Managing Access in an Enterprise Environment

Marc Colonna

December 12, 2018

ICTN 6810: Communication Technology

Abstract

Access control starts with the front door to the organization, continues with appropriate security in and outside of the data center, and finishes with good user education. Strong and competent companies will employ the appropriate security standards deemed necessary for their organization. "If your data could be of any value to someone without proper authorization to access it, then your organization needs strong access control" (Martin, 2018). Physical security such as security cameras and security doors are only as functional as the habits of those who are using them. Control over network access and network resources must be suitable for the data it is protecting. Policies are required to keep these systems in balance and always improving as technology changes.

In this study, we will discuss a mock company, and examine the proper methods that should be taken in their data security, specifically their network access and access control policies. The company in question, Allin Consulting, represents an organization with needs to address client personal identifiable information, human resources items, payroll, and company data. For this study, Allin Consulting employs an estimated 2,500 employees and brings in an annual estimated revenue of $50 million.

Introduction

Allin Consulting has hired a third party security and risk management company to assess the company's potential for threats. Normal company operations were assessed over a period of three months, ranging from access to different areas of the company building, monitoring for potential social engineering threats, and network access. Allin Consulting put into place the recommendations they were given, and discuss how these measures protect against potential attacks.

Managing Access in an Enterprise Environment

Defining Social Engineering

A man is walking towards a company building, and is holding two vases of flowers. In a good gesture, an employee of the company holds the door open for the vendor walking behind them, as they likely would have had trouble with the door. The man holding the vases thanks them for their polite act. They both enter the building and part ways. General human decency can sometimes be the worst enemy of physical site security, as now the man in question has access to the main floor of the building. There are wireless access points available, digital company directories in the lobby, and areas to leave a malicious flash drive in plain sight, in hopes a passing employee of the company will be curious of its contents and plug it into a PC on the network (Perkins, 2018).

Krombholz, Hobel, Huber and Weippl (2015) define social engineering as '"the art of getting users to compromise information systems. Instead of technical attacks on systems, social engineers target humans with access to information, manipulating them into divulging confidential information or even into carrying out their planned attack' (p. 114)."

Many different factors encompass what is defined as social engineering, as the attempts can be physical or digital. This paper will focus on the physical aspects of social engineering when applied to network security. Physical social engineering attacks include ways an unauthorized person can obtain access to locked areas. Research conducted by Tetri & Vourinen in 2013 found that,

> The techniques of impersonation seek to build a particular role through which it is easier to get inside the system. For instance, name-dropping and using jargon imply that the

> intruder is an insider who knows people; in piggybacking the impression of belonging to the group is created; and wearing a fake ID badge or a stolen uniform involve obvious indicators of position (p. 17)

An attacker following authorized users through locked doors into areas they do not have access is known as 'piggybacking'. Stealing access cards off of desks or from a wallet would also allow an attacker access to an unauthorized location, unless that location contained a two-factor authentication access. Dumpster diving can grant an attacker access to company documents. "'A dumpster can be a valuable source of information for attackers, who may find personal data about employees, manuals, memos and even print-outs of sensitive information, such as user credentials' (Krombholz et al, 2015)." Limited access to a company office may even allow an attacker to view post-it notes with credentials, or gain access to a network device that may have been left logged in by a user who left their desk.

Controlling Physical Access

Allin Consulting considered physical vulnerabilities when deciding on the appropriate countermeasures for their environment and desired security. Biometrics were implemented in the form of fingerprint scanners, and keycard access employee badges. These two items together have allowed a two-factor authentication system for building access. Security cameras and digital locks were also implemented and paired with the access doors.

Allin Consulting's location consists of three main entry points to the outside. One entry point is a maintenance corridor. This entrance point has been updated with a locking mechanism, requiring a keycard access along with a fingerprint scan. Also installed in this

entryway was a security camera with viewpoints on the door and the walkway. A second entry point, a visitor's door, has implemented a digital locking door with access granted by a monitored reception desk. The door also includes a security camera with viewpoints on the visitor and the walkway up to the door. Communication to the visitors is now possible with an intercom. This visitor's entrance also includes access to an entry point to the main building, which now requires a keycard and fingerprint scanner to unlock. Although a mantrap in this location would provide better coverage, the outer and inner doors having separate locking security schemes will suffice in an attempt at a more welcoming visitor area.

The main employee access door has been equipped with a keycard access to a mantrap, and keycard/fingerprint scanner on the second door of the mantrap. Security cameras in this area have visuals on the walkways up to the entrance, as well as each door and the lobby. There are two of these entryways in this area to facilitate traffic.

Various doors around the building have been modified to include locking mechanisms with keycard access only. Not all keycards will work in all doors, as access will be granted based on access groups in active directory. The only additional two-factor authenticated area is the data center where the network equipment is located.

Network Access Control

Allin Consulting has implemented a 'defense in depth' framework regarding network access control. Defense in depth can be defined as the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise. The strategy is based on the military principle that it is more difficult for an enemy to defeat a complex and

multi-layered defense system than to penetrate a single barrier (Rouse 2007). To be allowed network access, users must connect either wirelessly through a wireless access point or physically through an Ethernet interface (remote access is also available via VPN). Once connected, the devices will use MAC address filtering to determine the proper access level. The MAC address filtering uses a defined list, which will be generated to only allow company-deployed devices and those personal devices that had been previously registered and approved to be allowed access. Wireless devices will use a MAC address table within the Wireless LAN controller, physically connected devices will use a table within the firewall.

An additional layer of security beyond MAC address filtering will apply in Access Control Lists on the network switches. Once connected to the network, the user will be assigned to one of two IP address groups; devices which are registered within the enterprise, and those that are public/guest devices. All internal switches beyond the firewall will be configured with Access Control Lists. Access Control Lists are a list of IP addresses within a switch that are allowed to transmit packets through the switch or router interfaces. Users granted a guest IP address will be limited to only internet access to approved content only. Packets sent from these IP addresses to try to reach internal network resources will be dropped once they do not meet the criteria of the access control lists on the switches. In their research discussing network access control lists, Liu, Torng & Meiners state:

> Each rule in an ACL has a predicate over some packet header fields and a decision to be performed upon the packets that match the predicate. A rule that examines d -dimensional fields can be viewed as a d -dimensional object. Real-life ACLs are typically four dimensional (over four packet fields: source IP address, destination IP address, destination port number, and protocol type) or five dimensional (over five packet fields:

> source IP address, destination IP address, source port number, destination port number, and protocol type). (2017, p. 1969)

Using this method, administrators at Allin Consulting will also be able to review logs regarding access to network resources as the packets filter under each rule in the access control list. This information will assist in reviewing and strengthening rules as the environment changes.

Packets that are approved for network resources will be passed along the channels internally. Packets meant for outbound traffic will be forwarded or dropped based on the firewall content filters in place to protect the network. Users will also use their credentials in the firewall to determine access on an individual/group level. Guests will be given a guest password and only the minimal approved access for outbound traffic. Employee credentials are imported from active directory. A third layer of network security will be added via access control permissions on the network resource systems and files.

Access Control on Company Resources

Defining a set of rules or policies on how company documents and information is accessed, and defining what employees are granted that access, can be a large undertaking. Careful consideration must be made to accommodate both adequate security of the data and user access. When trying to balance these items, enterprises will typically turn to predetermined control scheme structures to fit the needs of their environment.

Two major access control schemes commonly implemented in the enterprise world are ABAC, “Attribute Based Access Control”, and RBAC, “Role Based Access Control”. Samuel Carter (2017) explains role based access control as a system where the access is based on the

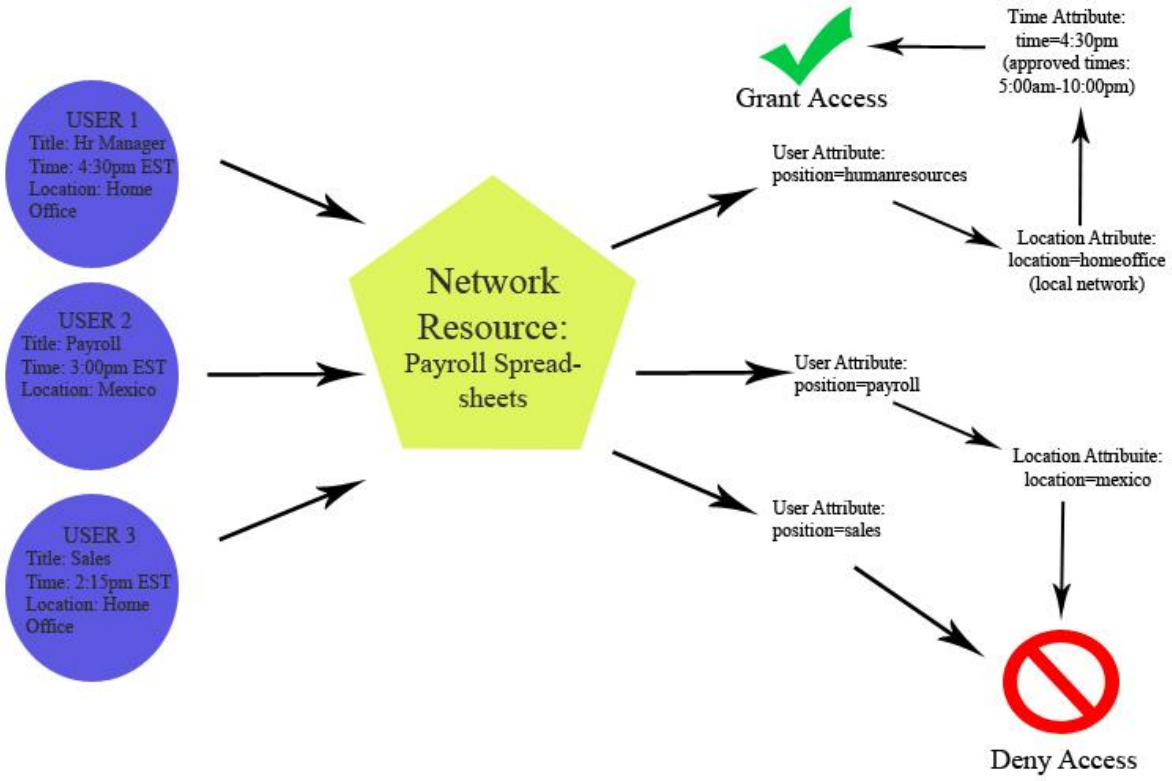
roles the users have within the network. The rules state which roles are allowed access to certain files and folders, and what levels of access those roles are granted (2017). In Windows environments, for example, role based access control lists use user groups in active directory to determine file and folder access. Sometimes, this process can become complicated and demanding in larger environments. While discussing the process of RBAC, Pan, Sun, He & Zu state the following in their 2017 work:

> With the increasing number of users, resources and permissions, more and more organizations have deployed RBAC since it makes the security administration more manageable and flexible. However, an RBAC system needs to be updated continuously as the result of dynamic changing in users, permissions, and assignments. (p. 40389)

For Allin Consulting, attribute based access control was determined to be more practical. Attribute based access control is based on three different attribute types: user attributes, attributes associated with the application or system to be accessed, and current environmental conditions (Carter, 2017). Attribute based access control can be more granular and fine-tuned. Users can be granted access not only via their role attributes in the organization, but also by other parameters such as location, IP address, time of day, and content of the files themselves. ABAC decisions are based on the use of subject and object attributes and enables very flexible access control capabilities. ABAC also introduces the concepts of obligations and access based on environment conditions (Lee, Vanickis, Rogelio & Jacob, 2017).

The network security team at Allin Consulting decided to implement a three layered attribute based access system as the initial access control. The first of the three attributes for granting access would be categorized by position, an employee's role in the company (these will be separated into groups). Second, the location (determined by IP address) will be considered.

Location will also allow for the network administrators to enforce VPN security when connecting to the network off-site. Third, time of day will be implemented to avoid any activity that may be prominent in time zones well known for malicious activity. The team decided on these factors because they can be manipulated on the fly, and additional attributes can be added (such as MAC filtering).



In the above example, three company employees are trying to connect to a file server to open a payroll spreadsheet document. The document has been protected in that only employees with the Human Resources or Payroll roles will be granted access, and only within the local network.

The files have also been given the added attribute of time access, only allowing access from 5:00am to 10:00pm Eastern Standard Time. User 3 is denied access once the user fails the position attribute, as this user is in the sales department. User 2 passes the position attribute, as this employee works in payroll, however fails when the location attribute is applied. The location notes the user's IP address is in Mexico, and this could be an insecure connection or a malicious attempt to collect the information from the payroll document with compromised user credentials. User 2 would have been given access had the employee connected to the local network via VPN. User 1 is granted access to the payroll spreadsheet, as this user matches the position attribute for Human Resources, the location attribute as within the local network, and the time attribute between 5:00am and 10:00pm.

> Attackers are very likely to experience difficulties in their bid to compromise a system grounded together with its users, to a particular location. Knowing, for instance, that an employee is expected to be in the office within specific time duration, access packets from a remote location, using stolen authentication details of the employee, would not be permitted. In the same vein, an attacker who removes an employee's system to another location would not be able to access any service on the application of network of the enterprise, since the system would have been configured to access only from its original position (Yisa, Meshach, Osho, & Sule 2018)

Conclusion

Considering the access control needed to safely secure the employee and client data, as well as company data, Allin Consulting's decision to apply the defense in depth strategy can be easily understood. Physically, the organization's environment can be protected starting with the front door. User education can also be continued in the best interest of data security, as users and employees tend to be the weakest link in the security chain, as well as the most targeted. Guests using the network will have appropriate access and rights to keep their traffic safe for the environment. Employees will have access not only to the company network, but to the resources that are appropriate for their job roles. In addition to all of these strategies, Allin Consulting can also apply the appropriate anti-virus software, whether host or network based. This can include threat detection software or appliances that will update signatures and control malicious activity on the network. Network security encompasses a vast variety of subjects, and access control needs to be addressed properly to allow all the security policies to function as designed, and protect the enterprise, its data, and its employees.

After implementation of the recommendations given to Allin Consulting, social engineering observations were made and compared to pre-mitigation data. Employees are consistently traveling through doorways one at a time, which allows for more comprehensive access monitoring. Employees trying to access locations that are not allowed under the keycard access control have been negated. It is recommended that data continue to be compiled regarding the new safeguards, as new vulnerabilities might present themselves now that the environment is changed.

References

Carter, S. (2017, January 19). RBAC vs ABAC Access Control Models. Retrieved November 01, 2018, from https://blog.identityautomation.com/rbac-vs-abac-access-control-models-iam-explained

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and Applications, 22, 113-122. doi:10.1016/j.jisa.2014.09.005

Lee, B., Vanickis, R., Rogelio, F., & Jacob, P. (2017). Situational awareness based risk-adapatable access control in enterprise networks. doi:10.5220/0006363404000405

Liu, A. X., Torng, E., & Meiners, C. R. (2011). Compressing Network Access Control Lists. IEEE Transactions on Parallel and Distributed Systems, 22(12), 1969-1977. doi:10.1109/tpds.2011.114

Martin, J. A. (2018, February 05). What is access control? 5 enforcement challenges security professionals need to know. Retrieved November 1, 2018, from https://www.csoonline.com/article/3251714/authentication/what-is-access-control-5-enforcement-challenges-security-professionals-need-to-know.html

Pan, N., Sun, L., He, L., & Zhu, Z. (2018). An approach for hierarchical RBAC reconfiguration with minimal perturbation. IEEE Access, 6, 40389-40399. doi:10.1109/ACCESS.2017.2782838

Perkins, M. (2018, July). PREVENTATIVE SECURITY: START WITH THE FRONT DOOR. Door Security + Safety, 82(7), 22+. Retrieved from http://link.galegroup.com.jproxy.lib.ecu.edu/apps/doc/A546286538/PPSB?u=ncliveecu&sid=PPSB&xid=1959a69b

Rouse, M. (2007, June). What is defense in depth? Retrieved October 29, 2018, from https://searchsecurity.techtarget.com/definition/defense-in-depth

Tetri, P. , Vuorinen, J. (2013) Dissecting social engineering, Behaviour & Information Technology, 32:10, 1014-1023, DOI: 10.1080/0144929X.2013.763860

Yisa, V. L., Meshach, B., Osho, O., & Sule, A. (2018). Application of geo-location-based access control in an enterprise environment. International Journal of Computer Network and Information Security, 10(1), 36. doi:10.5815/ijcnis.2018.01.05