SYGNIA

MARCH 2024

SYGNIA'S ANNUAL FIELD REPORT

THE DEFENDER'S PERSPECTIVE: PREPAREDNESS

As we continue into 2024, the cybersecurity world faces increasing challenges. Last year's trends showed a rise in both classic and novel cyber-attacks, and this trend is expected to continue. In this installment of **Sygnia's Annual Field Report: The Defender's Perspective - Preparedness** the Sygnia Enterprise Security team analyzes last year's key cybersecurity developments, forecasts upcoming threats and emphasizes the need for agile and proactive security strategies to effectively combat these evolving cyber threats.

BACK TO BASICS: UNCOVERING THE SIMPLICITY BEHIND MAJOR CYBER ATTACKS

Attackers frequently **leverage basic, well-known methods** rather than uncovering or exploiting zero-day vulnerabilities. It is crucial to recognize that most of these attacks do not stem from complex, unknown exploits, but from exploiting misconfigurations, vulnerabilities in unpatched systems located in the perimeter or through phishing attacks that compromise credentials. This trend underscores the **importance of addressing fundamental security weaknesses** to enhance an organization's cyber resilience.

Learn more: Threat Actor Spotlight: RagnarLocker Ransomware

On the defense side meanwhile we are witnessing a shift in mindset with a growing focus on enhancing backup policies and tools, especially as a strategic response to ransomware attacks. Organizations are beginning to understand the **critical importance of backups**, not just as operational necessities for data recovery, but as **essential elements of their cyber security strategy**.

However, while backups play a significant role in cyber security strategies during the recovery phase, this often leads to deprioritizing cyber resilience measures. Many large networks remain poorly segmented, and there is a tendency to overly-trust identities within the network perimeter, contrary to the principles of Zero Trust. A further concern among less mature organizations is the insufficient enforcement of multi-factor authentication in publicly accessible resources, including cloud services and remote access solutions as well as in internal access to critical infrastructures and management systems. Furthermore, while cyber security pioneers and mature enterprises are standardizing MFA in their security policies, attackers are utilizing sophisticated techniques to bypass these measures, such as proxy-based phishing, token hijacking, and SIM swapping. These risks are driving enterprises to consider further advancements into FIDO-based Passwordless authentication methods and novel token-binding features offered by identity providers.

The above-mentioned concerns highlight a significant gap in security measures; while backups are vital, they cannot be the sole defense against ransomware. Adversaries are increasingly shifting their tactics towards data exfiltration rather than encryption, necessitating a broader range of mitigation measures against potential data leakage.

Learn more: Ransomware Declines as InfoStealers and AI Threats Gain Ground

THE DUAL CHALLENGE OF SEC COMPLIANCE AND CISO ACCOUNTABILITY

The SEC's (Securities and Exchange Commission) new rules, which mandate public companies to report on material cyber security incidents within four business days and to annually disclose their cyber processes and risk management procedures, have already had a major impact; the prompt reporting of the MGM breach resulted in a negative credit assessment from Moody's and the BlackCat group exploited these new SEC regulations to pressure the victim during the MeridianLink incident. Clearly cybercriminals are not only advancing technologically but also manipulating regulatory environments to amplify their extortion efforts.

While these rules aim for transparency, they can pose new challenges; early disclosures during stealth investigations, particularly before the eradication stage, might unintentionally reveal your awareness of the threat actor, potentially prompting them to escalate their attack.

Recent high-profile lawsuits against CISOs also raise concerns. Cases like Uber and SolarWinds highlight a growing trend towards accountability in cyber security leadership roles. In each case it is alleged that the organizations failed to fully comply with the stringent cyber security standards set by their CISOs and did not disclose that.

Increasingly stringent standards could enhance cyber awareness through increased senior management involvement. However, it may also lead cyber security managers to adopt less comprehensive compliance standards, therefor reducing the risk of legal challenges by adhering to more achievable standards and frameworks, even if they are less rigorous and therefor less secure. In addition, the CISO might emphasize ongoing processes and general security principles instead of divulging specific vulnerabilities or technical configurations. Consequently, it is crucial for CISOs to ensure alignment with the organization's board by clearly communicating the current cybersecurity strategy, the associated risks, the current and targeted security posture, and the potential business implications of the proposed approach. This communication should translate technical considerations into tangible business consequences to resonate with board members' priorities.

Learn more:

> Extortion Using New SEC Rules
> MGM Extortion and Report According to New SEC Rules
> Lawsuits Against Individual CISO Roles

AI REVOLUTION: TRANSFORMING CYBER ATTACK DYNAMICS AND ACCESSIBILITY

The rise of AI and generative AI in cybersecurity marks a turning point in attack strategies. Not only are we witnessing a significant reduction in the time required to execute attacks, but also an increase in their targeted capabilities. This shift is largely due to AI's ability to rapidly analyze extensive amounts of data and to craft phishing attacks and other offensive tools with greater accuracy. Cyber attacks are subsequently becoming more sophisticated and challenging to defend against.

Attackers have openly admitted using AI to drastically shorten the attack phase and this is not just a technical evolution; it lowers the barrier for entry into cybercrime, potentially leading to a spike in the number of attackers. These attackers are increasingly leveraging AI to orchestrate sophisticated phishing and voice phishing (vishing) campaigns, as well as to exploit vulnerabilities within organizations' AI-driven interfaces.

This shift in attack strategies necessitates a proactive response from cybersecurity managers. It is imperative to not only elevate employee awareness regarding these emerging threats but also enhance existing phishing simulation exercises. Organizations can thus better prepare for and counteract the advanced adversarial tactics . For cyber security professionals, our prediction is that treating the task of keeping up with AI trends and advancements as optional may widen the gap with threat actors. Consequently, actively developing effective defense mechanisms is critical to reduce this growing inequality.

Learn more:

> Attackers Using AI to Enhance Conversational Scams Over Mobile Devices

> OpenAI's Research on Abuse of Generative AI for Malicious Cybersecurity Tasks

THE CONSTANT CHALLENGE OF SECURING SUPPLY CHAINS AND EXTERNAL PARTNERSHIPS

In alignment with the persistent challenge of securing supply chains and external partnerships, an increased focus on supply chain risk management is becoming a key component of security strategies. The continual evolution of ransomware attacks, where attackers are not only becoming more creative in securing payments but also expanding their extortion tactics is necessitating an increased focus on supply chain risks. These tactics increasingly involve not just the primary data owner but also third parties and customers, thereby extending the impact and escalating the leverage of these attacks. Additionally, the rise in software supply chain attacks, impacting numerous victims globally, further underscores the substantial risk inherent in relying on third-party vendors, as evidenced by the FBI's warning regarding the Citrix Bleed vulnerability, which was also addressed in the SEC's new regulatory rules.

Learn more:

> Citrix Bleed Widely Exploited Warn Government Agencies

> Okta Cyberattack Exposed Data of All Customer Support Users

> The JetBrains TeamCity Software Supply Chain Attack: Lessons Learned

> What You Need to Know About the MoveIT Hack

Cybersecurity management is inherently dynamic, requiring CISOs to possess interdisciplinary skills and adopt flexible strategies. Legal and procurement aspects are crucial elements and external advisors can be invaluable for navigating complex regulations, as subject matter experts. **New regulations, AI-powered threats, and inventive tactics by adversaries** demand continuous adaptation. **Recent data breaches** show that cyber resilience is an ongoing process, not a one-time achievement. **Understanding adversaries' evolving operational methods, especially regarding third-party attack vectors**, demands a diverse CISO team bolstered by professional advisors when necessary.

WANT TO KNOW MORE ABOUT ONE OF OUR SOLUTIONS?

As the trusted advisor and cybersecurity service provider of leading organizations worldwide, Sygnia protects the enterprise through a variety of solutions that are aligned with the current threat landscape. From OT and Cloud Security to Ransomware Readiness, our Enterprise Solutions are borne out of frontline experience and a deep understanding of the threat actor mindset.