Cyber Hygiene: Uncool but necessary

Automate Endpoint Patching to Mitigate Security Risks

Overview

If you analyze any of the recent published attacks, two patterns emerge,

1. 80-90% of the attacks exploit an unpatched vulnerability or an unhardened, widely open system
2. 70% of the attacks begin at endpoints

On average, 30-40 new vulnerabilities are published each day. About 14,000 vulnerabilities were published last year, and it looks like 2018 will see even more. A progressive organization performs risk assessment scans just once a month or once a quarter. It then takes between 30 and 120 days to mitigate the risks, even for organizations using expensive and resource-intensive security tools.

Organizations know endpoints are targets of attack, but they do not implement adequate security measures. With endpoints comprising a major share of any organization's IT assets, potential for damage is huge. At the same time, unpatched, unhardened systems are easier to target and exploit.

While 'cool' new products create a lot of buzz, cyber hygiene is often ignored. But it must be managed daily. If it is, the benefits far outweigh the effort.

Challenges faced by IT Security and Operations Teams

Lack of Visibility and Control

An organization's first step toward security is having visibility into its assets and devices. Without visibility, there is no security. A traveling workforce and a BYOD (Bring Your Own Device) scenario complicate this further.

Organizational inventory should provide quick access to all devices, operating systems, hardware configurations, software assets, vendors/publishers, procured licenses, versions, physical locations of devices, and visibility into personal devices if they are being used for business.

Along with visibility, organizations should ensure that only whitelisted applications are running and that access to certain devices is restricted. They also need tools to query devices and act upon any aberration.

Audit-based Risk Assessment vs Continuous Assessment

Most organizations rely on audit-based risk assessment in which a monthly or a quarterly scan is performed. While newer vulnerabilities are discovered daily, and patches are made available more regularly, quarterly audits to identify risk are insufficient. Auditing is a useful secondary check, but continuous assessment of all IT assets is mandatory.

Risk auditing tools generate pages of reports. Understanding the reports and creating a mitigation strategy is a tedious task. Organizations spend between 30 and 120 days to implement the strategies. During this time, endpoints are subject to attack and exploitation.

Some organizations do not even perform quarterly or yearly assessments. Their systems remain vulnerable even though vendors released patches a year or more before.

Isolated Solutions and Teams

Tools are operating in silos and so are teams. Organizations use one tool for asset inventory, another for risk assessment, another for patching, and yet another for compliance assurance. None of these tools feed into each other, but they need to be integrated. Asset inventory is the basis for risk assessment. Risk assessment is the basis for patching. And all these feed into compliance. For example, a patch management tool needs to know what vulnerabilities exist to apply appropriate patches.

These tasks are frequently performed by individuals that may be on different teams, causing further delay in securing endpoints.

Excessive Network and System Resources

When most of these tools perform scans, they overload network resources and consume system resources, impacting productivity. To offset this, assessment scans are performed on the weekend or at night. Scanning can take days depending on the size of the network. Generating consolidated reports across an organization can also take days or weeks.

The number of agents installed on each endpoint is another issue with system resource utilization. Typically, five to six agents from different vendors are installed, distressing the system and reducing productivity.

Heterogeneous Environments and Patching Complexity

IT environments typically have Microsoft Windows, various distributions of Linux, Unix and Mac OS X running on desktops, laptops and server systems. This comprises about 90% of the IT assets in most organizations. All these operating systems (OS) and a large number of third-party applications need to be covered by unique and different patching mechanisms.

Mobile devices and network devices, such as routers, firewalls, switches, storage devices and IP-enabled phones, further complicate risk mitigation.

Investing in tools that only address Microsoft environments is not the answer. Tools like SCCM can help push Microsoft patches and some third-party applications, provided organizations make an effort to identify risks, download patches, and create and roll out packages. Most organizations don’t effectively apply third-party patching for Microsoft environments.

What about Linux package and Mac OS X packages, what about third-party applications that run on these OS?

Traveling Workforce

Defining an organization’s perimeter has become a great challenge in recent years. People work from anywhere, organizations are more integrated with partners and customers, and offices span multiple geographical locations. In the physical world, there is a definite boundary. In the digital world, there is no set boundary.

Is defining a boundary essential for securing it? Probably not in a few years. It may even sound like a silly question by then. But it is important to recognize that attackers are currently going directly to endpoints rather than the perimeter.

Knowing where assets are and securing each asset is essential. Whether on the move, working from a different location, or connecting from a partner site, the asset needs to be assessed and the risks mitigated daily.

Traceability for High Profile Vulnerability and Attacks

As high-profile vulnerabilities and attacks have received widespread publicity it has become increasingly necessary for organizations to detect vulnerabilities, recognize attack symptoms and get that data in real-time. Key questions are: Does my network have that vulnerability? Can it be easily penetrated? Are the attack symptoms present in my asset base? Are the vulnerabilities on my systems being attacked in the wild?

Knowing these answers is essential so that the highest priority mitigations are rolled out immediately.

Steps to Improve Endpoint Cyber Hygiene

You can prevent 90% of attacks by correctly implementing a few simple steps. If you can make these parts of your daily routine without too much time or effort, you will yield great results.

1. **Maintain continuous visibility into your assets and devices across the organization**
    - Gather up-to-the-minute information on software, hardware assets, device locations, and asset tagging for easy recognition.
    - Decommission unused assets and use only supported OS and applications.
    - Set up an application white-listing policy and grant access to devices only as needed.

2. **Perform on-going risk assessment to identify vulnerabilities and misconfigurations**
    - Continuously assess risk. Relying on scans performed weeks before to apply remediation may not completely address the most recent and most critical issues. Newer vulnerabilities are discovered daily.
    - Use up-to-date detection rules.
    - Perform daily automated scans without affecting user productivity.

    Misconfigured systems are being used repeatedly to either launch attacks or spread attacks from one system to another. Easy and guessable passwords, open SMB shares, anonymous logins or shares, guest logins, outdated protocols, auto code execution, DEP protection, and privilege management, to name a few, are critical issues that require remediation. Systems need to be hardened and they should remain that way.

3. **When a high-profile vulnerability is reported, or an attack breaks out, implement mechanisms to search for potential impact across the organization.**
    - Search to determine if any of the systems are affected by the vulnerability (aka Meltdown, Spectre, wavethrough, EternalBlue) and if there are symptoms of an attack.
    - Implement quick response options to block the progress of the attack or to mitigate vulnerabilities.

4. **Consolidate application of patches for heterogeneous operating systems (Windows, Mac and variations of Linux) and third-party applications through one system to reduce complexity.** Using one system to patch all organization devices regardless of device type or location simplifies the patching exercise.

5. **Apply high-critical patches immediately.** IT Security and Operations teams must collaborate to do this activity in a timely manner.
    - Invest in tools that help identify critical vulnerabilities that are being exploited in the wild.
    - Perform risk-based patching instead of ad-hoc or blind scheduled patching.

6. **Cover traveling or roaming employees with live patching.**
    - Deliver patches over the Internet directly to devices.

7. **Automate patching of non-production environments.**
    - Roll out patches to production environments only after testing in an identical setup and evaluating functionality.
    - Automate patching through a solution that automatically rolls out patches for all selected applications on all end user devices. This assumes a risk of breaking a functionality if a patch were to corrupt or damage an application. However, if the solution were to provide rollback of installed patches, automated rollouts are safe. The benefits are huge, especially the time saved doing mundane work.
    - Schedule maintenance activities for patching the production environment.

8. **Enforce compliance to either regulatory or organization's internal security benchmark.**
    - Define a security benchmark and ensure all the devices adhere to these benchmarks.
    - If you detect a deviation, immediately fix the deviations to bring the device back to compliance.
    - Automate this activity to be performed daily, not quarterly or yearly with audit-driven risk management.

Conclusion:

Cyber hygiene, just like a healthy exercise routine and eating habits, forms a major step in safeguarding organization’s endpoints.

An ideal solution would provide all these through a single console,

- Up-to-date asset visibility, identification of asset changes, help managing all devices and assets.
- Risk assessment on all identified devices and assets.
- Risk-based patching and prioritized patching activity.
- Remediation of misconfigurations and compliance deviations.

SecPod’s SanerNow platform (https://www.sanernow.com) addresses this need with its array of tools for managing and securing endpoints.

SecPod’s SanerNow platform and tools provide a paradigm shift in endpoint security and systems management. SanerNow simplifies endpoint security, increases IT and security effectiveness, and reduces IT management cost. Platform specific tools provide vulnerability scanning, patching, compliance, asset, endpoint, and threat management. SanerNow provides one dashboard with one agent to address multiple high value business use cases.

Request a demo: **info@secpod.com**

About SecPod

SecPod is an endpoint security and systems management technology company. Founded in 2008 and headquartered in Bangalore with operations in USA, SecPod creates cutting edge products to manage and secure endpoints.

Contact Us
Enquiry: info@secpod.com
Technical Support: support@secpod.com
Phone: +91 080 4121 4020

INDIA
1354, 9th Cross, 33rd Main,
JP Nagar, I Phase, Bangalore – 560078
. Karnataka, India
Phone: +91 080 4121 4020

USA
303 Twin Dolphin Drive, 6th Floor
Redwood City, California 94065
United States of America
Phone: +1 918 625 3023