Creating the right habits for cyber hygiene success

Preventing risks and breaches through cyber hygiene across endpoints is safer than remediation. And if done well, cyber hygiene can become a lightweight part of the way the company operates.

Jason English
Principal Analyst, Intellyx

Cyber hygiene offers a preventative approach to future attacks in order to avoid costly remediation and recovery incidents – much like dental hygiene recommends flossing and brushing to avoid later cavities and painful procedures.

Asking a good CISO which applications and devices should be inventoried and secured is like asking a dentist which teeth you should floss between. Four out of five will tell you, "Only the ones you want to keep."

Cyber hygiene, while considered a key aspect of cybersecurity, is also a distinct preventative practice that uncovers data, application, infrastructure and network risks – especially the ones we're not looking for.

A SecOps pro shared a story with me about their first sitewide inventory exercise, which discovered a PlayStation 5 running in a break room in the headquarters. That may not sound like a big deal, but that game console is also a full-fledged computer that can see file systems and devices on the corporate network, capture pictures and sound from the room, surf websites and download automatic software updates.

Prevention is easier than treatment if we can remember to do it. We all know it would be safer to prevent risks and breaches through cyber hygiene across all of our endpoints rather than remediate them once they are deployed across production and exposed to attackers.

So why isn't cyber hygiene a good habit all enterprises can stick to?

The cultural challenges of preventative measures

Work for a few years in any decent-sized company that leans heavily on its digital backbone, and you will find preventative processes that get in the way of progress.

Maybe it's a draconian unit testing requirement that churns out thousands of meaningless results and fails builds. Or a tedious change approvals process. Or a mandatory code freeze that causes development teams to regularly miss delivery windows.

DevSecOps teams that have experienced such entanglements are likewise worried that too much security oversight can block releases and stymie innovative improvements for customers when time-to-market means everything.

Maybe if cyber hygiene was an executive-level priority, prevention would improve. Unfortunately, **a recent cybersecurity study by Tanium** found that 63% of respondents said leadership is only concerned about cybersecurity following an incident, while 79% said executives are more likely to sign off on more cybersecurity spending following a breach. Yikes.

Cybersecurity practices and tools are often concerned with protection from outside attacks – setting up secure network perimeters, creating access, authorization and authentication policies, detecting attacks, and monitoring networks and systems for the telltale signs of threat behaviors and data breaches in progress.

By contrast, cyber hygiene takes a holistic inside-out approach to prevention. This may start with a diagnostic solution such as a **risk assessment,** but good hygiene also represents the management plans, employee policies and the security posture of the entire organization around maintaining secure technology practices across all IT assets of the enterprise.

If done well, it should become a lightweight part of the way the company operates. Making cyber hygiene second nature might require a little evangelism and up-front planning, but once in place, it will actually make software releases, migrations and updates of on-premises and cloud-based software and infrastructure easier.

Good habits that drive cyber hygiene success

Most security breaches (anywhere from 88–95%, depending on which research you find) involve some degree of human causation.

Therefore, organizations with a strong cyber hygiene posture exhibit several common practices that incorporate changes across people, processes and technology – in that order:

Education and behavior change. The most successful cyberattacks walk through the front door, using some combination of phishing, credential theft, rogue downloads and social engineering rather than brute force to gain entry.

Cyber hygiene and security awareness should be part of the core training of every employee, and educational resources should be provided for customers as well to help them recognize and avoid potential threats. Education is the best way to mitigate human fallibility and prevent malicious payloads from compromising your systems.

Continuous discovery and inventory management. The first run of an automated discovery will undoubtedly turn up lots of unexpected surprises and vulnerabilities. But discovery isn't a one-time compliance check, especially in today's constantly changing cloud and hybrid IT environments. New ephemeral cloud instances, device endpoints and software can be introduced to the operating environment at any moment.

Once every IT asset is exposed to the light of day, security and departmental leaders need an inventory of the current environment, with a view toward regular maintenance, updates and end-of-life decommissioning of any asset that remains past its shelf life.

Triage and prioritization. Even with the best vulnerability scanning and threat detection setup, no company will ever have enough skilled security and SRE professionals to respond to 100% of the potential issues.

Organizations must prioritize issues that are detected, using a risk scoring system that takes into account the asset's criticality to ongoing business, the value of the data it handles, as well as its level of integration with other systems, or exposure to the outside world. An old system that is no longer connected to anything can wait for decommissioning, while a critical data store with private information demands immediate attention.

Zero-trust policies mean every user is considered untrusted by default and is therefore blocked from access without explicitly defined authorization in IAM (identity and access management) systems.

Zero trust policies shouldn't just cover users. They need to be extended to every device endpoint as well. API calls from a medical device on a hospital network, or a query from a microservice in AWS or GCP shouldn't be able to set off a chain reaction. In practice, this policy often includes a *least access privilege* model, where each of the endpoints can only access the minimum resources necessary to support a business function.

The Intellyx take

One thing is certain: cybercriminals and hackers haven't overlooked the expansion of the enterprise attack surface so much change has created.

In a modern application world where cloud instances and endpoints come and go in an instant, security and resiliency can often get overlooked in favor of speed to market, scalability and interoperability concerns.

Don't get tunnel vision racing your organization past the preventative warning signs and guardrails a robust cyber hygiene practice can offer.

Learn how Tanium is bringing together teams, tools, and workflows with a Converged Endpoint Management platform.

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.

Intellyx is the first and only industry analysis, advisory, and training firm focused on customer-driven, technology-empowered digital transformation for the enterprise. Covering every angle of enterprise IT from mainframes to artificial intelligence, our broad focus across technologies allows business executives and IT professionals to connect the dots on disruptive trends.

Read and learn more at intellyx.com or follow them on Twitter.