UNIT 42
BY PALO ALTO NETWORKS

paloalto NETWORKS

The CISO's Guide to Incident Readiness and Response

UNIT 42
THREAT-INFORMED INCIDENT RESPONSE

Table of Contents

As a CISO, your mission is to protect your organization's systems, users, critical data and customers against cyberthreats.

To keep your organization ready to handle rising threats, you must motivate your entire organization to have a strong security culture. This is hard. You have an expansive and dynamic attack surface to defend, supply chain risks to consider, and limits on your budget.

Our "CISO's Guide to Incident Readiness and Response" sheds light on today's evolving threat landscape. It will help you better understand the most prevalent risks your organization faces, not to mention prepare for today's most significant threats.

In the following pages, you will find expert guidance and insights on protecting your organization without stifling its innovation. And we start by shining a light on the methods and security shortcomings threat actors exploit to great success. Unit 42 researches and investigates hundreds of incidents a year, and we've evaluated those incidents to determine the most prevalent attack methods used by threat actors to successfully compromise organizations. We share many of our findings within this guide.

You will also find recommendations for securing your organization against these attack methods, as well as advice on how to stay ahead of the evolving cyberthreats that exist today and those still taking shape on the horizon.

It is also critically important that your peers—fellow leaders who are also responsible for ensuring business operations run smoothly and securely—understand the security risks the organization at large faces. So, we've structured this guide to help you effectively communicate today's cybersecurity threats with leadership teams and board members as well as legal and regulatory departments.

We know how tough it is to keep up with the rapidly evolving threat landscape, but we've got your back.

Wendi Whitmore
Senior Vice President, Unit 42
Palo Alto Networks

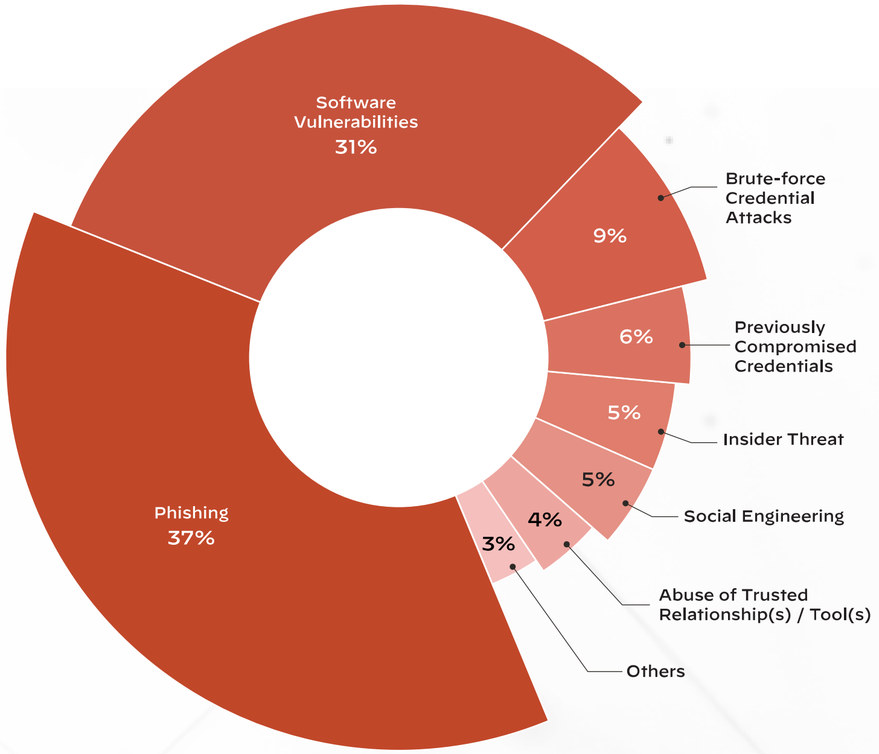
Did You Know?

Before you can protect your organization against cyberattacks, you must first understand where most attacks are coming from and where your critical assets reside. Only then will you know where to spend your limited resources where they matter most: Focused on the threats that represent the biggest risk to your organization.

Based on findings from Unit 42 incident response cases over the past year, the top three access vectors that threat actors used to get into an organization's environment were phishing, the exploitation of known software vulnerabilities, and brute-force credential attacks. Combined, they make up over 77% of the suspected root causes for intrusions.

Having a big picture understanding of the security challenges organizations face will enable you to more readily identify the specific areas attackers are targeting. And knowing how attackers are doing it can help you take the necessary proactive steps to better prepare for future threats.

How Attackers Gain Initial Access to Organizations



The 5 Areas of Concern

Applying Unit 42's firsthand case experience and the in-depth industry knowledge from the Unit 42 Threat Intelligence team, we arrived at five core areas of concern that contribute to the proliferation of the attack vectors. In the following pages, we'll take a look at each one in greater depth.

1. Supply chain attacks
2. Multifactor authentication (MFA)
3. Cloud security and identity and access management (IAM)
4. A growing attack surface
5. Overloaded security teams

Concern #1:
Supply Chain Attacks

DevOps and agile software development practices have helped organizations speed up development cycles allowing for more rapid release timelines. But speed often results in a reliance on third-party code in vendor applications, which could come from anyone, including an advanced persistent threat (APT), allowing attackers to take advantage and launch supply chain attacks.

Given modern cloud software development practices for sharing and incorporating third-party code—and creating complex structures that depend on many other building blocks—if an attacker compromises third-party developers or their code repositories, it's possible to infiltrate thousands of organizations.

OUR RECOMMENDATION

Embed Security into the Software Development Pipeline

Extending security beyond the runtime phase (the last phase in the build, deploy, and run model of development) and integrating it into every stage of development enables you to create automated security guardrails.

With these guardrails, you can:

- Catch vulnerable code prior to deployment (i.e. in the pre-commit stage).
- Check builds for defects prior to pushing code to production.
- Conduct efficient vulnerability scanning in runtime environments.

The first step in extending security across development starts with creating a shift-left security strategy that can evolve over time. A shift-left security strategy—named for its intention to "shift" security to phases that come before the run phase—is a brief document. It defines success and lays out ownership, milestones, and metrics for embedding security processes and tools into all stages of the continuous integration/continuous development (CI/CD) pipeline.

After creating your strategy, you'll need to understand where and how software is created in your organization. Start by looking organization-wide and documenting the overall flow of software in your company. Key items to identify include who is developing code (people), how it flows from development laptops to production (process), and which systems you use to enable the process (technology).

Learn more about steps you can take to better protect your organization against supply chain attacks.

Based on a global analysis[1], Unit 42 researchers found that:

63%

of third-party code templates used in building cloud infrastructure contained insecure configurations

96%

of third-party container applications deployed in cloud infrastructure contain known vulnerabilities

1. Unit 42 Cloud Threat Report, Volume 5

Concern #2:
MFA

Looking at a selection of recent Unit 42 incident response cases, 89% of the organizations that fell victim to business email compromise (BEC) attacks had failed to turn on MFA or follow email security best practices. Additionally, in 50% of all Unit 42 incident response cases—BEC or otherwise—organizations lacked MFA on key internet-facing systems such as corporate webmail, virtual private network (VPN) solutions, and other remote access solutions.

MFA, if configured correctly, is an effective way to set up a layered defense, making it harder for threat actors to access your system with just a stolen password.

OUR RECOMMENDATION

Implement MFA as a Technical Control and Security Policy for All Users

Integrate MFA for all remote access, internet-accessible, and business email accounts to greatly reduce your organization's attack surface. To prevent threat actors from circumventing MFA, disable legacy authentications/ protocols and confirm that MFA is not only deployed, but that employees are also using it correctly, and avoid using SMS as a second form of authentication. Effective forms of MFA include one-time passwords (OTPs) and cryptographic token-based authentication.

Remember to implement MFA internally as well. Too often, after authenticating MFA once, a user can bounce around the network without re-verifying MFA, even when moving to a system with a different trust level (e.g., from workstation to server).

Learn more about the consequences of missing or improperly deployed MFA and 7 Common Security Gaps You Can Address to be More Secure.

> "Work on the basics. Organizations like to follow the news and go after the new 'named' vulnerability while still lacking in the fundamentals such as patch management and multifactor authentication."

Clint Patterson
Unit 42 Principal Consultant

Concern #3:
Cloud Security and Identity and Access Management (IAM)

Improperly configured cloud environments essentially leave the door unlocked for malicious actors, allowing them to gain initial access without needing to find and exploit a vulnerability or make use of sophisticated techniques. It's no surprise that attackers commonly look for improperly configured cloud environments.

According to a recent volume of the Unit 42 Cloud Threat Report, IAM misconfigurations alone contributed to 65% of the observed cloud security incidents. Based on research conducted between January and June 2021, Unit 42 found that cloud environments are more susceptible to attacks today than in October 2020 (when we released a report that detailed the security risks IAM misconfigurations can pose to cloud environments).

To better secure your cloud environments, you can safeguard IAM permissions by:

- Checking for misconfigurations, default and overly broad permissions, and other weaknesses.
- Instituting procedures to identify exposed IAM access keys.
- Continuously monitoring IAM access keys to cloud resources.

To learn more about security shortcomings in the cloud and the latest threat tactics, download our Unit 42 Cloud Threat Report, Volume 6.

OUR RECOMMENDATION

Secure Your Cloud Environments with Proper Training and Configuration

Access to cloud controls such as Cloud Services Provider (CSP) consoles, APIs, and command-line interfaces in the cloud should be restricted to only those who need it. Such Role-Based Access Control (RBAC) is essential to minimizing risks of misconfiguration and other security errors. We also recommend your organization invests in a cloud-native security platform to routinely monitor cloud environments for IAM misconfigurations both within production and development environments.

Your organization should also:

- Deploy data loss prevention solutions.
- Regularly audit your cloud data to understand what is sensitive and know where it's located.
- Use MFA for authorized users as well as certificates and digital signatures.
- Separate administrative and user credentials, and limit everyday users to production environments.
- Evaluate your options for managed security services if you do not have the in-house expertise or your cloud environment is particularly complex.

In a separate analysis, Unit 42 researchers studied identity and access management (IAM) controls of more than 680,000 identities across 18,000 cloud accounts from 200 different organizations. **Nearly all (99%) lacked the proper IAM policy controls to remain secure.**

> "Right now, threat actors in the cloud don't have to try very hard to be successful at what they do. They may look around and say, 'Okay, there is a door, here are the keys—nobody even knows we found them. Let's see if this works. Oh, it does!' Then they take what they think is worth something, leave a ransom note, and kick over a few flowerpots on the way out—just to add a dash of destruction."

Ashlie Blanca
Unit 42 Consulting Director

Concern #4:
A Growing Attack Surface

Modern attack surfaces are inherently dynamic, and constantly shifting, moving and growing over time. This means that as attack surfaces grow, the number of unmanaged assets across those surfaces grow, too. As a result, attackers are becoming increasingly adept at scanning the internet in search of vulnerable systems and exploiting gaps in security before they can be patched.

OUR RECOMMENDATION

Be a Champion for Proactive Visibility

Security can be hard. Sometimes it's as simple as that. Security teams do the best they can with the resources and the data they have, but visibility is often the deciding factor as to whether an asset is secure. Another tool in the SecOps arsenal should be an attack surface management platform that can provide a comprehensive and continuously updated inventory of all internet-connected assets and potential exposures.

An attack surface assessment can help you gain visibility into your internet-facing assets. Specifically, a Unit 42 Attack Surface Assessment combines visibility into your internet-facing assets with actionable recommendations to help you mitigate threats and reduce business risk. This Unit 42 service discovers shadow IT infrastructure, identifies assets susceptible to common vulnerabilities and exposures (CVEs), and ranks risks and recommendations based on Unit 42 security expertise and threat intelligence.

Learn more about the benefits of a Unit 42 Attack Surface Assessment.

If you don't know where exposures live, it's impossible to ensure issues are remediated. Unfortunately for defenders, attackers just need one crack to find their way in. Attackers thrive on the complexity and ever-changing nature of attack surfaces because they can scan the entire internet looking for those weak points. The best option for security teams is to ensure they have the same view of their own attack surface. With an attacker's point of view, identifying and prioritizing issues for remediation gets far easier.

Patch Open Vulnerabilities Quickly

Out of the 600+ Unit 42 incident response cases evaluated, poor patch management contributed to 28% of all successful breaches. Your organization must ramp up patch and vulnerability management to apply patches as soon as due diligence allows. Patching open vulnerabilities should be prompt and prioritized with a high sense of urgency, oversight and validation.

4 Trends on the State of the Global Attack Surface

From March to September, we monitored scans of 50 million IP addresses—over 1% of the entire internet—associated with 100+ global enterprises to understand how quickly adversaries can identify vulnerable systems for fast exploitation. Based on observed scan data, not self-reported surveys, we identified the following trends:

1. Low-hanging fruit like basic security hygiene (e.g., strong passwords, MFA deployment) remains unaddressed.
2. End-of-life software could mean end-of-life for your security.
3. The unmanaged attack surface continues to grow.
4. Issues are persistent, complex and unique.

Concern #5:
Overloaded Security Teams

The challenges facing security teams continue to expand, not coincidentally, as attack methods grow and evolve. Consider these three challenges of an average cybersecurity team:

Too many alerts
In 11% of Unit 42 incident response cases, important security alerts got lost without sufficient review/action.

Too many security products
Administrators are often monitoring the network using a patchwork of tools. And, they're forced to rely on disparate sources of information from those tools.

Too many manual/ time-consuming processes
Poor processes for patch management tasks contributed to threat actor success in 28% of the Unit 42 incident response cases. These cases involved vulnerabilities that were disclosed publicly with patches available. However, the threat actors were able to exploit vulnerabilities that remained unpatched.

Learn more key takeaways from our in-depth case review. Download our 2022 Unit 42 Incident Response Report.

OUR RECOMMENDATION

Automate Where Possible

Intelligent automation can help your team prioritize scarce resources, consolidate visibility and control over a dynamic network, and reduce response and recovery tasks.

Consider implementing automation tools and take advantage of pre-made playbooks to respond and recover from incidents quickly. Incident response, SecOps and threat intelligence teams can save many hours of manual labor trying to piece disparate sources of information together from multiple tools.

Security orchestration, automation, and response (SOAR) products can automate the whole process of user investigation, endpoint isolation, notifications, enrichment, and threat hunting. By orchestrating across security information and event management (SIEM), firewalls, endpoint security, and threat intelligence sources, response teams can act quickly in the face of a breach or attack.

Advantages of Intelligent Automation

- Ensure proper use of scarce resources.
- Gain clarity and control across the network.
- Accelerate response and recovery timelines.

> “Humans are biologically programmed to make mistakes. We are consistently the weakest link in cybersecurity. It is crucial that organizations incorporate automation and intelligent, data-driven tooling wherever feasible. It seems like common sense, but reducing human error is one of the best strategies for bolstering organizational security posture.”

LeeAnne Pelzer
Unit 42 Consulting Director

As the saying goes, “Proper preparation prevents poor performance.”

If that isn’t your organization’s rallying cry for IT security preparedness, it should be. And the first step is to ask and answer three critical questions:

1. Are the right people in place and are processes optimized?
2. Have you invested in the necessary tools and technology?
3. Is there proper governance to protect the organization?

Based on your answers, redefining your security strategy can begin. We’re ready to help you:

- Build a strategic roadmap that makes transformation easier.
- Stay up to date on the latest threats against your organization.
- Develop an actionable incident response plan.

Your board has questions.
How will you answer?

Now with a clear picture of today's most prevalent threats on the security landscape, it's time to act. Don't make the mistake of going at it alone.

Taking a proactive approach to cybersecurity isn't the job of one person or a specific group. It's an all-hands-on-deck initiative that requires active participation and buy-in from everyone in your organization.

And it starts at the top. Your board may not be on the front lines of assessing and testing the organization's security posture, but members need to feel confident about the strategy you're putting into practice. Otherwise, the funding and resourcing you need to be effective in this high-stakes fight is a lot harder to come by.

Your board is going to have questions. You'll have the right answers—if you share your insights in a way decision-makers can understand.

The first step is yours to take. Check out our Unit 42 executive content for inspiration and proven ways to talk to your board and key stakeholders about cybersecurity risks.

Get the Unit 42 toolkit for talking to your board

3000 Tannery Way
Santa Clary, CA 95054

Main +1.408.753.4000
Sales +1.866.320.4788
Support +1.866.898.9087

www.paloaltonetworks.com

© 2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.