DESIGNERS SHOULD ALWAYS KEEP THEIR USERS IN MIND
Use relevant charts and graphs

IDENTIFYING VULNERABILITIES

Adam Palmer *explains why it is time to take control of your cyber risk*

The last 12 months have been a challenge for organisations for a variety of reasons. However, front and centre in the response has been technology. With governments globally imposing work-from-home mandates, a rapid move to remote work caused many businesses to address cybersecurity concerns with a 'good enough for now' band-aid solution. Security leaders rushed to secure an environment where unpatched and misconfigured personal devices could be leveraged to attack enterprise networks. These new technologies are mixed with traditional IT systems rife with data silos and outdated operational processes.

The challenge is that legacy security approaches weren't designed to handle an attack surface of this size and complexity. And the repercussions are evident as attackers thrive during times of uncertainty. Breaches affect hundreds of organisations every year and the number of exposed records grows with each new affected party.

Analysis by Tenable's Security Response Team of publicly disclosed data breaches, from January to October 2020, found that there were 730 breach events resulting in over 22-billion records exposed, not to mention the untold damage to reputation and trust. Furthermore, over 35 percent of breaches were linked to ransomware attacks, resulting in an often tremendous financial cost.

While ransomware remains the most disruptive global cyberthreat, in 2020 a new array of extortion tactics emerged. These include operating so called "leak" websites to name and shame victims, which proved to be lucrative for attacker groups looking to secure ransom demands. This threat affects virtually every industry and stems from a variety of root causes all of which security teams must account for in their defender strategy.

It's important to understand an organisation's cyber exposure gap and update the cyber-incident response plan by meeting with the rest of the C-suite

Troublingly, the primary theme of the threat landscape last year was that threat actors rely on unpatched vulnerabilities in their attacks. This isn't anything new, but last year government agencies issued several advisories warning of attackers leveraging vulnerabilities that have patches available and yet remain unmitigated. While finding and fixing vulnerabilities would appear a no brainer, the reality for security teams is a lot less straightforward.

In 2020, there were 18,358 new common vulnerabilities and exposures (CVEs) assigned, a six percent increase from 2019. However, looking at the last five years, the data reveals that from 2015 to 2020, the number of reported CVEs increased at an average annual growth rate of 36.6 percent.

While the sheer volume of new vulnerabilities is daunting, there is cause for optimism as analysis of the attacks organisations faced also highlighted one clear trend – only a small minority of the total CVE detected are ever successfully exploited and even fewer are used in attacks. This means that focusing on critical vulnerabilities can be very effective.

EXTREME RISK

Finding and patching critical vulnerabilities will close off entry points that the majority of threat actors look to exploit. In 2020, pre-existing vulnerabilities in virtual private network (VPN) solutions – many of which were initially disclosed and patched in 2019 or earlier – were a favourite target for cybercriminals and nation-state groups. Organisations that have yet to prioritise patching these flaws are at extreme risk of being breached. Add in the dramatic workforce changes necessitated by the Covid-19 pandemic and it's clear that securing VPN solutions is critical.

In fact, of the top five exploited vulnerabilities particularly worth addressing, three were 'legacy' VPN vulnerabilities: CVE-2019-19781: Citrix Application Delivery Controller (ADC) and Gateway; CVE-2019-11510: Arbitrary File Disclosure in Pulse Connect Secure; and CVE-2018-13379: Fortinet FortiOS SSL VPN Web Portal Information Disclosure.

One of the common threads across these vulnerabilities is the fact that they are all directory traversal flaws. As the name implies, a directory traversal vulnerability allows an attacker to traverse the directory tree to access files outside of the parent folder. An attacker can accomplish this by sending a specially crafted request containing a directory traversal string (eg "../../") to vulnerable endpoints. This would enable an attacker to potentially read sensitive information or write to the underlying disk in a limited fashion. This type of vulnerability has been around for over two decades and it appears that a variety of software applications were susceptible to directory traversal flaws in 2020.

While a single vulnerability can be compromised, threat actors have found novel ways of leveraging multiple vulnerabilities in a single attack, often referred to as daisy chaining. On 9 October, CISA and the FBI issued a joint advisory that a foreign threat actor was exploiting "multiple legacy vulnerabilities" in an exploit chain including CVE-2020-1472, a critical elevation of privilege vulnerability in Windows Netlogon dubbed 'Zerologon'. Attackers can chain together multiple legacy vulnerabilities with Zerologon in order to elevate privileges by granting themselves the ability to reset the password for and gain access to domain controllers within the network.

This demonstrates how important it is for security teams to consider the contextual risk of each vulnerability, including its potential to be leveraged in a full system compromise. The severity of any given vulnerability is no longer an independent measure and should be interpreted based on the context of the environment in question.

Identifying all affected systems in the organisation that have vulnerabilities is helpful, however this doesn't detail how day-to-day operations would be affected if the vulnerability were exploited.

Security teams must work in lockstep with business partners in order to identify what it is any given business unit does, and the services and applications that are critical to accomplishing core tasks. This intelligence informs the security team enabling it to focus protection efforts on what poses a real versus theoretical risk to the business. When it is unclear how different assets are connected, patching and mitigation efforts can even have unintended negative impacts.

WORKING FROM HOME HAS MADE THE NEED TO SECURE VPN VULNERABILITIES ABSOLUTELY ESSENTIAL

This illustrates how responsibility for ensuring an organisation effectively addresses cybersecurity risk can not belong solely to the CISO. Now more than ever, modern organisations have connected devices across the network. For example, operational technology (OT) devices, commonly managed by physical security teams, are now increasingly connected to IT networks and are often a blind spot for cybersecurity managers. However, a CISO can only be effective in mitigating risk when risk management is understood and supported by the entire organisation.

The CISO may be the primary cyber risk manager, but every business asset owner should have a fundamental grasp of the requirements for cybersecurity. Using car ownership as an analogy, a driver does not have to know how to assemble an engine. It is reasonable, however, to expect a competent driver to understand how to change a flat tire, and most crucially when to listen to a professional mechanic. Each business leader should make an effort to understand the basic concepts of cybersecurity and take ownership for mitigating cyber risks in their unit.

Accountability: Organisations should have policies that hold each business unit and asset owner accountable for end-to-end IT security management. This provides each asset owner oversight of their security controls and ensures that remediation tasks

▶

are completed. Automated remediation workflows can also help with effective remediation tracking.

Prioritisation: Effectively prioritising vulnerabilities is fundamental to cybersecurity. Yet, knowing where an organisation is most exposed can be increasingly difficult. With thousands of vulnerabilities identified in enterprise environments each day, security teams don't have the time and luxury to guess which ones to focus on first. Organisations need solutions to help them better understand the actual, not theoretical, impact of vulnerabilities. They also need to understand how to focus remediation efforts based on business risk.

IN 2020 THERE WERE 730 BREACH EVENTS WITH OVER 22-BILLION RECORDS EXPOSED

Establishing internal SLA for priority risks may also help establish clear goals and improve accountability.

Create a 'living strategy': Progressive organisations can't work in watertight compartments when it concerns cybersecurity. It's therefore important to understand an organisation's cyber exposure gap and update the cyber-incident response plan by meeting with the rest of the C-suite frequently to avoid any surprises. Oversight of security may be led by the CISO, but the entire C-Suite should embrace a cross-team leadership approach. This assures that the security strategy will be a flexible, 'living' strategy, with leadership support.

Eliminate silos: There used to be a sharp divide of responsibility between the 'guns and guards' – in this case, the physical security team and the IT-focused cybersecurity team. OT security now requires more internal collaboration among teams. Security leaders need to coordinate more closely with their physical security counterparts to monitor access to connected devices and manage the convergence of IT and OT security risk.

Effective governance and communication: Every department relies on an organisation's technical infrastructure, therefore it's crucial for IT leaders to regularly communicate with relevant stakeholders to look for ways to improve productivity and security.

The remote working 'hybrid' model is likely to continue into 2021, and possibly beyond. This shift to a remote, distributed workforce has led to a higher volume of critical and confidential information being transmitted electronically. Security leaders must ensure that their strategies are in lockstep with business priorities and can effectively communicate the security programme to business asset owners.

Cybercriminals are hoping that security teams will be distracted, but the truth is that security needs to focus and ensure basic cyber hygiene is maintained. The best defence against attackers is to make sure that systems and applications have been updated and patched. This will reduce the risk of criminals being able to leverage known flaws or vulnerabilities in the systems. By identifying what matters to the organisation and collaborating more effectively internally from the beginning, organisations will have greater security without compromising efficient business operations ●

Adam Palmer is Chief Cybersecurity Strategist at Tenable and has over 20 years working in cybersecurity. His experience includes executive positions at large cybersecurity vendors, leading the UN Global Programme against Cybercrime and working as the Global Director for IT & Cyber Risk at one of the largest EU banks.

Operational technology devices are increasingly connected to IT networks and are often a blind spot for cybersecurity managers