3-25-2017

Applying Comprehensive Least Privilege: A Framework for Endpoint Security

Kenneth Knapp
University of Tampa, kknapp@ut.edu

APPLYING COMPREHENSIVE LEAST PRIVILEGE: A FRAMEWORK FOR ENDPOINT SECURITY

Kenneth Knapp
University of Tampa
kknapp@ut.edu

ABSTRACT

A common target of cyberattacks today is the endpoint device. Through a combination of social engineering and technical means, hackers can exploit vulnerable endpoints as an entryway into an organization. This paper presents an endpoint security framework through the comprehensive application of the principal of least privilege. The framework is applied to endpoint devices across the overlapping domains of people, processes and technology in organizations. The framework emphasizes nine key elements to endpoint security with an associated policy statement for each to promote an organizational culture favorable to least privilege thinking. As a contribution, this framework is one of the first scholarly efforts to apply the principle of least privilege to endpoint security.

Keywords

Information security; principle of least privilege; people, process and technology triad; endpoint security

INTRODUCTION

When targeting an endpoint device, malicious attackers typically use social engineering techniques to initially engage an end user. An endpoint can include all computers that end users operate such as laptops, desktops, printers and mobile devices. The attack may contain a combination of emails or social media posts designed to trick a user into clicking on a malicious link or opening an infected attachment. Securing the endpoint is difficult because of both the wide variety of devices in the enterprise and the tendency to favor functionality and convenience over security. As a result, malicious hackers will exploit vulnerable endpoints because they are easy targets. Further troubling is that a single compromised endpoint can serve as an attacker's entryway into an entire corporate network.

Organizations face serious cybersecurity implications if they allow an individual to run with unlimited administrator rights or 'most privilege'. Least privilege as a security approach goes beyond limiting individual account rights and can include controlling user's access to applications, data and security settings through group policy (Mutch & Anderson, 2011). Unlimited rights is dangerous because it allows users to download and run any software they choose. It permits users to set their own security policies, in effect, by choosing when and if they upgrade installed software.

This paper explores how the comprehensive application of a least privilege philosophy can be used to secure critical endpoint devices. To accomplish this, a theoretical framework is proposed that explores how least privilege can be used to secure endpoints. The framework goes beyond the technology dimension of endpoint security and emphasizes securing people, processes and technology as an overall strategy. After providing a literature background, the framework is introduced along with the research methodology. A brief discussion follows along with contributions and limitations of the proposed model.

BACKGROUND

The principle of least privilege can be applied in different levels and aspects within an organization. The notion that security is not only about technology but also involves *people*, *processes* and *technology* is a popular model for promoting comprehensive security. The people, processes, technology triad has origins in the organizational research literature (Leavitt, 1964) and has been applied to diverse fields. While several variations exist, an image search on 'people processes technology' reveals this model is commonly illustrated as a triad of overlapping circles. This parsimonious model is valuable for understanding the ways that least privilege may be manifested in an organization.

Each of the elements of the people, processes and technology triad are now introduced within the context of the principle of least privilege.

People

The people node represents the human resource and is often described as the 'human element' when discussing information security. In terms of least privilege, organizations must decide what level of access to information each person must have and if they have a 'need-to-know'. Their roles and responsibilities must correspond to the level of access given to systems, information, business processes and technology. People view, store and manage data to accomplish a particular task. People must also be trained to properly interact with data and systems in a secure manner that exemplifies least privilege.

Processes

In the context of this paper, processes refer to the business methods and practices that support the mission of an organization. These include the mechanisms to accomplish work and achieve goals within an organization. Organizational processes and rules can tie individual functional units into one operating as a whole by providing the administrative context with which persons work (Garud, Kumaraswamy, & Sambamurthy, 2006). Regarding least privilege, management must decide which business processes with requisite software applications must be given to employees. Deciding this access will often be based on the job description of the employee.

Technology

Includes the applications and infrastructure (i.e. software, hardware, networks) that comprises the tools that automate processes and make them more efficient (ISACA, 2009). In modern organizations, technology is central to both people and processes; it is technology that automates nearly every business process and customer service. With least privilege, decisions must be made on which applications and tools will be given to people to accomplish their jobs.

Having provided a definition of least privilege and the people, process, technology triad, the framework will be introduced after covering the methodology used to develop it.

RESEARCH METHODOLOGY

This paper introduces a comprehensive framework of the most critical aspects of applying the principle of least privilege to endpoint devices in an organization. The development took place in two general phases described as *software requirements* and *model construction*.

Software Requirements Phase

The framework resulted as a by-product from a consulting relationship between the author and the leadership of a technology startup company. The company developed a software application to better harden and secure endpoints in a Windows enterprise environment. The software consisted of an agent that enforced organization policy while hardening endpoint devices by controlling user privileges and removing unnecessary protocols and services. After an initial feature list for the software was enumerated, the framework was developed to illustrate the philosophy of the software features and promote an understanding of how least privilege is used to harden endpoint devices. During this process, five significant meetings with several phone conversations took place with the author and the development team between July 2015 and April 2016. Each meeting lasted about two hours and consisted of a discussion of how to automate security capabilities into product features. These capabilities were finalized into an enumerated list of product features that effectively implement least privilege at the device level. Once the initial product features were developed into an operational product, the development team refined its feature list with feedback from its beta-test collaborators. The initial product feature list of the software along with additional development information is available from the author.

Model Construction Phase

This phase refers to the development of the theoretical model. The evolving model was used as a framework to help think about the software features list. The software development team reviewed the model and provided input during its formation. During model development, the author referenced the academic literature for appropriate guidance and potential constructs for inclusion. The addition of the organizational policy construct is an example of this.

Looking for additional feedback, the near-final model was reviewed by a panel of six graduate business students who together had over fifty years of professional experience. The purpose of this step was to enhance the understandability and validity of the model. In this step, while minor edits were made to enhance understandability, no significant changes occurred. Many of the comments were positive such as "Overall, the framework is very easy to understand." The most substantive change from panel input was the reduction and rewording from six elements in the technology dimension to five elements; this rewording was done to enhance understandability and reduce unneeded overlap. During this entire process, the model was continually refined until finalized as shown in Figure 1. The resulting model will now be discussed.

RESULT: A FRAMEWORK FOR ENDPOINT SECURITY

Figure 1 offers a theoretical framework for the hardening of endpoints using the people, processes, technology triad with the principle of least privilege as an enveloping construct. Resulting from a review of the academic literature, an overarching construct was included to emphasize the relationship of organizational policy to the successful implementation of least privilege.

Writing the actual security policies are critical because a poorly written or wordy policy can cause confusion among employees. A policy statement should express the goals to be achieved by the organization and not provide the details of how to do it; organizational procedures can provide the necessary details. Instead, policies are written in a general fashion so not to get in the way of implementation. A best practice for policy writing is to use a formal but simple style without buzzwords or technical jargon. Formal words like 'shall' or 'shall not' are recommended (Barman, 2002). Once a draft policy is written, it must be coordinated within the organization and potentially reworked based on any feedback received. During this time, policy writers should spend the required time and effort to gain top management agreement on the proposed policy. Doing so will pay off throughout the life cycle of the information security policy program. Once management agreement is received and the policy approved, the policy document(s) should be signed by senior management.

To summarize at this juncture, implementing a strategy of endpoint security using the least privilege approach is difficult without supportive organizational policy. Each of the three elements of the people, process, and technology triad will now be discussed as it impacts least privilege.

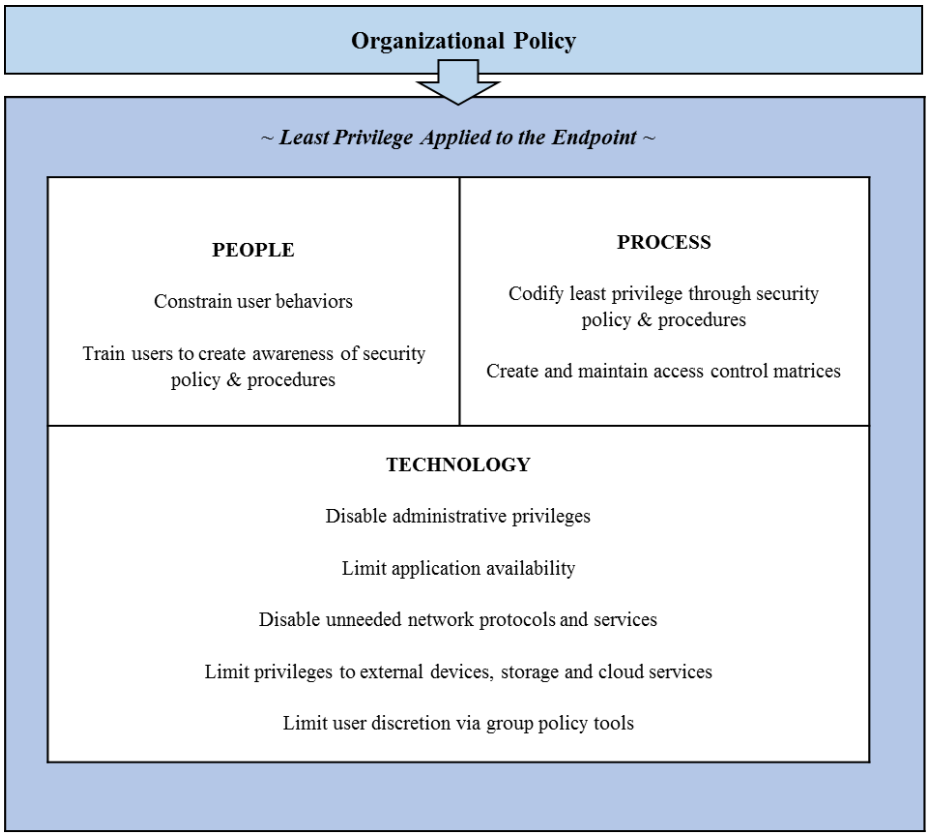

FIGURE 1. Framework of least privilege applied to the endpoint in organizations

Applying Least Privilege: People

The human element stresses the way people interact with endpoint devices as well as the policies that define acceptable behavior. It's critical because, even with secure technology and processes, an untrained or irresponsible user can fall victim to

a social engineering attack which can compromise an endpoint and thus an entire network. An irresponsible click on a link embedded in a phishing email can negate other technology and administrative control (Knibbs, 2015).

The goal of applying least privilege with people is to constrain their behavior so they comply with official policy and best practices in order to deter risky conduct. Examples include training people in how to handle social engineering attacks, educating users about policy and then enforcing the policy when it's violated. One example policy statement can state that official-use-only will be applied to the use of company resources: *Employees shall not engage in any unofficial business on company-owned computer devices without explicit permission*

To help ensure the success of least privilege as it relates to people, organizations must have a robust training and education program. If social engineering is a primary attack vector into an organizational network, then few will argue against the value of 'hardening' the end user through training. An example of related policy statements to help achieve this goal follow:

All new employees shall receive initial security training covering information security policies and procedures. Training refreshers shall occur annually for all employees. All training materials will promote the least privilege mindset with employees.

Applying Least Privilege: Process

In the context of the framework, a business process is a collection of related activities and tasks that produce a certain goal or output; it describes how work is done within an organization (Davenport, 1993). Ensuring business processes are done in a way consistent with least privilege is essential. Initially, key processes would need to be identified, developed and documented. Each process should then be analyzed to ensure that only employees with a need-to-know have approved access. With critical business processes such as an employee hiring process, it is highly desirable to control who has access to any candidate information or hiring decision outcomes.

Controlling a business process can be accomplished by the creation and maintenance of an access control matrix (ACM) or access control list (Harris, 2013). A comprehensive ACM can trace each subjects (persons) access to objects. Objects can include accounts, information and applications that pertain to critical business processes. Thus, an ACM can effectively limits a person's access rights to objects. An example policy to help mandate the use of an ACM can be: *The HR and IT organizations shall together ensure the development and maintenance of an access control matrix that specifies each employee's access rights to company data and business processes.*

It should be noted that other types of access control systems exist that can help implement least privilege goals when dealing with business processes. An identity and access management (IAM) system is an example of a framework for providing access control for individuals and business processes. An IAM system includes access management which contains authentication and authorization services as well as the management of access policies. The IAM system may include some type of single sign-on (SSO) capability that can serve across a business enterprise (Pulkkinena, Naumenkoa, & Kari, 2007). This is not an easy task especially with larger businesses. Often, a holistic enterprise architecture (EA) approach is needed to fully implement least privilege across an organization. An accompanying policy statement can then say: *The IT organization shall implement an identity and access management (IAM) system to manage employee credentials and control access to systems and business processes*.

Applying Least Privilege: Technology

This node in the people, process and technology triad emphasizes securing the hardware, software and network connectivity of the endpoint. For this area, the current paper reviews five critical aspects of how least privilege impacts the technological dimension of the endpoint.

Disabling administrative privileges

Turning off high-permission or administrative accounts and configuring them as low-permission or 'standard' accounts is arguably the most important single action an organization can take to implement a least privilege environment. Reports have stated that over 90% of critical exploits against Microsoft systems can be mitigated by simply not running computers in full administrative mode (Shah, 2014). Ensuring that users are not given full privileges is the most direct way to achieve this. If this is not possible in an organization because a mission essential application requires administrative rights to run on a device, for example, other actions can mitigate risks. These include turning off as many administrative tools as possible, disabling auto-run and enabling user account controls. A suggested policy statement: *Users shall not be given administrative-level account privileges on company computer devices unless explicit approval is given.*

Control application availability and functionality

As previously noted, least privilege stresses it's best to give users the necessary software applications to conduct their job and nothing more. When users are given unneeded software, the chance of a security incident increases. This is because the more software installed on a system, the more vulnerabilities and attack vectors are introduced into the system. By reducing applications to those only necessary to conduct business, the number of vulnerabilities and attack vectors likewise decreases. As a general rule, every single software application has intrinsic vulnerabilities, some known while others unknown. The overall process of removing unneeded services, software and privileges may be called 'system hardening' (Harris, 2013, p. 1248). Unauthorized applications that can be risky in the hands of users include games, client-based virtualization tools and web browsers. A suggested general policy statement to help implement least privilege in this area can state: *Users shall only be given access to software applications needed to perform their official duties.*

Disable unneeded network protocols and services

To illustrate this element, the Server Message Block (SMB) protocol is a network file sharing service in Windows. SMB negotiates and determines protocol configurations on a network that impact print ques, file access authentication, file locking and file directory change notifications in a client/server environment. However, SMBv1 has serious vulnerabilities. In one case, a corruption vulnerability allows a remote code execution in Windows when SMB incorrectly processes logging activities, resulting in memory corruption. An attacker could take administrative control of a target system, including the right to install, change programs, delete data or create and modify user accounts (Microsoft, 2015). Newer versions including SMBv2 and SMBv3 have addressed the vulnerabilities in SMBv1. Needless to say, if an environment doesn't need SMBv1, the protocol should be turned off and removed. A suggested policy statement: *Network and system services and protocols that are not actively used to support business technology functions should be removed from the corporate network.*

Limit access to external devices, storage and cloud services

Policies can be circumvented and data exposed if users have the ability to write to external media such as a USB drive. Software products and limited account settings can restrict the ability to write to a USB and to disable the auto-run feature. Consideration should be given to removing or limiting the ability of a device to use the Bluetooth protocol to act as a hot-spot, for example. A suggested policy statement can say: *No organizational endpoint devices shall use external devices, attachments, media and storage unless such access is necessary for official business and explicit permission is given.*

Limit user discretion via group policy tools

Administrative tools exist to implement group or collective policies for end user devices, effectively removing or restraining user privileges and discretion in these important areas (Microsoft, 2006). Areas such as enforcing robust password standards, requiring multi-factor authentication, mandating password protected screensavers, disabling guest accounts, curtailing software installers and ensuring that event monitoring and logging are enabled are all features in this category. Other policies can include requiring specific anti-malware software, enabling host-based intrusion detection or prevention systems, and requiring automatic updates of operating system or other third-party software applications. Least privilege effectively removes user discretion and the ability to set their own security policy on a device. A suggested least-privilege style policy could state: *The IT organization shall implement an effective group-policy for all company devices. This group-policy must implement least privilege and prevent users from changing important security and management settings.*

CONTRIBUTION

The contribution of this framework lies in its uniqueness and practical applicability in a business setting. After a search of the extant literature, no article was found using a scholarly research methodology that addresses implementing least privilege as an overall security strategy in organizations. This article will be the only article in the academic literature addressing the importance of endpoint device hardening using the principle of least privilege. The model provides a straightforward and useful framework that is especially suitable for small and medium sized enterprises since they typically lack the security expertise and resources of larger organizations. This model derived from a consulting relationship and is geared toward benefiting others in similar engagements.

LIMITATIONS

No single model can address every possible security concern just as no 'silver bullet' exists that will solve all security problems. The current paper is limited in scope and is not intended to provide a framework of all possible security criteria within a specific organization. Instead, the paper provides a framework for thinking about and applying the principal of least privilege at the endpoint. Also, the proposed model focuses on endpoint devices and does not directly address non-endpoint systems like network firewalls, intrusion detection or security information and event management (SIEM) systems.

CONCLUSION

In organizations today, the comprehensive implementation of the principle of least privilege is a valuable approach to secure an environment. The application of least privilege can protect endpoint systems by securing the three dimensions of people, process and technology to promote holistic security in organizations. This is timely considering that today the endpoint device is often the target of attacks and thus better securing the endpoint can significantly improve overall cybersecurity in organizations.

REFERENCES

1. Barman, S. (2002). *Writing Information Security Policies.* Indianapolis: New Riders.
2. Davenport, T. (1993). *Process Innovation: Reengineering Work Through Information Technology.* Harvard Business Press.
3. Garud, R., Kumaraswamy, A., & Sambamurthy, V. (2006, Mar/Apr). Emergent by design: Performance and transformation at Infosys Technologies. *Organization Science, 17*(2), 277-286.
4. Harris, S. (2013). *CISSP Exam Guide, Sixth Edition.* McGraw Hill.
5. ISACA. (2009). *An Introduction to the Business Model for Information Security.* Rolling Meadows, IL. Retrieved from http://www.isaca.org/
6. Knibbs, K. (2015, February 2). Bank security is so bad that a simple phishing scam can cost $1 billion. *Gizmodo*. Retrieved June 16, 2016, from http://gizmodo.com/bank-security-is-so-bad-that-a-simple-phishing-scam-can-1686131646
7. Leavitt, H. J. (1964). Applied organizational change in industry: Structural, technical and human approaches. In W. W. Cooper, H. J. Leavitt, & M. W. Shelly, *New Perspectives in Organizational Research* (pp. 55-71). New York: John Wiley.
8. Microsoft. (2006, January 18). *Applying the principle of least privilege to user accounts on Windows XP*. Retrieved June 2016, from TechNet: https://technet.microsoft.com/en-us/library/bb456992.aspx
9. Microsoft. (2015, September 8). *Vulnerability in Server Message Block could allow remote code execution (3073921)*. Retrieved 2016, from https://technet.microsoft.com/en-us/library/security/MS15-083
10. Mutch, J., & Anderson, B. (2011). *Preventing Good People From Doing Bad Things: Implementing Least Privilege.* New York: Apress. doi:10.1007/978-1-4302-3922-2_3
11. Pulkkinena, M., Naumenkoa, A., & Kari, L. (2007). Managing information security in a business network of machinery maintenance services business – Enterprise architecture as a coordination tool. *Journal of Systems and Software, 80*(10), 1607-1620. doi:http://dx.doi.org/10.1016/j.jss.2007.01.044
12. Shah, S. (2014, February 18). *Remove Microsoft admin rights to mitigate 92 per cent of vulnerabilities*. Retrieved from Computing: http://www.computing.co.uk/ctg/news/2329496/remove-microsoft-admin-rights-to-mitigate-92-per-cent-of-vulnerabilities