MINIMIZING CYBER RISK WITH SMARTER CYBER-HYGIENE PRACTICES

FedScoop | CyberScoop Report

Simulating network rules through modeling and applying the basics of cyber-hygiene can help agencies mitigate their growing cyber risks.

To give network defenders the edge in defending against cyberattacks, federal agencies must get back to the basics of cyber-hygiene. This includes identifying out-of-date configuration rules still lurking in agency networks.

This message was reinforced in a January 2020 ***bulletin*** issued by the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency team, warning of an increase in cyberspace activity from actors such as Iran and Hezbollah.

To best prepare, DHS warned agencies to "implement basic cyber-hygiene practices" and cautioned that they may experience heightened "cyber disruptions, suspicious emails, and network delays."

However, given the scale and complexity of agency networks, implementing basic cyber-hygiene has become a herculean task that requires a combination of new strategies and more sophisticated tools.

Limiting cyber risk – underneath the layers of past decisions

Every change an agency makes to modernize its network environment can leave behind a trail of outdated configurations. Each of those unattended connections carry a certain amount of vulnerability and potential risk.

Agencies that have built their network infrastructure over decades face more significant challenges today due to legacy accesses, especially if they haven't kept up with basic cyber-hygiene practices. Those practices that allow an agency to know how applications and devices are connected to the network, and ensure rules are current, are imperative to minimize cyber risk – especially when third-party connections are taken under consideration.

Agency staff turnover contributes to cyber-hygiene issues as well. As network architects and managers come and go over time, the current IT team may not know why or when rules were put in place for the routers, firewalls, access control lists (ACL) and applications.

"Consider an agency that has been around since the 1940's," illustrates Wayne Lloyd, federal chief technology officer for RedSeal. "At some point in time they gave access to their IP address to multiple contractors. At another point in time they allowed phone lines from countries overseas to dial into their networks. Access privileges were put into place for both mission and business reasons — for all sorts of valid justifications — but nobody today knows why."

> “
>
> **Consider an agency that has been around since the 1940's … Access privileges were put into place for both mission and business reasons — for all sorts of valid justifications — but nobody today knows why.**
>
> - Wayne Lloyd, Federal CTO, RedSeal

Because of poor hygiene practices, Lloyd says that unknown connections to the network could allow an adversary to just walk in because there was a rule that said they could.

Cyber risk management is a growing concern for both private sector and government agencies. Threats are targeted and sophisticated, and organizations must manage several risk factors: financial, operational and reputational. For agency leaders the ramifications of poor cyber-hygiene practices will carry greater risk and higher costs.

Cyber-hygiene – a monumental undertaking

To deal with increased workloads, including the basics of cyber-hygiene, agencies need to firmly establish which systems and data are most critical to protect. Only then can they implement best practices for monitoring, configuring and patching systems effectively.

To accomplish this requires tackling the challenge of scale. For example, Lloyd points out that to update a typical firewall, it would require reviewing and validating up to a million rules. Even if an experienced engineer could validate a rule a minute, working 7 days a week, it would take a little over a year to evaluate one firewall.

But if an agency has hundreds or thousands of firewalls — and countless other ACLs — the job of maintaining proper cyber-hygiene practices can easily overwhelm any one IT team.

Equipping IT teams with tools that are up to the task

An additional step to tackling the workload starts with fully incorporating the guidelines spelled out in the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Among other provisions, it details how to prioritize risk assessments across an agency's operations and the steps to take for monitoring and mitigating those risks.

One of the dilemmas agencies face in following these guidelines, however, occurs when they acquire a host of security solutions, including network mapping tools, that may tell them what's on their network without fully providing context into those connections that can help better understand where their vulnerabilities lie.

For instance, using a two-dimensional network mapping tool only gives insight into how network devices are currently connected to one another other. Network modeling, in contrast, provides agencies with greater context into the rules of each device as well as the forwarding decisions of those devices. Network modeling is a simulation tool – much like flight, weather or engineering simulators – to help IT solve hypothetical problems.

Routing rules, access control rules, network rules — all of these feed into the model so it can more accurately treat a theoretical packet the same way a physical network would treat a real packet, Lloyd explains.

In this way, agencies can use network modeling tools to help its IT workforce not only evaluate the impact of planned changes to its network, but also review past connections and rules to see where vulnerabilities lie.

Another critical consideration in maintaining cyber-hygiene, Lloyd says, involves folding in the necessary automation tools so that your IT teams won't have to constantly revisit configuration rules across routers, switches, firewalls and cloud interfaces.

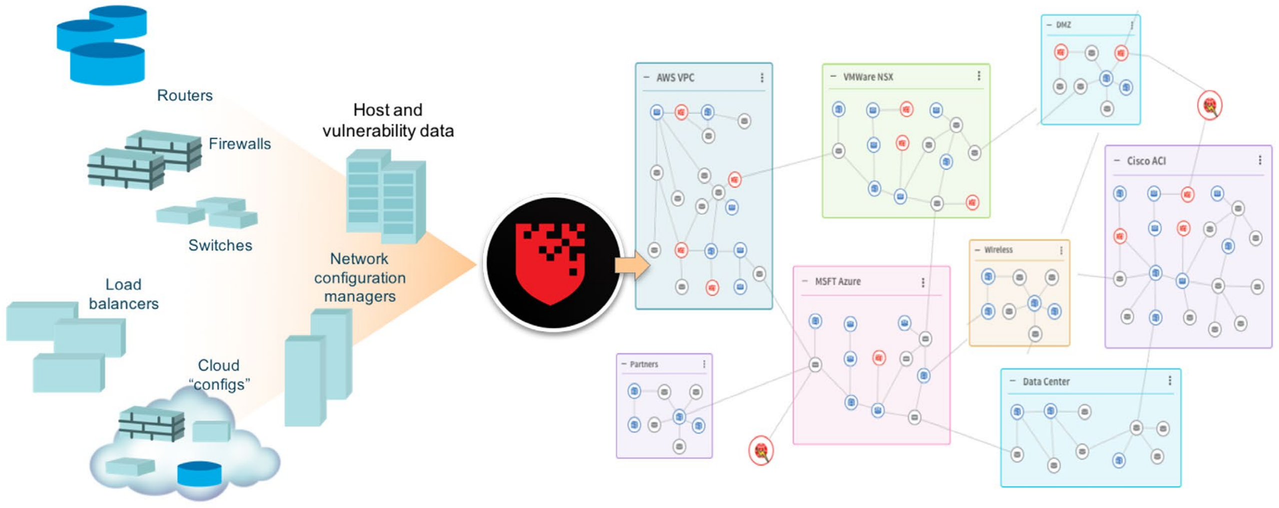
"You are still going to need a human there, to pull it into context," he says, but automation greatly enhances their ability to manage enterprise networks that require repetitive and continuous verification.

Helping leaders build context into business decisions

When considering an organization's overall security posture, agency leaders need to be aware of external threats, but they also should focus their attention on internal metrics about network state, health and configuration that may be more informative.

To help executives more accurately understand the costs associated with cybersecurity risks, they need to have access to data which can drive decisions on budget and where to allocate spending.

The primary input for the network model comes from configuration files RedSeal takes in from switches, routers, firewalls and load balancers. RedSeal integrates with public cloud and private cloud managers to include all network environments in the model.



RedSeal's Digital Resilience Score helps organizations understand their overall security it three key areas: defensive gaps, weaknesses revealed by attack simulations, and blind spots in network awareness.

> **When you know what your network looks like and how everything is connected, you can also identify what's the greatest risk.**
>
> - Wayne Lloyd, Federal CTO, RedSeal

"Agencies need a tool that enables them to be more effective with their time," says Lloyd. "If you think about when your engineer is reading a million rules, is that time well spent? There's an argument to be made that its absolutely time well spent. But is it really time well spent out of everything else that needs to be accomplished?"

Empowering executive decision-making on how to get better results from the IT team and turning that around to speed up incident response means that cyber risk management is now informing smarter business decisions on how agencies prioritize cyber-hygiene practices.

Tools that help mitigate cyber risk and hygiene at scale

Lloyd shares the ultimate importance of practicing cyber-hygiene at scale is to understand your risk and taking the appropriate steps to move forward.

That's why incorporating a network modeling platform like RedSeal's is important to provide context to vulnerabilities. "When you know what your network looks like and how everything is connected, you can also identify what's the greatest risk," he says.

More specifically he recommends that agencies evaluating network modeling platforms look for key features, including the ability to:

- Evaluate network device configuration, network segmentation policies and application-based policies in addition to endpoint information from multiple sources.
- Continuously monitor compliance with policies and regulations.
- Work with public and private cloud managers.
- Integrate with existing security tools for greater contextual awareness.
- Provide network mapping for greater situational awareness to contain threats and prevent downstream infections

"There are many [tools] out there, and we have all heard about the customers having tool bloat — too many tools and not enough people to run them," says Lloyd. But the benefit of RedSeal's platform is that it is dynamic.

"All you have to do is ask the question, 'Hey RedSeal, show me this network path – and it shows you,' Lloyd says.

Learn more how network modeling tools can help improve cyber-hygiene practices.

This report was produced by FedScoop and underwritten by RedSeal.

fedscoop | cyberscoop

REDSEAL