Applying Least Privilege to Achieve Endpoint Security: Using Third Wall™ to Protect Your Business

Kenneth J. Knapp, Ph.D., CISSP, CEH
Owner, Cyber Secure Advising LLC

Executive Summary. *This paper describes why a product like Third Wall™ for LabTech® is a critical element of an organization's cybersecurity strategy. Third Wall significantly increases endpoint security in Windows-based environments by implementing the principle of least privilege. This strategy not only enhances endpoint security at the point of attack for malicious hackers today, but Third Wall also promotes good risk management and regulatory compliance. This paper outlines five key ways that Third Wall implements least privilege at the endpoint. It also provides a summary on how Third Wall can help with the compliance of specific standards. (Note: This paper addresses Third Wall version 1; additional versions will add new features.)*

Today, any organization that uses computer devices and connects to the Internet must take cybersecurity very seriously. Business organizations of all sizes and industries are under the constant threat of cyberattack particularly from organized crime. Criminals are after any type of data that can be monetized to include financial, medical, retail, social as well as intellectual property.

A critical point of attack today is the endpoint device. External attackers typically use social engineering techniques to initially engage an end user. The attack may consist of emails or social media posts designed to trick the user into clicking on a malicious link or opening an infected attachment. Internal employees can also steal information or inadvertently misconfigure an endpoint device, leaving it vulnerable to attack. Endpoint devices include laptops, desktops, smart phones and more. Securing the endpoint is difficult because of both the wide variety of devices needing to be secured and the general tendency to give users as much functionality and convenience as possible. Yet, hackers exploit vulnerable endpoints because they are easy targets. Most troubling is that compromised endpoints can serve as an entryway for an attacker into an entire corporate network.

Overall in the United States in 2015 alone, over 220 separate data breaches compromising over 150 million records were reported publically in the news media (Privacy Rights Clearinghouse, 2016). This is a staggering number of compromised records for a single year. Today, the typical breach involves an end user on their device. One report stated that 55% of security incidents involved privilege abuse where employees misuse the access they have been entrusted with. In these cases, privilege abuse in computer information systems is *the* defining characteristic of the internal actor breach (Verizon, 2015). Negligent users are seen as the greatest source of endpoint risk (Ponemon, 2015) -- this provides significant insight because users who abuse privileges on their endpoint device can make their device a vulnerable target if they weaken a security setting, for instance. Governance and control processes are considered the biggest enablers in stopping these type of endpoint attacks. In one survey, security professionals believe that 72 percent of attacks on an organization's endpoints can realistically be stopped by enabling technologies, business processes and in-house expertise (Ponemon, 2015).

The Principle of Least Privilege

Implementing the principle of least privilege ensures that every system program and user is given the least set of privileges necessary to complete a job and nothing more (Indiana University, 2016). This principle limits the damage resulting from a security incident, whether malicious or accidental, internal or external. Least privilege reduces the number of interactions among programs and users to a minimum so that unintentional, unwanted, or improper uses of privileges are less likely to occur. The military security clearance rule of "need-to-know" is an example of this principle: even if a person has the proper clearance, they must also have a need-to-know to be given access to privileged or classified information.

Least privilege through hardening the endpoint. From a security standpoint, it's best to give users the necessary software and access privileges to conduct their job and nothing more. When users are given more privileges than they need, the chance of a security incident increases. As such, the more software applications installed on a system, the more vulnerabilities and attack vectors into the system. By reducing software access to those only necessary for 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. Thus, removing an unused application, service, protocol or unneeded privilege can significantly reduce the likelihood of an incident. This is especially true regarding 'zero day' vulnerabilities that are in the wild but unknown to the public: the fewer applications on a system, the lower the likelihood of being compromised by a zero day vulnerability. In this regard, for example, Third Wall version 1 has a valuable feature that disables the Windows® Installer. Future Third Wall versions will add on this capability such as disabling risky applications like Adobe Flash. This overall process of removing and preventing the installation of unneeded software, services and privileges is called 'system hardening'.

Hardening the Endpoint in Five Ways. Very few products do what Third Wall does. Many security strategies focus on perimeter security and tools like firewalls, proxy servers and intrusion prevention systems. These are essential. But when it comes to the endpoint, many focus too narrowly on anti-virus software and ensuring that regular updates occur. While both are vital, endpoint security today must go beyond this and implement a hardened, least privilege configuration on all devices. However, this is easier said than done. It can be administratively burdensome and labor intensive to harden dozens, hundreds or even thousands of endpoint devices in an organization without a tool like Third Wall.

Third Wall is unique in that it focuses on endpoint security using the LabTech® foundation. In doing so, Third Wall accomplishes endpoint security in five key areas.

1. *Disabling or Limiting Administrative Privileges*. Turning off high-permission or administrative accounts and configuring them as low-permission or 'standard' accounts is probably *the most important single action* an organization can take to

implement a least privilege environment. Multiple reports have stated that over 90% of critical exploits against Microsoft systems can be mitigated by simply not running computers in full administrative mode (Protalinski, 2010; Shah, 2014). Moreover, many ransomware or 'cryptolocker' attacks can be stopped by running in low-permission mode (Saiyed, 2016). Ensuring that users are not given full privileges is the most direct way to achieve this. Other actions such as turning off as many administrative tools as possible, disabling auto-run, enabling user account controls can all mitigate risk in this area as well.

2. *Disabling Unneeded and Insecure Protocols.* For example, 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. Third Wall can do this and disable other risky protocols and services that are common in Windows environments, like obsolete authentication services such as the LM Hash.
3. *Liming user discretion through endpoint policies.* Third Wall provides the ability to implement group policies for end user devices, effectively removing user privileges in these areas. Areas such as enforcing robust password standards, mandating password protected screensavers, disabling guest accounts, disabling the Windows Installer and ensuring that event monitoring and logging are enabled are all features that fall into this category.
4. *Limiting Cloud Access.* The term 'cloud' is simply a metaphor for the Internet. This is critical because if left unchecked, organizational policies can be circumvented and data exposed in the cloud. Third Wall version 1 already includes capabilities to limit what users can do in the Cloud with additional features coming in future upgrades. In version 1, Third Wall can restrict Microsoft Accounts and block access to the Microsoft Store, both of which can present security issues if left unblocked because it gives users the ability circumvent policy and install unapproved software. If a user doesn't need access to their personal Microsoft account as part of their job, then the service should be turned off.
5. *Limiting Privileges to External Media.* Policies can be circumvented and data exposed if users have the ability to write to external attachments and devices such as a USB drive. Third Wall version 1 provides the option to restrict the ability to write to a USB and to disable the auto-run feature.

More Third Wall Features Coming. As of this writing, Third Wall is a new product with an impressive set of initial features to help with the critical task of securing endpoint devices. Over the coming months, future versions will add functionality giving administrators more tools to enhance cybersecurity in their business. We plan to update this white paper to keep up with the new features in Third Wall.

Risk Management and Regulatory Compliance

Risk Management. Hardening and securing endpoint devices is a must in today's environment. Doing so demonstrates organizational due diligence considering that the endpoint is often the point of attack today. A risk management program will assess all the threats facing an organization and take actions to reduce the likelihood of an incident. When an incident occurs, organizations should have the tools needed to mitigate damages caused by such an event. A product like Third Wall reduces the number of attack vectors into an organizations' endpoints. Third Wall makes a significant reduction in an organization's overall cyber risk by implementing least privilege by hardening endpoint devices.

Compliance. Several laws and industry standards require the implementation of cybersecurity programs in their organizations. While Third Wall is not designed to accommodate specific laws and standards, it does significantly help organizations with holistic compliance to various security standards. I will briefly review how Third Wall helps achieve compliance of four common standards and laws:

- The Health Insurance Portability and Accountability Act (HIPAA) requires healthcare organizations to implement access controls and maintain confidentiality of electronic health records. Third Wall features like restricting administrative privileges, requiring screen savers and alerting on unencrypted disks all help with compliance.
- The Payment Card Industry Data Security Standard (PCI-DSS) has a robust section on access control as it relates to customer cardholder data. The standard requires restricting access rights to privileged users based on giving the least privileges necessary to perform a job, an area that Third Wall can help with.
- ISO 27001. This international standard is growing in popularity and requires organizations to implement an information security management systems as a systematic approach to managing sensitive information and risk. It does so by requiring technical controls addressing user access management, system and application access control, encryption, and operations security such as logging, monitoring and software installation. Again, features in Third Wall can help here.
- The Gramm-Leach-Bliley Act (GLBA) requires companies that offer consumer financial products or services like loans, investment advice, or insurance, to explain their information-sharing practices to their customers and to safeguard sensitive data. The Act requires that services and applications should be the minimum necessary to accomplish the required business functions, essentially it's recommending the least privilege approach. For example, passwords shall be changed from the vendor defaults and

endpoints should be "hardened" to a recognized standard. Again, a tool like Third Wall significantly helps.

Conclusion

The criticality of securing the endpoint device cannot be overstated. The endpoint device is where users interact with computers and it has become the target of choice for many attackers, both internal and external to an organization. Third Wall is a product that can help organizations secure their endpoints through central management as part of their existing LabTech environment. Moreover, Third Wall can help substantially to manage risk and comply with the standards and regulations that impact their industry.

About the Author. Dr Kenneth J. Knapp is the owner and manager of Cyber Secure Advising LLC, an information security consulting firm. He is also an Associate Professor and Director of Cybersecurity Academic Programs at the University of Tampa, Florida. Dr Knapp is a Certified Information System Security Professional (CISSP) and a Certified Ethical Hacker (CEH).

References

Indiana University. (2016, May 3). *What is the principle of least privilege?* Retrieved from https://kb.iu.edu/d/amsv

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

Ponemon. (2015, January). *2015 State of the Endpoint Report: User-Centric Risk*. Retrieved from Ponemon Institute: http://www.lumension.com/Lumension/media/graphics/Resources/2015-state-of-the-endpoint/2015-State-of-the-Endpoint-Whitepaper-Lumension.pdf

Privacy Rights Clearinghouse. (2016). Retrieved April 26, 2016, from www.privacyrights.org/data-breach/

Protalinski, E. (2010, March 31). 90 Percent of Windows 7 Flaws Fixed by Removing Admin Rights. *Ars Technica*. Retrieved from http://arstechnica.com/information-technology/2010/03/half-of-windows-flaws-mitigated-by-removing-admin-rights/

Saiyed, C. (2016, April). Cryptolocker. *ISSA Journal, 14*(4), 14-18.

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

Verizon. (2015). *2015 Data Breach Investigations Report.* Retrieved from verizonenterprise.com