SKYBOX SECURITY

2020 VULNERABILITY AND THREAT TRENDS

Mid-Year Update

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

The COVID–19 crisis has made a significant impact on the cybersecurity landscape. The sector's existing challenges — including the cybersecurity skills shortage, under–resourced security programs and increasingly fragmented estates — have been exacerbated as organizations scramble to enable their remote workforce and secure expanded network perimeters. While this critical work has been taking place, cybercriminals and nation–state threat actors have been working hard to capitalize on the chaos.

The *2020 Vulnerability and Threat Trends Report Mid-Year Update* shows how criminals have taken advantage of the disruption caused by the pandemic. While organizations were vulnerable and distracted, hackers developed new ransomware samples and advanced existing tools to attack critical infrastructure — including vital research labs and health care organizations.

The sophistication of the malware and methods used by attackers over the first half of 2020 highlight just how complex cybersecurity management has become. Add to this the 20,000 new vulnerabilities likely to be reported in 2020, and it's clear that the burden placed on security teams is only going to increase — even if we manage to enter a post–COVID reality later this year. If organizations do not have full visibility over their entire security environment, and if they are unable to focus remediation on their most exposed vulnerabilities, then they could fall victim to attack at a time when business continuity, brand trust and fiscal stability are paramount.

The report emphasizes the need for organizations to adopt risk–based strategies so that they can manage the mass of new vulnerability reports and deal with heightened threat levels. It is only through gaining full and unerring network visibility, modeling the environment and analyzing exposure that organizations will be able to gain the insight and focus that they need to emerge from the pandemic unscathed.

Full Report > 2020 Vulnerability and Threat Trends Mid–Year Update

KEY FINDINGS

20,000+ New Vulnerability Reports Likely in 2020

Over 9,000 new vulnerabilities have been reported in the first six months of 2020 (a 22–percent increase on reports published over the same period in 2019), and we are on track to see more than 20,000 new vulnerabilities this year — a new record. This will be a figure that defines the complex landscape within which security professionals operate.

50% Increase in Mobile Vulnerabilities Highlights Dangers of Blurring Line Between Corporate and Personal Networks

Vulnerabilities on mobile OSs increased by 50 percent, driven solely by Android flaws. This rise has come at the same time as home networks and personal devices increasingly intersect with corporate networks as a result of the move towards a mass, remote workforce. These trends should focus the need for organizations to improve access controls and gain visibility of all ingress and egress points to their network infrastructure.

Ransomware and Trojans Thrive During COVID–19 Crisis

The creation of new ransomware and malware samples has soared during the COVID–19 crisis, a time that has also seen a significant increase in exploits taking advantage of Remote Desktop Protocol (RDP). These tools are enabling cyberattackers to capitalize on individual concerns and take advantage of overwhelmed security teams.

Attacks on Critical Infrastructure Adding to the Chaos

Attacks on national infrastructures, pharmaceutical firms and health care companies have increased as criminals become emboldened by chaos spurred by the pandemic. These attacks have added to the turbulence and could hamper countries' abilities to respond to the health crisis.

REMEDIATE THE RIGHT VULNERABILITIES

Strong remediation practices are going to be crucial if you are going to weather the current storm. You need to gain a full, unerring understanding of how exposed each of your vulnerabilities are to attack. To do this, you first need visibility — of vulnerabilities themselves, the assets they exist on and the surrounding network topology and security controls. All of these elements from within the organization as well as intelligence of the external threat landscape give context to a vulnerability and will inform remediation priorities.

By modeling the organizational environment in which a vulnerability occurrence exists, security teams can effectively understand the exposure of vulnerabilities to threat origins — a critical component of risk-based vulnerability prioritization. Analyzing exposure takes vulnerability prioritization out of the theoretical realm occupied by generic scoring systems like CVSS and places it in the real world, revealing which vulnerabilities are most likely to be used in an attack on your organization.

For example, if a security program bases vulnerability prioritization solely on CVSS scores, it could waste resources patching a vulnerable asset protected by layers upon layers of defense-in-depth security controls. At the same time, a medium-severity vulnerability may never be prioritized for patching, despite it being left exposed to a known threat origin. Considering the volume of vulnerabilities accumulating every year, risk-based strategies are going to be key to focusing action where it has the biggest impact on reducing the risk of attack.

To focus remediation efforts on this small subset of vulnerabilities, organizations need to better understand the context of their vulnerabilities within their infrastructure and the threat landscape. This includes having a firm grasp on several details regarding the vulnerability itself, as well as:

- Asset exposure to threat origins considering surrounding network topology and security controls
- Asset value and potential impact to the organization if compromised
- Exploit activity in the wild
- Exploit use in packaged crimeware (e.g., ransomware, exploit kits)
- Exploit availability and potential impact of the exploit

By analyzing the interconnections of the vulnerability and these elements, organizations can firmly tether remediation to risk reduction. It's a "quality over quantity" approach that may see vulnerability totals within an organization remain high but the likelihood of attack dramatically decrease.

Read More > Risk-Based Vulnerability Management

HOW TO ENFORCE SECURITY IN A POST-PANDEMIC WORLD

The chaos surrounding COVID-19 has forced seismic and unprecedented change upon businesses around the world, many of which now have to be concerned with securing a large, remote workforce. This has placed a great deal of pressure on security teams as they strive to manage new risks that have emerged from their expanded network perimeter.

This shift can have a large, short–term impact on over–stretched IT and security teams. One of the biggest risks that they have to manage concerns employees who generally do not work remotely and who need to access corporate resources remotely. If this risk is not properly mitigated, it could open the door to new viruses, malware or other digital interlopers due to their lack of secure home networks and other personal devices.

As the dust settles and we cautiously start to think about a post–pandemic age, organizations need to reassess their security strategies and posture. This report has highlighted the landscape that lies ahead for security teams — they will potentially have over 20,000 new vulnerabilities to sort through and will be contending with heightened threat levels — as they battle to avoid non-compliance and avoid attack during an era of great economic uncertainty.

To address these new vulnerabilities, you need to develop a clear roadmap. You need to access and analyze data to learn about how prepared they are to contend with increasingly sophisticated threat agents. .This roadmap needs to incorporate several critical capabilities:

- Having an infrastructure–wide view of all corporate assets wherever they reside
- Analyzing access and network paths to critical systems and between network segments
- Addressing critical–risk vulnerabilities on vital business assets, especially those that have exposures from external attack or less secure internal network segments
- Ensuring proper secure configuration of VPN, firewalls, security and networking device and all other ingress and egress points to critical assets

Gaining these capabilities will allow you to better support the necessary digital transformation initiatives that will have to be introduced to support your remote workforce.

MITIGATING RISK OF RANSOMWARE

The strategy behind detecting and mitigating a ransomware attack should be grounded in a holistic approach. You first need to investigate and identify all affected endpoints. When you suffer a ransomware attack, you need to assume that all credentials present on these endpoints are now available to attackers, whether the accounts associated with them were active during the attack or not. Using indicators of compromise (IOCs) alone to determine the impact of a ransomware attack will not be enough because threat actors are known to change their tools and systems once they can determine their victims' detection capabilities.

After initial identification has been conducted the following steps are necessary:

- Isolate affected devices as soon as possible by either removing the systems from the network or shutting them down to prevent further ransomware attacks throughout the network
- Isolate or power off affected devices that have yet to be fully corrupted to gain more time to clean and recover data
- Take backup data and devices offline immediately
- Secure any hijacked data that can be secured
- Change all account and network passwords — once the ransomware is removed from the system, you also need to change all system passwords

The best form of defense against ransomware attacks is to ensure that they never happen in the first place. This can be achieved by modeling your entire attack surface — including infrastructure, assets and vulnerabilities — to gain full and unerring visibility over your entire security environment, understanding the context that surrounds your critical assets and vulnerabilities, and establishing remediation strategies that empower you to target your most exposed flaws before criminals can exploit them.

HOW TO IMPROVE OT SECURITY

Operations teams should first look to introduce rule flows, take advantage of dynamic firewalls, improve control access and establish ways to mitigate risk that originates from connected third–party environments. Being in command of each of these areas will give them the confidence to embrace solutions that allow them to identify and mitigate all vulnerabilities within their environment without disrupting uptime.

Further, they need to increase the pace of their scans — many only perform one or two scans a year and then only on the devices that they can take offline. The ability to discover the vulnerabilities that exist within critical OT devices and technology needs to be a prime concern for operations teams.

Only when these core capabilities are achieved will organizations with hybrid IT–OT networks be able to holistically manage risk. At that stage, they must:

- Passively collect data from the networking and security technology within the OT environment
- Build an offline model encompassing IT and OT to understand connectivity and how risks could impact either environment
- Use purpose–built sensors to passively discover vulnerabilities in the OT network
- Incorporate threat intelligence and asset exposure to prioritize OT patches
- Leverage the model to identify patch alternatives to mitigate risk when patching isn't an option

Read more > Hybrid IT-OT, A Unified Approach

ABOUT SKYBOX SECURITY

At Skybox Security, we provide you with cybersecurity management solutions to help your business innovate rapidly and with confidence. We get to the root of cybersecurity issues, giving you better visibility, context and automation across a variety of use cases. By integrating data, delivering new insights and unifying processes, you're able to control security without restricting business agility. Skybox's comprehensive solution unites different security perspectives into the big picture, minimizes risk and empowers security programs to move to the next level. With obstacles and complexities removed, you can stay informed, work smarter and drive your business forward, faster.

www.skyboxsecurity.com | info@skyboxsecurity.com | +1 408 441 8060