Sponsored Content

FCW

Putting Dashboards to Work for Real-Time Cyberthreat Analysis

Implementing near real-time Continuous Diagnostics and Mitigation (CDM) into a cybersecurity program is becoming the best way to thwart breaches

Federal agencies have gone to great lengths to protect sensitive information from falling into the wrong hands by installing intrusion-detection systems, data loss prevention systems, firewalls and much more. With these systems, they have made a lot of progress, yet breaches still occur.

Much of the disconnect is due to the increasingly sophisticated, ever-changing methods hackers are using to gain access, and it is extremely hard for agencies to keep pace. No longer is it good enough to track these systems using spreadsheets and point-in-time snapshots—the hackers are smart enough and fast enough to circumvent any tracking method that isn't close to real time.

Federal cybersecurity experts understand this, and are urging agencies to move to near real-time dashboards to track and manage threats. Agencies are being required to implement the Continuous Diagnostics and Mitigation (CDM) program, which provides a current, at-a-glance status of network issues. The CDM program, administered by the General Services Administration and the Department of Homeland Security (DHS), is designed to help network administrators understand risks to their networks in near real-time so they can quickly mitigate them.

Underlying the CDM program is the dashboard—a system that collects current network trends and vulnerabilities from the appliances, tools and software connected to it and provides that information on an easy-to-read display. Dashboards provide an instant "big picture" of an enterprise's cybersecurity posture.

The CDM program is still in its early phases. Phase 1 focuses on controlling assets residing on networks and ensuring that any vulnerabilities are identified and mitigated. DHS has chosen the RSA Archer governance risk and compliance platform as the federal-level dashboard to be released in conjunction with the implementation of Phase 1.

Next up is Phase 2, focusing on account access and privilege management, ports and protocols for infrastructure devices, and configuration settings; and Phase 3, focusing on boundary protection and event management. Agencies are just now awarding Phase 1 contracts, but the goal is for all federal networks to be using CDM by 2016.

"Federal CISOs are finding their jobs evolve. They are being asked to look beyond compliance to providing cyber-related insights to executives for mission planning," said Mike Brown, Vice President and General Manager of RSA Global Public Sector. "The dashboard is designed to allow federal agencies to collect data, such as scan reports from sensors, and export customized reports for IT leaders to enable them to make more informed decisions."

DIFFERENT DASHBOARDS FOR DIFFERENT REQUIREMENTS

Dashboards can take various forms, and they can be targeted to different roles within the agency. For example, an executive dashboard would show these threats at a high level, providing Chief Information Security Officers (CISOs) with real-time information they can use for both mitigation and budget justifications. A network manager or cybersecurity manager might have a dashboard with more specific, actionable information based on their role, such as virus information or patch availability and installation status.

> DASHBOARDS PROVIDE AN INSTANT "BIG PICTURE" OF AN ENTERPRISE'S CYBERSECURITY POSTURE.

The most effective dashboard tools allow agencies to customize based on the audience, says Dan Waddell, Director of U.S. Government Affairs at (ISC)². Waddell has extensive experience in information security as a former advisor for numerous federal agencies.

"A legal or compliance team focused on FISMA would want information that could help them ensure that the agency was on track

from an IG and audit perspective, while your security operations center would be more focused on the operational side," he said.

GETTING THE BASICS RIGHT

Getting the dashboard right requires a lot of input and thought. It's worth the effort; getting it wrong can result in security missteps. "Any missing item is one less piece of the security puzzle to base decisions on," said Louis Magnotti, former CISO for the U.S. House of Representatives and currently Vice President of IT Services and Security for Pentagon Federal Credit Union.

The primary function of a dashboard is to collect relevant data from networks, security monitoring tools, IP addresses, hardware, software, and whatever else the agency relies on, such as GPS. Making sure you are collecting information from the right systems is critical to success.

The second piece of the puzzle is tracking the right metrics. There are many metrics that are relevant to all organizations and users, but some will depend on the agency's mission, while others will depend on who will be using the dashboard. A metric that might be relevant for the CISO, for example, may not be relevant for the compliance team.

In general, a dashboard devoted to cybersecurity should include metrics such as type and number of malware found, number of IDS hits, firewall blocks, failed log-ins, patch availability and installation, number of unknown IP addresses, and sensitive information that has been removed or redacted. There are many others that can be tracked, depending on the mission of the agency.

With the right metrics, agencies should be able to answer questions like:

- What events are occurring or have occurred during a specific time period against the current network and operating environment?
- What are the cyber risk trends?
- Have we quickly tested and implemented patches as they are issued?
- Have we lost data in recent incidents?
- Is the current situation critical, or is it just a penetration attempt that has failed?
- How long did it take us to respond and mitigate the most recent threat?
- When and where did the cyberattacker enter the network?
- How long did it take us to shut them down?
- Have we fixed the vulnerability that caused the most recent breach?

MAKING SURE YOU ARE COLLECTING INFORMATION FROM THE RIGHT SYSTEMS IS CRITICAL TO SUCCESS.

Along with collecting the right data and measuring the right metrics, it's important to prioritize monitoring and notification. Not everything can be top priority, and the devices and metrics that rise to the top will be different for every agency and situation.

"Knowing that you aren't going to be able to defend and fix everything at the same time, you want to be able to defend and fix the most important IP addresses and servers," Waddell said. "Start by identifying those critical assets first, and then prioritize from there, creating groups. Group A would be your absolutely critical group of systems where you must know right away if anything happens. Group B might be your cloud-based email and servers, where a 24-hour response is acceptable."

FINE-TUNING THE DASHBOARD APPROACH

Dashboards can make all the difference in protecting agencies against cyberthreats, but the dashboards themselves are only one piece of the solution. The others are people, policies and adaptability.

People are a critical asset. Once the dashboard is in place, it is important to train users how to both interpret the data and act on it. It's also important for cybersecurity teams to learn from dashboard missteps. If, for example, the dashboard misses an attack, make sure the team understands why it happened. Did the dashboard fail to report something? Is there an appliance we aren't monitoring? Use that after-action report to fix the dashboard and make sure it doesn't happen again.

Finally, make sure the team is focusing more on improving security and less on simply doing what it takes to change the "red" flags to "green." "It's not about getting to green," Waddell said. "Green will happen naturally if you focus on making the environment more secure."

With a dashboard approach, incorporated in government programs such as CDM, agencies can clearly improve the speed and accuracy of tracking and managing threats. With a clear view of network issues, real-time dashboards are an important advance in the war against cybercrime.

For more information, visit:

carahsoft.

carahsoft.com/cdm
or call 703-230-7534