The Four Pillars of Cyber Hygiene

DAVID L HENDERSON

Originally published on govloop

What is cyber hygiene?

The term "cyber hygiene" is appropriate for several reasons, but mostly because the vast majority of people would agree on the importance of keeping something healthy, cyber or otherwise. For us cybersecurity practitioners, the term works well to explain simple, readily available technologies and practices that are foundational for any organization.

What are those simple technologies and practices that support a solid approach to cyber hygiene?

As I explained in a recent blog, the capability to "know what assets there are, how they are configured, what's vulnerable, what's changing, what's failing, who's doing what—and having a log footprint to back it all up..." is at the core of any good cyber hygiene effort.

In my experience, the four core areas, or "pillars," that enable an organization to accomplish this are:

1. Known inventory
2. Configuration and patch management
3. Log management, and
4. Data management.

Organizations then use security frameworks as a baseline to determine their organization's cyber hygiene foundation using these four pillars.

Is it widely practiced?

Given the simplicity, does that mean every agency has a strong cyber hygiene foundation? The answer is "no." In our survey of 306 IT security professionals, we found that nearly two-thirds of organizations didn't use hardening benchmarks to establish a secure baseline.

This negatively impacts the quality of an organization's cyber hygiene in several ways:

» More than half (57%) of respondents to Tripwire's report said it takes hours, weeks, months—or longer—to detect new devices connecting to the corporate network

» 40% of organizations admitted that they don't conduct vulnerability scans weekly or on a more frequent basis, and just half run more comprehensive scans

» The majority (54%) of survey participants stated that their organization is not collecting logs from all critical systems and amassing them into a central location

» About a third of organizations stated that they don't require default passwords to be changed and don't use multi-factor authentication, at 31% and 41%, respectively

Organizations in both the public and private sectors are guilty of neglecting even the most basic cybersecurity practices. For government agencies, the budget factor tends to be the primary driver of cybersecurity maturity. Depending on the agency, the administration's proposed 2020 budget could really strengthen the government's cybersecurity efforts (i.e. the DoD with a proposed $9.6B) or leave it as the status quo (i.e. DHS with no real increase proposed).

Given the likely continuance of budgetary restraints, government security personnel need to shift their thinking from "tough, battle-hardened" warriors, to knowing how to simply "make our beds."*

What does that look like? The following processes are rooted in security basics, but need not be complicated.

*Editor's Note

Since this piece was published on GovLoop in May 2019, almost $2B in funding has been made available to support technology and cyber improvements in the federal government. Also since then, the SolarWinds breach—one of the government's most widespread and damaging cyber-espionage incidents—took place. As a result, there is a renewed focus on the importance of cyber hygiene throughout the federal government. Secretary of Homeland Security Alejandro Mayorkas said during his confirmation hearings, "CISA must improve the cyber hygiene of the federal government, of the many departments and agencies throughout it." Given the available funding and renewed focus, agency personnel must revisit their cyber hygiene approach and increase their efforts to get back to the basics.

The four pillars

Know Your Inventory

In a world with mobile devices and cloud installations everywhere, it's not easy to know what's on the network. That's why knowing your inventory is a foundational pillar.

Consider the following:

- Are systems in place to acquire and manage a reliable inventory *and* to keep that inventory up-to-date?
- Is your agency able to block devices that don't belong on the network?

Configuration and Patch Management

The key to configuration and patch management is using a software that can harvest endpoint baselines of systems and then using that baseline to monitor the endpoints for deviations or changes from its baseline in real-time or on a scheduled check basis.

Consider the following:

- Does your agency document all policies for configuring devices and systems on your network?
- Can your security systems detect configuration changes and enforce proper settings?
- Do you have a patch management system, including a testing, deployment and rollback process?
- Are unnecessary processes running on servers? Are unused ports open on firewalls?

Log Management

Does your agency take user authentication seriously? That means auditing user activity and attributes, global policy and other Active Directory attributes, as well as, local endpoint users and group data.

Consider the following:

- Can your security systems identify anomalous user behavior?
- Does your agency document where data is allowed to go — and where it is NOT allowed to go?
- If a user or system behaves strangely, how timely and effective is the response?

Data Management

Agencies should have a complete picture of where sensitive data resides on the network. Similar to knowing your inventory, securing data requires knowledge of its location and acceptable destination.

Consider the following:

- Does your agency document data locations and does it maintain up-to-date diagrams of data flow between systems?
- Are baselines kept for all endpoints within an agency or within an agency's cloud infrastructure?

Conclusion

If the advice provided above sounds mundane, that is because it is. As it relates to maintaining good cyber hygiene, mundane practices are essential.

Like the foundation of a house, if it is not solid, the building will ultimately collapse. That's why cyber hygiene is absolutely indispensable to a solid security program.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook