Network Policies within an Enterprise Level

Jerrette McCrimmon

East Carolina University

Abstract

The computer has assisted with variations of job functions and the ability to connect devices to networks for the intent and purpose of communicating with other users. The transformation of information over networks has created a world of virtual and a social connection between users. In the workplace networks rely on levels of security that allow the ability of sensitive and public information to be distributed without any type of compromise. Enterprise networks are the focus of multiple levels of information and cybersecurity, mainly for its user credentials, devices, and network infrastructure. Some enterprise networks have group policies in place that provide network administrators the simplicity of combining network patches and updates to be pushed out over the network. Group policies allow the capability to block certain devices from accessing sites or the ability to use computers that have not cleared the network's authentication certificates for use on the network. The implementation of network policies involve the creation of certain users within a group category, that restricts or allows access to certain instances of the network such as administrators, power users, and users. The focus of this paper is to show how enterprise network policies are implement and how there compliance regulates for use. Assigning user access privileges would govern the accessibility to certain actions that will grant access based on their user group. Group policies tend to be a security access that controls the user's ability to navigate or restrict the role within the enterprise network.

Network Policies within an Enterprise Level

The enterprise level of computer networks have given systems and devices a new way of providing end users with performing job duties onsite and remotely. When implementing an enterprise group policy the structure of the network must be planned accordingly with thoughts of information protection from compromise, usage restrictions, security, administration of rights and cost in mind. “Through the selection and application of appropriate safeguards, security helps the organization to meet its business objectives or mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets.” (Peltier, 2016). New advances in network technology have introduced Intrusion Detection Systems (IDS) as a new source of security, which prevents unauthorized users, hackers, and other possible system attacks that could be a result of a possible breach from disrupting an enterprise network infrastructure. “An Intrusion Detection System is an application which ensures monitoring the network and protecting it from the intruder.” (Fayaz, 2017). Security is the first line of defense for protecting a network environment its users and devices that are connected internally, remotely, or VPN at the enterprise level. “The use of enterprise policies provides one mechanism for an administrator of a network to secure an enterprise network, while enabling remote access and connectivity.” (King, 2016). Thus network security policies must have updated and continuous monitoring software if it is to maintain a defense in preventing data and unauthorized access to user information. “Providing effective information protection requires a comprehensive approach that considers a variety of areas both within and outside the information technology area.” (Peltier, 2016).

Network policies require detailed and strict approach for accessibility and user rights to be considered an effective start to data security. “A policy is a set of usage rules, a set of commands, a set of parameters, or a set of criteria that is used to precisely define how the ND operates.” (Chan, Leung, Chan, H. M., & Sung, 2019). The group policies within enterprise networks need to have a message with the Service Level Agreement (SLA), appearing on the screen prior to the user log in screen, prompting users what the purpose and guidelines of the network usage is intended for. With an acceptance screen prior to signing in the network whether read or not the user has been informed of the policies enforced by the network administrator and the expectations of end user activity is required. To help keep user access restricted some enterprise networks may provide an intranet as a way for network access of company and user databases. In some environments Internet Explorer is used as the default browser for logging in and accessing the worldwide web, while other browsers are restricted from allowing access to enterprise databases. “Today, web browsers are a major avenue for cyber-compromise and data breaches. Web browser hardening, through high-granularity and least privilege tailored configurations, can help prevent or mitigate many of these attack avenues.” (Jillepalli, Leon, Steiner, Sheldon & Haney, 2017).

There are various policy requirements that can make the enterprise network a safeguard against intrusion defense, including virtual machines, wired to wireless, and domain assigned devices. " There are many types of policy settings, including but not limited to, access policy settings, security policy settings, accounting policy settings, services policy settings, routing policy settings, wireless channel management policy settings, network traffic policy settings, Internet Protocol (IP) packet management policy settings, network address translation (NAT) policy settings, quality of service (QoS) policy settings, virtual private network (VPN) policy settings, etc." (Chan, Leung, et el, 2019). Policies help set the boundaries for user management within the network structure and allow for customization of authority distribution, user rights, and compliance of network management. "Network management refers to the strategies, activities and managerial skills implemented by the network manager(s) to steer actors' interactions, to solve problems, to build consensus among participants and to coordinate inter-organizational activities in order to achieve network's goals." (Molin, Masella, 2016). Security policies help provide a guarded measure with the activity of information exchange within the network. "In order to have a truly enterprise-wide unified security policy, there must be the sharing of the stateful endpoint connectivity context with other permitted network functions, which may leverage this invaluable information for policy enforcement, network visibility, and also troubleshooting." (Yakasai, Zheng & Guy, 2017).

An enterprise network level of security is only good as the personnel responsible for implementing, the administration, governing and monitoring of the overall structure. Hackers have targeted enterprise networks within the past five years using brute force attacks such as ransomware, viruses, and phishing as intrusion methods. Malware intrusions are carried out to gain unauthorized access to personal files, to destroy sensitive files, and to steal information." (Singh, Kumar, Singla & Ketti, 2017). With various intrusion attacks publicly announced as precaution measures against social engineering attacks, email has become a common choice as a form of attack. With email the attacker can disguise emails to look as if it came from a known contact, which in turn is using familiar wording or names as if it were harmless to open without being dangerous. Enterprise environments have been victims of the largest DoS attacks in recent years because the user database may have a weak link to allow for easier access to distribute destruction. "A DoS attack is an attempt to make the affected services unavailable to the authorized users. In such an attack, the server providing the service is flooded with a large number of applications and therefore the service becomes unavailable for the authorized user." (Achbarou, kiram, & Bouanani, 2017). With social engineering attacks rising and network security becoming a need in information technology, the chances of successfully enforcing an attack is greater because users may not be aware of a harmful phishing attack in emails.

In today's enterprise networks users have the capability to work remotely or onsite, which requires wireless connectivity to the network's domain. The wireless portion have monitoring of controllers that produce the signal to access points to expand the ability for a device to connect wirelessly within a certain range. "Enterprise security needs to be seamlessly embedded and integrated everywhere across the extended network, thereby protecting attack targets, as well as the diverse endpoints that must connect to the network." (Yakasai, Zheng & Guy, 2017). The need for wireless networks have allowed the implementation of cloud-based networks. A cloud-based network can give ease of access to software through deployments, mapped drives, and shared folders to users who are given access permissions. Users need to keep in mind that cloud-based platforms can also have its share of security flaws and can have unauthorized breaches

within or outside the network. “Despite the enormous technical and business benefits of cloud computing, concern for security and privacy has been one of the main obstacles that impede its widespread.” (Achbarou, kiram, & Bouanani, 2017). “If a system has external users, its owners have a responsibility to share appropriate knowledge about the existence and general extent of control measures so that other users can be confident that the system is adequately secure.” (Peltier, 2016). One of the most popular cloud-based networks is Google because of its browser’s online accessibility of apps such as Drive, which is a storage database free to its users who have a registered Google account.

Enterprise group policy requirements are usually strict on password selections and mandatory characters, numbers and symbols that the user must choose before password creation is accepted as secure. Password implementation policies usually have the users change the password every 90 days as a precaution to network policy guidelines as a way of providing a more secure user experience. “Enterprise risk management (ERM) began to take root in the late 1990s and has since become generally recognized as an expectation of good management and corporate governance.” (Fraser, 2016). With enterprise group policy there are ease of migration for administrators, who may need to remotely administer software across platforms without the need to be present within the physical environment needing the installation of the software. Implementing a good structure of network policies involving documenting the types of structure, guidelines, hierarchy of staff at an administrative level, container for access controls and user groups detailing their permission within the network. “When creating an information protection policy, it is best to understand that information is an asset of the enterprise and is the property of the organization.” (Peltier, 2016). The information protection policy provides the security standards that are geared towards protecting user confidentiality and data while on the protected network.

To conclude the research provided is about enterprise level security network policies and how they affect users and the infrastructure. Users must have a sense of knowledge about password creativity and policies pertaining to the implementation and level of rights administered to them through group policy access. Network security has been a lifeline to computers and mobile devices over the past 20 years since the implementation of the worldwide web became a popular avenue for digital communication such as social media and email. Enterprise networks have set the standard for security policies and network infrastructure because of its continuous availability for users to interact for the purpose of business transactions, cloud-computing, file sharing and email communications whether it be corporate or educational. The need for group policy standards allow for secure protection of user data, confidentiality protection of information and secure sign in access.

Works Cited

Achbarou, O., kiram, M. A. E., & Bouanani, S. E. (2017). Securing cloud computing from different attacks using intrusion detection systems. International Journal of Interactive Multimedia and Artificial Intelligence, 4(3), 61. doi:10.9781/ijimai.2017.439

Chan, A. W. H., Leung, W. C., Chan, H. M., & Sung, P. H. W. (2019). *U.S. Patent Application No. 10/204,073*.

Fayaz, H. (2017). Cloud security enhancement through intrusion detection system. International Journal of Advanced Research in Computer Science, 8(2)

Fraser, J. R., & Simkins, B. J. (2016). The challenges of and solutions for implementing enterprise risk management. *Business horizons, 59*(6), 689-698.

Grindle, M. S. (2017). *Politics and policy implementation in the Third World* (Vol. 4880). Princeton University Press.

Jillepalli, A. A., de Leon, D. C., Steiner, S., Sheldon, F. T., & Haney, M. A. (2017, November). Hardening the client-side: A guide to enterprise-level hardening of web browsers. In *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)* (pp. 687-692). IEEE.

Molin, M. D., & Masella, C. (2016). Networks in policy, management and governance: A comparative literature review to stimulate future research avenues. Journal of Management & Governance, 20(4), 823-849. doi:10.1007/s10997-015-9329-x

King, G. (2016). *U.S. Patent No. 9,356,933*. Washington, DC: U.S. Patent and Trademark Office.

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. Auerbach Publications.

Singh, R., Kumar, H., Singla, R. K., & Ketti, R. R. (2017). Internet attacks and intrusion detection system. *Online Information Review, 41*(2), 171-184. doi:http://dx.doi.org.jproxy.lib.ecu.edu/10.1108/OIR-12-2015-0394

Yakasai, S. T., Zheng, F., & Guy, C. G. (2017). Towards policy unification for enterprise network security. Paper presented at the 1-5. doi:10.1109/NETSOFT.2017.8004205