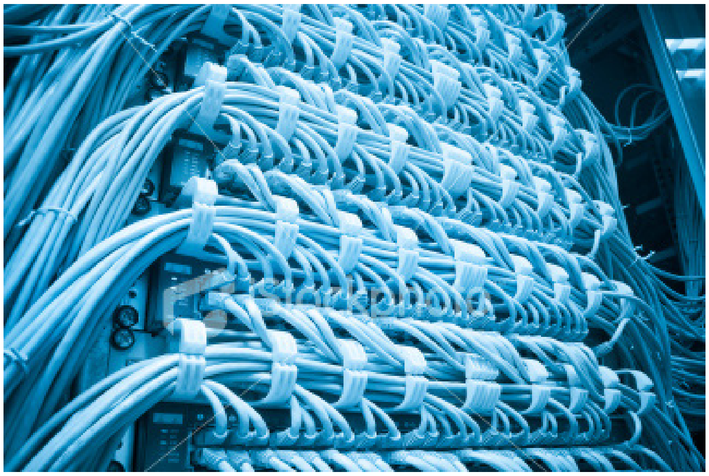
Government Executive

UNDERWRITTEN BY NetIQ

Data-Driven Security

How agencies can spot threats and trends amidst reams of data.

By Carolyn Duffy Marsan



Malware. Phishing. Stolen laptops. Rogue insiders. A constant barrage of increasingly sophisticated cyberattacks is aimed at the U.S. government, which is struggling to find a successful and cost-effective strategy for battling these threats.

Agencies spent $14.6 billion on information technology security in 2012—$1.3 billion more than the previous year, according to an annual report on compliance with the 2002 Federal Information Security Management Act published in March 2013. Despite this massive investment, FISMA scores declined governmentwide. The report cited inadequate training, lagging use of smartcards to restrict network access and a failure to automatically configure system settings as reasons for the lower scores.

To improve their cybersecurity posture, agencies are gathering more data about network activity than ever before. They're monitoring traffic flows between federal networks and the public Internet, and they're deploying standards-based dashboards with real-time reporting about security-related incidents. Looking ahead, one of the big challenges will be sorting through all of this data to proactively identify threats and security breaches.

Here are four things you need to know about where the cybersecurity threat is headed in 2014 and what you can do about it.

Scope of the Problem

The cybersecurity challenge is enormous, and IT leaders with tight budgets must figure out a way to keep threats at bay without additional resources.

iStock

Agencies reported 49,000 computer security incidents during 2012, up 11 percent from the previous year, according to the FISMA report. The most common problem cited was phishing, a type of social engineering attack that accounted for 68.3 percent of reported security breaches. Other problems included mishandling of personally identifiable information (8.9 percent of incidents), security policy violations (6 percent) and malware (5.8 percent). Another big problem was lost or stolen equipment, including laptops, mobile devices and smartcards.

Even more alarming, the number of incidents reported to the U.S.-Computer Emergency Readiness Team increased 42 percent during the last year. This includes all reported breaches from every sector of the U.S. economy — a sign of the growing cybersecurity threat the nation faces.

Focus on Data Gathering

To protect the nation's information assets, the federal government is focusing on several initiatives: the Trusted

Internet Connections program, continuous monitoring and smartcard-based authentication.

Through the TIC program, agencies are reducing the number of access points to the Internet and deploying state-of-the-art firewalls and intrusion detection systems at each of these access points. They are now implementing TIC version 2.0, which supports IPv6, the next-generation Internet Protocol.

IT executives also are encouraged to deploy continuous monitoring systems to maintain ongoing awareness of vulnerabilities, threats and overall cybersecurity posture. The National Institute of Standards and Technology is developing a standards-based approach for data gathering and reporting, in which a key component is the Security Content Automation Protocol. In addition, the Homeland Security Department has issued a request for proposals for a cloud-based continuous monitoring service that would provide a dashboard with agency and governmentwide tracking views.

For access to facilities and information systems, agencies are required to follow specific rules on the use of smartcards for authentication and how to issue them to federal employees and contractors.

Data-Driven Security

With the federal government gathering more cybersecurity data than ever before, interest in data-driven security is growing. This involves data mining, data analytics and quantitative statistics to identify threats. It essentially applies big data tools to the cybersecurity problem.

The financial services industry is already adopting data-driven security. Banks are analyzing the data they gather about their users, systems and networks from data feeds such as SQL server logs, firewall logs and NetFlow data. Then they are figuring out ways to extract the most important data, correlate it with other data and contextualize it to provide useful information. Instead of relying on standard reports from network devices, they are analyzing the raw data using metrics that are more meaningful to their operations.

With the federal government gathering more cybersecurity data than ever before, interest in data-driven security is growing. This involves data mining, data analytics and quantitative statistics to identify threats. It essentially applies big data tools to the cybersecurity problem.

What they've found is that answers to important security questions are already in their IT environment. It's just a question of figuring out where and how to get to that information. An organization could look at how many rogue systems are on their network, for example, alongside data about who has accessed them in the past week.

Proponents of data-driven security say agencies can use the huge volumes of data that they are already gathering to spot new threats, sharpen defenses and develop more effective risk-management strategies. Data analytics tools are expected to evolve over the next three to five years to enable a range of predictive capabilities and automated real-time controls that could give agencies a powerful weapon against cyberattacks.

At NetIQ, we make your challenge our mission.

In today's be-productive, be-competitive business world, your business users need to access mission-critical data and services any time business demands—and from anywhere. But if your access capabilities aren't identity-aware—based on who is trying to access what, where are they located and what devices are they using—you're increasing risk to your environment. At NetIQ, we work to understand your unique needs and help you secure, manage and monitor the services your business is using—including who is trying to use them, when, how often and from where. The result? Intelligent access that delivers value at the speed your business demands.

Learn how to turn challenge into opportunity.
www.netiq.com/GovExecMag

NetIQ®