THE BANKING MALWARE SCOURGE | INSIDE WINDOWS 7 SECURITY

INFORMATION SECURITY®

MAY 2010

DATA: Do You Know Where It's Going?

Database activity monitoring keeps watch over your data

TechTarget

INFOSECURITYMAG.COM

contents

MAY 2010

VOLUME 12 NUMBER 4

FEATURES

ALSO

Lacking Details

The Cybersecurity Act of 2010 has potential but raises a lot of questions. BY MARCIA SAVAGE

t

THE ROCKEFELLER-SNOWE cybersecurity legislation is promising on several fronts, but if you actually plow through the bill's text, you'll find some questionable provisions and parts that beg for clarification.

To be sure, the new draft of the Cybersecurity Act of 2010 (S. 773) is an improvement over last year's version, which included an infamous "kill switch" that would give the president the authority to shut down the Internet in the event of a massive cyberattack. The idea went over like a lead balloon and Sen. Jay Rockefeller, who co-sponsored the revised legislation with Sen. Olympia Snowe (R-Maine), was careful to note that it "does not give any new or broader authority to the president." However, it does allow the president to declare a cybersecurity emergency—without defining what would constitute a cybersecurity emergency.

Rockefeller says the legislation is designed to prepare the U.S. for a major cyberattack by providing a framework for private-public sector collaboration. Among other things, the bill would support major new R&D into cybersecurity, establish a certification program for security professionals, initiate a new cybersecurity public awareness campaign, and call on the private sector and government to share threat and vulnerability information.

Rockefeller says the legislation is designed to prepare the U.S. for a major cyberattack by providing a framework for private-public sector collaboration.

Certainly, the bill takes several positive steps. With new threats emerging all the time, more cybersecurity R&D and increased efforts to develop and recruit the next generation of information security pros are critical. And the bill addresses a long-standing sore spot in the security industry by supporting research into integrating secure coding into core computer science curriculum.

But here's where it gets sketchy. The legislation also includes a plan for "positive recognition" for critical infrastructure companies that report compliance with cybersecurity risk measurement techniques and best practices. NIST is designated as the body to recognize and promote these best practices, but it's unclear what they would be. Moreover, how many companies would be eager to publicly proclaim themselves secure? What about a company that doesn't receive the positive recognition? Either way, a company could become a target for hackers based on public disclosure about the state of their security, says Paul Rohmeyer, a faculty member in the graduate school at Stevens Institute of Technology and consultant. "It's a bad idea all around," he says.

The legislation also doesn't account for differences between industries and doesn't describe how it relates to existing mandates such as Gramm-Leach-Bliley, Sarbanes-Oxley and HIPAA, Rohmeyer says. Also, the creation of a training and certification program for critical infrastructure security pros will create a huge market for trainers, he adds, but there's no provision for how the trainers themselves would be qualified.

Other parts of the bill—like the call for public-private collaboration on cybersecurity and information sharing—are nothing new. Perhaps giving cleared private sector executives access to classified threat information, as the legislation proposes, would make a difference. However, as industry analyst Richard Stiennon points out, the FBI's InfraGard already provides businesses with threat information.

Ultimately, how much the Cybersecurity Act would prepare the country for a cyberattack is anybody's guess. Rohmeyer for one isn't convinced it would help. He's hesitant to be too critical—cybersecurity legislation is needed and this bill is generally headed in the right direction, he says—but it leaves too many unanswered questions.

"If I'm a compliance officer in a company that's in one of the critical infrastructure industries, I don't know what my obligations are under this law," he says.

The Rockefeller-Snowe cybersecurity legislation is a good start but needs some work to truly address the country's pressing cybersecurity needs and not create more compliance headaches for businesses. ▸

Marcia Savage is editor of Information Security. *Send comments on this column to feedback@infosecuritymag.com.*

COMING IN JUNE

Endpoint Encryption

Increasingly mobile workforces mean more sensitive customer and corporate data floating around on laptops outside the enterprise. A lost or missing laptop could have costly and damaging consequences. But organizations can protect data on laptops – and avoid breach notification requirements - with encryption. This feature will examine the different types of laptop encryption available, including full disk, file/folder, and pre-encrypted drives. It also will cover deployment options (key management and policy management) and look at the product landscape, including both commercial and open-source tools.

Cloud Computing Risks

Business managers are eager to move enterprise operations to a cloud computing model in order to cut costs. However, security managers remain wary of the risks associated with cloud computing. In this feature, we'll examine how enterprise risks change with cloud computing, what use cases are best suited for the cloud, and what information security pros should do to prepare for moving into the cloud. We'll also look at emerging standards for cloud computing.

Governance, Risk and Compliance

Governance, risk and compliance is a term that's been hyped in the industry to the point where it's become a catch-all phrase for most information security strategies and various products. The promises of GRC–reduced risk and streamlined compliance–were obscured. This feature will look at how an organization can successfully develop a GRC program to achieve those goals. It will offer strategic advice for enterprise security managers and include an examination of tools and frameworks in the GRC market.

In every issue: *Information Security* magazine is the insider's publication for security professionals. In every issue, we tackle the trends and technologies that most impact your day-to-day responsibilities. We complement that coverage with opinion from our editors, the industry's leading practitioners and experts such as Bruce Schneier and Marcus Ranum.

MUST READ!

Early Case Assessment
Pre-Collection Analytics
Legal Hold
EnCase eDiscovery
Analysis/ Review
Preservation & Collection
Processing

The Real Risk Equation

BY RON WOERNER

A simplified risk equation helps translate risks to users and allows security to partner with the business.

RISK MANAGEMENT is a fundamental requirement of information security. Without it, the safety of the information or system cannot be assured. In information security, risk is a variable that must be understood in order to best create cost-effective solutions to minimize negative risks with minimal impact to usability and cost. Risks are often uncertain, misunderstood, and can change based on circumstances. Risk management provides a way for you to understand and handle risks that are optimal for security, IT, and the business. It creates a common language to identify, assess, and understand potential threats and vulnerabilities while identifying means for mitigating, accepting, or avoiding the risk.

However, one of the reasons we have difficulty in translating risks to our users is that many security practitioners maintain an unrealistic view of risk because we use an overly complex risk equation. It typically contains variables for threats, vulnerabilities, and mitigation. This isn't how people naturally think.

Security guru Bruce Schneier described this disconnect between users and security staff in an article published last year entitled, "People understand risks—but do security staff understand people?" He described how the way people think about risk works for people but can cause failures for security: "They know what the real risks are at work, and that they all revolve around not getting the job done… The risks of not following security procedures are much less real."

One of the reasons we have difficulty in translating risks to our users is that many security practitioners maintain an unrealistic view of risk because we use an overly complex risk equation.

Besides the disconnect with average users, there's another argument against a complex risk equation: the difficulty of quantifying the variables. Is it possible to put an accurate number to a threat or vulnerability? The numbers used in these cases tend to be biased based on the perspective of the assessors. If it's something they are familiar with or feel strongly about, they will always rank it high. Plus, the value of a threat or vulnerability is variable based on the use or user. For example, if your CEO has a keylogger on his PC, then this is a huge risk. However, for most line employees, there won't be as much damage if there is an incident. This fact is rarely a consideration when quantifying threats or vulnerabilities in a risk equation.

The risk equation I use is quite simple: risk equals impact multiplied by probability weighed against the cost: *Risk=Impact X Probability / Cost.* Impact is the effect on the organization should a risk event occur. Probability is the likelihood the event could occur within a given timeframe. Cost is the amount it takes to mitigate or reduce the risk to an acceptable level. This risk equation is how people naturally assess risks; in its simplicity comes its usability.

When assessing risks in this way, it helps to use a scale of one to five for the impact, probability, and cost variables. While it's subjective, it allows for some quantification of the risks in an easy-to-understand fashion. This also allows for the prioritization of the risks based on their total values.

When we identified a risk associated with Web browsing, this simple risk equation helped to influence a human resources director to take action. We needed the HR director to weigh in on the decision to block certain malicious websites, and I explained the problem to her. Without any prompting from me, she used the risk equation to understand the impact, likelihood of the risk and the cost of implementation, and ultimately agreed to our security measures. The simple risk equation allowed security to partner with the business and secure a potential vulnerability.

By using this simple risk equation, we can solve the conundrum described by Bruce Schneier. Through its simplicity, security staff can understand people by better understanding the true risks to an organization. And by working together, we all become stronger.▸

Ron Woerner is a security analyst at a large architecture and engineering firm in the Midwest. Send comments on this column to feedback@infosecuritymag.com.

Analysis | SECURE CODING

OWASP Adds Risk to the Equation

Organization aims to make Top 10 list of coding errors easier to use by adding risk to the methodology.

BY ROBERT WESTERVELT

THE OPEN WEB APPLICATION SECURITY PROJECT (OWASP) is hoping an overhaul of its top 10 vulnerabilities list will help enterprises more easily apply the list to their software development lifecycle. The organization changed the methodology it uses to categorize coding errors in the latest version of the top 10 list issued in April, adding risk to the equation.

"Wherever we rate a risk, we have a big question mark so that you can fill in your threat agent and your business impact," says Jeff Williams, volunteer chair of OWASP and a co-author of the OWASP Top 10. "You can rate these risks for yourself, for your application and for your organization."

It's the first time in three years since the last major revision to the OWASP list. Ultimately, the change in methodology has resulted in ranking the 10 most critical Web application coding errors by risk rather than vulnerability frequency. Factoring in risk has bumped injection errors ahead of cross-site scripting (XSS) flaws. It also stirred some debate in the organization, according to Williams, because two common coding errors that had long been on the list—malicious file execution and information leakage—have been dropped from the top 10. In their place are two new risk categories: unvalidated redirects and forwards and security misconfiguration errors.

The OWASP coding errors list was first released in 2004 and was modeled after the SANS Top 20 vulnerabilities list, which at the time focused on network security vulnerabilities, says Williams, who also heads Columbia, Md.-based application security services firm Aspect Security. While OWASP always tried to focus on risks, it used the term "vulnerabilities," creating some confusion, he says.

"People would look at the list and say that that's not really a vulnerability, that's more like an attack or that's more like an impact," says Williams.

For example, SQL injection is an attack, but people also use the term to describe an outcome when a SQL database gets compromised. People also use it to describe a vulnerability if a developer didn't do proper quoting or escaping of data that's gone to the database or failed to use a prepared statement that prevents injection.

"We're trying to mature people's understanding of application security a little bit," says Williams. "They shouldn't just be focused on vulnerabilities. They should really think about how vulnerabilities can be exploited in their environment and the impact a successful attack could have."

The purpose of the OWASP Top 10 is to raise awareness, but the changes to the list make it even more useful, says Ryan Barnett, an OWASP volunteer and director of application security training at Breach Security.

"You want something that's a bit more consumable for end users," he says. "If you start talking to C-level executives about vulnerabilities, their eyes glaze over. You have to start talking about risk and how it impacts the business."

> "If you start talking to C-level executives about vulnerabilities, their eyes glaze over. You have to start talking about risk and how it impacts the business."
>
> –RYAN BARNETT, OWASP volunteer and director of application security training, Breach Security

While vulnerability lists can get people thinking more about software security, they could be misleading, says application security expert, Gary McGraw, chief technology officer of Cigital, a provider of software security services.. McGraw has long been an outspoken opponent to the usefulness of public vulnerability lists.

McGraw studied 30 enterprises last year and developed what he calls a Building Security in Maturity Model (BSIMM), which includes a framework designed to help other firms put software security best practices in place. He says none of the firms he studied use publicly available vulnerability lists. The lists often can't be applied to an organization's specific use case, ending up helping auditors more than developers. McGraw advocates the use of code analysis tools to find bugs and a greater reliance on security requirements to conduct software testing.

"It's time to start doing science and talk about what's actually happening and the impact of what we're doing and no longer time to be theorizing from our arm chair," McGraw says.

OWASP's Williams says the list is no longer a simple catalog of bugs, but a starting point where companies can apply their specific risk profile to determine the areas that deserve the most attention.

"In our work we look at millions of lines of code every month and test lots of apps and there is a lot of commonality among Web applications," Williams says. "It's not a simple checklist. A lot of organizations are using it to improve their processes." ▸

Robert Westervelt is the news editor of SearchSecurity.com. Send comments on this article to feedback@infosecuritymag.com.

Avalanche of Patches

SECURITY PROS were deluged with multiple critical software patches from Microsoft, Adobe and Oracle, all released on April 13. Oracle's quarterly patch update covers 47 fixes and coincided with Microsoft's monthly update, which repairs several critical media handling vulnerabilities across its product line. At the same time, Adobe issued a critical security update for its Acrobat and Reader software.

—*Information Security* staff

Microsoft Security Bulletin • 11 security bulletins, including five critical, to fix 25 security vulnerabilities. One of the bulletins repairs a flaw in Microsoft MPEG Layer-3 audio codecs that could leave machines vulnerable to drive-by attacks. Another critical patch fixes a remote code execution vulnerability in Windows Media Player, which could be exploited via website hosting malicious media content. Another bulletin, rated critical on all versions of Windows including Windows 7, repairs two vulnerabilities in Windows Authenticode Verification that could allow an attacker to take complete control of a computer.

Adobe Security Bulletin • Quarterly update addressees 15 vulnerabilities in Adobe Reader and Acrobat, including buffer overflows and memory corruption flaws. With the update, Adobe rolled out its new updater service with the goal of keeping end users updated in a more streamlined and automated way. In beta testing since January, Adobe on April 13 activated the service for all users needing Adobe Reader and Acrobat 9.3.2 and 8.2.2 for Windows and Macintosh. The company says it has no plans to activate the automatic update option by default without prior user consent.

Oracle Critical Patch Update Advisory • 47 security patches across its product line, including seven fixes for Oracle Database Server, five patches for Oracle Fusion Middleware, eight fixes for Oracle E-Business Suite, and 16 fixes for the Oracle Solaris suite. Most of the patches are rated as critical. The next update from Oracle is scheduled for July 13.

OVER-HEARD

> "Cyberattacks that may constitute a national security threat are no longer science fiction."
>
> –JAAK AAVIKSOO, minister of defense of the Republic of Estonia, talking about the 2007 cyberattacks on Estonia

what drives *your* approach to IT security?

Balancing business priorities and risks is key to a solid approach.

SystemExperts helps you build a comprehensive and cost-effective information security plan that makes sense for your company. Right now, our **ISO 17799/27002 Compliance Program** helps you to focus resources on your most important business risks and comply with regulations such as **Sarbanes-Oxley, FFIEC, HIPAA, PCI,** and **Gramm-Leach-Bliley.** Best of all, our approach works equally well for "Main Street" businesses and the Fortune 500 clients we've proudly served for years.

If you want a practical IT security plan that addresses your real business risks, contact us today at 888.749.9800 or visit our web site at www.systemexperts.com/public.

- ISO 17799/27002 Compliance
- HIPAA and PCI DSS Compliance
- Application Vulnerability Testing
- Security Audits and Assessments
- Security Architecture and Design
- Identity Management
- Penetration Testing
- Security Best Practices and Policy
- Emergency Incident Response
- System Hardening
- Technology Strategy
- ASP Assessments

SystemEXPERTS
LEADERSHIP IN SECURITY & COMPLIANCE

Take Four Steps Toward an Information Security Career Plan

BY LEE KUSHNER AND MIKE MURRAY

Having a long-term information security career goal isn't enough. You must also understand your current skill set, set goals toward enhancing your capabilities and how to reach them.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
DATABASE ACTIVITY MONITORING
BANKING MALWARE
WINDOWS 7 SECURITY
SPONSOR RESOURCES

FORMULATING YOUR CAREER plan is the cornerstone of successful career. In our 2008-2009 survey of information security professionals, the research revealed those who have a career plan are more likely to hold senior titles, earn more money, and have increased job satisfaction. These findings demonstrate that effective information security career planning has a measurable impact on your success.

Like any successful information security engagement, career planning should be based on a solid methodology that will provide you with the best chance of achieving success. The four key components to career planning include: the development of a baseline; understanding your ultimate career goal; determining intermediate milestones; and planning in reverse.

1 DEVELOP A CAREER PLANNING BASELINE

Before starting on the career planning process, you need an idea of what your current situation is. Former General Electric CEO and management guru Jack Welch is often quoted saying that the first step in management of anything is to get a solid understanding of the reality of your situation.

Unfortunately, this is difficult for most people. Most of us are weak in at least a couple of key areas, and it's not fun to take stock of your weaknesses. So this is where a lot of people stop the career planning process; it's difficult enough to take the time to sit down and plan, but even more difficult if that process involves understanding what you're not so good at.

2 DETERMINE YOUR INFORMATION SECURITY CAREER GOAL

Once you know where you are, the next step is to figure out where you want to end up long term. Not surprisingly, most of our industry has some idea of this. When we asked about ultimate career goals in our survey, 37 percent responded they hoped to be a CISO/CSO, 20 percent said architect/subject matter expert, and 7 percent an entrepreneur.

If you have any of those goals, this should scare you because those people are your competition. If your goal is to be a CISO, think about this: When you go to the RSA Conference or Black Hat Briefings, three of every 10 people you run into share your career goal. And there are thousands of people at each of those conferences.

In choosing your outcome, realize that the competition is going to mean that you're going to have to work hard. If your goal is to be a penetration tester or a vulnerability researcher, you're going to have to put in long hours and a huge amount of effort to get there. And there will be tradeoffs and sacrifices.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

CAREERS

DATABASE ACTIVITY MONITORING

BANKING MALWARE

WINDOWS 7 SECURITY

SPONSOR RESOURCES

After you have decided on your goal, you should research which skills, education, and experience would be required to achieve that position. At that point, you should be left with an understanding of where you are currently and what kind of commitment, sacrifice, and personal investment you would need to make in order to achieve your long-term career goal.

At the end of this exercise, you will be able to determine your personal willingness to achieve this goal. If you determine that you are unwilling to put in the necessary work and professional development, you should select another goal that is better aligned with your level of commitment. Please keep in mind that developing career goals is easy, achieving them requires a great deal of hard work.

3 FIGURE OUT CAREER MILESTONES YOU MUST REACH

Once you've decided on an outcome and a baseline, the next step is to figure out what intermediate milestones you need to reach. It's great to know that you want to be a CISO, but it's the steps along the way that most people have trouble with. So research what path most CISOs take. Most have certain certifications and education, and all of them at some point manage a team of people, learn to manage projects, budgets and more. You need to set goals and milestones that allow you to get from where you are today to accomplishing all of the steps on the path of a CISO.

4 PLAN IN REVERSE

Finally, with your milestones set out, you need to figure out what you're going to do over the next three, six and 12 months to reach your first milestone. What do you need to accomplish *this* year to move you toward your ultimate career goal? What do you need to learn?

This is all about planning backwards from your final outcome to the current day. If you know, for example, that you want to be taking a more managerial role a year from now, what skills would you need to obtain? What books would you need to read? What training would you need to take? And who would you need to meet and know?

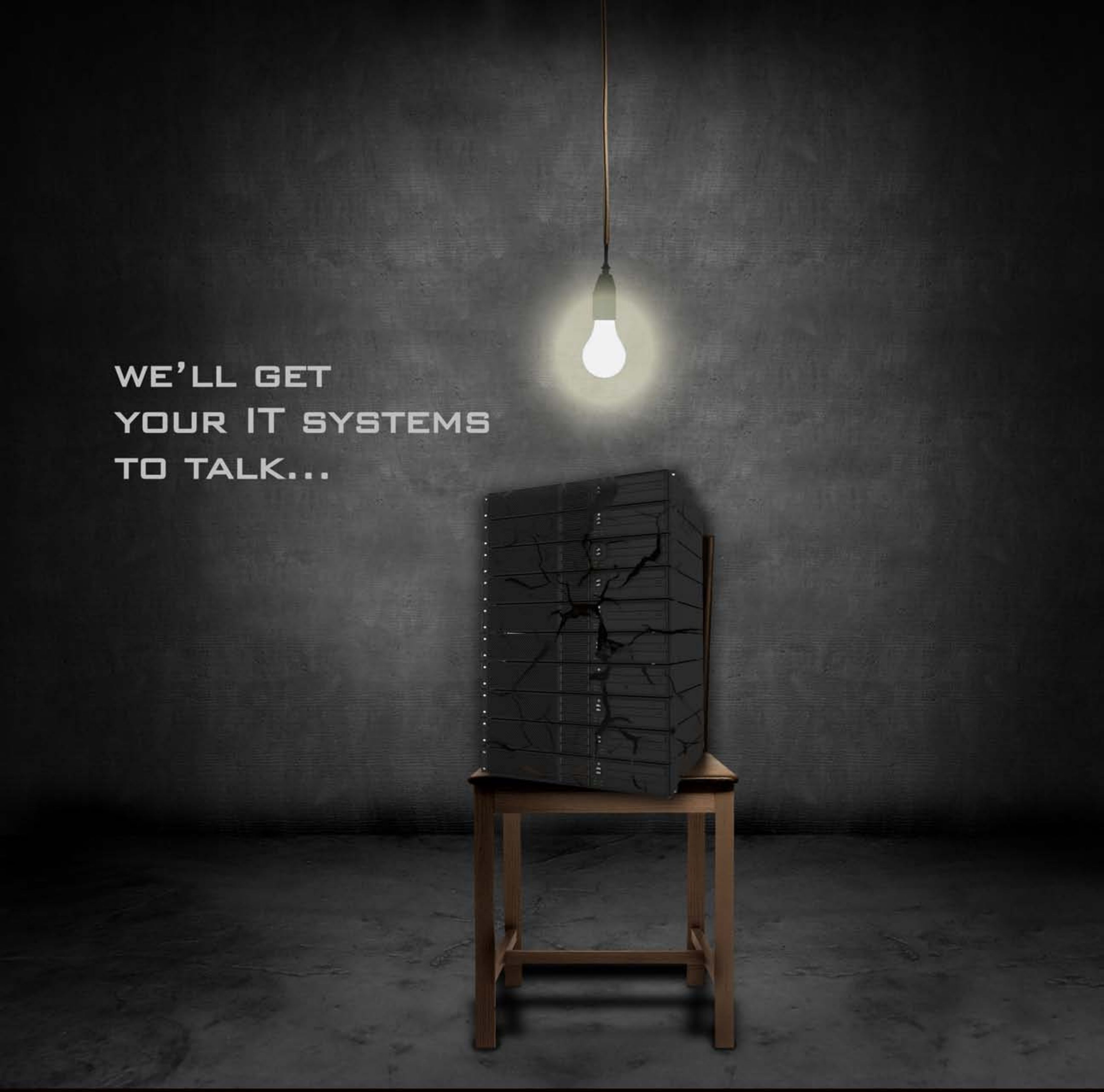
Once you have this written plan, it will provide you with a guide for making career decisions and assessing specific career opportunities. As your information security career progresses, you will be presented with a variety of different opportunities to either utilize your current skill set or develop new skills. As an example, you may move from the role of an individual contributor toward a more management-oriented role—this may cause you to use less of your technical skills and more of your managerial skills.

Following these four steps should allow you to put together a plan that gives you a good understanding of where you want to go and how you get there. ▸

Lee Kushner is the president of LJ Kushner and Associates an information security recruitment firm and co-founder of InfoSecLeaders.com, an information security career content website.

Mike Murray has spent his entire career in information security and currently leads the delivery arm of MAD Security. He is co-founder of InfoSecLeaders.com where he writes and talks about the skills and strategies for building a long-term career in information security.

Send comments on this column to feedback@infosecuritymag.com.



We'll get
your IT systems
to talk...

DATA IN CHECK

Database activity monitoring keeps watch over your data.

BY ADRIAN LANE

DATABASE ACTIVITY MONITORING (DAM) has emerged as a powerful and effective tool for security and compliance. By design, DAM technologies have the ability to monitor all database activity, including administrators, and alert on policy violations. These features enable compliance controls, operations monitoring and data protection not otherwise possible, and does so without interfering with business processes. While the promise to advance security and compliance is significant, not all tools are created equally, with fundamental differences in architectures, database support, blocking capabilities and performance.

We'll discuss the business use cases, explore the inner workings of these tools, and make recommendations on evaluating, purchasing and deploying database activity monitoring. We'll provide a definition for DAM that explains how it differs from database auditing and intrusion prevention systems, and then illustrate these differences in applied use cases for compliance and security tasks. We will then drill into the technology as to understand the difference between network, external monitoring and agent architectures, evaluate the major features of DAM, including workflow and advanced capabilities such as change management, and determine deployment expectations to aid buying decisions.

WHAT IS DATABASE ACTIVITY MONITORING?

Database activity monitors capture and record database events, which at a minimum includes all Structured Query Language (SQL) activity, in near real-time, including database administrator activity, across multiple database platforms and generate alerts on policy violations. What does that mean? DAM is the only tool that sees everything going on inside your database. This means every action by an application, user or administrator can be collected, analyzed and can prompt a reaction if the query violated a policy.

Further, the ability to analyze use of objects, user behavior, volume of data, source and destination, application and content means we can apply compliance and security policies in a very granular and precise way. While a number of tools can capture various levels of database activity, database activity monitors are distinguished by several features:

- The ability to independently monitor without help from database administrators to collect information or enforce policies.
- Collecting activity from multiple sources in and around the database.
- The ability to apply multiple forms of analysis and react in near real time.
- The ability to store this activity securely outside the database.
- The ability to aggregate and correlate activity from multiple heterogeneous database management systems (DBMS).
- The ability to enforce separation of duties on database administrators, auditors and security personnel.

While commonly confused with database auditing, the ability to collect from multiple databases of different types, the capture of SELECT statements to understand how data is viewed and not just changed, and capture important system alterations not stored in the audit trail sets DAM apart. When coupled with real-time analysis of content and behavior, not just attribute-based reports, dozens of new uses for controlling and securing databases and data are possible.

WHAT IS THE BUSINESS VALUE OF DAM?

Let's move beyond the technical nitty-gritty and jump into the real reasons you consider database activity monitoring: the business problems it solves. Database activity monitoring tools are very flexible, and purchases are typically prompted by one of the following drivers:

- **Auditing for compliance.** The single greatest adoption of DAM has been increasing auditor requirements to record database activity for Sarbanes-Oxley (SOX) compliance. Despite the fact that nowhere in SOX or accounting guidelines does it specify the need for database monitoring, accounting fraud has evolved to bury evidence within the millions of daily transactions that occur in automated financial systems. Bogus general ledger and accounts-receivable entries are easily lost in the vast sea of transactional information.

Prompted by the discovery of fraud in the WorldCom scandal by scanning raw database activity, companies have demonstrated the ability to implement financial controls at the database level. This type of monitoring is simply not possible for auditors to manually accomplish, both because of the volume of activity, and their inability to navigate the complexities of the database system. Some external auditors recommend the collection of all database activity for SOX, and DAM tools can do this with less overhead and cost than alternatives.

- **As a compensating control for compliance.** Monitoring adoption is used to complement the Payment Card Industry's Data Security Standard for access to credit card related information, as well as monitoring access to sensitive health care data as it relates to HIPAA requirements. We are seeing greater use of DAM tools to address specific compliance requirements, even though database auditing isn't the specified control. While access controls and encryption are specified technologies, their respective cost, impediment to normal business operations and lack of ability to verify data usage has prompted firms to support other security efforts with DAM, or replace them entirely.
- **As a security control.** DAM tools offer significant security benefits and can sometimes even be deployed in a blocking mode. They are particularly helpful in detecting and preventing data breaches for Web-facing databases and applications, or to protect sensitive internal databases through detection of unusual activity. Advancements in statement analysis of the DAM platforms makes it possible to detect and stop SQL Injection attacks, as well as insider misuse. As both of these attack vectors remain the biggest security threats to databases, the relevance and value of DAM for security is unquestioned.

WHAT ARE SOME EXAMPLES USE CASES?

The following are several use cases that illustrate how database activity monitoring is used to enact security, operations and compliance policies:

Security: Security is the reason DAM products exist. The ability to detect and respond to any activity that appears malicious or where the database is being misused, either by attackers or insiders, was missing from the market. Some of the things DAM can sniff out include:

- If an application typically queries a database for credit card numbers, a DAM tool can generate an alert if the application requests more card numbers than a defined threshold (often a threshold of "1").
- Detection of SQL injection variants to confuse the database into revealing information, or allow the execution of arbitrary code.
- Recording failed logins and other events that indicate an attack or attempted misuse.
- Blocking unwanted statements.
- Application whitelisting by blocking connections of unapproved applications.
- Alteration of user administrative permissions.

Regulatory Compliance: It's beyond the skill of most IT security and audit personnel to locate information within a database, and separation of duties requires information collection and policy analysis be implemented independent of DBAs and IT administrators. DAM platforms provide this separation of duties, and most vendors pre-package thousands

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

CAREERS

DATABASE ACTIVITY MONITORING

BANKING MALWARE

WINDOWS 7 SECURITY

SPONSOR RESOURCES

of compliance polices to aid in the deployment. Typical polices include:

- Enforcement of separation of duties on database administrators for SOX compliance by monitoring all their activity and generating SOX-specific reports for audits.
- Verification the audit trail is being produced.
- Access to sensitive data audit reports.
- Change order verification.
- Access control and authorization reports.

Operations: Changes to database applications are complex, often comprised of hundreds of individual steps, with the ultimate result not evident from any single action. Transactional analysis of common database administrative tasks are recorded, analyzed, and depending upon the result, results can feed workflow or trouble-ticket systems. The types of operations may include:

- Installation of patches.
- Appropriate use of service accounts.
- Alteration of database function, access or accessibility.
- Backup and recovery detection.
- Change order verification.
- Business process failures.

HOW DOES DATABASE ACTIVITY MONITORING WORK?

We have covered the business value, now let's talk about the tools and platforms to help understand the core functions, and how to differentiate one vendor's offering from another. We're not going into a lot of detail here, but just enough to guide you in a selection process. Note that to perform their function, DAM products follow a consistent process: collection of the events from the database, analysis of the activity in relation to established policies, and alerting when a policy violation is detected. As each phase represents a core piece of the product, let's look at each of these in greater detail:

Monitoring systems are deployed as software, an appliance, or in some cases as a virtual appliance running on top of a virtualization platform. These platforms are remote and not stored on the same platform as the database. All will offer a Web interface for remote administration, policy management and report development. All of the products will have some form of internal database to store collected data, policies and reports. You will likely select a deployment option that matches your environment today, but keep in mind that each option has different performance, flexibility and cost associated.

Where the platforms begin to diverge is on one of the most important features: data collection. The collection of SQL statements, in addition to monitoring of programs and batch jobs stored within the database, are the types of activity collected. There are three methods used to collect activity: network monitoring, local agent and remote credentialed access. Network monitoring is still used as a lightweight, non-invasive method to collect activity, but fails to collect administrative commands and is blind to the use of encrypted sessions. Remote credentialed access is a common collection technique when using native auditing and tracing functions, but is limited to native database capture methods. Agent-based data collectors are increasingly common as they allow for local, credentialed access to leverage native data capture, but can also employ other collection techniques such as protocol monitoring, memory scanning and event tracing.

It should be noted that you will likely use not only multiple deployment models, depending upon the business need that prompts the use of activity monitoring, but multiple data collection techniques depending upon the specific security or regulatory requirement. Having a platform that offers, at a minimum, remote credentialed and database agent options is important. Further, you should look for multiple collection options for each platform, such as a method that captures the database audit trail and one that collects all console and administrative activity so you have the ability to enforce a breadth of compliance and security policies.

Having a platform that offers, at a minimum, remote credentialed and database agent options is important.

The second major platform differentiator is analysis; this is what separates DAM from auditing. Monitoring systems are designed to find violations instantly, utilize more advanced inspection techniques, alert, and even block activity.

All monitoring and auditing platforms provide basic reporting based upon the analysis of data and SQL query attributes. What we mean by attributes are things such as which user, what time of day, what query operation, what application issued the query, the columns affected and other associated variables. Unlike auditing, when a statement matches the attributes specified, an alert is generated and, with some platforms, the action is blocked. Common policy examples are more than three failed logins, a single user issuing queries from different locations at the same time, or when any user selects more than one customer record at a time.

As threats evolve, such as SQL injection and buffer overflow attacks, new analysis techniques have been implemented. Statement or lexical analysis is one such variant, where you examine the structure of the SQL statement. Examining components of the query for such tricks as "where 1=1" to force statement execution, abnormal activity is detected because the statement just doesn't look right.

Behavioral analysis is another advance in analysis techniques used to detect insider threats and misuse. This variation combines one or both of the above analysis techniques, but augments the comparison with a behavioral profile. The profile is created by establishing a baseline of user behavior that represents normal activity to establish a reference point. Every subsequent query is examined not only for typical attribute violations, but attributes that differ greatly from the established norm.

Other important considerations are performance, policy management, integration and reporting. During your review, make sure you mimic load and scalability test to ensure that the product you purchase will in fact cover your entire organization.

With policy management, as this is where your IT team will spend the majority of time making updates, verify that policies are easy to create, adjust and apply to different databases as needed. You will want to double-check vendor claims that their solution will integrate with any existing workflow, trouble-ticket or data management systems you have in place. And be sure if they do not cover all of the databases you need to protect, that they will commit to doing so within the next six months or you should receive a partial refund. Finally, as reports and alerts will provide key notification to events as they occur, verify that you can adequately build and maintain distribution of information, based upon the criticality of the data, to responsible parties. Take the time to understand these key aspects of the platform because your satisfaction with any given product will be largely dependent on how easy it is to manage on a day-to-day basis.

COMPLIANCE DRIVES DAM ADOPTION

Solving database security problems was the genesis of the DAM market, but compliance is what drives adoption of the technology today. While there is overlap with other security and management platforms, database activity monitoring offers features and functions found nowhere else. Access control systems, SIEM and WAF technologies can offer some of these features, but not all at once—and not from a single product. Database activity monitoring is a much more recent addition to our database security toolbox, and utilizes different approaches to analysis and data capture, and when coupled with near real-time results, are much more appropriate for the securing of data and keeping track of application activity. ▸

Adrian Lane is CTO of consultancy Securosis. Send comments on this article to feedback@infosecuritymag.com.

UNDER ATTACK

Cybercriminals are using increasingly stealthy and sophisticated malware to hijack online business banking accounts. BY MARCIA SAVAGE

AT FIRST, it was hard to tell what was causing the "phantom" money transfers from the online bank account of a small North Carolina company. Investigators didn't know if the fraudulent wire and Automated Clearing House transfers were caused by an insider or malware, recalls Don Jackson, director of threat intelligence with the Counter Threat Unit at SecureWorks, an Atlanta-based security services provider.

But the cause became quite clear when Jackson and his team examined the bookkeeper's computer: an infection by the Zeus Trojan. "In the past, Zeus was just spyware and wanted user names and passwords," he says. "This was the first banking version of Zeus. It got into the browser and changed things on the fly."

The malware caused the business to lose nearly $98,000, Jackson says. That was in late 2007. Today, criminals are using the Zeus crimeware kit with astonishing success, pulling off six-figure heists from the online bank accounts of scores of small businesses, municipalities and nonprofits. The Federal Deposit Insurance Corporation estimates losses from fraudulent electronic funds transfers in the third quarter of 2009 at about $120 million. The attacks have been mounting over the past 18 months or so and haven't slowed, experts say.

Zeus is among an emerging brand of stealthy malware that steals online banking and other sensitive credentials with ever changing capabilities to evade detection and defeat security controls. Bought and sold on the Internet and continually upgraded with new features, Zeus and its ilk represent the evolution of malware into a vast commercial enterprise. Banker Trojans accounted for 61 percent of all new malware in the first quarter of this year, according to a recent study by Panda Security. It's become an arms race with the criminals behind these malware-fueled business operations, says Joe Bernik, CISO at Fifth Third Bank.

"They're constantly looking for ways to improve the functionality to overcome whatever technical controls the financial services industry or whatever industry they're targeting puts into place," he says.

Malware has surpassed phishing as the top threat, says David Shroyer, vice president of online security and enrollment at Bank of America. "The speed of evolution and the shifting of threat vectors are astounding. It's light speed, so we have to be on our toes to protect our customers and our industry," he says. "What I'm seeing in the industry is this is now the big thing we're all worried about and we're cooperating like we never have before."

Let's take a closer look at Zeus, its emerging competition in the banking malware market, their impact, and how the financial services industry is responding.

"They're constantly looking for ways to improve the functionality to overcome whatever technical controls the financial services industry or whatever industry they're targeting puts into place."

–JOE BERNIK, CISO, Fifth Third Bank

ESCALATING BATTLE

Malicious code designed for banking fraud has been around as far back as 2003, says Jamz Yaneza, threat research manager at Trend Micro. Most early banking malware came in the form of keyloggers, which captured all kinds of sensitive information, not just online banking credentials.

In the U.S., banks stepped up their defenses against spyware and keyloggers with added security, particularly two-factor authentication. In 2005, federal banking regulators issued authentication guidance for online banking, and regulators say attacks dipped for a couple years. Criminals had to figure out a new method of attack.

"Banks and online providers have done a good job putting in place authentication methods that made it hard for the criminals to make money," says Laura Mather, co-founder and CEO of Silver Tail Systems, a Palo Alto, Calif.-based provider of fraud prevention systems. "The bad news is the criminals didn't give up. They had to employ even more sophisticated technology in order to subvert the protections that have been put in place."

Fraudsters shifted their focus to malware because their returns from phishing were diminishing, says Sean Brady, identity protection and verification product marketing manager at RSA, the security division of EMC. "The more sophisticated groups were willing to put the extra investment into Trojans because they demonstrated return," he says.

To circumvent strong authentication methods, criminals have to impersonate the victim, Mather says. "Instead of just having a password, they have to look just like the victim, so they're accessing the victim's account from the victim's own computer, which means they have the correct IP address. It's very difficult for the bank to tell the difference between the malware and the legitimate user," she explains.

The Silentbanker Trojan, which surfaced a couple years ago, had this interception functionality but Zeus and other newer banking Trojans have honed it, experts say. Today's banking malware attacks a victim's Web browser instead of the online session, Bernik explains: "It modifies and intercepts the data that is being passed to the browser and it can actively modify Web pages."

"The bad news is the criminals didn't give up. They had to employ even more sophisticated technology in order to subvert the protections that have been put in place."

–LAURA MATHER, co-founder and CEO, Silver Tail Systems

Criminals have used Zeus to add fields to obtain additional data for authenticating to a bank website and to alter balances to hide fraudulent withdrawals. Researchers have detected variants of Zeus that have used the Jabber instant messaging protocol in order to use stolen credentials in real time and circumvent the security provided by one-time password tokens. Victims often receive an error message as the fraudster uses his or her credentials behind the scenes.

These kind of man-in-the-browser attacks are much harder to detect than the older man-in-the-middle attacks where the hostile party inserts itself between the authenticating server and the valid user, Bernik says.

"It becomes increasingly difficult for financial institutions to detect because some of the defense mechanisms we were using such as device ID and geo ID have limited value when dealing with a man-in-the-browser attack," he says.

A FORMIDABLE FOE

Zeus, also called Zbot, has been the most pervasive and damaging banking malware so far to date, researchers say. According to Microsoft, infections by Zeus have skyrocketed

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

CAREERS

DATABASE ACTIVITY MONITORING

BANKING MALWARE

WINDOWS 7 SECURITY

SPONSOR RESOURCES

in recent months. *(see chart, below)*.

The malware spreads via phony emails that pretend to notices from legitimate organizations like NACHA, the association that oversees the Automated Clearing House (ACH) network, spear phishing emails targeting specific individuals and containing links to malware-rigged websites, and drive by downloads. Researchers believe criminals in Eastern Europe, particularly Russia and Ukraine, are behind the Zeus-fueled attacks.

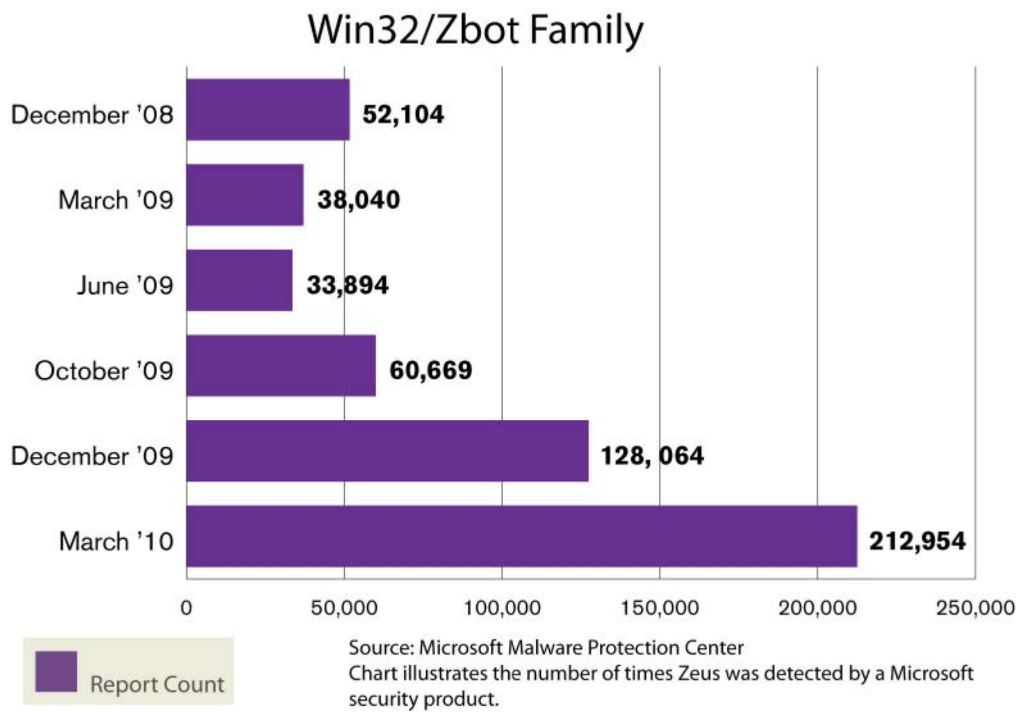
The Zeus crimeware kit has three components, according to an analysis by Trend Micro: the Trojan, a configuration file, and a drop zone where stolen credentials are sent. After the Zeus Trojan is executed, it downloads its configuration file from a predetermined location then waits for the victim to log in to a particular target included in the configuration file, Trend Micro researchers say. Criminals conduct extensive research on banking websites to hone their attacks.

"They will do extensive research on the sites—logging in, understanding the page flows

STATISTICS

Zeus Infections Skyrocket

Microsoft data shows the number of reported Zeus (also called Zbot) infections shot up early this year.



Source: Microsoft Malware Protection Center
Chart illustrates the number of times Zeus was detected by a Microsoft security product.

and thresholds to perform transactions with, down to the HTML code of the actual pages because they will frequently use that knowledge to manipulate the page in the user's browser," Brady says.

The highly configurable nature of Zeus is one of its most powerful aspects, experts say. "Zeus is a lot of different botnets," Mather says. "Criminal A can buy Zeus and have his own command-and-control and his own botnet, and criminal B buys Zeus and has his own botnet that will be different from criminal A's because it's targeting victims in South America while the other is targeting victims in Europe."

Earlier this year, security firm NetWitness reported finding a 75GB cache with stolen data, including credentials for online banking sites and social networks, from more than 74,000 Zeus infected systems; the company named the infected PCs tied to the Zeus attacks the Kneber botnet. In March, security researchers reported ongoing efforts to shut down Kazakhstan-based Troyak.org, an ISP serving a large chunk of a Zeus botnet. Spanish authorities in December shut down the Mariposa botnet, which stole banking and other sensitive data by infecting 12.7 million computers with Zeus and other malware.

East European cybercriminal operations using the Zeus malware kit have capitalized on the recession to successfully recruit "money mules" in the U.S. to move money siphoned from business online banking accounts, experts say. Fraudsters lure money mules over the Internet with bogus work offers and use them to receive the stolen funds, instructing them to wire money overseas after deducting a commission. Oftentimes, the money is stolen in amounts less than $10,000, apparently in an attempt to not to trigger Suspicious Activity Report (SAR) requirements.

> "They will do extensive research on the sites–logging in, understanding the page flows and thresholds to perform transactions with, down to the HTML code of the actual pages because they will frequently use that knowledge to manipulate the page in the user's browser."
>
> –SEAN BRADY, identity protection and verification product marketing manager, RSA, the security division of EMC

Jackson and other researchers at SecureWorks have been tracking each new version of the Zeus Trojan, which is constantly updated with new functionality. In March, they wrote that the latest version featured a level of control they hadn't yet seen in malware: a hardware-based licensing system so the malware can only be run on one computer. "Once you run it, you get a code from the specific computer, and then the author gives you a key just for that computer," wrote Jackson and Kevin Stevens, security researcher at SecureWork's CTU.

A beta version of a new Zeus variant they examined this spring featured polymorphic encryption, which allows it to re-encrypt itself each time it infects a computer, making each infection unique and harder for antivirus systems to catch, Stevens says.

Various modules, including a Firefox form grabber, a Jabber chat notifier, and Windows 7/Vista support, for Zeus are available on the Internet for prices ranging from $500 to $6,000, according to SecureWorks.

The developers behind Zeus also are very sensitive to detection rates of their malware by antivirus systems, says Mickey Boodaei, CEO of online security provider Trusteer. "Each variant they release goes through a kind of quality assurance process to make sure it's not detected by many antivirus solutions," he says.

New York-based Trusteer released a study last fall that showed the Zeus Trojan infecting PCs with updated antivirus software 77 percent of the time.

> "Each variant they release goes through a kind of quality assurance process to make sure it's not detected by many antivirus solutions."
>
> –MICKEY BOODAEI, CEO of online security provider Trusteer

THE COMPETITION

While Zeus has proven the most popular toolkit for criminals targeting online banking, the Clampi Trojan has also done its share of damage. Jackson says it's the number two threat to online banking after Zeus, but isn't available for sale like Zeus; rather, it's used by one criminal group in Eastern Europe.

Like Zeus, Clampi has advanced man-in-the-browser capabilities and uses state-of-the art polymorphic cryptors to conduct fraudulent ACH and wire transfers, according to Jackson. SecureWorks last summer documented the Clampi Trojan and how it targeted thousands of websites, including large banks, small banks and mortgage companies. Those behind Clampi use encryption adeptly, making it difficult for researchers to track it, Jackson says: "It flies under the radar a lot."

Last fall, Finjan researchers reported a new bank Trojan that criminals used to intercept online banking sessions and steal thousands of euros from German accounts last summer. URLzone minimizes the risk of being detected by banks' antifraud systems by systematically transferring random, moderate amounts of money from compromised accounts. According to RSA researchers, the Trojan uses money mules in a highly sophisticated way in order to foil researchers trying to identify the mule accounts it's using: It if detects that a computer isn't part of its botnet, it delivers a fake mule account to the researcher's computer.

The Silon Trojan, meanwhile, targets only customers of major U.K. banks and has managed to infect thousands of computers, according to Trusteer. Silon steals banking credentials, bypasses specific security controls and can update itself to counter banks' defensive measures.

Earlier this year, SecureWorks researchers discovered a new banking Trojan designed to facilitate fraudulent ACH and wire transfers. Bugat's capabilities include many of those common in banking malware, including Internet Explorer and Firefox form grabbing and stealing and deleting IE, Firefox and Flash cookies. Bugat mainly targets regional banks and smaller national banks, Jackson says. "It's fairly sophisticated, but not up there with Zeus and Clampi," he adds.

However, the emergence of Bugat indicates the strong demand for malware to commit financial fraud, according to SecureWorks. Indeed, the competition for Zeus appears to be heating up, especially with the emergence of SpyEye. According to Symantec, the first version of the malware kit appeared for sale on Russian underground forums in December. Retailing for $500, "it is looking to take a chunk of the Zeus crimeware toolkit market," Symantec researchers wrote.

The SpyEye toolkit is similar to Zeus in many ways and is updated regularly with new features, including one called "Kill Zeus" designed to delete Zeus from an infected system and leave SpyEye running, Symantec researchers noted.

THE FALLOUT

Government agencies and financial services associations began sounding the alarm about a sharp increase of fraudulent ACH and wire transfers hitting small and midsize

ADVICE

New Approaches

Vendors offer alternative technologies to secure online banking from fraud.

AS CRIMINALS USE increasingly sophisticated malware to commit online banking fraud, new technologies have appeared to combat the problem.

Trusteer's Rapport product is a browser security plug-in that works to prevent malware from tampering with online banking sessions. While traditional desktop security products try to prevent malware, "we're locking down the session," says Trusteer CEO Mickey Boodaei.

Desktop protection products like Rapport and a similar technology from Prevx provide another strong layer of security but many banks are reluctant to go that route, says Avivah Litan, vice president and distinguished analyst at Gartner.

IBM offers an alternative technology to foil online banking fraud: a USB-attached hardware device called Zone Trusted Information Channel (ZTIC) that runs the TLS/SSL protocol to create a proxy for connecting with banking websites; the SSL session bypasses any malware on a PC. IronKey recently launched Trusted Access for Banking, a USB device with a virtualized operating system and secure Web browser.

"We're creating a separate secured operating environment on your computer without you needing a separate computer," says David Jevans, CEO of IronKey.

Both IronKey and IBM are offering locked down computing environments but the technologies still use the keyboard, Litan says: "You could still record the keystrokes, so there's still an issue."

Silver Tail Systems offers a different approach with technology that watches for changes in how a website is used and alerts website owners to possible fraudulent activity. "We watch the behavior of the Web session to identify whether we think the behavior is a normal way to interact with a website," says Laura Mather, co-founder and CEO.

Litan says many of the alternative technologies, like ZTIC, aren't new but are getting more attention now. "There's nothing new under the sun but the situation is getting so bad that people are looking at these solutions," she says.

Litan recommends that financial institutions take a layered approach to fighting online fraud, including fraud detection that monitors transaction behavior and desktop protection. ▸

—MARCIA SAVAGE

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
DATABASE ACTIVITY MONITORING
BANKING MALWARE
WINDOWS 7 SECURITY
SPONSOR RESOURCES

businesses last August. In November, the FBI estimated that the fraudulent activity had resulted in approximately $100 million in attempted losses.

"We're not hearing about it as much on the consumer side. It does happen, but these bad guys are going after the big fish," says Bill Nelson, president and CEO of the Financial Services Information Sharing and Analysis Center (FS-ISAC). "They're sending spear phishing emails to individuals at businesses they've checked out."

Investigative reporter Brian Krebs has documented many cases in which small businesses and municipal agencies have lost thousands of dollars through fraudulent money transfers. Oftentimes, Zeus is cited as a culprit, such as in the case of small New York marketing firm that lost $164,000 after a Zeus infection. Business banking customers hit by online banking fraud typically lose out because they don't have the same regulatory protections to limit losses from fraudulent electronic funds transfers as consumers.

ADVICE

Fighting Fraudsters

NACHA says financial institutions can take several steps to help protect their business customers from ACH fraud.

NACHA, the nonprofit association that oversees the Automated Clearing House (ACH) network, released a bulletin late last year with tips for financial institutions and their customers to combat the problem.

According to NACHA, one of the reasons criminals are targeting small and midsize organizations is because–generally unlike individual banking consumers–many of them have the ability to initiate ACH credits and wire transfers via online banking. This funds transfer capability is usually related to the company's origination of payroll payments; criminals who hijack the corporate account may add fake names to a payroll file.

NACHA offered five steps financial institutions can take to protect corporate accounts from being taken over and used for ACH fraud:

- Deploy multifactor and multichannel authentication.
- Require business customers to initiate payments under dual control, with distinct responsibility for transaction origination and authorization.
- Enable out-of-band confirmation of payment initiation for certain types of payments.
- Provide out-of-band alerts for unusual transaction activity.
- Establish and monitor exposure limits related to customers' banking activities.

The association also offered tips for spotting the "money mules" used by fraudsters in their account takeover schemes. Banks need to watch out for these activity patterns, according to NACHA:

- A new account opened by an individual with a small deposit, quickly followed by one or more large deposits by ACH credit or wire transfer.
- An existing account with a sudden increase in the number and dollar amount of deposits by ACH credit or wire transfer.
- A new or existing account that withdraws a large amount of cash shortly after a large deposit by ACH credit or wire transfer. ›

–MARCIA SAVAGE

The fraud surge has led to a spate of lawsuits. For example, Bullitt County in Kentucky sued its bank, First Federal Savings Bank of Elizabethtown, last summer after cybercriminals stole $415,989 through fraudulent ACH transactions, according to court documents obtained by *The Courier-Journal.* The bank, which claims the county's security failures led to a Zeus infection, refused to reimburse the county for $310,176 that wasn't recovered.

In another case, which has been widely reported, Hillary Machinery of Plano, Texas was sued by its former bank, Dallas-based PlainsCapital, after being victimized by online banking fraud late last year. Hillary countersued the bank over the cyberheist, in which criminals stole about $800,000; PlainsCapital recovered almost $600,000.

For the financial sector and other industries, customer education has been a major weapon in successfully beating back phishing to the point where it's not the threat it was five years ago, Bank of America's Shroyer says. But customer education is less powerful of a weapon against stealthy malware that is constantly finding ways to avoid detection, he says.

Malware also is trickier from a customer resolution standpoint, Shroyer says: "I can fix a customer who's been exposed to phishing in a matter of minutes. A customer exposed to malware is a very difficult conversation. I can't just tell them to change their ID and passcode. I have to tell them that their endpoint, their PC, has been compromised by something that isn't just impacting their Bank of America relationships, but their Yahoo email account and other financial accounts like PayPal."

Banking malware is a newer problem in the U.S., Shroyer adds, noting that banks in Australia, Brazil and the U.K. have been combating sophisticated banking Trojans for longer.

Mather, a former director of fraud prevention at eBay, says phishing was the top concern when she worked at the company; malware wasn't much on the radar. "Now when I talk to banks and other large organizations, they're having to assume the customer's computer is compromised. That's a very different way to look at your customers than worrying about whether they're going to give away their passwords."

INDUSTRY REPSONSE

Financial industry groups, keenly aware of the critical need to preserve confidence in the online banking channel, have provided a slew of recommendations for fending off malware attacks.

FS-ISAC, NACHA and the FBI, in their joint advisory last August, recommended financial institutions implement strong authentication, fraud detection and mitigation best practices including transaction risk profiling, out-of-band transaction authentication together with fraud detection, and network defense in depth.

They also advised banks to educate their corporate and small business customers about security, including: reconciling accounts on a daily basis; initiating ACH and wire transfers under dual control (with one person initiating the transfer and another authorizing it); and possibly carrying out all online banking from a locked down, standalone computer with email and Web surfing disabled.

"We're emphasizing an integrated, layered security strategy," FS-ISAC's Nelson says. "Any single defense you come up with they can circumvent…If you implement a layered defense strategy, you have a better chance of defeating these bad guys."

American Bankers Association backs the layered approach, says Doug Johnson, vice

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

CAREERS

DATABASE ACTIVITY MONITORING

BANKING MALWARE

WINDOWS 7 SECURITY

SPONSOR RESOURCES

president of risk management policy for ABA. "One of the most important lessons we've learned from Zeus is that sometimes we hang our hat too much on security technological fixes," he says, adding that internal controls like dual authorization also are critical.

The association is working with other industry groups to address the problem on an ongoing basis. "It is something we take very seriously because it gets to the heart of the relationship between the bank and its commercial and municipal customers," he says. "Obviously, we need to counteract anything that could disrupt the trust that's built up between those two parties."

> "One of the most important lessons we've learned from Zeus is that sometimes we hang our hat too much on security technological fixes."
>
> –DOUG JOHNSON, vice president of risk management policy, American Bankers Association

Fifth Third Bank's Bernik notes that new technologies are emerging to deal with the challenge of the compromised host *(see p. 32)* but adds, "There's no silver bullet to solve all the challenges when it comes to the online channel."

Fifth Third, aiming to be a "trusted advisor" to its customers, provides them with education and certain technologies to combat the malware problem, he says. Making sure customers are aware of security best practices is critical, he adds.

Citing security concerns, Shroyer declines to detail strategies and techniques the financial services industry is using to fight the malware problem. But he says that Bank of America is in the process of requiring customers to upgrade their online IDs and passcodes to meet its security requirements, and recently rolled out a browser upgrade for its customers to upgrade from older, vulnerable browsers. Customers can be resistant to change, but the uptake was surprising and heartening, he says. "We've got to drive the message that we're here to help you protect your assets."

In the wake of the malware attacks, though, the industry is coming together like never before, Shroyer says. He's having weekly calls with other banks in which they discuss what they're seeing and possible solutions. "You would not have seen that before," he says. "But now we have that collaboration."

Malware, he says, is "going to drive us towards an opportunity to react faster than we have in the past out of necessity." ›

Marcia Savage is editor of Information Security. *Send comments on this article to feedback@infosecuritymag.com.*

Your One Stop Shop for All Things Security

Nowhere else will you find such a highly targeted combination of resources specifically dedicated to the success of today's IT-security professional. Free.

IT security pro's turn to the TechTarget Security Media Group for the information they require to keep their corporate data, systems and assets secure. We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security standard compliance, videos, webcasts, white papers, podcasts, a selection of highly focused security newsletters and more — **all at no cost.**

Feature stories and analysis designed to meet the ever-changing need for information on security technologies and best practices.

INFORMATION SECURITY®

www.SearchSecurity.com

Breaking news, technical tips, security schools and more for enterprise IT professionals.

SearchSecurity.com

www.SearchSecurity.com

Learning materials geared towards ensuring security in high-risk financial environments.

SearchFinancialSecurity.com

www.SearchFinancialSecurity.com

UK-focused case studies and technical advice on the hottest topics in the UK Security industry.

SearchSecurity.co.UK

www.SearchSecurity.co.UK

Information Security strategies for the Midmarket IT professional.

SearchMidmarketSecurity.com

www.SearchMidmarketSecurity.com

Technical guidance AND business advice specialized for VARs, IT resellers and systems integrators.

SearchSecurityChannel.com

www.SearchSecurityChannel.com

TechTarget®
The IT Media ROI Experts

TARGET: Security and Simplicity

With Windows 7, Microsoft aims to improve security in the enterprise but without the headaches of Vista. Here's what you need to know about the security functionality in the latest version of Windows.

BY BETH QUINLAN

SEVEN YEARS AFTER kicking off its Trustworthy Computing initiative, Microsoft launched Windows 7 last October. The software giant touts the operating system, which builds on the security features of Vista, as key to its "End to End Trust" vision for a more secure Internet. With Windows 7, Microsoft also aims to make security easier to use; Vista, which debuted three years ago, caught criticism for security functionality users and administrators alike found clunky and obtrusive.

Let's take a look at several of the security features of Windows 7, including a more flexible BitLocker for data protection, auditing enhancements to help meet compliance requirements, an improved User Access Control with fewer prompts, and new functionality to ensure system integrity.

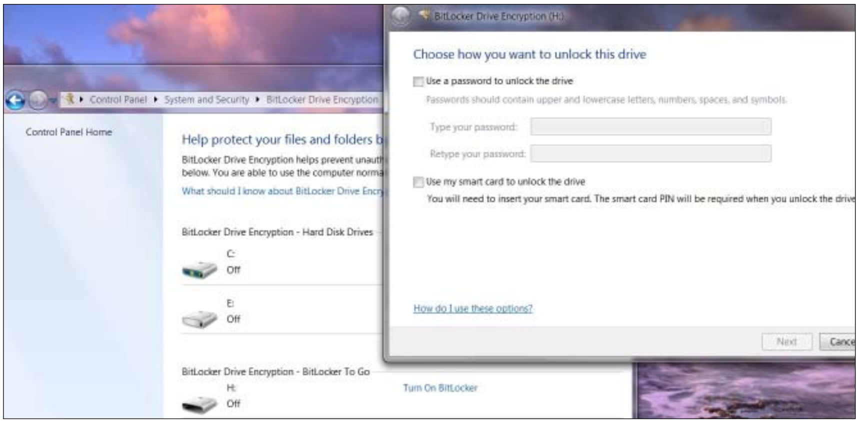
DATA PROTECTION

In today's fast-paced, mobile environment there is more opportunity than ever before for data to fall into unauthorized hands. Hundreds of thousands of laptops containing sensitive information are lost, stolen or decommissioned every year. Additionally, portable USB devices are inexpensive, easy to use, and everywhere. Failure to protect corporate data can result in critical consequences, including lawsuits, regulatory penalties, loss of brand reputation and consumer confidence, and even criminal prosecution. As such, organizations are implementing data encryption technologies to help mitigate the risks of data loss or exposure. Windows 7 helps organizations on this front with enhanced Encrypting File System protection and an easier to install BitLocker Drive Encryption (BDE).

EFS can be used to encrypt individual files or folders that have been stored on NTFS-formatted drives to protect them from unauthorized access. In Windows 7, EFS has been enhanced to support Elliptic Curve Cryptography (ECC), a second-generation Public Key Infrastructure algorithm. For protection of "top secret" documents, U.S. government agencies must comply with encryption requirements referred to as Suite B. Because Suite B does not permit the use of RSA cryptography, organizations with existing RSA implementations must find a streamlined transition path toward compliance. Windows 7 facilitates the transition because it permits the concurrent use of both RSA and ECC algorithms, thus promoting regulatory compliance while maintaining backward compatibility.

In Windows Vista, Microsoft introduced BitLocker Drive Encryption (BDE) to protect computer hard drives (operating system volumes and fixed data volumes) from unauthorized access. In addition to drive-level encryption, BitLocker provides pre-boot verification and integrity checking to ensure that a system has not been tampered with and that the drives have not been moved between computers. This built-in technology was exciting from a cost and security standpoint, but administrators were less enthused about its implementation. For instance, installation often required that a system's hard drive be repartitioned.

In Windows 7, BitLocker is available in the Enterprise and Ultimate editions, and has been updated in a variety of ways to improve both administrative and the


Control Panel ▸ System and Security ▸ BitLocker Drive Encryption
Control Panel Home

Help protect your files and folders b

BitLocker Drive Encryption helps prevent unauth
below. You are able to use the computer norma

What should I know about BitLocker Drive Encry

BitLocker Drive Encryption - Hard Disk Drives

C: Off

E: Off

BitLocker Drive Encryption - BitLocker To Go

H: Off — Turn On BitLocker

BitLocker Drive Encryption (H:)

Choose how you want to unlock this drive

□ Use a password to unlock the drive

Passwords should contain upper and lowercase letters, numbers, spaces, and symbols.

Type your password:

Retype your password:

□ Use my smart card to unlock the drive

You will need to insert your smart card. The smart card PIN will be required when you unlock the drive

How do I use these options?

FIGURE 1: After configuring BitLocker encryption to work without a TPM by enabling additional authentication at setup in Group Policy, all non-TPM BitLocker settings will be visible in the BitLocker Setup Wizard in the Control Panel.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
DATABASE ACTIVITY MONITORING
BANKING MALWARE
WINDOWS 7 SECURITY
SPONSOR RESOURCES

user experiences. Full implementation requires a computer with a Trusted Platform Module 1.2 chipset and a compatible BIOS. It's possible to implement BitLocker on a computer that doesn't support TPM 1.2 if the BIOS supports USB devices during startup, but you'll lose the pre-boot checks and system integrity verification. To configure BitLocker encryption to work without a TPM, you must enable the "Require additional authentication at setup" Group Policy setting and select the "Allow BitLocker without a compatible TPM" checkbox. After the setting is applied, all non-TPM BitLocker settings will be visible in the BitLocker Setup Wizard in the Control Panel *(see Figure 1, p. 38)*.

BitLocker encryption capabilities now extend to removable media in a feature called BitLocker To Go. For a detailed review of Windows 7 changes to BitLocker, see p. 40.

SECURITY AUDITING

In addition to facilitating encryption, Windows 7 aims to ease compliance requirements related to IT security through new policies and a greater level of detail in security logs. Enhancements include:

1. **Advanced Audit Policy settings:** In Windows XP there were nine categories of auditable events that could be monitored for success, failure or both. In Windows Vista the number of available categories was expanded to 53 to provide better targeting and granularity of data collected. This helps to eliminate unwanted data that makes log files large and difficult to analyze. Unfortunately, these categories and settings were not integrated with Group Policy for centralized management. In Windows 7 (and Windows Server 2008 R2), all 53 new auditing event categories have been integrated into Group Policy under Local Policies\Audit Policy.

2. **"Reason for access" reporting:** The list of access control entries (ACEs) provided in logs shows the privileges on which the decision to allow or deny access to an object was based. Forensic analysis is improved because auditors can determine the reason why someone had access to specific resources based on specific permissions.

3. **Global Object Access Auditing:** Administrators can define system wide, per-object type system access control lists (SACLs) for the file system and the registry, which will automatically be applied to all objects of that type.

AUTHENTICATION AND AUTHORIZATION

Windows 7 includes several features to help in the critical areas of authentication and authorization. For example, previous versions of Windows had the built-in Administrator account that was intended to facilitate setup and disaster recovery, but because the account was always called "Administrator," had the same security ID on all computers and was often given a consistent password throughout the enterprise, was a prime target for attacks. If a system was compromised, an attacker would have access to the password hash, which could then be used to authenticate to any other computer that used that same account. With Windows 7, the Administrator account is now disabled by default. Only local accounts specifically created with administrator privileges or domain accounts that are members of the Domain

DATA PROTECTION

Easier Encryption

Windows 7 makes BitLocker easier to manage and provides encryption for portable devices.

A MAJOR SECURITY FEATURE in Windows 7 is a new and improved BitLocker that removes the management headaches previously associated with the data protection functionality. When combined with policies that control the use of portable media devices, BitLocker provides a level of control over data on the client side that wasn't previously possible, without being overly intrusive to users. Among the improvements:

- In Windows 7, fixed hard drive requirements for BitLocker implementation have been reduced and simplified. The computer's hard drive must be formatted with a 100 MB hidden system drive separate from its encrypted operating system drive, a drastic reduction from the 1.5 GB required by Vista.
- It's no longer necessary to pre-create the system drive because the BitLocker installation creates it automatically. The drive is hidden by default and not assigned a drive letter, so files cannot be inadvertently written to it; however, it can be used by administrators to store recovery tools, etc.
- While operating systems drives must still be formatted with NTFS to be encrypted using BitLocker, data drives can now be formatted as exFAT, FAT16, FAT32 or NTFS.
- While premium editions of Windows 7 are required to create and write to encrypted drives, any version of Windows 7 can be used to unlock them. When a BitLocker-encrypted device is connected, Windows 7 will automatically detect that the drive is encrypted and prompt for the information necessary to unlock it. Windows Vista and Windows XP systems can use a BitLocker to Go Reader to read encrypted files if they are stored on FAT-formatted devices. Users need to be warned that if an encrypted removable drive is formatted as NTFS, it can only be unlocked on a computer running Windows 7 or Window Server 2008 R2.
- BitLocker To Go extends encryption capabilities to portable data storage devices (IEEE 1667 compliant USB devices), including removable devices that contain FAT partitions. Even if the media is lost, stolen or misused only authorized users can access its data.
- BitLocker To Go can be utilized separately from traditional BitLocker encryption; the fixed drives on the system need not be encrypted.
- Users can easily encrypt their removable media by right-clicking on the drive and selecting "Turn on BitLocker." They will then be asked for either a password or a smartcard; upon providing the requested credentials they will be asked to print or save their recovery password. Policies can be set to allow the recovery password to be stored in Active Directory Domain Services and used if other unlock methods fail.
- Members of the Local Administrators group (or the Domain Admin group) can control how removable devices can be utilized within their environments along with the strength of protection required. Policies can be enforced which restrict the ability to write to portable devices, while still retaining the ability to read from unprotected drives.
- Windows 7 includes new Group Policy settings to improve upon an administrator 's ability to centrally manage BitLocker.
- Policies can be implemented to set requirements for use of passwords, domain user credentials, or smartcards when users attempt to access a portable or fixed drive. Fixed drives can also be set to automatically unlock after the initial use of a password or smartcards to unlock them. ▸

—BETH QUINLAN

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

CAREERS

DATABASE ACTIVITY MONITORING

BANKING MALWARE

WINDOWS 7 SECURITY

SPONSOR RESOURCES

Admin group can log on locally to a Windows 7 computer. In addition, the built-in domain Administrator account in Windows Server 2008 R2 (first account created) will not run in Windows 7 Admin Approval mode, but subsequently created domain administrator accounts will.

Other ways in which Windows 7 helps facilitate authentication and authorization include:

Managed Service Accounts. For application services or processes to function, they must be assigned an account under which to interact with the operating system and other applications. Sufficient privileges must be granted to a "service account" for it to function, but granting unnecessary rights increases security risks. Windows operating systems have long provided local computer accounts that can be used to run services on the computer (Local Service, Network Service, or Local System). Managing local accounts across multiple computers in the enterprise would be a nightmare; as such, administrators frequently create domain-level accounts to be used as service accounts across the enterprise. Unfortunately, this solution does not eliminate the need to manually manage the account passwords or perform Service Principal Name (SPN) maintenance. Failure to timely manage these accounts can result in a disruption of services.

Each application and service on the Windows 7 computer can have its own managed service account or a single account can be used by multiple applications; however, the account cannot be shared across multiple computers.

To alleviate this problem, Windows 7 supports a new type of account called a managed service account. This allows administrators to create a group of domain accounts that can be used with services and specialized applications (like IIS and SQL) on local computers. The accounts provide security isolation for services and applications, but do not require SPN or password maintenance (passwords are reset automatically). In addition, management of these accounts can be delegated to non-administrators.

Each application and service on the Windows 7 computer can have its own managed service account or a single account can be used by multiple applications; however, the account cannot be shared across multiple computers. In a domain environment, the managed service account can be created and managed from a new Active Directory container called "Managed Service Accounts." This means that accounts on multiple machines throughout the enterprise can be centrally maintained. When using these domain-level accounts, support for both password and service principle name (SPN) management is automatic when the account is on a Windows Server 2008 R2 Domain Controller and the domain is at the Windows Server 2008 R2 functional level. Regardless of the functional level, if the Domain Controller is running Windows Server 2008 or Windows Server 2003, SPN management will still be manual.

User Account Control. User Account Control is a feature which was introduced with Windows Vista to improve security by allowing organizations to deploy operating systems without granting administrative rights to the accounts under which

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

CAREERS

DATABASE ACTIVITY MONITORING

BANKING MALWARE

WINDOWS 7 SECURITY

SPONSOR RESOURCES

users would function on a daily basis. While UAC achieved this objective, its implementation created frustration among users who were forced to respond to multiple prompts. Even administrators (who know better) were tempted to disable the feature. Windows 7 includes changes to UAC that maintain its security benefits while improving the usability experience for both standard users and administrators.

The number of prompts presented to users has been greatly reduced in the following ways:

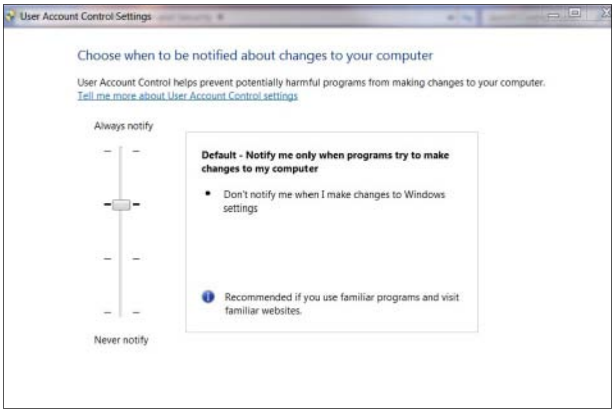
- The following tasks will no longer trigger a prompt: Reset network adapters and perform basic network diagnostic and repair tasks; install updates from Windows Updates; install drivers that are included with the operating system or are downloaded from Windows Updates; view settings; and connect to Bluetooth devices.
- Prompts for multiple tasks within an area of operation have been merged. As a result, there are fewer prompts to respond to when performing file operations, running Internet Explorer application installers or installing ActiveX controls.

New security policies give administrators greater control over UAC behavior, including control of the UAC messages presented to both standard users and local administrators (when they are working in Administrative Approval mode).

Users with administrative privileges can configure the UAC through a control panel applet. A simple slider *(see Figure 2, below)* allows a choice of four levels of protection ranging from always notify to never notify. Always notify essentially duplicates a Windows Vista UAC experience. Never notify provides an alternative to completely disabling UAC: While it will suppress the prompts, core UAC protections such as protected mode Internet Explorer will remain functional.

Certificates. In Windows 7, issuance of certificates is simplified with support for new HTTP enrollment protocols based on open Web services standards. Because remote users, business partners and customers can perform certificate enrollment over the Internet or across forest boundaries, fewer certificate authorities will be required for the enterprise.

To take advantage of this new enrollment capability, the Windows 7 computers must connect to a Windows Server 2008 R2 server running the Active Directory Certificate Services (AD CS). Lightweight Directory Access Protocol (LDAP) support


User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Default - Notify me only when programs try to make changes to my computer

- Don't notify me when I make changes to Windows settings

Recommended if you use familiar programs and visit familiar websites.

FIGURE 2: A control panel applet allows users with administrative privileges to configure User Access Control. A slider provides a choice of four levels of protection.

is also provided for enrollment compatible with existing CAs running Windows Server 2003 or Windows Server 2008. Administrators can use Group Policy to distribute Certificate Enrollment Web Services locations to domain users.

From a user perspective, Windows 7 makes certificate selection easier. Many applications and Internet browsers utilize a certificate selection dialog box to prompt users when multiple certificates are available. Unfortunately, users are often uncertain which selection to make. Windows 7 improves the user interface and underlying filtering logic to reduce the number of certificates presented to users; the ideal result is a single certificate that requires no action from the user.

Smart Cards. As the use of smart card technology increases, administrators are demanding more simplified methods for deployment and management. Windows 7 includes new features designed to both simplify deployment and expand smart card capabilities, including better support for plug-and-play devices. Any software developer who adheres to the Personal Identity Verification (PIV) standard can publish their drivers through Windows Updates. When a user inserts their smart card, Windows will attempt to download the driver from Windows Update; for PIV compliant smartcards, if a driver is unavailable, a compliant minidriver will automatically be used. As a result, in these types of scenarios middleware is no longer required for domain authentication using PKINIT, email and document signing, unlocking Bitlocker protected data, etc.

Windows 7 includes new features designed to both simplify deployment and expand smart card capabilities, including better support for plug-and-play devices.

Biometrics. Security professionals have long championed the need for multi-factor authentication, but because biometrics requires special hardware many organizations have hesitated to implement it with client computers. Fingerprint readers are becoming more common in computer systems, particularly portable computers, making it more feasible for organizations to utilize them as part of their authentication design. Windows 7 includes a Windows Biometric Framework which helps to provide a consistent user experience when utilizing a variety of devices. Provider support enables biometrics devices to perform UAC elevation when logging on to a local computer.

Driver management for biometric devices is now supported under Device Manager, but there is also a Biometric Devices Control Panel item that allows control over biometric devices and whether they can be used to logon to a domain or local computer. Policy settings have been added to Group Policy to ensure that administrators can easily enable, disable or limit the use of biometrics. With Group Policy, it's possible to prevent the installation of biometric device driver software or force it to be uninstalled.

DirectAccess. DirectAccess is a new Windows 7 connection capability that securely connects remote users to a Windows Server 2008 R2 server on which the Direct Access feature is installed. Once connected to the Direct Access server, enterprise applications, Web sites and network shared folders points are available. Direct access eliminates the need to first connect to a VPN before being granted access to internal resources. The goal is to securely and transparently provide a remote user with the exact same experience they would encounter while working in their office. Every time a user connects their portable computer to the Internet (even before they log on), DirectAccess establishes a bi-directional connectivity with the user's enterprise network using IPSec and Internet Protocol version 6 (IPv6). IPSec is used to authenticate the computer allowing it to establish an IPSec tunnel for the IPv6 traffic which acts as a gateway to the organization's intranet. IPSec is also used for user authentication, but smart cards can be required for stronger authentication. With DirectAccess, administrators can manage remote computers even when they are not connected to a VPN.

To establish a direct access connection, a Windows 7 computer must be a member of a domain with a Windows Server 2008 R2 Direct Access server. The client machine must be configured for IPv6 and be issued a certificate for use when connecting to the Direct Access website. While there are a number of elements that need to be configured on the server side (IIS, PKI, etc.), it's not complex or difficult, especially since Microsoft has provided a step-by-step deployment guide.

SYSTEM AND INFRASTRUCTURE INTEGRITY

Each time a user downloads or installs unauthorized items to a computer, the attack surface of the system is increased, along with corresponding risks to the organization. Controlling what users can download and install to client computers is essential for maintaining the health and security of an enterprise infrastructure. Windows 7 has features to help with on this front, including:

AppLocker. Software restriction policies were used in Windows XP and Vista to control which applications could be installed on users' computers. Because the rules were predominantly based on hashes, new rules had to be created each time an update to an application was released. This created a major management burden for administrators. AppLocker is a Windows 7 technology which eliminates this management burden.

AppLocker can be used to achieve three primary security objectives:

1. Prevent installation of malware.
2. Prevent users from installing and using unauthorized programs.
3. Meet compliance requirements regarding application control.

AppLocker provides flexibility and is easily implemented through new rule creation tools and Group Policy. Traditional allow and deny rules are expanded through the ability to create "exceptions." For example, you can specify a rule which allows Microsoft Office Suite but creates an exception to block specific users from using Microsoft Outlook 2010. New "Publisher Rules" are based on digital signatures and allow for creation of rules that will survive changes to a product; for instance, a rule that allows users to install updates and patches to an application as long as the product version hasn't changed.

ActiveX Controls. The ActiveX Installer Service (used to manage deployment of ActiveX controls) is now installed by default in Windows 7 and is configured to allow automatic startup when standard users access sites on the Trusted Sites list. Administrators can easily control the trusted sites list through Group Policy, but must also configure Internet Explorer trusted zones such that users cannot edit the Trusted Sites list. This is simple to implement but be aware that the site to zone list must have at least one entry to prevent standard users from installing arbitrary ActiveX controls.

Multiple Active Firewall Policies. Beginning with Windows Vista, firewall policies were based on the type of network connection (home, work, public or domain). While this simplified the configuration of appropriate firewall rules when mobile computers moved between locations, unfortunately it presented an entirely different security problem for administrator to overcome. If a user connected first to a home or public network and then connected to the corporate network through a VPN, the corporate firewall settings will not be applied. Windows 7 overcomes this obstacle by supporting multiple firewall policies on a single system. This allows domain-based settings to be applied to the computer regardless of what other networks it may be connected to.

MOVING FORWARD

Overall, the changes to Windows 7 are good steps that will assist enterprise administrators in better securing their environments while reducing the corresponding effort involved. In particular, the changes to BitLocker promise to increase client-side data protection to a higher level than previously possible. And enhancements to auditing capabilities allow an organization to more easily comply with regulatory requirements without implementing costly third-party solutions.

While Microsoft has made significant improvements in the ability to control what information is downloaded or installed to a computer, Windows could still benefit from a more robust built-in firewall. The basic protection of a system should not be largely dependent on third-party products, even those available from Microsoft.

Still, Windows 7 is a clear indication that Microsoft continues its commitment to security but is equally committed to finding ways to simplify implementation and ease the burden on administrators. ▸

Beth Quinlan is a trainer/consultant in infrastructure technologies and security design. Most recently she was the Project Manager and contributing author on several Microsoft Windows Server 2008 R2 and Windows 7 projects. Send comments on this article to feedback@infosecuritymag.com.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

CAREERS

DATABASE ACTIVITY MONITORING

BANKING MALWARE

WINDOWS 7 SECURITY

SPONSOR RESOURCES

ADVERTISING INDEX

Guardium, an IBM Company 2
http://www.guardium.com
- Databases at Risk - An ESG Research Brief
- 8 Steps to Holistic Database Security

Courion Corporation 4
http://www.courion.com/courion-identity-access-management.html
- New Meaning for ROI: "Risk of Insiders"
- Identity and Information Security Integration

Guidance Software, Inc. 8
www.guidancesoftware.com
- Tackling the Causes of Data Leakage and Data Loss
- Understanding Data Location is Imperative for Data Loss Prevention

The Academy Pro 11
www.theacademypro.com
- Free infosec videos for the information security community.

SystemExperts. 15
www.systemexperts.com

Glasshouse Technologies 18
http://www.glasshouse.com/

TECHTARGET SECURITY MEDIA GROUP

INFORMATION SECURITY®

EDITORIAL DIRECTOR Michael S. Mimoso

EDITOR Marcia Savage

ART & DESIGN
CREATIVE DIRECTOR Maureen Joyce

COLUMNISTS
Marcus Ranum, Bruce Schneier,
Lee Kushner, Mike Murray

CONTRIBUTING EDITORS
Michael Cobb, Eric Cole, James C. Foster,
Shon Harris, Richard Mackey Jr., Lisa Phifer,
Ed Skoudis, Joel Snyder

TECHNICAL EDITORS
Greg Balaze, Brad Causey, Mike Chapple, Peter
Giannacopoulos, Brent Huston, Phoram Mehta,
Sandra Kay Miller, Gary Moser, David Strom,
Steve Weil, Harris Weisman

USER ADVISORY BOARD
Edward Amoroso, AT&T
Anish Bhimani, JPMorgan Chase
Larry L. Brock, DuPont
Dave Dittrich
Ernie Hayden
Patrick Heim, Kaiser Permanente
Dan Houser, Cardinal Health
Patricia Myers, Williams-Sonoma
Ron Woerner, TD Ameritrade

SEARCHSECURITY.COM
SENIOR SITE EDITOR Eric Parizo

NEWS EDITOR Robert Westervelt

SITE EDITOR William Hurley

ASSISTANT EDITOR Maggie Wright

ASSISTANT EDITOR Carolyn Gibney

INFORMATION SECURITY DECISIONS
GENERAL MANAGER OF EVENTS Amy Cleary

EDITORIAL EVENTS MANAGER Karen Bagley

VICE PRESIDENT/GROUP PUBLISHER
Doug Olender

PUBLISHER Josh Garland

DIRECTOR OF PRODUCT MANAGEMENT
Susan Shaver

DIRECTOR OF MARKETING Kristin Hadley

SALES DIRECTOR Dara Such

CIRCULATION MANAGER Kate Sullivan

ASSOCIATE PROJECT MANAGER
Suzanne Jackson

PRODUCT MANAGEMENT & MARKETING
Corey Strader, Jennifer Labelle, Andrew McHugh

SALES REPRESENTATIVES
Eric Belcher ebelcher@techtarget.com

Patrick Eichmann peichmann@techtarget.com

Jason Olson jolson@techtarget.com

Jeff Tonello jtonello@techtarget.com

Nikki Wise nwise@techtarget.com

TECHTARGET INC.
CHIEF EXECUTIVE OFFICER Greg Strakosch

PRESIDENT Don Hawk

EXECUTIVE VICE PRESIDENT Kevin Beam

CHIEF FINANCIAL OFFICER Eric Sockol

EUROPEAN DISTRIBUTION
Parkway Gordon Phone 44-1491-875-386
www.parkway.co.uk

LIST RENTAL SERVICES
Julie Brown
Phone 781-657-1336 Fax 781-657-1100

REPRINTS
FosteReprints Rhonda Brown
Phone 866-879-9144 x194
rbrown@fostereprints.com

TechTarget
Where Serious Technology Buyers Decide

INFORMATION SECURITY (ISSN 1096-8903) is published monthly with a combined July/Aug., Dec./Jan. issue by TechTarget, 275 Grove Street, Newton, MA 02466 U.S.A.; Toll-Free 888-274-4111; Phone 617-431-9200; Fax 617-431-9201.