HC3: Analyst Note
July 21, 2023 TLP:CLEAR Report: 202307211200

Remote Identity Management

Executive Summary
Identity theft is not limited to stolen medical records, social security numbers, and financial data. Threat actors can also target institutions by capitalizing on gaps in user access protocols, hiring processes, and mitigation capabilities to conceal some aspect of their identity and attentions. Identity verification, fraud detection and user authentication are imperative when implementing a robust Identity and Access Management (IAM) program.

Report
The global digital transformation era has changed how enterprises interact with customers, clients, and employees. A comprehensive Identity and Access Management (IAM) program allows all parties to build mutual trust when performing transactions both online and in-person. Institutions are under pressure to transition high-risk interactions online, ultimately expanding their threat landscape. Security professionals and institution leaders are becoming increasingly faced with fraud from misrepresentation of identity. Balancing establishing trust in a user's real-world identity and optimizing user experience can be challenging.

According to the Federal Trade Commission (FTC) Consumer Sentinel Network Data Book, there were 5.2 million fraud reports in 2022, with identity theft and imposter scams representing the top two categories, respectively. Cyber criminals will look for avenues to manipulate and obfuscate their true identities for gain. The U.S. Treasury, the State Department, and the Federal Bureau of Investigations have issued alerts warning businesses that North Korean cyber criminals are posing as remote IT workers for hire from the U.S., Eastern Europe, Japan, South Korea, and China. The scammers also sub-contracted with other more legitimate workers to enhance their credibility. This threat emphasizes the need for a strong IAM program to protect data from espionage, intellectual property theft, and spills.

Digital On-Boarding and Verification
The capability to securely onboard and verify an employee or a customer's identity remotely is critical to enterprises. The COVID-19 pandemic significantly contributed to the adoption of remote work as a mainstream business model. The remote work trend does not appear to be going away anytime soon, as 48% of employees have continued to work remotely post-pandemic, and 62% of employees expect their employers will allow them to work remotely moving forward.

Without well-thought-out and implemented IAM policies, organizations can be susceptible to individuals who have misrepresented their employment history, applicants who have committed crimes or offenses under a different name than the one provided during the hiring process, and candidates with employment sanctions for your industry. More than ever, those inside the network cannot automatically be trusted. Stringent IAM policies should be in place to protect against compromises and data leaks. These policies include identity proofing, which focuses on cases when an organization is interacting with someone for the first time (account openings, registration, or enrollment), and identity affirmation, which is verification that a real-world identity exists, and that the individual claiming the identity is the true owner of that identity and is genuinely present during the process.

Insider Threat and Identity Management
Insider threats can be one of the most harmful to healthcare organizations; these include individuals

within the organization who wittingly or unwittingly expose sensitive data like Personally Identifiable Information (PII), proprietary data, etc. These individuals can be a trusted third-party or an employee – they are entrusted with knowledge about an organization's products, services, strengthens, and weaknesses.

Hackers attempt to approach/recruit employees and even leaders to commit potentially even more disastrous acts. Surveying IT and security executives by industry, cybersecurity professionals found that employees and leaders are increasingly being approached to assist in nefarious insider threat activities, such as ransomware attacks. Regardless of the size of the institution or business, insiders consistently prove to be one of the biggest threats to organizational security. Leaders and administrations can work together throughout the hiring and employment processes to significantly curb and mitigate insider threats. By implementing and designing an IAM security framework and technologies which tie your governance and subsequent policy rules into a centrally managed identity and access system, the ability of your organization to prevent and detect insider threats will be greatly enhanced.

Administrative Mitigations

The most effective mitigations need to span the entire enterprise with IT working along with Human Resources (HR) to proactively create robust policies to evaluate, identify, and mitigate insider threats.

- **Pre-Employment:** Probe for red flags during the screening and hiring of candidates and prospective employees, such as verifying accuracy of resume and references.
- **Employment:** Ensure that all individuals on the network are the same as those who interviewed for the role. Create and communicate clear organizational policies, such as establishing a baseline of normal behavior for both employees and IT networks to help identify significant changes, including monitoring network activity for potentially dangerous or inappropriate activity. Conduct routine and mandatory insider threat physical security and cyber-security awareness training. Consider leveraging automated, continuous monitoring services to notify HR when employees have become a post-hire security risk.
- **Post-Employment:** Establish detailed policies to retrieve all provided equipment such as laptops, badges, etc., and terminate all access/accounts of separated employees. Review intellectual property and/or non-disclosure agreements with separated employees.

It is also recommended by cybersecurity governance agencies that organizations form a multi-disciplinary threat management team to collaborate along all business lines, including upper management, to mitigate insider threats. A disciplined threat management team can prevent and respond to insider threats by monitoring and surveilling, investigating, escalating, responding to incidents, containing, post-response, and remediating.

- **Monitoring and Surveillance:** A threat management team can source and implement applicable security practices to help assess whom and what is accessing company resources. These practices include Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), Privileged Access Management (PAM), and Data Loss Prevention (DLP).
- **Investigation:** A capable threat management team will be experienced in evaluating key indicators to uncover the origins, causes, and extent of insider threat incidents.
- **Escalation:** Threat management teams will raise awareness and mitigation regarding insider threats incidents amongst stakeholders.

- **Incident Response:** Threat management teams are trained in the process of incident response, including threat management and response.
- **Containment:** A vigilant threat management team can lower the impact of attacks by quarantining, blocking, and securing compromised endpoints and/or essential business operations.
- **Post-Response:** Assess lessons learned and the readiness of the organization to respond to future insider threats, such as the efficiency of communicating with stakeholders to provide impactful recommendations to help reduce and mitigate future insider threats.
- **Remediation:** Implementing a comprehensive remediation plan to repair and restore essential business lines and functions, etc.

Additional Administrative Mitigations

ID Documents: In an on-site work environment, identity documents such as an I-9 and government-issued identification would typically be submitted during the in-person onboarding process. These documents need to be properly inspected and may require travel by prospective employees to physical locations for review and approval.

Databases: Fraud detection repositories can be part of a layered approach to reduce risk and improve trust. Checking identity data (e.g., name, date of birth, phone number, address) against sources such as credit bureau data, census information, and electoral records, etc., can affirm identity claims.

Software: Choosing the right IAM software should be a tailored approach for your business and industry. Knowing how many employees work remotely, what data they have authorized access to, what type of applications they use, and what security compliances must be considered, are all important questions to answer to secure your organization from potential threats.

- Biometrics: Authentication and verification technologies that can identify an individual by means of unique characteristics are very effective to securely on-board employees. That said, determined threat actors will try to circumvent even the most sophisticated IAM technologies such as biometrics, by spoofing (falsely purporting) to be a targeted employee. To help mitigate an identity spoofing attack, organizations should employ layered security and detection mitigation, such as a Presentation Attack Detection System (PAD).

- Presentation Attacks: Commonly referred to as spoofs, presentation attacks (PAs) are the process of subverting a biometric system using tools called presentation attack instruments (PAIs). Currently, there are three levels of presentation attack sophistication. In Level 1, which requires little to no expertise, equipment is readily available to include mobile phone display of face photos, paper printout of the face image, and high-definition challenge/response videos. Level 2 requires moderate skill and practice, and equipment is available, but requires panning and practice; attack instruments include paper masks, resin masks (targeted subjects), latex masks (untargeted subjects), and video displays of faces (with movement and blinking). In Level 3, extensive skill and practice is needed, equipment is not readily available, and attack instruments include silicone masks and theatrical masks.

- Remote Fingerprinting: Organizations can obtain fingerprints remotely, and individuals can use their smartphones to capture and verify multiple fingerprints in a contactless and non-intrusive manner.

For sectors such as the healthcare sector, where fraud is common and requires more comprehensive fingerprint verification and compliance, tele-fingerprinting services are available to safely and securely collect, verify, and submit FBI-approved fingerprints.

- Video Chats: Live video chats between employees and employers can provide an interactive and more secure way to capture and verify identities.

- Continuous Monitoring: A bad actor can and will look for gaps in the hiring process, such as during and even after hiring, to circumvent identity verification; they can even utilize surrogates to help conceal their true identity and nefarious intentions. By using behavioral analytics such as acritical intelligence (AI) to analyze the attributes of individuals, including how they interact with devices, data entry patterns and more, organizations can detect fraudulent usage of a user's device and account.
    - Location: A combination of IP address, Wi-Fi, GPS, and cellular data can be correlated with the presented identity to check for consistency and to affirm the identity claim.
    - Device: Attributes of a user's device like browser language and time zone, etc., can be correlated with the presented identity for consistency and identity affirmation.
    - Email: Link analysis can be used to verify when the email has been used prior with the presented identity.
    - Phone Number: Cross-referencing a phone number to the network operator and other dates can reveal identity data to affirm or refute an identity claim.

Additional Resources

- Identify Theft | Guidance Portal (hhs.gov)
- 202204211300_Insider Threats in Healthcare_TLPWHITE (hhs.gov)
- Defining Insider Threats | CISA
- HR's Role in Preventing Insider Threats (cisa.gov)

References

Federal Trade Commission. "Consumer Sentinel Network Data Book,". Feberuray 2023. Consumer Sentinel Network Data Book 2022 | Federal Trade Commission (ftc.gov)

Wired.com. "Good Luck Not Accidentally Hiring a North Korean Scammer". May 2022. Good Luck Not Accidentally Hiring a North Korean Scammer | WIRED

Prnewswire.com. "Telehealth Market Size Worth USD 224.87 Billion, Globally, by 2030 at 18.81% CAGR - Exclusive Report on Telemedicine Industry by Facts & Factors". April 2023. Telehealth Market Size Worth USD 224.87 Billion, Globally, by 2030 at 18.81% CAGR - Exclusive Report on Telemedicine Industry by Facts & Factors (prnewswire.com)

Intuition.com. "Remote Working Statistics You need to Know in 2023. January 2022". Remote Working

Statistics You Need to Know In 2023 - Intuition

IBM.com. “Cost of a Data Breach, A Million-Dollar Race to Detect and Respond”. 2022. Cost of a data breach 2022 | IBM

Hitachi-id.com. “The Rising Insider Threat: Hackers Have Approached 65% of Executives or Their Employees To Assist in Ransomware Attacks”. January 2022. [Infographic] The Rising Insider Threat | Hackers Have Approached 65% of Executives or Their Employees To Assist in Ransomware Attacks.pdf (hitachi-id.com)

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback