TANIUM

An Ultimate Guide for Cyber Hygiene and Vulnerability Management

This eBook covers how the Australian Financial Services sector should respond to IT hygiene problems, disconnected and manual processes, lack of visibility and poor patching and compliance.

tanium.com

Introduction

This eBook is intended to provide a broad, conceptual understanding of vulnerabilities in the financial services sector, cyber hygiene guidelines, vulnerability management lifecycle best practices and insights to consider to help IT teams more effectively defend the endpoints they manage.

Vulnerabilities in the Australian Financial Services Industry

The Australian finance industry is an attractive target due to its stable and wealthier economic profile compared to many others. The combination of a considerable online presence and an increase in transaction activity means there is a strong focus from adversaries on the region.

TANIUM

Contents

Vulnerabilities in the Australian financial services industry

The financial industry in Australia is under immense pressure to keep up with technological advancements to safeguard against the threat of hacking. "We think the risks have escalated since COVID; the economy has moved to the cloud, much more digitation, changes in the way people are working with working from home." APRA's deputy chairman, John Lonsdale, told the Australian Financial Review that cyber was one of the regulator's top priorities.

Westpac chief executive Peter King agrees and commented that the number of attacks increased during the pandemic and ranged from opportunistic to much more sophisticated. "We have seen a massive increase in scams," Mr King said.

Additionally, Australian Banking Association Chief Executive Anna Bligh said the pandemic had created a perfect storm for banks, with employees and customers spending more time connected to devices. "During the last 12 months [through 2021], every bank has had an escalation in cyberattacks and hacking and scams on customers."

An example of this was seen in September 2020 when an Australian hedge fund was subject to a Business Email Compromise (BEC) and forced to declare bankruptcy due to a cybercrime incident.

But IT leaders mustn't be swept up in the media hype. Scott Lowe, founder of EndpointX and former Director of Technology at Barclays and Bank of America, warns, "There is this perception in the press that most hacks are done by nation-states on shiny zero-day vulnerabilities. But the reality is that most happen due to an unmanaged server, missing patch, or a vulnerability on a browser. It is normally the most fundamental IT hygiene issue that leads to breaches."

"Visibility into all things on your network is one of the most important things," Lowe continued. "It only takes one server or workstation that isn't patched for a malicious actor to get access to the network, and then to move laterally across it. The ability to see and manage endpoints across the network is key."

Fundamentals

Maintaining and securing enterprise networks requires pairing the right tools with hygiene best practices to yield the best results. Cyber hygiene is fundamental to enterprise security and systems management.

Improving cyber hygiene requires creating a process to continuously identify assets, risks, and vulnerabilities across an environment and fixing them with speed at scale. Focusing on cyber hygiene can help prevent the breaches, outages and disruptions that haunt IT organisations.

As IT environments grow in size and complexity, device and workload varieties also grow. Most organisations have disconnected manual processes but still must manage everything from laptops and virtual machines (VMs) to containers across vast, distributed networks that span multiple offices. Under these demands, cyber hygiene often suffers.

Part of the basic security hygiene for all businesses, especially for financial services, is the frequent, timely and reliable patching of all endpoints. Timely patching is critical as it helps reduce the attack surface that adversaries can exploit. Still, it is an ideal more than reality for many organisations, even with the knowledge that a majority of successful security breaches can be traced in some way to patch hygiene.

In this eBook, we explain the components of cyber hygiene, such as gaining visibility and how various tools help or thwart efforts to improve it.

Chapter 1

Know Everything

To preserve and improve cyber hygiene, you need to know what assets you have. Do you have 10,000 or 500,000 computers and servers in your organisation? Where are they, what are they, what's running on them, and what services do they provide? Answering those questions might seem difficult if you don't have the right platform. In this chapter, we dig into why that foundation is so important. You can't manage what you don't know you have.

To manage your endpoints, you need three levels of knowledge:

1. What assets do you have, and where are they?
2. What software is running on them, when was it last used and is it licensed?
3. How do the machines on your network relate to one another, and what is their purpose?

Regardless of size, organisations need to know that information in modern IT environments will constantly change. Network assets come and go, especially with "bring your own device" (BYOD), a standard and growing policy in many financial services organisations. With more companies encouraging employees to work from home, complexity increases, and some unknown assets may occasionally appear on the network.

To quote renowned novelist Paulo Coelho, "No one can hit their target with their eyes closed". If you can't see an asset, you can't manage it and can't secure it. There may be attack vectors you're entirely unaware of — like an unpatched vulnerability.

Let's also consider the financial implications and look at the example of software licensing for a program like Microsoft 365. Teams may have licenses for 10,000 copies, but 20,000 might be in use. Not having the correct information is a serious compliance issue where organisations may be subject to expensive legal action.

Moreover, compliance isn't just about software licensing. Australia's financial services organisations must comply with GDPR, Australian data privacy regulations and PCI-DSS provisions.

You need to know where the data lives. If not, you can’t prove compliance. Inability to prove compliance has two significant downsides: regulatory sanctions and unhappy customers.

Demands of modern IT on aging tools

Tools built ten years ago preceded many modern IT ecosystems. They can't handle the rate of change we see now. Yet organisations often remain attached to what they're used to. They may also have invested thousands of hours in customisation developing custom scripts to make them work more effectively. Entire partner ecosystems have often been created to enable this behaviour.

The unintended and unfortunate consequence of this is that the IT policies and processes crafted are not created because they are the best way to address an issue but because they fit the capabilities of the tools in use. Entrenched tools become part of the IT infrastructure. But the best IT policies should be tool agnostic. A tool built-in 1993 or even in 2010 can't offer that flexibility.

So how have IT leaders responded? Gartner found that 80% of IT organisations plan to pursue a vendor consolidation strategy in the next three years. With so many disparate, legacy tools plaguing IT ecosystems, no wonder organisations are adopting this strategy. Source: 2020 Gartner Security & IAM Solution Adoption Trends Survey.

An example of one such global organisation headquartered in Sydney that has adopted this strategy is GenesisCare, a leading global healthcare provider. They had up to two dozen separate security tools deployed across the IT stack. They used to wrangle them all to extract and combine the necessary data, and this was daunting, if not impossible.

Prioritised patching

We often read in the news about a business having been compromised by cybercriminals because of some unpatched critical vulnerabilities. A recent example is the BlueKeep security vulnerability in Microsoft's Remote Desktop Protocol, allowing remote code execution. WannaCry is perhaps the most famous recent example of a malware outbreak created by a failure in patch management.

So why is real-world patching so challenging? Because it is hard to achieve, even today, despite all the advances made in the technologies available to help manage it. Additionally, many businesses still do not take the importance of regularly patching seriously enough. They do not dedicate (or have) the resources to do so or ownership for identifying where to patch (Security), and the deployment of the patches (IT Operations) sits in often-siloed units with a historically fractious relationship between them.

In most cases, the technology itself isn’t helping. Existing technologies that specialise in patching are unreliable and even untrusted by some. Due to a tiered hierarchy, they can't get patches distributed across an entire estate and quickly report their success rate. The technology is slow to process change. They have unreliable client agents installed on endpoints and have complex networking requirements that struggle with roaming devices. These factors add up to increased complexity, reduced reliability and unsuccessful patching.

Achievable automation

There are many reasons why an enterprise would want to automate its monthly patching process. Automation makes organisations efficient, reduces the chance of human error, and frees up skilled administrators to tackle more interesting and complex tasks. In addition, faster and more complete installation of new security patches translates to a better overall security posture.

That said, fully automated patching can have its drawbacks. As we saw with the patching mess in July 2018, sometimes released patches are problematic and unintended or have adverse side effects on an enterprise, so they cannot be mitigated effectively in time if the process is fully automated.

The preferred middle path is to automate most aspects of monthly patching while still testing sufficiently before patch rollout. The aim is to implement a soft touch, safe, and effective monthly patching strategy.

The four primary goals to accomplish are:

1. Increase security patch coverage
2. Reduce the time to install security patches
3. Reduce the monthly person-hours required to do so
4. Do all of this while still going through multiple stages of patch testing before the production rollout

Read how Elsevier introduced critical automation into their IT operations and security programs to allow them to focus on addressing threats rather than wasting time identifying them.

Endpoint discovery is a moving target

IoT device is anything with processing power that is not usable as a computing device. That covers point-of-sale (POS) devices, security motion detectors and even internet-connected coffee machines, to name a few. Gartner predicted that the world would see nearly 21 billion IoT devices by next year.

The Internet of Things (IoT) offers financial services firms improved customer service and significant business efficiency.

The proliferation of internet-connected devices has made it easier for customers. Whether it's online banking or submitting a loan application, "smart devices" such as phones, watches, and digital assistants let customers perform the tasks that they previously needed desktop computers, or even face to face experiences with customer service teams, to do.

Financial service providers can use data from each online engagement to build a better picture of credit risk and identify habits and trends that will allow them to improve their services for customers.

But the popularity of the IoT has brought perils as well. These devices are sources of vast quantities of potentially sensitive data that must be protected and managed. And the sheer number of smart devices and their inherent vulnerabilities make it difficult for financial services firms to implement IoT security measures to protect against data breaches and other risks. Some IoT devices are equipped with sensors that communicate via wireless networks to web-based applications, called operational technology. It makes every device a network device.

No single asset discovery tool can identify every device type, so the tool or platform organisations use must integrate and work well with supporting applications that recognise phones, tablets, printers, and other devices.

When everything is a network device, everything is a potential security vulnerability. Organisations need policies and procedures that break endpoints into three categories: managed, unmanaged and unmanageable. Endpoint discovery is the first crucial step toward Zero Trust. It means a security architecture assumes devices or users can't be trusted without verification. Endpoint discovery is where cyber hygiene and security begin, which is where you need to start.

Chapter 2

Where to start

Threat actors are better at finding weak links exploiting vulnerabilities and misconfigurations before security and IT operation teams know about them. Regulatory pressure is also turning up the heat on organisations already struggling to manage breaches reputational and financial fallout. Vulnerability and configuration management are at the heart of any good cyber risk management strategy and a key element required for good cyber hygiene.

The five vulnerability management lifecycle stages include:

Follow this five-step framework to help you enhance your vulnerability management program and minimise cyber risk.

Discover what assets you have and what security protocols are in place.

Assess the types of security and vulnerability standards you want to evaluate against and deploy tools to figure out how to collect relevant information.

Prioritise the importance of items you want to address and when to tackle them.

Remediate vulnerabilities by updating patches and changing security configurations and policies.

Verify and reassess to validate that the changes you've made have conformed to security policies.

Chapter 3

Piviot from insight to action

Responding to a cybersecurity incident, whether it's a data breach, a ransomware event, or one of several other types of cyberattacks, can dramatically compromise an organisation's routine business operations. When news gets out about the incident, it shatters public confidence, erodes brand value and takes a big chunk out of top-line revenue.

Organisations can adopt the six-step PICERL framework to improve and fine-tune their incident response plans. PICERL stands for Prepare, Identify, Contain, Eradicate, Recover and Lessons Learned. Read more about the PICERL framework.

The pivot from insight to action is where cyber hygiene often breaks down. Information is lost between the cracks of fragmented tools and teams. Effectively coordinating patch and software deployments across an environment requires that IT ops and security teams be aligned, collaborative and accountable.

This alignment requires systems must be in place and shared workflows clearly defined. A cyber hygiene assessment offers organisations visibility into the health of their IT environment. They can understand the state of their endpoints, identify critical gaps and learn how they can improve your cyber hygiene to decrease their organisation's chances of becoming the next headline.

Top four requirements for your tools and platforms

We have discussed the growing need to consolidate and update the tools or platforms you use. When choosing a platform, you should look for these mandatory four elements:

1. Accuracy
2. Speed
3. Scale
4. Ease of use

If you don't have an accurate view of your environment, you are blind to acting. It is critical to gain a comprehensive, accurate and real-time understanding of your IT environment at any scale, wherever your endpoints exist. You should continuously measure and report critical security and operations metrics, such as patches and vulnerabilities.

Speed can not be underestimated as a critical factor. As an example, if it takes two weeks or a month to do an inventory, by the time you're finished, the network has changed, and you've undoubtedly missed something you need to scope incidents and stop threats quickly.

Historically, the Barclays team had to wait until the end of the deployment run before measuring the success or failure of the patch deployment. With Tanium, a patch deployment is measured near-realtime, so any server compatibility issues are immediately detected and remediated. Source

You need to outrun breaches when traditional safeguards fail with a platform that provides real-time data. Take action on thousands of issues with lightning speed and precision, from patching to killing processes without adding more agents or complexity. The more extensive the network, the more of a problem this presents. That's why speed and scale matter. Ease of use comes into play because a tool that's hard to configure produces errors, and people won't want to use it.

And finally, ease of use. Adopting new capabilities with ease as the needs of your business evolve will give you flexibility into the future. Ensure you can ask questions in plain English to understand the state of your endpoints, examine results and take action in real-time. Can you deploy your platform in a matter of hours with preconfigured solutions across IT operations, risk and security?

Single source of truth with end-to-end action

With the Tanium platform, in one automated and integrated workflow, customers take end-to-end action in their environment, which saves them resources, lowers their risk and gives them fast, comprehensive visibility into their patch environment. They scan their endpoints for patch compliance and develop a real-time picture of what needs to be applied where. Through modern distributed edge computing, they can rapidly and automatically distribute patch files to all relevant endpoints — remote, mobile or on-premises, with minimal load.

Organisations can achieve effortless, consolidated patching with a single agent and console through a proactive approach to IT management. With Tanium, they know the whole truth about their environment and can fix problems fast. They will typically see 99% patch visibility and compliance within 24 hours of installing the platform.

Tanium customers like GoDaddy can continuously monitor for out-of-date versions of typically exploited applications like Java and Adobe Flash. Once identified, remediation can be done immediately using Tanium. Before Tanium, vulnerabilities could exist for days on GoDaddy's environment before addressing regular patch cycles. Source

> *"If we hadn't invested in Tanium, we would lack complete visibility into our assets and still have hundreds of thousands of missing critical patches. It would only be a matter of time before we were targeted by cybercriminals and potentially put in a really difficult position," said Mark Wantling, CIO, University of Salford.*

The Global Manager CSIRT & CyberTech, Luxury Group, described their success with automated patching. When Tanium was deployed, "zero-day" patching went from nearly one week to less than one day." Luxury Group's IT operations team also started noticing compliance rates in the upper 90s after only several hours of patching.

Rather than siloed tool sprawl, Tanium provides a single platform capable of scaling to hundreds of thousands of endpoints without impacting bandwidth. In doing so, it provides a single source of truth for siloed IT operations and security teams to unite around. The right type of collaboration matters, but it adds days to the patching process when it adds complexity. One study found that incorporating other parts of the business into the patching process can add an extra 12 days.

Tanium’s unique value

The unique value that Tanium brings to customers is through its linear chain architecture and lightweight Tanium agents on endpoints. The increased visibility and control that customers experience allows them to find and remediate vulnerabilities, enhancing risk mitigation. This visibility reduces data breaches' frequency, duration, severity and business-disrupting outages. It lowers the cost of responding to and recovering from incidents. By decentralising data collection, aggregation, and distribution down to the endpoint, Tanium architecture harnesses the speed of LAN traffic and reduces direct client-to-server communications. The benefits enjoyed are eliminating inefficiencies caused by bloated databases, overloaded connections, and heavy traffic across WAN segments.

Conclusion

Customers choose Tanium to gain visibility control and help them know everything fast. Through the power of the Tanium platform, they can:

- Take control whether on-premises or in the cloud.
- Fix it fast by containing, remediating and patching at scale in minutes with a proactive approach to IT management.
- Know the truth through aligned teams and a shared understanding of all the data across their environment.

See how Tanium can help strengthen your organisation's security defenses. Request a demo or test-drive Tanium in your own environment with a free two-week trial.