TECHNOLOGICAL ADVANCEMENTS AND HACKER INGENUITY: THE EVOLUTION OF CYBER SECURITY AND A ZERO TRUST MODEL

Roger Brown, CCO, DipMgmt (Open) MAPM

Christian Bailey, Regional Director, Zscaler

Stafford Hunt, Chief Technology Officer

Peter Tarbitten, Group Director

Chris Finch, Director, SOM3

Eric Forcythe-Reid, Director, Cyber Security

We examine the evolution of cybersecurity across time, tracing its inception in technology.

Collaborating with key global cybersecurity organisations, we retrospectively analyse and project the necessary adaptations organisations and technology must undergo for heightened vigilance and adaptability.

THE CYBER SECURITY THREATS AND CHALLENGES

The history of cybersecurity is a fascinating journey that parallels the rapid development and evolution of computer technology. Here is a brief overview of key milestones in the history of cybersecurity:

1940s-1950s: The Birth of Cybersecurity

The earliest form of cybersecurity focused on protecting classified government and military information during and after World War II.

Pioneering work was done in encryption and cryptography, such as the development of the Enigma machine during World War II.

1960s-1970s: The Emergence of Hacking

The first recorded instance of hacking took place at MIT in 1961 when students hacked into the university's computer systems.

The concept of "computer security" began to emerge as more computers were connected to networks.

In 1971, Bob Thomas created the first computer worm, called the "Creeper" virus, which highlighted the need for security measures.

1980s: The First Computer Viruses

The 1980s saw the emergence of the first computer viruses, such as the Elk Cloner, which infected Apple II computers.

The term "computer virus" was coined by Fred Cohen in 1983. The first antivirus software, known as "Reaper," was created to remove the Creeper virus.

1990s: The Internet and Cybercrime

The widespread adoption of the internet in the 1990s brought new opportunities for cybercriminals.

Major incidents, like the Morris Worm in 1988 and the first recorded case of ransomware (AIDS Trojan) in 1989, highlighted the growing need for cybersecurity measures.

The Computer Emergency Response Team (CERT) was established in 1988 to respond to cybersecurity incidents.

2000s: Rise of Cybersecurity Industry

The 2000s saw a massive expansion in the cybersecurity industry with the development of numerous antivirus, firewall, and intrusion detection systems.

Notable incidents include the Code Red worm in 2001, the Blaster worm in 2003, and the emergence of botnets.

Government agencies and organizations worldwide began to take cybersecurity more seriously.

2010s: Advanced Persistent Threats and Data Breaches

The 2010s witnessed an increase in sophisticated cyber attacks, such as Stuxnet (2010) and the Sony Pictures hack (2014).

High-profile data breaches, including those of Target, Equifax, and Yahoo, raised concerns about data security.

The emergence of state-sponsored hacking groups and advanced persistent threats (APTs) became a significant concern.

2020s: Continued Challenges and Advancements

The 2020s continue to see an increase in cyber threats, including ransomware attacks, supply chain attacks, and nation-state cyber-espionage.

The importance of securing critical infrastructure, such as power grids and healthcare systems, has gained significant attention.

Advancements in cybersecurity technology, including artificial intelligence and machine learning, are being used to defend against evolving threats.

Cybersecurity has evolved significantly over the years, reflecting the changing landscape of technology and the increasing sophistication of cyber threats. As technology continues to advance, the field of cybersecurity will remain critical in protecting information and critical infrastructure.

IN RELATION TO 2023

Tech headlines were dominated by apocalyptic, doom-laden discussions of AI and how this will impact everyday life. As is the case with other major advances in technology, we don't really know the full cybersecurity impact yet.

What we do know is that these tools will lead to a quicker time to market both for attackers and defenders. Cyber hacking tools are now commoditized and available as Malware as a Service (MaaS) on the Dark Web for Threat Actors of all kinds. AI will bring productivity increases, both beneficial and harmful. For example, AI can be used to quickly generate vast quantities of, better quality and highly tailored, Phishing attacks (known as Modern Phishing) via email, social media, or even Voicemail.

From a defence perspective, AI will also be used to learn, model, and analyse large amounts data to provide organisations with a synthesised, holistic view of their Indicators of compromise and user behaviour. These 360 views allow organisations to spot abnormal suspicious behaviour and to focus resources accordingly and in real-time.

Organisations are expected to continue increased investment in Cyber Security during 2024. Key to this is how they invest. At the top of the market the BFSI (Banking, Financial Services and Insurance) have the additional challenge of responding to regulatory pressure, but continue to struggle with legacy technology, which is out of support and requires wholescale change.

Small medium enterprises (SMEs) will seek to outsource their defences to cloud security providers and make greater use of subscription-based Secure Operations Centres and virtual CISOs (vCISO stands for virtual Chief Information Security Officer) providing expertise to raise their Cyber Security Maturity and provide expertise on demand.

The trend to converge Operational Technology with Information Technology continues at pace, bringing once isolated critical infrastructure into view for organisations and their attackers.

In summary, 2024 will see the same kind of threats as in previous years (Ransomware, Phishing, Insider, Malware)), but as more devices are connected the attack surface rapidly increases. We call this the Internet of Things (IoT). This number has doubled over the last 5 years and will double again over the next 5 years, estimated to be around 50bn by 2030.

Cybercrime operates as a booming industry — more than just flourishing, it holds considerable sway. In 2015, global GDP suffered a staggering $3 trillion hit due to cybercrime. By 2022, this number skyrocketed to $6 trillion. Projections for 2025 loom even larger at $10.5 trillion, an almost unfathomable sum. To put it in perspective, by 2025, cybercrime will erode the global GDP by $332,952 every single second.

2024 RANSOMWARE STORY

A UK-based small business with 45 employees recently experienced a devastating cyberattack orchestrated by a Cyber hacker. This company, which supplies raw materials to the UK military industry, suffered a complete system shutdown, including email and IT services, halting operations for 48 hours. The hacker then demanded a ransom of £4,000 per month to restore and safeguard the company's systems. After negotiations, the business made a substantial one-time payment exceeding £40,000 to regain access and resume normal operations.

These figures, already staggering, become more alarming when considering: Approximately 30,000 websites/businesses face attacks daily, equating to nearly one attack per second.

The edge not only widens the vulnerable surface for hackers but also introduces a whole new array of attack vectors.

The cloud, similarly, offers a new avenue for enterprise IT attacks. In 2022, about 45% of cyberattacks stemmed from cloud origins. This open, widely distributed environment, propelled by interconnected APIs, data, and applications, along with open-source software, serves as a fertile ground for cyber threats.

Valuable Practices in Identity Management

Weak Authentication Methods: Relying solely on passwords without implementing additional authentication factors increases the risk of unauthorised access in case of password compromise.

Overly Permissive Access Controls: Granting excessive access privileges to users increases the likelihood of unauthorised access and potential data breaches.

Manual Identity Management Processes: Manual provisioning and de-provisioning of user accounts are prone to errors and delays, leading to security vulnerabilities and compliance issues.

Lack of Regular Access Reviews: Failing to regularly review and update user access privileges can result in outdated access permissions and increased exposure to insider threats.

Failure to Encrypt Identity Data: Storing identity data in plaintext or using weak encryption methods makes it vulnerable to interception and unauthorised access.

GOOD PRACTICES IN PREVENTION:

Strong Authentication Mechanisms: Implement multi-factor authentication (MFA) or biometric authentication to enhance the security of user identities.

Regular Access Reviews: Conduct regular access reviews to ensure that users have appropriate access privileges based on their roles and responsibilities.

Centralised Identity Provisioning and Deprovisioning: Establish centralised processes for provisioning and de provisioning user accounts to ensure timely access management throughout the user lifecycle.

Least Privilege Access: Follow the principle of least privilege, granting users only the minimum access required to perform their job functions.

Encryption of Identity Data: Encrypt sensitive identity data both at rest and in transit to protect it from unauthorised access.

Continuous Monitoring: Implement continuous monitoring of user activities and behavior to detect and respond to suspicious or anomalous activities.

User Training and Awareness: Provide regular training and awareness programs to educate users about the importance of strong password management, phishing awareness, and other security best practices.

IDENTITY GOVERNANCE MANAGEMENT

Identity Governance: Identity management involves establishing policies and procedures for managing user identities, including provisioning and de-provisioning accounts, managing entitlements, and ensuring compliance with regulatory requirements. This helps organizations maintain a centralized view of user identities and their access rights.

Single Sign-On (SSO): Identity management systems often integrate with SSO solutions, allowing users to authenticate once and access multiple applications or services without having to log in separately for each one. This enhances user experience while improving security by reducing the number of passwords users need to remember.

Identity Federation: Identity management also facilitates identity federation, enabling users to access resources across different organizational boundaries using their existing credentials. This streamlines collaboration between organizations while maintaining security and control over access to shared resources.

CLOUD BASED SOLUTIONS FOR CYBER PROTECTION

Various companies specialize in cloud-based security solutions, each offering unique services. Cisco Umbrella, formerly known as OpenDNS, delivers cloud-delivered security services encompassing secure web gateway, DNS-layer security, and cloud firewall functionalities. Palo Alto Networks provides a suite of cybersecurity products and services, including Prisma Access for cloud security solutions. Symantec, now under Broadcom, offers the Web Security Service (WSS), focusing on cloud-based web security. Microsoft Cloud App Security serves as a cloud access security broker (CASB) solution, aiding organizations in monitoring and managing their cloud applications and data. Akamai Technologies offers cloud security solutions like Kona Site Defender and Akamai Secure Web Gateway, designed to defend against web-based threats. Forcepoint specializes in cybersecurity solutions such as secure web gateway, CASB, DLP, and next-generation firewalls. McAfee delivers cloud security solutions like McAfee Web Gateway, which provides web filtering, malware protection, and DLP capabilities for both cloud-based and on-premises environments.

Additionally, Zscaler stands out as a prominent cloud security company, offering diverse solutions to thwart cyberattacks and safeguard digital assets. Zscaler's comprehensive suite of security solutions empowers organizations to bolster defences, mitigate security risks, and maintain regulatory compliance through the utilization of cloud-native architecture and advanced security technologies.

2023 BRINGS ZERO TRUST SECURITY MODEL, IDENTITY MANAGEMENT PLAYS A FOUNDATIONAL ROLE

Zero Trust Architecture: Zero Trust is based on the principle of "never trust, always verify," where access to resources is continuously evaluated and authenticated based on various factors such as user identity, device health, and contextual information. Identity management provides the necessary mechanisms for verifying and validating user identities as they attempt to access resources, aligning with the principles of Zero Trust.

The Zero Trust is a cybersecurity framework that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are inside or outside the network perimeter. Traditionally, network security models assumed that everything inside a network is safe and trusted, while anything outside the network is not. Zero Trust flips this model on its head, asserting that no entity, whether internal or external, should be trusted by default. Instead, trust is continuously evaluated based on factors such as user identity, device health, location, and behaviour.

Continuous Authentication: Zero Trust requires continuous authentication and authorization based on user behaviour and the security posture of the devices they use. Identity management systems can integrate with behavioural analytics and risk-based authentication solutions to continuously assess user identities and detect anomalous behaviour that may indicate a security threat.

Micro-Segmentation: Identity management enables organisations to implement micro- segmentation strategies, where access to resources is restricted based on user identity and least privilege principles. This ensures that even within the network perimeter, users only have access to the specific resources required for their roles, reducing the attack surface and limiting the potential impact of security breaches.

Dynamic Policy Enforcement: Zero Trust architectures rely on dynamic policy enforcement to adapt to changing security requirements and threat landscapes. Identity management systems can dynamically adjust access controls and authorisation policies based on contextual information such as user location, device type, and security posture, ensuring that access decisions are always aligned with the organization's security policies.

If adopted by organisations, Zero Trust can bring several benefits:
Enhanced Security Posture: By adopting a Zero Trust model, organizations can significantly strengthen their security posture. Traditional perimeter-based security measures are increasingly inadequate against sophisticated cyber threats. Zero Trust emphasises a "never trust, always verify" approach, minimising the attack surface and making it more difficult for attackers to move laterally within the network Reduced Risk of Data Breaches: Zero Trust helps organizations minimize the risk of data breaches by implementing strict access controls and continuous monitoring of network activity. By enforcing the principle of least privilege, where users are granted only the minimum level of access necessary to perform their jobs, organizations can limit the potential impact of a security breach.

Improved Compliance: Many regulatory frameworks and industry standards, such as GDPR, HIPAA, and PCI DSS, require organisations to implement robust security measures to protect sensitive data. Zero Trust can help organisations achieve compliance with these regulations by implementing strong access controls, encryption, and monitoring capabilities.

Better Visibility and Control: Zero Trust enables organisations to have better visibility into their network traffic and user behaviour. By implementing solutions such as micro-segmentation and continuous monitoring, organizations can identify and respond to security incidents more effectively.

Adaptability to Modern Workforce Trends: With the rise of remote work and the increasing use of cloud services, traditional perimeter-based security models are becoming less effective. Zero Trust is well-suited to address the security challenges posed by these trends by focusing on securing identities and devices rather than network boundaries.

In conclusion, Identity management is foundational to cybersecurity management, and its integration with Zero Trust principles enhances organizations' ability to protect their resources, data, and networks from evolving cyber threats. As cyber security continues to evolve, Identity management will play an increasingly central role in ensuring secure access to digital resources in a Zero Trust environment.

Overall, adopting a zero-trust approach can help organizations mitigate cybersecurity risks, protect sensitive data, and adapt to the evolving threat landscape more effectively.

Their will be a follow up to this article next year to expand on Zero Trust Frame work and how its been implemented in organisations. ■