ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Identity and Access Management Solutions

Automating Cybersecurity While Embedding Pervasive and Ubiquitous Cyber-Hygiene-by-Design

December 2016

Authors

James Scott (Senior Fellow – Institute for Critical Infrastructure Technology)

Drew Spaniel (Researcher – Institute for Critical Infrastructure Technology)

`

Underwritten by:

Centrify®

Identity and Access Management Solutions: Automating Cybersecurity While Embedding Pervasive and Ubiquitous Cyber-Hygiene-by-Design

December 2016

Authors
James Scott, Sr. Fellow, ICIT
Drew Spaniel, Research, ICIT

Upcoming Event

Learn More about Identity & Access Management at the 2017 ICIT Winter Summit.

Registration is Now Open – www.ICITWinterSummit.org

Visit the ICIT Library to view additional research and publications

https://www.amazon.com/James-Scott/e/B01IPLQKSQ/ref=dp_byline_cont_pop_ebooks_1

Introduction

Cyber-hygiene is the collection of behaviors and best practices that ensure responsible decision-making, accountable actions, and continuous security (in terms of confidentiality, availability, and integrity), throughout the daily routine of personnel and in the daily operation of systems and assets. Unlike Cybersecurity, which is predominantly a cooperative effort between individual personnel, the organization, stakeholders, and associated third-parties, cyber-hygiene is a metric of each distinct individual. Aspects of cyber-hygiene include, but are not limited to, minimization of online data leakage; curation of digital profiles; adherence to policies, procedures, and guidelines; informed and intelligent decision making; avoidance of social engineering lures; reliance on complex and secure user credentials; and many other sub-routines and behaviors that supersede any one daily activity. Comprehensive cyber-hygiene requires every stakeholder to consider the implications of their every action and to always act according to the optimization of the cybersecurity posture of the organization and according to the minimization of the risk that an adversary will be able to harm the organization as a result of the stakeholder's action. Effective cyber-hygiene depends on every employee always acting intelligently and in response to the hyper-evolving threat landscape. In short, comprehensive and effective cyber-hygiene can be daunting, exhausting, and distracting, to personnel and stakeholders whose cybersecurity awareness and training may already be limited and whose responsibilities within the organization may already demand their entire attention. As a result, many organizations either fail to implement cyber-hygiene programs or rely on undertrained and underqualified personnel to bear the burden of cyber-hygiene. In both cases, adversarial compromise and exploitation of the organization's critical assets is an inevitable reality and is as easy as launching a social engineering attack which targets staff email lists. An attacker needs only to compromise a single employee account or system in order to establish a persistent presence on the network.

Employees ignore, or fail to adhere to, cyber-hygiene initiatives that impede productivity or that frustrate the user due to over-complication, due to an over-abundance of steps or checks, or due to over-utilization of attention, time, or other resources. Cyberattacks depend on the prevalent negligence derivative of failed cyber-hygiene policies, procedures, and controls that inundate personnel into ignoring or disregarding intelligent and informed actions and behaviors that protect the employee and the organization from compromise. Responsible organizations recognize the need to train personnel in cybersecurity best practices and in cyber-hygienic behavior; however, not every organization recognizes its responsibility to streamline and optimize cyber-hygiene efforts. Cyber-hygiene and cybersecurity practices best protect the organization and its interests when they are ubiquitous throughout the workforce, when they permeate the organizational culture, and when they seamlessly integrate into systems to alleviate a portion of the burden on the workforce. Identity and Access Management (IAM) solutions are fundamentally ubiquitous, culturally permeable, and integrate into existing systems by necessity.

Identity and Access Management (IAM) solutions are an essential cornerstone of any cyber-hygiene initiative because IAM solutions unburden personnel of a portion of cyber-hygiene responsibility by automating digital identity verification, credential distributions, privilege management, authentication mechanisms, authorization and access controls, cryptographic controls, auditing and reporting mechanisms, and other services. By securely automating these processes with an IAM solution, organizations gain holistic access controls, user accountability, and system auditability and threat

detection. By automating these functions with an IAM solution, organizations weaken adversarial attack chains that rely on compromising un-cyber-hygienic personnel.

Access Controls

An incident occurs when an adversary or malware gains unauthorized access to a system. Adversaries follow the path of least resistance into the system. In order to obfuscate malicious activity, threat actors often employ social engineering and other attack vectors to compromise legitimate employee system credentials, to obtain legitimate remote access credentials, or to leverage unmanaged third-party access. In 2015, 1 in 3 organizations was not cognizant of their current third-party access policies or contracts and 77% of information security professionals did not update third-party agreements or address third-party cyber-hygiene and system access in response to the hyper-evolving cyber-threat landscape [1].

Users, who fail to adhere to cyber-hygiene best practices, are the weak link in enterprise cybersecurity. Password-based security is an antiquated and inadequate defense against modern cyberattacks, data breaches, and fraud. As of 2015, 77% of organizations had a password policy or standard and 59% of organizations had a user/ privilege access policy [1]. Nevertheless, obtaining privileged credentials remains a fundamental and often trivial step in the typical attack cycle. Threat actors can even obtain compromised credentials on Deep Web markets and forums. In a 2016 study, Forrester estimated that 80% of security breaches involved the use of privileged credentials [2].

Identity and Access Management (IAM) solutions mitigate the risk of obsolete password-based access. For instance, multi-factor authentication (MFA), an IAM subcomponent, adds a layer of security and access and privilege based control by requiring users to provide extra information or factors in order to access corporate applications, networks, or servers. MFA validates the user identity through a combination of something the user knows (such as a username, password, PIN, security question response, etc.); something the user possesses (such as a smartphone, smart card, token, one-time passcode, etc.); and some information characteristic of the user (biometrics, retina scans, voice recognition, gait analysis, etc.). After OPM and other high-profile breaches, MFA adoption is rapidly advancing; however, many organizations fail to realize that decisions to only apply MFA to certain applications, systems, resources, or by certain users, leaves the organization exposed. Consistent and comprehensive authentication policies and applied technologies can eliminate the security gaps that result from asymmetric user privileges and cyber-hygiene levels. Instead, organizations can best mitigate cyberattacks at multiple points in the attack chain by requiring MFA for every end-user, every privileged user, and every tertiary user (such as third-party, contractors, etc.) and for every IT resource (applications, VPNs, endpoints, servers, cloud systems, etc.) [3].

Similarly, IAM solutions from trusted and reliable vendors can be integrated into existing systems to improve employee productivity and to make cyber-hygiene seamless and ubiquitous, through services that consolidate identities across applications and platforms, or that manage user authentication after a single sign-on (SSO). These services mitigate the risk of password reuse and user cyber-hygiene fatigue. Adaptive authentication services enable organizations to adapt their security posture to the hyper-evolving threat landscape through flexible, context-based policies that incorporate location, device details, network characteristics, time of day, user attributes, and other deterministic factors. Scalable IAM solutions from

trusted vendors, further protect organizations by securing cloud and on-site applications, as well as mobile, BYOD, and remote-access devices [3].

User Accountability

IAM solutions validate a user's identity and thereby, establish an accountability chain that can be used to track suspicious activity and preempt the evolution of incident to breach. If an information security professional is managing or monitoring to detect suspicious activity through analysis tools or through access control rules (i.e. time of day, etc.) then a user account can be monitored and treated as either compromised or malicious. With MFA, it is significantly more difficult, though not impossible, for threat actors to leverage legitimate user accounts and credentials in an attack. In other cases, malicious insider threats can pose a serious threat to organizations by compromising internal defenses, by compromising fellow personnel, by exfiltrating data, by intentionally installing malware, by orchestrating cyber-kinetic lone-wolf attacks, or by providing information to external threat actors, such as nation-state APTs. For instance, in 2015, 72% of Financial sector incidents could be traced to a current or former employee [4]. IAM solutions, such as MFA, provide a mechanism to hold users legally responsible or to detect and monitor active malicious activity.

System Auditability

IAM solutions can be used to establish context-based rules, to generate log information, and to enable the organization to forensically trace an incident. Information security professionals can use the information to improve incident response plans, to mitigate system vulnerabilities, to monitor the cyber-hygiene of the personnel base, and to improve cybersecurity awareness and training in response to the hyper-evolving threat landscape.

Conclusion

Identity and Access Management solutions are a critical component of organizational cyber-hygiene and cybersecurity initiatives because IAM solutions automate cyber-hygiene best practices, reduce user fatigue, provide access controls, establish user accountability, institute system auditability, and enable users to mitigate cyberattacks from unsophisticated actors (script kiddies, hacktivists, etc.) and to disrupt and detect attacks from sophisticated attackers (informed malicious insiders, nation-state APTs, etc.). Through the implementation of robust IAM solutions for all users, systems and networks, organizations can realize viritually immediate improvements to their cybersecurity posture while reinforcing cyber-hygiene best practices among personnel.

Sources

[1] "Bridging the Data Security Chasm: Assessing the Results of Protiviti's 2014 IT Security and Privacy Survey," Protiviti, 2015. [Online]. Available: http://resources.idgenterprise.com/original/AST-0135695_2014-IT-Security-Privacy-Survey-Protiviti.pdf. Accessed: Nov. 30, 2016.

[2] A. Cser, S. Balaouras, L. Koetzle, M. Maxim, S. Schiano, and P. Dostie, "Forrester Wave™: Privileged Identity Management, Q3 2016," Forrester, Jul. 2016. [Online]. Available: https://www.centrify.com/resources/centrify-leader-in-forrester-wave-pim-2016/. Accessed: Dec. 1, 2016.

[3] C. Corporation, *Centrify*, 2016. [Online]. Available: https://www.centrify.com/. Accessed: Dec. 3, 2016.

[4] "Global state of information Security® survey 2015," in *PWC*, PwC, 2016. [Online]. Available: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html. Accessed: Dec. 3, 2016.