.Backdoor.TDSS, Win32.Trojan.Alureaon.A and MAC.Bot.Flashback.K/I. Of the 13% of home networks infected with malware in 2012, almost 50% had a botnet-related issue, and 7% of broadband customers were infected by a botnet, banking Trojan or rootkit.

Macintosh systems were not immune. The Mac Flashback bot, used for ad-click fraud and to steal passwords, emerged as the top malware threat in Q2 2012, according to Kindsight's data. At its peak in April 2012, it infected 1.1% of homes—roughly 10% of homes with Mac computers, according to the researchers' estimates. Spread via a Java applet, the fake Adobe Flash update, ended the year in the top five home network infections detected in Kindsight deployments.

BLASTS FROM THE PAST

Previously, botnets, such as Cutwail, were spam-based, observed Ziolo. The botnets sent out massive numbers of unsolicited emails per day, but most researchers have seen declining levels of spamming. According to Kindsight's data, this trend continued in the second half of 2012.

Trustwave has reported similar findings. "The volume of spam has significantly decreased during the last couple of years," Mador said. "However, a much larger portion of it now includes malicious links and attachments, and the impact on users is, therefore, higher."

According to the 2013 Trustwave Global Security Report, released in February, 75.2% of inbound emails at most organizations are considered spam, and 10% of it is malicious. Cutwail sends 80% of the malicious spam, while 85% of "general" spam is generated by seven botnets, out of thousands.

The Fortinet security team expects to see new forms of Denial of Service attacks in 2013, stemming from cross-platform botnets made up of infected mobile devices and infected PCs.

Used in tandem with exploit kits, botnets are reaching even higher levels of criminal activity and effectiveness, according to Mador. "The malicious spam often includes links to pages of exploit kits, most commonly Blackhole," he said. "The exploit kit uses an arsenal of exploits to infect the local computer. Then typically it installs malware." Trustwave's research indicates that these types of campaigns actually work; in one instance, 10% of users clicked on the malicious message link to the Blackhole server.

Malware is also using sophisticated methods to embed itself and hide, according to researchers. "Botnet.ZeroAccess.1 actually installs two copies of itself, so that if one copy is detected and eradicated, the other copy just takes over," said Ziolo," so they have built redundancy into the whole system itself."

MOBILE MALWARE THREAT

Botnets for mobile networks have started to emerge and some security researchers expect the numbers to increase in 2013. "The term botnet here would be applied loosely as a system that can send and receive C&C messages to a central host," explained Mador. Spam Soldier is an SMS spamming botnet that is used to send premium rate messages on Android devices without the users' knowledge—until they see the bill.

A mobile version of the Zeus banking Trojan—known as Zeus in the Mobile or Zitmo—emerged in 2011, according to Derek Manky, global security strategist at FortiGuard Labs, a division of Fortinet Inc. Zitmo targets multiple mobile platforms and has been known to bypass SMS two-factor authentication, to steal banking data using mobile transaction authentication numbers.

Security researchers at FortiGuard Labs studied Zitmo in 2012, and determined that it has many of the same features and functionality as PC botnets. Based on this feature parity, the security team expects to see new forms of Denial of Service attacks in 2013, stemming from cross-platform botnets made up of infected mobile devices and

infected PCs, which are simultaneously acting on commands from the same C&C and attack protocol.

As employee-owned smartphones and tablets take hold in the workplace, the bring your own device (BYOD) environment poses malware threats for enterprises. "The real danger with BYOD is that most organizations have a fairly unsecured and uncontrolled device on the internal network," said Mador. "It would be easy to spearphish one user in an organization to install one bad piece of Android malware." Organizations should use firewalls to separate BYOD devices from the rest of the corporate network, he advised, with adequate protections from internal and external threats.

Security researchers expect to see more issues related to Android malware in 2013. Android malware also ranked in Kindsight's top 20 malware threats for the first time in Q4. The Trojan.Wapsx is described by researchers as a "trojanized app" that steals information from Android devices. According Kindsight, 0.5% of mobile devices—Android and laptops tethered to mobile devices and networks—were infected with high threat level malware in Q4 2012 up from 0.3% in Q3 2012.

BOTNET TAKEDOWNS

Trustwave's Mador does not see signs that botnets are increasing. "But as with the other metrics," he cautioned, "it doesn't necessarily reflect on the threat that these botnets impose on consumers and on businesses."

Security researchers expect to see more issues related to Android malware in 2013.

The Microsoft Digital Crimes Unit has worked within the legal system, and with technical partners, to successfully disrupt six botnets in three years.

Earlier this year, Microsoft partnered with Symantec to disrupt the Batimal botnet, which the companies claimed was infecting 8 million computers and hijacking online searches in order to perform ad-click fraud. Microsoft filed a lawsuit on January 31, 2013 against the botnet's operators "to sever all the communication lines between the botnet and the malware-infected computers under its control," according to blog written by Richard Domigues Boscovich, assistant general counsel, Microsoft Digital Crimes Unit. The court agreed with Microsoft and the company seized evidence from the botnet's Web hosting facilities in New Jersey and Virginia, with help from U.S. Marshals on Feb. 6. In what many viewed as an unprecedented move, Microsoft used C&C communications to forcibly redirect infected Windows computers to a Web page that told users about the malware and how to remove it.

"Microsoft's activities are important because quite

often they end up with bringing the people behind these criminal activities to justice," said Mador, formerly a Microsoft Malware Protection Center senior program manager, who worked closely with the Digital Crimes Unit during his 15-year tenure at the company. "That raises the risk for people who are involved in cybercrime or who consider doing that."

Devices that rely on URL reputations may not be as effective when it comes to blocking exploit kits.

Without international cooperation, botnets can simply switch servers and re-emerge within minutes or hours. Botnet organizations often choose Russia and Eastern Europe as a base because it is easier to avoid prosecution, according to Fortinet.

"The key thing that needs to happen to get this to expand further," said Alex Harvey, Fortinet security strategist, "is we need to get an international approach. So that if we determine that a botnet is sending millions of messages a day—the command servers are in Russia, part of the infrastructure is in Spain, and the bots are in North America—there has a be a way for all of these groups to cooperate in real time, or really quickly. Because when you take down a botnet, if you don't take down the whole structure at the same time; it is very easy for these guys to seize control and redirect all that traffic somewhere else."

At the RSA Conference 2013 in February, Tillmann Werner, the senior security researcher at CrowdStrike Inc. demonstrated a real-time takedown of a global peer-to-peer network. The demonstration was based on attacking the Kelihos botnet using a sinkholing technique to replace C&C communications on a P2P network. During the demonstration, Werner showed how he had coordinated the takedown with government and law enforcement organizations.

MULTILAYER DEFENSE

In addition to policies and disaster planning, security researchers advise enterprises to adopt a multilayer strategy to defend corporate assets against botnet infections and the DDos attacks that botnets may be harnessed to carry out.

According to Trustwave, a defense strategy should include the following:

- **Secure Web gateways.** These appliances filter Web traffic and block malicious content. Devices that rely on URL reputations may not be as effective when it comes to blocking exploit kits. "We saw one exploit kit, which modified its links on an hourly basis," said Mador.

- **Secure email gateways.** These devices keep spam, including messages with malicious links and attachments, from reaching corporate email boxes.

- **Antivirus software.** "These products can still block infection by bots quite often," said Mador, "in spite of the spike in the number of malware samples, and how frequently they are updated."

- **Web application firewall.** A server plug-in, appliance or filter designed to protect Web servers at the application-layer, by blocking code injections such as cross-site scripting, malicious links and files.

It's important to know how botnets work, and to continue to educate end users about best practices when it comes to opening email attachments and downloading unknown software.

Finally, organizations must also pay attention to attacks that cause their own servers to be used as a malware distribution point. Once a server has been detected as compromised and now distributing botnet malware, websites hosted on it have to be thoroughly cleaned, according to Mador. And this includes databases running "behind" the website: This means scanning the content carefully, looking for non-alpha numeric characters, hidden links and related elements, and checking the integrity of connected databases. "In the case of SQL injection," said Mador, "some database entries may include short script code."

Expect an increase in malware activity throughout the balance of 2013. And expect it on mobile devices as well. As with other aspects of security, a multilayered defense and continuing end user education offer the best strategy against botnet infections. ■

KATHLEEN RICHARDS *is the features editor at Information Security magazine. Contact her at krichards@techtarget.com.*

ADDRESS IPv6 BEFORE YOUR SECURITY TIMES OUT

Most networks already have partial deployment of IPv6, even if IT doesn't know it.

By Fernando Gont

TIME AND SPACE—address space, that is—are running out.

Internet Protocol version 4 (IPv4), the networking standard on which the Internet has been built, is expected to reach its IP address limit of roughly 4.3 billion in a few years. While most enterprises can survive for now with just a handful of IP addresses thanks to Network Address Translators (NATs), which allow multiple devices to be connected to the public Internet with a single public IPv4 address, the growing number of Internet-connected mobile devices and non-traditional objects—cars, appliances and smart meters—demands that the Internet's phone book expand its listings.

Enter Internet Protocol version 6 (IPv6). IPv6 was designed to succeed IPv4 and accommodate the future growth of the Internet by providing a much larger address pool than IPv4. Hopefully, this isn't the first time you've read about IPv6: awareness activities, such as the World IPv6 Launch Day, and the deployment of IPv6 in large content providers such as Google and Facebook, has been

going on for years, and recently resulted in a spike of emerging IPv6 deployments and global IPv6 traffic.

Enterprise information security teams have largely been able to ignore IPv6, until now. A wave of adoption among Internet infrastructure providers and network product vendors is about to crash over enterprise IT departments; many teams that haven't worked with IPv6 before will suddenly be charged with securing it.

IPV6 SECURITY IMPLICATIONS

There are a number of reasons why organizations should be concerned about the security implications of the IPv6 protocol suite. First, most operating systems include some sort of IPv6 support by default; this means that networks have at least partial deployment of IPv6, often without IT realizing it. The IPv6 support could be leveraged by attackers for a number of malicious purposes such as evading network security controls or triggering VPN leakages.

Secondly, IPv4 and IPv6 will co-exist for some time, so it will become common for allegedly "IPv4-only" nodes to communicate with IPv6 nodes through the aid of transition or co-existence technologies. This means attackers can more easily obfuscate attacks using IPv4 and IPv6. Finally, many organizations will need to deploy IPv6 sooner or later, and quickly learn the ins and outs of IPv6 security so that an informed deployment and transition plan can be implemented.

IPV6 SECURITY CONSIDERATIONS

While it is tempting to analyze the security implications of a communications technology based on a security assessment of the technology, the effective security level of emerging IPv6 deployments will depend on several facets coming together:

- Expertise of the technical personnel with respect to the IPv6 protocol suite
- Availability of skilled human resources
- Maturity level of IPv6 implementations
- IPv6 support in security products
- Complexity of the resulting networks, and of the Internet in general

Most enterprise IT staffs have many years of experience with the IPv4 protocols. This experience is not only reflected in the staff's ability to build networks, but also its ability to detect problems, and to differentiate between normal vs. anomalous traffic patterns. The same personnel typically have little to no experience with IPv6.

As a result, many IPv6 deployments may overlook security implications, and communications will be subject to fewer controls than their IPv4 counterparts. Therefore, IPv6 will likely become "the weakest link in the chain" of an organization's network security.

Even if an organization decides to hire specialists in this area, or to outsource IPv6-related tasks, the lack of

highly skilled professionals will become evident as IT consultants remain focused on the larger pool of IPv4 clients. This will not only have an effect on consulting and hiring costs, but may also mean that these tasks might end up being carried out by personnel with sub-optimal skills.

The maturity of implementations plays an important role in the security of emerging IPv6 deployments. Software has bugs, and it will take time for IPv6 implementations to reach the maturity level of IPv4 implementations. Based on the number of vulnerability advisories that have been published over the years about IPv4 implementations, it is not hard to conclude that it has taken quite a few years for IPv4 implementations to achieve acceptable maturity levels.

IPv6 is no different in this respect. Software bugs with security implications might be discovered and maliciously exploited by attackers, before vendors get a chance to fix them.

Besides the technical expertise of the IT staff, and the virtues, or lack thereof, of the IPv6 protocols, the effective security level of emerging IPv6 deployments will depend, to a large extent, on the availability of IPv6 security products, and the security features in the products. After all, these are the tools that finally enforce security controls on a network.

Security products today have less support for IPv6 than for IPv4 in terms of variety of products, availability of features and performance. Many firewalls simply do not support IPv6. When products claim to support IPv4 and IPv6, it is not unusual for them to contain more IPv4 features. And even when a security product claims to have feature parity, there might still be differences in how those features are implemented. It is not unusual for security devices to implement IPv4 functionality in hardware, and IPv6 functionality in software. Therefore, a security device might be able to handle some packet rates for IPv4, but unable to support the same traffic levels in IPv6—and this limits the scenarios in which IPv6 functionality can be deployed.

The maturity of implementations plays an important role in the security of emerging IPv6 deployments.

Finally, since IPv6 is not backwards-compatible with IPv4, there are a variety of transition technologies that aim to facilitate the co-existence of both Internet protocols, and eventually, complete migration to IPv6. These technologies range from dual-stack, to tunnels—whether configured or automatic—translators (NAT64, CGN) or different types of proxies. As the number of IPv6

deployments increase, so will the use of such transition technologies. Whether an organization deploys IPv6 or not, the Internet as a whole will become a far more complex network than the one we are used to today. This will have implications on every aspect of network operation and management, including security. When tracing an attack source, you may have to trace the attacker behind one or more translators, tunnels, and the like. When monitoring network traffic for malicious patterns, the use of tunnels might make traffic analysis much more difficult—if at all possible—than in IPv4.

IPV4 VS. IPV6: A BRIEF COMPARISON

From a functional point of view, IPv6 is no different from IPv4: it simply provides a "best effort" datagram delivery service. However, IPv6 uses different protocols and mechanisms to provide such service, and that is where most of the operational and security implications arise.

While a number of myths continue about the properties and benefits of IPv6, the only concrete improvement IPv6 has over IPv4 is its increased address space. This increased address space has a number of straightforward implications:

- With plenty of IPv6 addresses, it is likely that every host connected to an IPv6 network will be assigned a global IPv6 address. This global addressability might in turn increase host exposure.
- IPv4 NATs enable multiple devices to connect to the public Internet using a single public IPv4 address, but firewall functionality is limited to "only allowing outgoing connections." Emerging IPv6 deployments will not need to employ NATs. Unless a proper firewall is deployed to protect internal nodes, IPv6 deployment might result in increased host exposure. Although different, this is closely related to the global addressability issue.
- The typical IPv6 subnet is composed of 264 addresses, so it will have a much lower host density (i.e. number of hosts per number of available addresses). This will make traditional address scanning "attacks" more difficult than in IPv4. As a result, security practitioners will have to evolve how they do network reconnaissance when performing penetration tests.

Other than the increased address space, IPv6 protocols tend to have increased extensibility. An IPv4 packet can carry a maximum of 40 bytes of options, whereas an IPv6 packet can—at least in theory—carry an unlimited number of options. Unfortunately, this flexibility is seldom used for legitimate purposes; which makes the enforcement of security policies and monitoring of network traffic much more painful.

Most aspects that play a key role in the security implications of IPv6 are not related to the technical features

of the IPv6 protocols including the limited availability of skilled personnel and IPv6 security products, and the lack of mature IPv6 implementations.

> Some argue that the increased address space will mean that all IPv6 nodes will be directly reachable from the public IPv6 Internet.

IPV6 SECURITY MYTHS

One of the myths that has been created around IPv6 is that it has "improved security." However, generally speaking, there are no security features in IPv6 that were not readily available for IPv4.

It is widely assumed that "IPv6 will lead to increased IPsec usage," probably because, from a protocol-specifications point of view, IPsec support used to be mandatory for IPv6 implementations but not for IPv4 implementations. In practice, however, many IPv6 implementations never honored this requirement to an extent that this requirement has been removed from IPv6 implementations. And, even then, IPsec implementation or support does not necessarily result in IPsec usage. Many issues that led to a low level of deployment of IPsec are still valid for IPv6, and there are no legitimate reasons to believe that the actual use of IPsec will increase with the deployment of IPv6.

Finally, some argue that the increased address space will mean that all IPv6 nodes will be directly reachable from the public IPv6 Internet—a property usually referred to as "end-to-end connectivity"—and that, as a result, the security paradigm will change from network-centric to host-centric. Note, however, that most IPv4 networks currently employ a "hybrid" security paradigm, and that will continue with IPv6. Any changes in this area will not be motivated by IPv6 itself.

WHERE TO GO FROM HERE

It should now be evident that the security implications of IPv6 should be a concern not only to organizations planning to deploy IPv6, but also to organizations operating—allegedly—IPv4-only networks. A number of actions are warranted to mitigate the security implications of IPv6, and to allow for a smooth transition to this "new" Internet protocol:

1. Training of key technical staff
2. Mitigation of IPv6 security implications on—allegedly—IPv4-only networks
3. Creation of a test lab for the IPv6 protocols, devices, and applications
4. Development of an IPv6 deployment plan

Training key technical staff is mandatory to address

the challenges presented by the new Internet protocol. This is independent of whether an organization plans to deploy IPv6 in the short or near term.

Most general-purpose systems include some sort of IPv6 support "enabled by default," so concrete actions—such as enforcement of packet filtering—are needed in order to mitigate the security implications of IPv6 on the existing "IPv4-only" networks.

Since the necessary expertise can only be learned through practice, it will be essential to build an "IPv6 test lab," separate from any production networks, on which technical staff can build their expertise with the IPv6 protocols—virtualization technologies might be of help in this area.

Finally, an IPv6 deployment plan should be established to prepare for the deployment of the new Internet protocol. This plan need not imply IPv6 deployment through the organization in the short term, but rather prepare the organization for eventual IPv6 deployment. The deployment plan should cover IPv6 training of all technical staff, IPv6 requirements when purchasing software or hardware devices, and an IPv6 test lab.

Sooner or later your organization will need to deploy IPv6—in fact, your network probably already has partially deployed IPv6. It's time to take stock of the security implications before the attackers do. Time is indeed running out. ■

FERNANDO GONT *is a networking and security consultant, who has worked on a number of projects on behalf of the UK National Infrastructure Security Coordination Centre and the UK Centre for the Protection of National Infrastructure. Gont is an active participant at the Internet Engineering Task Force, where he contributes to several working groups and has authored a number of Request for Comments. Send comments on this column to feedback@infosecuritymag.com.*

TechTarget

TechTarget Security Media Group

EDITORIAL DIRECTOR **Robert Richardson**

SENIOR MANAGING EDITOR **Kara Gattine**

SENIOR SITE EDITOR **Eric Parizo**

FEATURES EDITOR **Kathleen Richards**

DIRECTOR OF ONLINE DESIGN **Linda Koury**

COLUMNISTS **Marcus Ranum, Gary McGraw, Doug Jacobson, Julie A. Rursch, Matthew Todd**

CONTRIBUTING EDITORS **Michael Cobb, Scott Crawford, Peter Giannoulis, Ernest N. Hayden, Jennifer Jabbusch Minella, David Jacobs, Nick Lewis, Kevin McDonald, Sandra Kay Miller, Ed Moyle,Lisa Phifer, Ben Rothke, Anand Sastry, Dave Shackleford, Joel Snyder, Lenny Zeltser**

USER ADVISORY BOARD

Phil Agcaoili, Cox Communications
Richard Bejtlich, Mandiant
Seth Bromberger, Energy Sector Consortium
Mike Chapple, Notre Dame
Brian Engle, Health and Human Services Commission, Texas
Mike Hamilton, City of Seattle
Chris Ipsen, State of Nevada
Nick Lewis, Saint Louis University
Rich Mogull, Securosis
Tony Spinelli, Equifax
Matthew Todd, Financial Engines

VICE PRESIDENT/GROUP PUBLISHER **Doug Olender**
dolender@techtarget.com

TechTarget
275 Grove Street,
Newton, MA 02466
www.techtarget.com

About TechTarget: TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.

COVER IMAGE: FOTOLIA