Insight Space

cyber insights programme

nccgroup

Technical Viewpoint

System operations: inventory through to management

Achieving real-world cyber resilience through objectives and performance measurement of IT operations

Ollie Whitehouse

Introduction

Cyber resilience and its foundational elements are broadly understood. These elements are not abstract concepts but rather the core hygiene principles of systems, software and broader environment management.

In our experience, organisations of all sizes often wrestle with one or more of these hygiene principles in practice. The root causes are varied but include the volume of legacy IT, shadow IT, underinvestment, organic evolution, mergers and acquisitions, and wider technical debt accumulation.

In Gartner's Top 10 Security Projects for 2020-2021, it states:

No. 2: Risk-based vulnerability management

Don't try to patch everything; focus on vulnerabilities that are actually exploitable. Go beyond a bulk assessment of threats and use threat intelligence, attacker activity and internal asset criticality to provide a better view of real organisational risk.

It is our view that the above goal is complex and a nuanced approach to vulnerability management. Situations can quickly change, and such a strategy requires a maturity and level of sophistication beyond many organisations today.

In a recent blog, NCC Group's Technical Associate Director, Lloyd Brough, discussed the often-complex remediation process following a security assessment, and what organisations can do to make sense of recommendations and know what to prioritise.

In this edition of Insight Space, we build on this by providing real-world experience and technical insights into what works and what doesn't when establishing a systems operations process that directly supports cyber resilience. We explore solutions, objectives and performance indicators that organisations should set to achieve real-world cyber resilience.

Asset inventory and management

The process of measuring IT operations success begins with knowing what needs managing and then actively doing so.

Whether on-premise or cloud, organisations need to know what their digital estate is made up of and be in a position to actively manage it across systems, applications and processes. The underlying aspects of IT asset management are covered in the NIST Special Publication 1800-5, released in 2018.

Without this knowledge, it is not possible to understand:

- Technology environment composition
- Overall status
- Attack surface
- Patch status
- End-of-life status
- Asset owner
- Business function

These insights all help in understanding risk and the associated follow-on processes for management and remediation.

INVENTORY CREATION AND MAINTENANCE

The creation and maintenance of the inventory will vary based on the technologies in use within the organisation. However, the creation process should typically involve the collection of asset data from a variety of means, including:

- Network passive – from physical and virtual switches, as well as DHCP and dynamic internal DNS, to understand what is connected
- Gateway passive – from network edges, proxies and firewalls, to understand SaaS usage
- Remote access passive – to correlate remote hosts.
- Hypervisor passive – to understand which virtual machines are running e.g. via Get-VM for HyperV
- Network active – to identify hosts e.g. via tools such as nmap or Rumble
- Directory services – such as Microsoft Active Directory.
- Cloud management APIs – such as GCP, Azure, AWS and Alicloud APIs and associated logging
- Endpoint management – such as mobile device management
- CI/CD pipeline – to discover deployed hosts and applications via tools such as Puppet
- Additional passive sources – to identify additional assets such as external DNS and TLS certificate transparency logs etc

These discrete information sources are then collated into a database or an IT asset management platform. IT asset management platforms range in size and complexity – from Snipe-IT, Solarwinds through to Spiceworks and ServiceNow. The key objective is to automate maintenance as much as possible. Starting with this objective, a sustainable and accurate source of asset information can be achieved.

This should then make it much easier to answer questions around which assets exist in your environment, what their business purpose is and who is the custodian, and to start important business impact and risk assessments.

ASSET MANAGEMENT

Asset management takes as an input, and may also contribute towards, the inventory to facilitate active management. Different assets will be managed in different ways. Some legacy hosts will need traditional mechanisms for management (e.g. SCCM), whilst newer hosts produced by continuous integration and delivery pipelines will require alternative solutions.

The way in-house software or third-party applications are managed will vary depending on the age and methodology employed. This can range from deployable packages and installers through to containers, and ultimately artefact platforms and processes, such as escrow to ensure continuing resilience.

Understanding the different approaches to asset management is imperative. The solution employed will often involve asset interrogation and potentially the use of an agent (e.g. osquery, SCCM, puppet and PDQ deploy).

The end goal of asset management is to be able to answer: **"What is the health and status of this asset, and is it up to date?"**

Along with being able to rectify issues, this capability should be complemented with an asset management lifecycle, which allows for the timely identification and retirement of products that could pose a risk to the security and integrity of your business.

CONTINUOUS VERIFICATION AND CORRECTION

It will come as no surprise that the most accurate inventories and management systems have clear owners with clear objectives around accuracy and the time taken to resolve discrepancies.

As environments change, ensuring accuracy is paramount to gain the maximum value. The objectives of this function include:

- Discrepancy detection and resolution
- Asset loss detection and reporting
- Real-time situational awareness and reporting

Ensuring that anomalies in the fleet are understood is crucial to gaining confidence in the platforms, systems and overall organisation posture.

Patch management

Once an inventory is established and maintained, and the means of asset management present, mature organisations can undertake active patch management at pace and scale. This includes having service level agreements associated with patch deployment.

The objective for the organisation is to be able to deploy patches at scale across hosts and applications in an automated way. The underlying asset management platform for hosts, containers and deployed applications provides the management information needed to articulate and quantify the enterprise state, time to patch and associated exceptions at any point.

We have found that the key overriding concern for customers utilising semi or automated patch deployment is the risk of service interruption from a bad patch. These concerns hint at a fundamental resilience issue and should be seen as symptomatic of wider challenges which need addressing in the first instance. Organisations who are resilient in their operations have the ability to detect, revert or roll back just as easily, even in the case of patch deployment causing a failure.

In relation to in-house software development, we see software component analysis in the pipelines providing similar functionality for applications. That is managing third-party dependencies and ensuring they are kept up to date.

The rise of immutable infrastructure in some quarters can be seen as a hyper example of patch management. This is when infrastructure is rebuilt to the next patch state and deployed into production to replace the other. The paradigm behind immutable infrastructure brings with it other cyber security benefits – namely a system whose software isn't intended to be modified, which allows integrity violations to be more readily detectable.

Vulnerability management

Vulnerability management can be seen as a subset of patch management, with exceptions for configuration issues. Organisations with a well-established and automated patch management solution invariably find vulnerability management a logical extension.

The pitfalls we see in vulnerability management in less mature or capable organisations are broad. They often include various strategies around prioritisation based on severity or with a focus on a subset of an estate.

These various strategies are often symptomatic of underlying patch capability or process performance issues. A vulnerability management mechanism should make it as easy to address 1,000 vulnerabilities as it is to address one. This capability, coupled with emergency processes to understand environmental exposure stemming from the absence of a patch and a means to resolve it quickly, is seen as the gold standard.

For software developed in-house, there are similar challenges and solutions. Synk, for example, enables organisations to carry out the automatic identification and resolution of vulnerable third-party open source libraries. Employing such solutions ensures the timely resolution of security vulnerabilities introduced by way of third-party libraries whilst managing levels of technical security debt.

Beyond technology, processes and performance indicators, one frequently overlooked area is the team responsible for delivering these changes. Their individual personality traits are as critical as their skills, along with the culture in which they operate.

The types of individuals that succeed will be details-orientated, have a high regard for problem solving, and work with transparency and autonomy. An appreciation for effective implementation of technology management is similarly important. There will often be trade-offs which need to be made, but ensuring you have the right people and promoting a safety-first culture, which has its foundations in measurement and management, is crucial to ensuring success.

Conclusions and summary

A lot of what we've discussed is not revelatory in nature. But it is complex, and organisations often wrestle with it, having performance indicators that focus on the volume and severity of vulnerabilities in an estate, rather than the accuracy of the inventory and time to patch.

The UK's National Cyber Security Centre outlines a number of situations where patching may not indeed be possible at all. These are related to ownership of the asset, responsibility for the asset, operational restrictions or end-of-life.

These wider issues should, as with the technical aspects, be actively discovered, measured and managed down. Without active reduction of these unmanageable assets or compensating controls, organisations will continue to wrestle with staying on top of patching.

In summary, our key tips for organisations looking to establish and implement robust measures across their system operations are:

- Asset inventory is the foundation
- Asset management is the key capability leveraging the asset inventory
- Patch and vulnerability management agility and scale come from having a robust inventory and integrated capability
- The people tasked with its delivery and operation are its core – so build considerately

These measures coupled with the correct performance indicators will drive the solutions and behaviours required to achieve real-world cyber resilience.

Three steps to system operations resilience

1. **Know what assets you have, who's responsible and automate maintenance as much as possible.**
2. **Ensure you have the information needed to articulate and quantify the enterprise state, time to patch and associated exceptions at any point.**
3. **Have a vulnerability management mechanism in place that makes it as easy to address 1,000 vulnerabilities as it is to address just one.**

Insight Space

cyber insights programme

nccgroup

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore.

www.nccgroup.com