Make the IT Asset Security Circle Unbreakable

Why Linking Assets, Configurations and Change Management is Critical

Executive Overview

Security vulnerabilities can lead to downtime that cost businesses billions of dollars each year, damaging reputations and wreaking havoc with productivity. As IT security professionals face constantly changing threats in their efforts to protect the organization's systems, data, and assets, one truism must be kept in mind: Trust, but verify.

It's estimated that up to 80 percent of IT downtime can be tracked back to ill-planned technology changes and misconfigurations -- the infamous "computer glitch" that leads to a string of technical failures. This percentage climbs much higher when you also consider that most cyber-attacks rely on ill-advised changes and misconfigurations (i.e., opening of unsecure comm ports, unpatched OS, disabled AV, unintentional installation of malicious code). Companies with a combination of manual and automated security scans find their piecemeal processes can fall through the cracks, especially when organizational silos exist. This white paper discusses what today's enterprises need — an end-to-end IT asset security circle — and three key critical areas that must integrate to keep the circle unbreakable:

1 - Asset Discovery & Relationship Mapping. Does IT Ops and IT Sec have a full and accurate inventory of all assets throughout the enterprise? Are their relationships fully understood?

2 - Configuration & Change Management. Does IT have deep visibility into how every asset is configured? How tightly are changes controlled? Does IT Sec have a say?

3 - Monitor and Verify. Does IT Ops/security know if a critical asset was introduced, removed, or changed?

Following are two real-world examples of the configuration & change management security cycle being broken (names withheld although one was a very public event). Global manufacturers and casinos compete in different markets, but two shared an all-too-common cybersecurity disaster: extended downtime and significant disruption throughout the enterprise linked to inadequate asset, configuration, and change management processes. The manufacturer experienced some pain and learned a valuable lesson but the casino suffered a deliberate attack that not only hurt profit and revenue, but also garnered international media attention that caused great harm to the company's reputation.

Let's look at how the IT asset security circle of each was broken, and what they could have done differently.

The forgotten server

It happens all too often- a server that was supposed to be decommissioned and catalogued as such was left to run unmonitored and maintained. Eventually, after years of staff turnover, it becomes known as the “do not touch” server for fear that some critical, albeit unknown, app or service relies on. In one particular case, a global manufacturer suffered a virus that propagated across their network because a server was mistakenly checked off on a spreadsheet as having been decommissioned. The server was eventually located, sitting in a closet in a local field office in Europe, still connected to the network and running an operating system that had not been patched in eight years. This forgotten server was a prime target for exploits and wasn’t re-discovered until after it had introduced a virus into the rest of the network. Although IT records indicated this server was decommissioned, the reality was that it remained online and highly vulnerable to malicious code.

How did it happen?

Obviously, the manufacturer’s IT department did not maintain an accurate inventory of all of their IT assets. It’s also safe to say that a proper change management process was not adhered to since they agreed to make the change by decommissioning the server but no one actually followed through on it. Lastly, there was apparently no way for anyone to detect that the server still existed, never mind that it had a very vulnerable OS and other software running on it. Once the server was marked as decommissioned on a spreadsheet, it was completely forgotten and left as an unintentional honey pot for exploits.

How could it have been prevented?

For starters, there should have been a more eff□ective way to track asset inventory. Today’s IT environments are just too big, dispersed, and dynamic for spreadsheets and manual entry.

Next, once it was determined that the server was to be removed, a decommissioning process should have been defined and followed.

Lastly, the asset inventory should have been kept current with an automatic and repeatable discovery process. Once the server was marked as decommissioned in the asset inventory, a subsequent scan of the environment should have immediately alerted to the fact that the server was very much still in existence and communicating with other assets. It’s even possible that it was still running applications that business services relied on. A truly decommissioned server can’t possibly contract and propagate a virus. Luckily for the manufacturer, it only affected some internal systems and did not become a big, embarrassing, and costly event.

Betting the house

An international casino and hotel operator made headlines when foreign hackers launched a well-planned and coordinated cyberattack in order to make a political statement. The hackers were able to exploit a vulnerable and apparently, a not closely monitored webserver located at one of the casino's smaller remote operations. This created what Bloomberg News called "a cascading IT catastrophe" as code loaded on the webserver was used to create a backdoor into the local IT environment. Once in, the hackers were able to locate a spreadsheet with system credentials, allowing them unfettered access to the real target: Las Vegas central IT operations.

Weeks went by while the hackers prepared for the big event. What at first seemed like just a Monday morning email problem quickly spiraled into a nightmare no IT professional ever hopes to find themselves in. Hackers loaded malware that quickly spread, causing infected servers and PCs to become unresponsive. When those machines were rebooted, the virus completely wiped the hard drives. The network was so congested with traffic that the IP phone system soon became useless. Employees had to turn to personal phones and email accounts to communicate with one another.

On Tuesday, the hotel's reservation website was hijacked so the hackers could share their political message and display some of the private employee data they had captured. On Wednesday, a video was released showing the huge amount of data that was stolen including the casino's VIP "whale" list.

Needless to say, this was a devastating and costly attack. Recovery efforts alone were estimated to be as high as $40 million. With lost revenue from the reservations website being down for days and the huge hit to the casino's reputation and distrust from its biggest clients, the ultimate price tag is actually much higher.

How did it happen?

Even with all of the IT monitoring and security systems likely deployed throughout the casino and hotels, apparently nothing alerted IT operations to the small code installed on the webserver. Could it have gone completely undetected or did someone notice it but think it was legitimate? Maybe being a small remote property - and not a likely target for cyberattack- meant laxer security. After all, safeguards were in place to block access from that site to the main operations center. However it happened, it's clear an illegitimate but detectable configuration change ultimately brought the whole house down.

How could it have been prevented?

There were clearly breakdowns through many layers of the so-called security onion, but when considered from an IT asset standpoint, it's clear better detection of, and response to, configuration changes were needed. Just as a "decommissioned" server should never be allowed to exist, neither should unverified config changes. It's impossible to believe that the only change occurred on the remote webserver. Surely the hackers made other changes while they accessed key systems, loaded the malware, and took over the reservation website. Systems that wouldn't normally communicate with each other probably were doing just that leading up to the attack. We certainly know they did after the virus was activated.

An ongoing discovery of configuration changes that includes new software installs, running processes, and network services/communications would have brought fast attention to the intrusion. It would have also alerted to systems that weren't configured with antivirus or properly patched to revent exploits. Proper and thorough discovery would also ensure no assets were completely unknown to IT. Without a doubt, an automatic and ongoing discovery process that includes detection of everything on the network, tracks configurations, and provides change notifications could have limited the scope of this cybersecurity disaster or prevented it altogether.

The IT Asset Security Circle

Why is the IT asset security circle so important? Of the many formidable issues facing today's IT security professionals, one of the most challenging is keeping up with the assets, dependencies, configurations, and changes that make up today's enterprise data center operations. Not to mention all those end-user assets connecting at the edge with access to the necessary IT services.

Gone are the days when companies could rely on spreadsheets or system-specific tools for an accurate inventory of all assets. There needs to be one system of record for all assets, configurations, and dependencies that all IT departments can access and actually trust. IT needs to know if antivirus software has been disabled, unapproved applications have been installed, or if a system has fallen out of the patch management program. They need to identify legitimate communications and quickly investigate exceptions. Finally, only approved changes should be allowed to take place with immediate notification if someone has circumvented the change management process.

Today's world of malware and cyber security threats calls for an end-to-end IT ops/security tool that links enterprise IT assets, configurations, relationships, and change management.

1: Asset Discovery and Relationship Mapping

Whether it's from mergers and acquisitions or corporate culture, too many organizations have information silos. Yet effective enterprise IT security depends on an inventory of assets that's accurate and complete including on premise and cloud environments. It's one thing to know there are 1,000 Windows servers, but is an in-depth inventory of what's on those servers available? A single physical server may host multiple applications on several virtual servers, possibly running many operating systems. IT Security needs to know how those servers are configured and what's on them. For example:

- Are all operating systems up-to-date on security patches?
- Is any unapproved or vulnerable software installed?
- Are there any suspicious or risky processes or services running?
- Are any hosts communicating to internal or external machines that shouldn't be?
- Which business services does each asset support?
- How are cloud and on premise assets connected?

As you can see, a physical inventory of hardware manually entered either into a spreadsheet or a CMDB just doesn't provide the kind of details IT Security needs to maintain a strong cyber security footing. IT Security needs to know about all hardware and virtual assets, such as databases, applications, and middleware.

Asset discovery and relationship mapping is the first phase in the security circle.

2: Configuration and Change Management

Whether their actions are intentional or not, it's a fact employees, even those in IT and who presumably know better, tend to be the biggest security risk. The best security processes only work if they are consistently followed by all. To err is to be human but IT staff making unauthorized changes to a server or network device is just one of many potentially harmful situations that occur far too often. Change management procedures must be followed but changes based on incomplete or inaccurate inventory and configuration information, or without a full understanding of relationships and interdependencies, can have unexpected consequences as well.

Configuration management best practices are vastly improved with ongoing monitoring, recording and updating of on premise and cloud assets such as hardware, software, operating systems, applications and web services, including their interdependencies. Here are some questions to consider:

- Is there an accurate record of all device configurations?
- Do those configs match baseline security standards?
- Which physical or virtual servers, operating systems, applications, load balancers, and networking infrastructure support which applications?
- Who "owns" and uses those assets and applications?
- What business processes depend on each asset and application?
- What dependencies exist between applications and technologies?

Without first answering these fundamental questions, changes to IT infrastructure may result in some business services not working because vital components were not incorporated into the new environment or necessary linkages were broken. Additionally, changes could introduce new security vulnerabilities not only for the target systems but also for those that are connected up or down stream from them.

Configuration and change management is the second phase in the IT asset security circle.

3: Monitor and Verify

When companies follow a disciplined and continuous configuration and change management process that's verified by automatic discovery, any suspicious changes are detected and a change management review can detect if the changes are legitimate. If not, they can be immediately flagged as suspect, investigated, and actions can be undertaken to mitigate damages.

The goal of a thorough change management process is to ensure any enterprise-sanctioned changes are implemented correctly to bring about the desired outcome for the organization. Any changes made should not result in new vulnerabilities. Additionally, an exception process to the change should be included, along with an automated way to confirm any changes.

It bears repeating: up to 80 percent of IT downtime can be tracked back to changes and misconfigurations. IT security should be part of the configuration and change management process and receive confirmation that changes are made the way they were originally approved. Any deviations need to be fully vetted and documented properly.

A comprehensive and repeatable asset and configuration discovery that includes dependency and relationship mapping, with change notification is critical to maintaining asset integrity for protection against security events. But it doesn't have to be a formidable job.

Monitor and verify is the third phase in the IT asset security circle.

About Virima

Virima Inc. (Atlanta, GA) is an innovator of SaaS-based asset and configuration management solutions for on-premise, cloud and remote IT assets. Through advanced infrastructure discovery, machine-learned dependency mapping, Autonomic Social Discovery™ and the Virima Visual Impact Display (ViVID™) featuring service maps with ITSM and vulnerability overlays, Virima helps organizations understand the complex and dynamic connection between business services and the technology and people that support them. The result is a heads-up display for IT that streamlines many function areas such as IT service management, IT asset management, business continuity, security, risk and compliance management.

To learn more about Virima solutions including our industry unique ViVID experience, visit **www.virima.com** or contact us at **sales@virima.com**.