Online report sponsored by:

Feature articles & full report available for download at:
www.FCW.com/SpecialReportCybersecurity

Cybersecurity

Inside

Concerns grow as sophisticated attacks, automation evade detection

This summer, cybersecurity is seemingly making news daily, as the number and variety of incidents reported are growing. At the same time, federal government agencies and departments are striving hard to keep up with current and emerging threats.

A rash of high-profile breaches suggests that conventional defenses aren't working well. Breaches have cost Citigroup an estimated $2.7 million, RSA an estimated $100 million and an untold sum from the numerous attacks on Sony. According to industry news reports, hackers allegedly released 400M of internal data from government cybersecurity contractor ManTech International Corp. as part of a reported "weekly campaign" to embarrass the FBI, as well as other government agencies and their partners. The batch of documents appears to mostly involve NATO, along with the Homeland Security Department, U.S. military branches, and the State and Justice departments, according to those news reports.

Yet another recognized concern — social media — still isn't getting the security focus needed, based on findings from a newly published Government Accountability Office report. In late July, GAO released a report that outlined how all but one of 24 major federal agencies engage in social media while most still lack a clear plan to mitigate records management, privacy and security challenges.

Only seven agencies identified and documented possible security risks — such as spear phishing, social engineering and Web application attacks — to federal information systems when engaging with social media, according to the authors of the GAO report.

Only eight agencies conducted and documented privacy impact assessments to identify potential privacy risks associated with social media use. Twelve agencies describe whether they use personal information obtained from social media in a formal, updated privacy policy.

"Social networking sites, such as Facebook, encourage people to provide personal information that they intend to be used only for social purposes," the GAO report states. "Government agencies that participate in such sites may have access to this information and may need rules on how such information can be used."

Only the Interior Department had developed records management, privacy protection, and security risk management policies and procedures for social media use, according to GAO. The Small Business Administration, the Social Security Administration, the U.S. Agency for International Development and NASA lacked any policies and procedures for the use of social media services, according to the report's authors. GAO recommended that agencies ensure that appropriate records management, privacy and security measures are in place and published specific recommendations for each agency. Read the report at www.gao.gov/new.items/d11605.pdf.

Finally, approximately one in every 280 e-mail messages was identified as malicious in July, a significant increase in activity related to aggressive and rapidly changing polymorphic malware. The rise accounted for nearly 24 percent of all e-mail-borne malware intercepted by

Cybersecurity tools for defense in depth

The right combination of defenses can keep agency networks secure. The tools considered most important include:

- Firewalls, to inspect traffic and permit or deny access based on set policies.
- Virtual private networks, to provide secure remote network access to an increasingly mobile workforce.
- Web filtering, to monitor and control Web access and block unsafe or inappropriate sites.
- E-mail filtering, to monitor e-mail for malware and confidential information.
- Intrusion protection, to analyze network traffic to detect signs of malicious behavior.
- Antivirus/anti-spyware, to inspect e-mail and other traffic for a variety of threats and eliminate or quarantine malware to prevent its spread.
- Anti-spam, to review e-mail messages for signs of spam and block or reroute them to a special spam repository.

Symantec in July. And this is more than double the amount tabulated six months ago, indicating a more aggressive strategy by cyber criminals along with perhaps a greater use of automation, which has allowed attackers to increase their output, according to Paul Wood, senior intelligence analyst at Symantec.

Crucial cybersecurity tools, circa 2011

Some of the leading hot-button technologies that public-sector organizations should strive to investigate and possibly incorporate to address the increasing number of threats include:

- Real-time Web content ratings.
- Web 2.0 content filtering.
- Inline threat analysis (stream scanning).
- Social networking threat protection.
- Compressed archive analysis.
- File and attachment filtering.
- Hardware-based Secure Sockets Layer.
- Data loss prevention.
- Proxy avoidance blocking.

Polymorphic malware is harmful, destructive or intrusive software (a virus, worm, Trojan or spyware) that constantly "morphs," making it difficult to detect with anti-malware programs. The evolution of malicious code can occur in a variety of ways, such as file name changes, compression and encryption with variable keys.

According to Symantec's analysis, the number of variants, or different strains, of malware involved has also grown dramatically, by a factor of 25 times the same quantity six months ago. This alarming proliferation in such a short time heightens the risk for many organizations because new strains are harder to detect using traditional security defenses.

Polymorphic malware is also likely to be causing pain for a great number of traditional antivirus companies that rely on signatures, heuristics and software emulation to detect malicious activity, Symantec's Wood reported. This type of malware is frequently contained inside an executable file within an attached ZIP archive file and often disguised as a PDF file or office document.

Because organizations can't rely on signatures and heuristics alone, they must also take into account the integrity of an executable file based on knowledge of its reputation and circulation in the real world, Wood reported.

A growing malware threat

An ever-growing malware threat is driving federal agencies to "investigate solutions that can detect and protect their online Web and social media environments, including blocking inbound malware and analyzing outbound traffic to detect compromised endpoint systems," said Will Hedrich, a security architect at CDW-G.

There are solutions available that can be effective. Agencies can incorporate tools that include traditional signature-based malware analysis and detection of known bad Web destinations, along with real-time analysis to detect new and targeted threats, Hedrich explained. Among other key anti-malware approaches, the Stamford, Conn., Gartner Inc. reports that URL categorization is used to classify URLs on the fly, along with site reputation analysis and real-time code analysis to seek out common malware techniques in Web code.

Perimeter-based anti-malware protection must be supplemented by enhanced security policies as well. Government organizations should seek solutions that offer granular policy controls for social networks to further protect Web resources. According to Gartner's research, there's also growing interest in cloud-based services that can address the malware threat in Web 2.0 environments.

According to Gartner's research, in 2010, the secure Web gateway market reached $817 million, achieving growth of 17 percent over 2009. In 2011, Gartner estimates the market will grow approximately 17 percent, to just under $1 billion. The market is still dominated by the on-premises solutions (approximately 90 percent), with "secure Web gateway as a service" making up the remaining 10 percent of the market (approximately 10 percent). However, this cloud-based segment is the fastest growing and expected to grow 55 percent this year. ▲

Understanding mobile computing security

As mobile devices stream into all types of organizations in both the public and private sectors, there's growing anxiety in government agency IT departments about how to properly manage and secure mobile devices against a range of possible security breaches and malicious code attacks.

The numbers are staggering: Early in 2011, smart phone shipments exceeded PCs for the first time, according to IDC Research. The market research firm also reported that 365.4 million units were shipped in the second quarter of 2011, up 11.3 percent from the 328.4 million phones shipped in Q2 2010.

And it's not just phones. Gartner Inc., Stamford, Conn., predicts sales of 54.8 million media tablets in 2011 and sales of more than 208 million units by 2014. While smart phones and mobile devices are already visible in most government agencies today, public-sector IT organizations face an immediate challenge in ensuring adequate security.

Attacks on mobile networks and devices have grown in recent months, both in number and sophistication. Early security threats from young, independent hackers have turned into sophisticated attacks driven by experienced criminals or even state-sponsored terrorists. Threats, including those that compromise user data or privacy, are now targeting widely supported services such as text messaging and voice. Phishing attacks and traditional malware problems have also affected a surprisingly high number of mobile devices.

Challenges for federal IT administrators arise from the influx of "personal" devices into the workplace, the popularity of various mobile operating systems, and the need to balance access to data and networks with growing security requirements. Not surprisingly, security ranks high among most survey respondents. IPhones, iPads and other employee-owned mobile gear are the most risky devices that can be connected to an organization's networks, according to a recent survey by ISACA, an international user group devoted to providing benchmarks and guidance for technology best practices. Previously known as the Information Systems Audit and Control Association, ISACA polled 2,765 IT leaders around the world. According to the survey's results, 58 percent of respondents said employee-owned mobile gear — including smart phones, laptops, notebooks, tablets and flash drives — represents the greatest risk to organizations. To see the full results, visit www.isaca.org/risk-reward-barometer.

Nevertheless, mobile device use is exploding among government employees. The Veterans Affairs Department, for example, has announced plans to allow the use of Apple iPads and iPhones beginning Oct. 1, with a longer list of devices expected for approval soon. Currently, only BlackBerry smart phones are authorized for use by 20,000 VA employees.

Meanwhile, in July, Research in Motion received FIPS 140-2 certification for its BlackBerry PlayBook tablet. PlayBook is the first tablet certified for deployment within U.S. federal government agencies. No competing tablet has gained Federal Information Processing Standard certification from the National Institute of Standards and Technology, although Apple and Google are both working on FIPS certification for iOS and Android, respectively.

Government workers are creating and sharing information through a multitude of mediums — from e-mail, instant message and USB flash drive to voice over IP, smart phone, social media, public Wi-Fi networks and home computers. Each medium introduces security vulnerabilities that require protection. According to Will Hedrich, a security architect at CDW-G, the technology supplier is working closely with government clients to help them reach three primary pillars of stronger mobile security:

- Content filtering — Adopting a heuristic-based content filter with an anti-malware engine. The filter actively analyzes every packet of information and blocks dangerous content in real time.
- Mobile device management — Locking down mobile

devices (iPads, PlayBooks, etc.) to ensure information isn't hacked or stolen.
- Employing data loss prevention — Classifying data and preventing sensitive information from being downloaded or e-mailed outside the agency or to unauthorized agency employees.

"Because so many government workers are using personal smart phones and other mobile devices for work purposes, IT organizations suffer a giant headache as they must strive [to] keep in compliance with federal security standards, while safely allowing employee and contractor access to data and information," Hedrich said.

Don't forget the basics

Even as the threat vectors and technologies change, some basic security requirements seem to remain timelessly important. These include:

- Antivirus software remains an important tool, even more important than ever as social networks and third-party resources for cloud services and software as a service become part of organizational ecosystems.
- Password protection is useful. But many organizations are adding or even replacing traditional passwords with token generators coupled with biometric or smart card tools. This has grown especially common for accessing highly sensitive data.
- Strong authentication plus encryption remains important. The IT team should build in validation to ensure that an accessing user is in fact an authorized user and that the user's device is certified. Encryption begins with the channel of communication between the end user and the network, which is why Secure Sockets Layer virtual private networks have become so popular for providing remote access to trusted and untrusted devices.

CDW-G typically proposes mobile device management solutions from Symantec or McAfee, Hedrich explained, to provide the encryption, complex passwords and enforcement policies agencies need to protect government information and network resources. Some of the advanced features of mobile device management solutions include multifactor authentication, disabling of camera functions and/or access to "apps" stores, and the ability to block access from wireless local-area networks or connect only to certain specified networks.

There's also a remote lockout capability so that when a phone is left idle, it can be locked out of network access after a certain number of minutes. And the ability to wipe data remotely from mobile devices is vitally important when a device is lost or stolen, Hedrich explained. In some cases, mobile management solutions can even boot users off the network if they attempt to jailbreak their devices to work around agency security controls.

Meanwhile, Hedrich added that data loss prevention solutions from leading suppliers such as RSA, Symantec and McAfee can help protect data at rest as well as data in motion. DLP is used on networks, in data centers and for endpoint devices. DLP can stop users from sending PDFs or Excel spreadsheets, alerting the user and manager via an e-mail message to allow or reject such requests. Also, DLP tools can seek information and even pictures that fall outside personally identifiable information compliance parameters to stop users from sending files that compromise security guidelines.

DLP isn't a quick fix, however, because it requires proper security policies and education for every group of users in an organization. This type of solution typically takes at least six months to implement, he said. Policy and management issues can slow implementation.

Another important tool in the mobile security arsenal is content filtering, which can address the majority of threats that arise from the Web. In typical Google searches, for example, users might see 20 links, and some of those links might contain malicious code that installs a bug, bot or some other peer-to-peer attack, Hedrich said. This is why organizations need a real-time filter to determine if a website is safe and accept or deny access for any websites deemed inappropriate or dangerous. Even on reputable sites, there might be malware in some links, and content filtering will block those links from appearing on a Web page, Hedrich explained. ▲

NIST: A closer look at upcoming NIST cybersecurity events and new guidance

Donna Dodson, chief of the National Institute of Standards and Technology's Computer Security Division, outlined important upcoming events and revisions to security-related Special Publications, along with events aimed at assisting agencies in ongoing education, planning and reporting efforts.

The SP guidance series reports are part of NIST's ongoing FISMA Implementation Project, which develops and updates security standards to help agencies create and maintain robust information security programs and effectively manage risk. In an exclusive interview with 1105 Government Information Group Content Solutions, Dodson explained how those in the cybersecurity arena face a variant of the established Moore's law of microchip technology (which doubles the power of integrated circuits every two years). "The power of attackers now doubles every 18 months," she said.

NIST's standards testing, guidelines and special events are considered crucially important to the public-sector cybersecurity arsenal to help agencies address an ever-growing array of security challenges as they emerge, she explained.

Upcoming updates and events of interest to all parties involved in cybersecurity efforts include:

- Sept. 20-22, at the NIST Campus in Gaithersburg, Md., an educational workshop is planned, "Shaping the Future of Cybersecurity Education: Engaging Americans in Securing Cyberspace." This three-day conference will highlight the work of the National Initiative for Cybersecurity Education, which is made up of cybersecurity experts from NIST along with the Homeland Security Department, Education Department, National Science Foundation, Defense Department and Office of the Director of National Intelligence. More details about this event are available online at csrc.nist.gov/nice.

- Also in September, there's a Technology Workshop planned to support the National Strategy for Trusted Identities in Cyberspace initiative. NSTIC is a NIST-supported partnership between government and industry that's focused on improving information assurance across the Internet. NSTIC is focused on developing ways to help reduce identity theft and build a vibrant marketplace that allows people to choose among multiple identity providers — both private and public — that would issue trusted credentials to prove identity. Interested parties both in government and the private sector should follow updates at www.nist.gov/nstic to learn more about this upcoming NSTIC event.

- Oct. 31-Nov. 2, 2011, NIST will lead the 7th Annual IT Security Automation Conference at the Hyatt Regency Crystal City in Arlington, Va. This upcoming conference will include educational tracks dedicated to continuous monitoring, software assurance, network security automation, management and compliance guidelines, and updates on IT security threats. "We will be featuring not just the tools and techniques to help agencies automate, manage and better control IT environments, but also the use cases that help prove how these technological tools really work," Dodson explained. More information is available at www.nist.gov/itl/csd/7th-annual-scap-conference.cfm.

- A new version of SP 800-30, "Risk Management Guide for Information Technology Systems," csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, is due to be released later in the summer (perhaps by the time this report publishes) to provide newly enhanced guidelines for agency risk assessment procedures.

- In the fall, agencies can expect Revision 2 of SP 800-18, "Guide for Developing Security Plans for Federal Information Systems," csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf, which will deliver updated security planning guidance

centered on the topics of security automation with Security Content Automation Protocol and continuous monitoring.

- Revision 4 of SP 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf, is due to be released late in 2011 and will deliver updated privacy controls guidance to strengthen the relationship between privacy and security in federal agency security procedures. "With the widespread use of small mobile devices in government, security and privacy issues are more critical than ever," Dodson said. New privacy controls to be added to SP 800-53 will cover transparency, individual participation and redress, data minimization and retention, use limitations, data quality, integrity and security as well as new accountability, audit and risk management controls. Other types of controls NIST is considering adding to SP 800-53 include those involving insider threats, Web-based and application security, mobile computing, cloud computing, and industrial control systems.

- Security and performance evaluations of finalists will occur in an SHA-3 cryptographic contest. NIST has launched this contest to develop a new cryptographic hash algorithm via a public competition to augment FIPS 180-4, the Secure Hash Standard. A winning algorithm will be selected in 2012, with a revised standard planned to be ready for approval in early 2013.

- Cybersecurity-related standards for the electric Smart Grid are expected in the first quarter of 2012. NIST is heavily involved in cybersecurity standards to support the development of the electric Smart Grid. Dodson described NIST's standards development work here as "a critical mission for us." NIST initiated the Smart Grid Interoperability Panel under the Energy Independence and Security Act of 2007. This group, with more than 600 members, is helping define requirements for essential communication protocols and other common specifications, including security. ▲

Argonne National Laboratory embraces holistic cybersecurity

The Argonne National Laboratory, a multipurpose Energy Department national laboratory based in the Chicago area, is working to maintain a holistic cybersecurity strategy, building in deeper levels of integration and situational awareness to adapt to ongoing threats and risks.

When the team at Argonne first investigated cybersecurity in 1999, everything was driven by network port numbers. The lab leveraged network data flow to figure out where servers were located, which served the Internet, and which were used to service the lab's internal community.

Now the mantra at Argonne has shifted from a focus on networks to one that centers on "know thy data." The lab's current cybersecurity architecture review group includes members from all the different business units in the organization. This committee was charged with developing the initial architecture, and meets on a regular basis to review and update the architecture.

Argonne has found it important to manage network security from the inside out, while coordinating involvement among all departments and business units. Argonne's security architecture now provides an example of a more holistic security policy that uses the cohesiveness of all internal business units to deal with every aspect of keeping a network from being vulnerable to attack.

The focus now is on risk avoidance and getting more involved in the daily operational decisions involved in running the organization. Unlike a decade ago, most applications no longer reside solely on local networks. More applications reside on the Internet, which causes difficulties for IT organizations because it's impossible to control everything users touch. Many organizations are also dealing with network perimeter erosion due to ever increasing numbers of mobile workers.

In general, public-sector organizations should assume that malicious users are in the network and they must find ways to protect access to critical systems and data. Maintaining secure networks is challenging when there's unknown traffic on the network and it can be difficult to control what this traffic is doing both internally between networks and outside of the organization to the Internet.

To achieve greater security, organizations such as Argonne have learned it's important to make sure security policy supports the organization's primary mission goals. To accomplish this goal, public-sector organizations assign risk and the probability of certain risks occurring to all important operational systems and applications. This can help managers determine how much it would cost to lose a critical system and whether that's a risk they want to assume.

Elements of strong security

A strong security policy must encompass three primary components:

- Confidentiality or role-based policies that state whom should see what data.
- Integrity or ensuring that the data for a particular system is in a known good state.
- Availability or access to systems or processes when a user needs it to perform a specific task.

All about risk

Federal agencies as well as organizations in the financial sector face strong requirements to protect critical information and avoid risks associated with data loss or exposure or misuse. This has led to a greater focus across most government organizations on consolidation – especially when it comes to the number of Web gateways used, which can lower costs and help reduce possible exposure to risks.

The lack of proper security controls would leave any organization vulnerable to compliance problems based on federal regulations designed to protect the security and privacy of agency information. Argonne deals with compliance problem with education. The lab has worked hard to make sure its personnel are aware of Energy's definition of personally identifiable information, which has helped the organization to better protect data with strict standards that define when problems need to be reported to Energy. ▲

Best practices advice for securing agency information

Symantec just issued new guidelines designed to help organizations better secure IT operations. Boiled down, the key advice includes:

1. Employ defense-in-depth — Emphasize multiple, overlapping, and mutually supportive defensive systems, including deploying updated firewalls, gateway antivirus, intrusion detection, intrusion protection systems, and Web security gateway solutions.

2. Monitor for threats — Watch for network intrusions, propagation attempts and suspicious traffic patterns. Identify attempted connections to known malicious or suspicious hosts. Receive alerts for new vulnerabilities for proactive remediation. Track brand abuse through domain alerting and fictitious site reporting.

3. Antivirus on endpoints is not enough — Signature-based antivirus won't protect against today's Web attacks. Deploy a comprehensive endpoint security solution with endpoint intrusion prevention, browser protection against obfuscated Web-based attacks. Consider cloud-based malware prevention, and file and Web-based reputation solutions that provide a risk-and-reputation rating of any application and Web site to prevent rapidly mutating and polymorphic malware.

4. Use encryption to protect sensitive data.

5. Use Data Loss Prevention to help prevent data breaches — Implement a DLP solution to discover sensitive data, monitor its use and protect it from loss. Data loss prevention should be implemented to monitor the flow of data as it leaves the organization and monitor copying sensitive data to external devices or Web sites. DLP can identify and block suspicious copying or downloading of sensitive data.

6. Implement a removable media policy — Where practical, restrict unauthorized devices such as external portable hard-drives and other removable media. Such devices can introduce malware and facilitate intellectual property breaches. If external media devices are permitted, automatically scan them for viruses upon connection to the network and use a DLP solution to monitor and restrict copying confidential data to unencrypted external storage devices.

7. Update security countermeasures frequently and rapidly — Organizations should update security virus and intrusion prevention definitions at least daily.

8. Aggressively update, patch and migrate from outdated and insecure browsers, applications and browser plug-ins to the latest available versions using automatic update mechanisms. Wherever possible, automate patch deployments to maintain protection against vulnerabilities across the organization.

9. Enforce an effective password policy — Ensure passwords are at least eight to 10 characters long and include a mixture of letters and numbers. Encourage users to avoid re-using the same passwords on multiple Web sites, and sharing passwords with others. Passwords should be changed at least every 90 days. Avoid writing down passwords.

10. Restrict e-mail attachments — Configure mail servers to block or remove e-mail that contains file attachments that are commonly used to spread viruses, such as .VBS, .BAT, .EXE, .PIF, and .SCR files. Organizations should investigate policies for .PDFs that are included as e-mail attachments.

11. Ensure the proper infection and incident response procedures — Keep security vendor contact information, know whom to call, and what steps to take if one or more systems are infected.

12. Educate users about new threats — Don't open

attachments unless they are expected and from a trusted source and don't execute software downloaded from the Internet unless the download has been scanned for viruses. Be cautious when clicking on URLs in e-mails or social media programs. Deploy Web browser URL reputation plug-in solutions that display the reputation of websites from searches. ▲

ACCESS GRANTED.
BREACHES DENIED.

It's a fine line. You need to let the right people in and keep the wrong ones out. With best-in-class vendors, dedicated account managers and highly trained solution architects, we'll help you do it. Through our risk assessment, we can identify vulnerabilities in your system. Find the holes. And help fix them. So you get mobility without vulnerability. All you need to do is call or click.

800.767.4239 | CDWG.com/security

Cisco® ASA 5510 IPS Solution Bundle
CDWG 1588383

- Security appliance – with advanced inspection and prevention security services module
- Provides intrusion prevention, firewall and VPN in a single, easy-to-deploy platform
- Protection against threats, including worms

Symantec™ Data Loss Prevention
CDWG 2372029

- Unified solution to discover, monitor and protect confidential data wherever it is stored or used
- Create an inventory of sensitive data and automatically manage data cleanup
- Gain enterprise visibility

Symantec Endpoint Protection 12.1
CDWG 2421088

- Unrivaled security, blazing performance, built for virtual environments
- Powered by Insight and provides fast, powerful security for endpoints
- Offers advanced defense against both physical and virtual system attacks

CDW·G PEOPLE WHO GET IT™

Offers subject to CDW·G's standard terms and conditions of sale, available at CDWG.com. ©2011 CDW Government LLC. CDW®, CDW·G® and PEOPLE WHO GET IT™ are trademarks of CDW, LLC.