Winter 2-15-2019

Privileged Access Management

Anea Cobia
La Salle University, cobiaa1@student.lasalle.edu

Privileged Access Management

Anea D. Cobia

La Salle University

Table of Contents

Abstract

Security breaches are becoming a common occurrence in society today. When breaches occur, people are often left wondering how they will be affected and what steps can be taken to protect them. The passing of stricter standards and regulations has not slowed would be hackers from crafting ways to breach networks. While there are many ways that a breach can occur, the focus of this paper will be to look at the usage of credentials and privileged accounts. Specifically, the idea of privilege access management and methods for protecting credentials will be examined.

Credential Loss

Credentials provide a mechanism to prove authority, entitlement, rights, and status. A driver's license is an excellent example of a credential as it shows that we are entitled to drive, but also has pertinent information that identifies only ourselves. This identifiable information on a driver's license would be items such as name, date of birth, height, and other items that pertain to a person's being.

From a cyber-security perspective credentials consist of user accounts. A user account is data that is associated with a user for access to a multiuser computer system (Butterfield and Ngondi, 2016) and would consist of a user name and password. The user account ties attributes to the specific user such as access levels for the system and permissions. Above regular user accounts there are administrator accounts which provision user accounts and set permission levels (Butterfield and Ngondi, 2016). An administrator account has more permissions than a normal user account and, in some cases, can be equated to a super user, one that has elevated permissions and more access to critical systems.

Credential loss occurs when user account information is lost or stolen. In many cases credentials are stolen from unsuspecting employees who fall victim to attacks such as phishing. Phishing is a social engineering attack that usually takes place by email. A user is tricked into believing that they are opening a link, document, or other file from a legitimate source that ends up installing malicious software or redirecting the user to fraudulent websites that can steal information (Encyclopedia of Social Deviance, 2014). Credentials could also be lost if stored

improperly, such as on an unencrypted device. Understanding how data travels across a network can also play a role in credential loss. If data is being transferred online in an insecure manner, without using encryption, then credentials can be lifted. For instance, if a person is logging into a website that is not using Hypertext Transfer over Secure Socket Layer (https) then credentials would be sent in plaintext. A hacker using a tool such as Wireshark, which captures network traffic, can capture the login details that were sent in plaintext.

The Results of Credential Loss

The effects of credential loss are widespread. An attack at its very infancy may begin using stolen credentials but can then span into higher level maliciousness. The 2013 Target breach provides an excellent example of this concept. An outside vendor, Fazio Mechanical Services, provided the gateway for access into Target's network. In 2006, Fazio Mechanical Services began working with Target installing and maintaining their store refrigeration systems. Target granted remote access to its systems to Fazio Mechanical Services for billing, contract and project management (Ziobro, 2014). By granting access to their system Target put itself at risk. Fazio Mechanical Services became the victim of a phishing attack which occurred at least two months prior to the Target breach, the attack compromised its credentials. Fazio Mechanical Service was using a free version anti-malware program (Bjorhus, 2014). By allowing access to their systems, Target opened itself up to the risks that Fazio Mechanical Services would not adequately protect its credentials.

The breach that took place at Fazio Mechanical Services, did not necessarily mean that Target should have been at risk. In fact, Target had implemented safeguards on their network that should have offered a decent level of protection. Prior to the breach Target had passed a compliance audit for Payment Card Industry Data Security Standards (PCI-DSS) (Maurer and

Plachkinova, 2018). The Payment Card Industry Data Security Standard was designed by the credit card companies, initially Visa and Mastercard, but expanding to others such as Discover and American Express. The PCI-DSS standard addresses the storage, transmission, and accessing of data as it pertains to credit card processing (Wright, 2011). Therefore, by passing their compliance audit, Target proved they had appropriate security controls in place for processing consumer transactions. In addition to showing PCI-DSS compliance, Target had also completed a $1.6 million implementation of a FireEye malware detection tool (Maurer and Plachkinova, 2018). The detection tool coupled with 24/7 security monitoring of their network should have provided adequate protection to the Target network.

Although Target had sufficient tools and safeguards in place, attackers were still able to steal information from over 110 million Target customers (Bjorhus, 2014). Using the stolen vendor credentials from Fazio Mechanical Services, hackers were able to gain access to Target's network. In the months prior to the breach, Target's cybersecurity staff recommended that its' payment systems be reviewed for malware vulnerabilities (Todd, 2014). However, this was not done as Target was upgrading its payment terminals at the time and the company was preparing for the upcoming holiday season. Another factor that contributed to the breach was unfollowed up security warnings. It was found that the FireEye security system alerted Target's security team to a possible breach, but these alerts were not acted upon. Instead, Target's spokesperson Molly Snyder stated, "the activity was evaluated and acted upon. Based on their interpretation and evaluation of that activity, the team determined that it did not warrant immediate follow up (Shaer, 2014, Pg.14)." The lack of follow up by Target's own security team allowed for the breach to take place in full force.

In 2017, a security breach at top accounting and consulting firm Deloitte occurred. What is notable about the Deloitte security breach, more so than others, is that part of Deloitte's business is cyber security. Gartner, a leading global research and advisory company, ranked Deloitte number 1 globally for security consulting in 2013 (Entertainment Close-Up, 2013). In their review of Deloitte's cyber security business, it was mentioned that Deloitte's services go above and beyond those of other providers (Entertainment Close-Up, 2013). Deloitte provides advice, auditing, and analysis looking at companies' current security posture and devising strategies to improve and create efficiencies.

Despite its preparations and experience, in March 2017 Deloitte experienced a security breach that compromised many of its systems. What is notable about this attack is that it started with one password from an administrative account for Deloitte's email system. Given that the compromised account was administrative, it had more access than a normal user account. Therefore, once the hackers gained access to the email system they were able to traverse it to get data of more significance. The hackers were able to obtain other account credentials, IP addresses, and more important security information (Chatham, 2017). Although the breach was discovered in March, it is believed that hackers began accessing Deloitte systems around October or November 2016 (Chatham, 2017). Attackers were successful at Deloitte as they only needed the compromised credentials of one account and because multifactor authentication was not enabled.

The ultimate result of credential loss is a breach of data, which means that an unauthorized entity has now seen data that was not intended for them. In the Deloitte breach the hackers gained access to emails, attachments, security information and more. The Target breach exposed information of over 110 million customers split between 70 million with personal

information stolen and 40 million whose accounts were hacked (Malcolm, 2014). Personal data could mean a mix of data such as addresses, email addresses, and phone numbers. This data may not be as detrimental as the financial data that was stolen such as credit card numbers, pins, and expiration dates. In theory, a hacker would need a combination of data to successfully make use of what was stolen. For instance, it is not enough to have just a credit card number without extra data. However, if a hacker has a name, credit card number, expiration date and security code they would be able to make fraudulent purchases. One of the sad truths about data loss is that there is no way to know if or when the data will ever be used. In 2014, the U.S. Office of Personnel Management (OPM) experienced a hack in which 22 million users' data was stolen. It is just now in 2018 that use of that data is beginning to be seen with the first reported case of financial fraud now pending in federal court in Maryland. Kariva Cross and Marlon McKnight both pleaded guilty to bank fraud and identity theft. Both were involved in taking out fake loans through a credit union using stolen information from the OPM breach (Weiner and Hawkins, 2018).

Data breaches also have financial cost tied to them that may cost companies millions of dollars. Target agreed to put aside $19 million to settle claims from credit card companies such as Mastercard, CapitalOne, and Citigroup (Beilfuss, 2015). The costs not only cover fraudulent transactions, but also the cost associated with reissuing new cards to customers. In May 2017, it was reported that Target's total cost for the breach was nearing $300 million. The total includes $10 million paid to customers from a class action lawsuit, $67 million paid to Visa, $39.4 million paid to banks and credit unions, and more (Huston, 2017). In another report done by KrebsonSecurity, it was estimated that the cost to credit unions was $200 million as they had to reissue over 21 million credit cards. Not only is there a financial hit taken when settlements are

paid, but a company also takes a financial hit in terms of profit. Directly after the announcement of the breach, Target reported several downward trends such as a 46% decline in net income and a 5.3% decline in revenue for the fourth quarter (Curran, 2014). In addition to the losses, Target also incurred multiple expenses tied to implementing security improvements. There was a $100 million cost to update technology across stores such as terminals that can read chip enabled debit and credit cards (Harris, 2014).

Another instrument that ties in with financial payments is cyber insurance. In many cases companies that must make big payouts are not as financially impacted due to insurance policies that they have purchased. The cyber insurance business is booming with a worth of $2.5 billion reported in 2016 (Campbell-Miller, 2017). It is predicted by Price Waterhouse Coopers, that premiums will jump from $2.5 billion to $7.5 billion by the end of 2020 (Campbell-Miller, 2017). With the frequency of breaches being on the rise and an average cost of $7.35 million per breach (Campbell-Miller, 2017), it makes sense that companies would want to protect themselves. In the aftermath of the Target breach companies have become more aware of the risk of breaches and their impact with many insurers tailoring custom solutions for buyers (Veysey, 2014).

It is important to make sure the correct type of insurance is purchased to match the business needs. For instance, in the cases of Target and Deloitte it would make sense to have network security and privacy protection insurance. Both network and privacy coverage protect from financial ramifications such as those from breaches of customer data. They differ in that network coverage deals more with malware related breaches while privacy deals with the intentional or non-intentional disclosure of private customer or company information (Cordell and Thomas, 2017). Cyber insurance is an essential component of a risk management strategy

especially given the rising costs of payouts to consumers and businesses as the result of breaches. It could be argued that having insurance may entice companies to skimp on their security programs. However, insurance itself is a form of transference, in which the security risk is transferred to another entity. In some cases, it may make sense to transfer the risk thereby safeguarding the company from financial damage if the cost of implementing an internal solution is higher.

When breaches occur, consumers are often put on edge which leads to damage of the company's reputation. As previously noted, immediately after the Target breach the company experienced a sales decline. In a survey conducted by the Ponemon Institute in 2011 of 850 executives, it was found that it takes about a year to restore a company's reputation after a breach (Entertainment Close-Up, 2011). A survey conducted by Deloitte also shed light on the weight that security plays when it comes to reputation. More than 300 chief-level leaders were surveyed with 45% listing security as a major risk to their company's reputation, only beaten by ethics and integrity (Ristuccia, 2015). Out of the participants, 20% had stated that they experienced a security related incident within the last three years that lead to reputation damage. The loss of reputation can be linked directly with a loss in revenue for companies. When breaches occur, consumers can become fearful and worried especially when there is a loss of their personal data. Consumers can hesitate to shop at stores if a breach took place, afraid that their data will not be protected and put at risk. In some cases, a company will release information to the public in a strategic manner that outlines security improvements and changes that the company is making to improve their security program. Having transparency after a breach helps to rebuild consumer confidence more quickly.

In the aftermath of security breaches, it is not uncommon to see companies do internal restructuring of personnel. Target's CEO Gregg Steinhafel and CIO Beth Jacob both departed after the 2013 breach. Information Technology is generally what we think of when a breach takes places, however Gartner in a survey done in 2014 showed that there is more of a link between CEO's and CIO's. This link is being established due to emerging technologies and the need to spur innovation. However, the flip side of such closeness is that when security issues arise both CEO's and CIO's bear the responsibility (Boulton, 2014). The Deloitte incident will no doubt influence their cyber security business, especially given the fact that the breach was able to take place due to a simple security standard not being followed. The problem was further exacerbated by the fact that the breach was going on for six months prior to being discovered. While no reports have been made yet addressing the hit taken to their business, this is surely not something that will make clients feel comfortable. In the months after the breach, Deloitte reached out to clients that were affected, at the time six in total. The company also made use of internal and external security experts to review their security programs (Marriage, 2017).

Data breaches can have different impacts based on what target information was accessed. The Deloitte breach dealt more with corporations and government entities, stealing the firms entire internal email database and information on all their administrative accounts. It is possible that the hackers by gaining access to Deloitte's emails would be able to see information that customers would not want made public such as intellectual property or strategic plans (Roberts, 2017). In the hands of criminals this data could be used to extort money or create knock off items depending on the industry. Another way criminals could use the data is to make use of the contacts gained from the emails to conduct sophisticated phishing and spear-phishing campaigns.

Affected businesses would have to work to safe guard their data and to make sure their users are informed enough to not fall into the traps of cyber criminals.

While businesses generally have established plans for recourse in case of a breach, on the consumer side things can be much more difficult. Breaches generally compromise the data of millions of customers as evidenced by the 110 million affected by the Target breach. More recently, there was a breach at social media company Facebook which exposed the private information of over 50 million users. This breach was just the latest in a string of cyber related issues for Facebook who last year was found to have given the private information of up to 87 million users to Cambridge Analytics (Frenkel and Isaac, 2018). Another significant breach was that of Equifax which exposed the data of more than 143 million consumers. What made the Equifax breach more significant than most is that the Equifax breach exposed users' social security numbers, which is far worse than just having personal information or credit card numbers stolen (Chicago Tribune, 2017). Unlike other data breaches where more than one piece of information would be needed to effectively conduct criminal activity, a breach that gives social security numbers gives almost instant gratification. With just a social security number a criminal can open a credit card or open other fraudulent accounts in a person's name.

Consumer protection becomes a big element when discussing data breaches. In most cases the normal consumer has no idea if they are one of the millions of consumers affected by a breach. In the case of Equifax, many consumers did not even know that Equifax had their data. Equifax, one of the major credit reporting agencies, would have information from consumers from other transactions not necessarily from dealing directly with them. Each state has their own laws for security breach notifications, so in theory consumers will be notified when their accounts have been compromised. Once a consumer knows that their account has been

compromised they have to consider what recourses they can use. In cases where credit card or sensitive information like a social security number is obtained, a company will offer a year of credit monitoring. Credit monitoring services allow a user to monitor their credit report looking for new account openings and inquiries that may not be authorized. If a consumer wants to be proactive they can subscribe on their own to a credit monitoring service. Another avenue a consumer could use is making use of the new General Data Protection Regulation, allowing for them to request that all their information be purged from a business' systems. Given the amount of data that is shared with and between businesses understanding all the places where personal information resides could be daunting. It would be prudent for consumers to understand how a business collects and uses their data and to know in some regards how their data is being protected.

The Problem with Credentials

There are integral problems with credentials that make them alone the weakest form of security. The weakness itself stems from the human element that is involved with the system of user names and passwords. In most organizations a user name consists in the form of an easily guessable structure such as first initial and last name of a user. Many companies have user directories on their websites with email address, phone numbers, and full names of employees. A cyber-criminal can easily access this information and begin compiling data to use for a potential attack by guessing what these users' credentials might be. The reason for the common user name structure is that it is easier for system administrators to create. When there are hundreds of employees within a company, designing a unique and non-generic username for each could be tedious. In addition to just regular user names, there are also credentials for

devices such as servers, switches, and routers. Most devices come with default credentials which administrators are instructed to change when doing initial configuration.

In 2016 security operations company Rapid7 conducted a test called Project Heisenberg which consisted of collecting data from honeypots that were deployed globally. A honey pot is a computer system that is purposely made to attract intruders. These systems allow companies to monitor and gather data on would-be attackers (Ince, 2013). The project which took place over a 334 day period provided information regarding passwords and logins that hackers attempted to use. The list of logins included usernames such as: administrator, user1, admin, db2admin, and others that are generic (Hodgman, 2016). These generic names show us that hackers are successful in using these generic, out of the box user names, otherwise they would not continue to try and use them. The study also looked at passwords the hackers were inputting. Some of the passwords used were: P@ssw0rd, admin, and x (Hodgman, 2016). When it comes to passwords, users are generally going to pick something that is easy to remember. In some cases, this leads to the reusing of already weak passwords or as evidenced in the Rapid7 study, the usage of simplistic passwords like the letter x.

The problem with passwords that are weak is that they are easier to break by hackers. Dictionary attacks are commonly used by hackers and consist of using known words from a dictionary to try and access a user's account (Barron's Business Dictionaries: Dictionary of Computer and Internet Terms, 2013). In addition to just commonly known words, a dictionary attack can also look at letters that are commonly replaced by numbers in the composition of words such as replacing an E with the number 3 or the letter O with a zero. An obvious solution to the weak password problem would be to require that users only use complex ones. However, the introduction of complex passwords opens a new set of issues. A complex password may be

harder for an individual to remember and can lead to submission errors. Helpdesks are already inundated with password reset requests and the requirement for complex passwords could increase these requests and lower productivity for both IT departments and users (Baldwin, 2012). Another issue with complex and weak passwords is the problem of some users writing down their passwords and worse yet leaving them in generally accessible areas like underneath a keyboard. Companies may also have policies to update passwords on a frequent basis which can provide some level of risk reduction, but this also can lead to a problem where users reuse passwords or use the same password but change a few characters. This becomes a problem as an attacker may have access to older passwords or may use variations of them.

Credentials are one of the most sought-after items for hackers, because if you have credentials you can access items that you otherwise would not. By having a users' credentials, a hacker can take over their accounts, gather sensitive information, and conduct fraudulent activities. Through sophisticated schemes such as phishing, criminals can trick users into providing their credentials to illegitimate sites. It could be an email which has a web link that redirects the user to a fake website that appears to be legitimate. Some phishing schemes do not direct the user to any website but may ask that the user call a phone number or reply with specific information under the pretense that an important account will be closed or some other negative action will be taken. In many cases an email will come with an attachment that a user will open and unbeknownst to them malicious code is installed that gathers information.

One of the biggest credential thefts in history was against Sony Pictures in 2014. A group called The Guardians of Peace took responsibility for the hack which stole over 100 terabytes of data that included employee passwords (Sulemon, 2014). The Sony breach is notable as it was said to be in retaliation for the release of an upcoming move -The Interview,

which subject matter revolved around a plot to kill North Korean leader Kim Jong-Un. The breach resulted in unreleased movies being leaked and emails that contained personal and sometimes unfavorable communications being exposed (Sulemon, 2014). Another large breach that happened in 2014 was a hack of online marketplace eBay. Hackers were able to make off with customer information including encrypted passwords and email addresses. The breach was serious enough that eBay reached out to its' entire user base of 145 million users and requested that they change their passwords (Peterson, 2014). Two years prior to the eBay hack, online search engine Yahoo reported that 400,000 user names and passwords were stolen from its systems (Irish Times, 2013). It is evident that the list of breaches involving credential theft is quite vast with many occurring on an annual basis. These credentials are often posted online on places like the dark web where they can be sold to other cyber criminals.

When a criminal has access to credentials there are different ways that they can be used fraudulently. In some cases, as mentioned previously, there is no activity reported on the data that was stolen. However, in others the criminals make good use of what they have found. In the Facebook breach hackers were able to get into user accounts, even those of Facebook executives including Mark Zuckerberg (Frenkel and Isaac, 2018). Gaining access to a users' Facebook account opens doors to gaining access to other connected systems that allow users to use their Facebook account as logins such as Instagram. The Deloitte breach gives a good example of what can happen when a hacker has information from just one account. A hacker may have a low-level credential that they can use to gain access to a network, but once on that network they can begin to work their way up to higher level credentials. A hacker can make use of privilege escalation, which is using vulnerabilities or flaws to bump up an account to a higher access level than originally granted. This type of privilege escalation is known as vertical

escalation which involves the attacker granting themselves higher privileges using the credential they already obtained (Rouse, 2010). With the Deloitte breach, the compromised credentials already had administrative rights which meant that whoever had the credentials would initially have a high level of access. Accounts with high levels of access can be used to modify data and give permissions to items that would normally be restricted to a regular user. A great example of this would be the Target case where first an attacker gained access to Fazio Mechanical's network but then was able to traverse the network enough to get additional access and then move on to the larger Target network (Bjorhus, 2014).

The Concept of Privileged Access

The purpose of credentials is to provide access control. In computer systems user access levels are determined or assigned to credentials by a person with administrative rights. The purpose of this type of system is to establish a structure where users have access to what they need to know or work on but nothing more. At a basic level this can demonstrated by thinking of the way you would access your home computer system. In a Windows system you can have a regular user account which only has privileges you allow it to such as running a program and accessing documents. The administrative account has elevated permissions such as the ability to make changes to the computer configuration, run executable files that add features and updates, and control the other users of the machine (Butterfield and Ngondi, 2016). This same concept applies on a broader scale to business systems in which an administrator controls what a user can see in a specific system. Privileged access would encompass any user that has access to a system beyond just the regular user level.

When thinking about the concept of privileged access one of the main hurdles is understanding what data requires elevated access. Classifying data entails discovering all data across the enterprise, and determining who is responsible for it, where and how it is stored, and how it should be disposed when the time comes (Woody, 2013). From a risk perspective a business must determine the level of risk the data presents if exposed, lost, altered, or otherwise compromised. Data types will vary according to the specific business type such as a bank, hospital, or technology firm. All businesses have employee data that must be protected such as data used by human resources and finance departments. It goes without saying that most employees should not have access to another employee's personal information. A person who works in payroll will need access to other employee's bank information to process transactions, but they would not need to have information on another employees' disciplinary history.

Internally data must be separated amongst employees. This can be accomplished in different ways such as role-based access. Access to internal systems is accomplished using credentials that are tied to the access levels that each employee is permitted to have (Ferraiolo, Kuhn, and Chandramouli, 2007). An example of this would be the Active Directory structure in Windows, which allows for the creation of users and the creation of groups that can tie down user access rights. The groups within Active Directory can be linked to outside systems and can also be controlled by Group Policy Objects. Externally, access can also be established using credentials, but more thought must be given as to how the data is transmitted across networks. Credentials will be required to authenticate and access the data, but a business must consider secure methods of transmitting the data such as using vpn or other encrypted tunneling methods.

Financial institutions have several regulations that stipulate how they can use customers' data. If you think about banking there are many facets that connect to provide customers the

services they need. For instance, a customer may have a checking and savings account, but the bank offers more services such as mortgages, and financial instruments like CDs, and lines of credit. Regulations such as the Gramm-Leach-Bliley Act (FDIC, 2003) made strides in trying to protect nonpublic personal data that financial institutions access. It required that customers be informed of the types of data collected and how the data will be used. Generally, consumers will receive an annual privacy notice from their financial institution that outlines the types of data they collect and how the data will be used. If a financial institution plans on giving the data to a third party it must notify the customer and give them the option to opt out (FDIC, 2003). Another financial standard that was discussed earlier is PCI – DSS which looks at the transmission and storage of credit card data. Banks have card reader systems that transmit data and stores have point of sale systems that do the same. These systems must provide point to point security and cover the many ways a person can access data whether it be from a mobile device or a physical system. Some of the requirements include implementing and maintaining firewalls, encrypting data during transmission over public networks, and restricting access to cardholder data (PCI DSS Quick Reference Guide, 2018). It is the institution's responsibility to make sure that appropriate controls are in place to restrict the unauthorized access of data.

Hospitals also have stringent guidelines for how data must be stored and protected. The Health Information Portability and Accountability Act of 1996 or HIPAA (Alic, 2018) was created to protect and secure health information. HIPAA guidelines in 2003 covered written and oral patient information and was then expanded in 2005 to cover electronic records. These guidelines apply to all healthcare professionals regardless of level such as administrative hospital employees all the way up to doctors. Outside of hospitals, HIPAA guidelines apply to insurers as they have access to patient records and to businesses for employee health related items (Alic,

2018). Patients have the right to dictate who can access their health records and must receive a Notice of Privacy Practices from healthcare providers (Alic, 2018). From an internal standpoint, hospitals must establish controls that constrain what each user can access. An administrative employee who is responsible for patient billing should not have access to see a patient's medical history or diagnosis. The concepts that can be applied in healthcare environments would be role-based access control and constrained user interfaces. Role-based access control allows for designating levels of privilege by role so that doctors, nurses, techs, and administrative staff would all have differing levels of access (Ferraiolo, Kuhn, and Chandramouli, 2007). Constrained user interfaces allow for an organization to control who sees what within the same system. For instance, if there is one system that houses all patient data, you may allow doctors to have access to the whole system, but only allow nurses to see a subset. All these types of controls still have one thing in common – credentials.

Protecting Privileged Accounts

Protecting privileged accounts must be a major priority for businesses. As noted in the breaches that have been discussed, the loss of even a low-level credential could lead to a security catastrophe. One way to protect privilege accounts is to separate them from normal user accounts. A normal user account should not be able to make system changes so having users have non-separate accounts with high level privileges creates unnecessary risk. A user with administrative privileges could inadvertently make changes that cause harm as they use the same account for everyday tasks. The account that is being used is also tied to email and possibly other external facing systems that hackers can exploit via phishing or malware (Burnette, 2017). The separation of accounts will make it harder for a hacker to gain higher level access. If a hacker can compromise a machine and obtain the user credentials they will only be able to access

what the user can access. However, if the one set of credentials also has administrative access they can begin to make changes and cause damage without the need to search for a higher privileged credential. Therefore, it is prudent to create administrative accounts that are separate from regular user accounts and have sufficient restrictions. Administrative accounts can be distinguished from regular user accounts by being cut off from services that are not needed such as email and access to local machines. Instead, all activity that consists of making system changes could be done from servers with more security than that of a regular user machine. One benefit of not allowing administrative accounts to login locally on a machine but on a server is that the credentials will not reside on the machine (Plett, Schonning, Poggemeyer, and Conlin, 2016). By not having the credentials stored on the machine if the machine were ever compromised or stolen a hacker still would not have access to the higher-level credentials.

Credentials can also be improved by requiring more complex passwords. The negative side to password complexity is that users may not be able to remember them, and this could result in them writing them down. However, this should not be a deterrent to making this a requirement as a part of a good security policy. Within in a Windows system, businesses can control user password requirements by Group Policy Object settings such as minimum password length, age, and character requirements. Setting a minimum password length makes passwords stronger as they shorter they are the easier it is for a hacker to break.

Depending on the risk level of the system being protected the password age should also be altered. If the system contains sensitive, high value data then a complex password with a lower maximum age should be used. By changing the password on a more frequent basis we insure that even if the account is compromised the credentials will not be usable after a shorter length of time. Finally, instituting complexity requirements adds to the difficulty of guessing or

cracking a user's password. Adding special characters instead of just letters and numbers is helpful in adding complexity. One of the best ways to create a better password is to build it by not just using a word, but by using a passphrase or a combination of unrelated words. By using passphrases or word combinations the password will be both complex, random, and lengthy (Burnett, 2006).

A way to combat the difficulty of remembering complex passwords is to make use of vaults. Many security solutions already have vault solutions that can be utilized. A password manager or vault is secured using a master password and eliminates the need to physically share passwords or store them in documents such as excel and word files. For online use, password managers can store credentials that are used for site logons based on the preferences you set. The next time the website is accessed the password manager will prompt for the master password and then proceed to fill in the login credentials for the website (Biersdorfer, 2016). A password vault like Keepass allows for the storage of passwords and sharing amongst other workmates. Keepass stores passwords in encrypted databases that are accessible only if users have the master password. If a database is shared with workers, they would need the password you created to protect it. Unlike the password manager, Keepass will not automatically fill in passwords when you visit websites or logging to other systems (Matthews, 2011). The downside to a vault like Keepass is that if the master password is lost there is no way to recover the encrypted passwords. The main goal is to move away from insecure methods of password storage and to move towards encrypted solutions.

There are third party solutions that also could help with implementing a privilege access plan. One of the main points previously discussed was how credentials can be obtained and used to gain access to a system in search of higher privileged credentials; but what if those higher-

level credentials were never known? In 2012, Cyber-Ark Software won the UK IT Industry Awards "Security Innovation of the Year" award for their Privileged Identity Management Suite. This software suite manages and monitors privileged access accounts across an enterprise, protecting credentials from both external and internal threats (CyberArk, 2012). The system itself uses policies that allow it to protect passwords and keys by rotating them when needed. Users can access resources that require elevated credentials without ever knowing what they are as the credentials are never presented to them, instead making use of jump servers. Each user session is logged within the system so that if needed they can be reviewed providing accountability (CyberArk, 2018). There are other privileged access system solutions available, but Cyber-Ark is considered one of the best.

One of the reasons that the Deloitte data breach occurred was the lack of multi-factor authentication. Multifactor authentication goes beyond just something that you know and adds in other parameters such as something that you have or something that you are. It can be established by several methods, such as a physical token, an application installed on a mobile device, or even biometrics. The concept is that having one piece of the puzzle will not grant access, but instead multiple forms of identification are needed to gain entry. The Deloitte breach only required knowing the administrator credentials, which could have been used by anyone who had them since further authentication was not required. Some of the common multifactor authentication solutions include OKTA, RSA, and Authen2cate. These solutions allow for the importing of users via Active Directory and the assignment of applications using Active Directory groups. When a user would like to access one of the programs that are managed by the system, depending on your configuration they could be sent an access code via text or through their perspective apps. If the user is legitimate they would have the additional piece for

authentication such as the cell phone that corresponds to the phone number that is on file in the multifactor authentication system. These systems also are used for single sign on, which means that instead of having to memorize multiple passwords, users just need to sign in once and will then have access to all assigned applications.

Another method to securing credentials is reducing a system's footprint. If a system does not need to have access to others or more importantly the internet, then it should not. By restricting internet access to systems that do not require it, the only avenue for a breach to occur would be from within the organization. This can be compared to the concept discussed earlier of administrative accounts not having access to email. If the account is only to be used to make changes, then it is not necessary to have access to other functions such as being able to send and receive emails (Plett, Schonning, Poggemeyer, and Conlin, 2016). Servers that house important data that do not require external internet access should have these services shut off. If a system does require internet access, then it is important to put appropriate measures in place to protect data. These measures can consist of host intrusion detection, antivirus, and keeping the data in encrypted storage while at rest.

An important component of any security plan is user awareness training. The Target breach started with a phishing scheme that a user at Fazio Mechanical fell prey to. While it is not possible to fully prevent all attacks, some user awareness will help to minimize the risk. It would be remiss to think that users who are unaware of the threats they face online could make appropriate judgement when it comes to risks. Humans create the weakest link in any security program. The most common link between all security breaches is the human element, especially given the success of social engineering attacks. Infamous hacker Kevin Mitnick after spending years in prison decided to make the switch from cyber-criminal to security expert and established

KnowBe4 a leading security awareness training company. The goal of Knowbe4 is to reduce the problems that occur from human error by making users aware of the threats they face. Their training programs include videos, tests, and simulations for phishing and spear phishing attacks (Urrico, 2015). There are also other companies that offer training and simulation services. The most important piece of training is being able to track user performance and to be able to gauge how users would react in a real-life situation. Conducting simulations is a great way to do this and is crucial to understanding where gaps exist and knowing what areas needs more focus. Users who are informed will think twice about responding to an email or clicking a link that could potentially put the company at risk (Ferrillo and Singer, 2015).

What Solution is Best?

Determining what solution works best must be based on the individual business needs. An organization must do a risk assessment to know which assets require additional solutions to secure and which do not. In all cases there is the risk vs. reward equation that must be evaluated. If the data is of low value, it would not make sense to put in a high cost system. However, when the data has a high value attached to it, such as intellectual property, it would make sense to spend the money to secure it. A way to mathematically calculate this would be to do an annualized loss expectancy calculation which looks at the annual rate of occurrence multiplied by the single loss expectancy (Czagan, 2018). The solution that should be implemented should cost less than the annualized loss expectancy; otherwise the company would lose money by paying more for a solution than the potential loss is worth.

A solution also may be determined by regulations and therefore be non-negotiable. Standards such as PCI DSS and HIPAA have rules that must be followed to maintain compliance. Therefore, there are certain components that must be in place that cannot be

bypassed. Hospitals must have systems in place that separate privileges and secures patient information (Alic, 2018). Banks, stores, and any entity that processes credit card data must have systems that are encrypted (PCI DSS Quick Reference Guide, 2018).

The basis of any security solution should be the concept of defense in depth. Networks should be protected behind firewalls insuring that only allowed traffic can get through to the network. Appropriate intrusion detection and prevention systems should be in place and adequately monitored. As was seen with the Target breach, their security team received alerts but did not recognize or apply the appropriate significance to the threats. It is not enough to have these systems, but it is also necessary to have the right team in place to address incidents as they occur.

There are low cost solutions that can be put in place that do not require a lot of time and effort to implement. When considering implementation, a company must look at the resources it has and the ongoing business needs. If a company is small, it may not make sense to purchase an expensive system that it does not have the resources to maintain. It may make sense to purchase a simple system that can track changes and send alerts when anomalous activity occurs. For instance, ManageEngine, a IT management software company, has a product called ADManager Plus. This software can log and send alerts for failed logon attempts which can alert IT departments to potential unwanted activity. In addition to software solutions, other low or no cost changes could be made within Active Directory that help to prevent credential misuse (ManageEngine, 2018). The setting for allowed logon attempts should be set low, which will help to prevent brute force attacks as the account will lock after a certain period. Organizations should make sure that terminated users and accounts that are no longer being used are disabled

and eventually removed. The less accounts that are active means that hackers will have one less account to compromise.

Securing Credentials

It is evident from the many security breach examples that credentials play a vital role in the success of a hack or preventing a hack. The importance of protecting credentials should not be overlooked by anyone. To protect credentials companies, must focus on the human element. Regardless of the systems put in place such as firewalls and other access controls, all is for naught if the human element fails. Therefore, it is suggested that the main methods of securing privilege access accounts consist of appropriate user training, separation of accounts, and implementation of a credential management system.

Training will keep users aware of the threats they face and help them to recognize those threats once presented. Hackers are becoming much more sophisticated, moving beyond the old Nigerian Prince scheme to more tailored email phishing schemes. It is not uncommon to get an email with what appears to be legitimate letterhead from a financial institution claiming that your account will be closed if no response is received. These types of scams work, otherwise criminals would not continue to use them, and employees need to be made aware. A training system should be in place that requires users to finish appropriate modules at a set date and that logs completion rates. The training system should also have tests that show that the users have sufficient knowledge and if they fail it should be recorded. By having a system that logs the progress and knowledge of users, security professionals will know which areas need more focus, which users should be monitored more closely, and what solutions may be needed to help minimize risk.

Separation of accounts is a measure that does not cost an organization any money to implement. This solution keeps good separation of duties for user accounts. It is simple enough to give lower access rights to a user account and require the use of an administrative account for privilege level access. This privilege level access is more for the IT side of the spectrum, while other non-information technology privilege access can be granted using role-based access controls. The administrative accounts should be designated as such and should be limited in terms of access to programs that are internet facing such as email. These accounts should have logging enabled and should also be logged so that when an employee leaves the privileged account is immediately disabled.

Lastly, a credential management system is needed to secure privileged accounts. A credential management system can be used on both ends of the spectrum, from regular user accounts to privileged accounts. The problem of remembering passwords is one that must be considered, especially given the fact that complex passwords are expected to be used. Solutions such as KeePass or password management solutions that are included with security software could help to alleviate this problem. Storing passwords in an encrypted vault is much more secure than having them listed in a spreadsheet that could fall into the wrong hands. Alternatively, if a more robust solution is required a system such as CyberArk could be used which masks privileged account credentials from users, so they are never exposed. Another facet that would help with credential security is making the usernames more complex and not just the passwords. It is easy for a hacker to go onto a website and find out who works at an organization and make an educated guess as to the usernames. It would make sense then that the way usernames are created and issued should change to add some complexity such as not using first initial and last name but employing some randomness. This could be as simple as using the users

initials or continuing to use first initial, last name and adding random numbers or characters that would be impossible to guess.

The problem of protecting privileged accounts will take a combination of solutions to address. They include solutions that cost nothing, to ones that cost thousands of dollars but implement robust security features. The first step for any organization is to take a full accounting of user accounts and access rights assigned to them. It may be feasible to do monthly user access reviews to look across all systems and make sure that users are adequately purged and that users have appropriate access levels assigned.

Securing credentials is always going to be an ongoing process. Organizations should have security policies in place and they should require that they are reviewed annually by employees. A part of this policy should include rules for passwords, how they should not be shared, stored, etc. If there are approved methods of password storage and sharing for accounts that use one credential, this should be outlined in the policy. Risk assessments should be conducted on a regular basis so that systems with more sensitive data have more safeguards around the credentials used. This could be a policy of making sure that the password is changed on a frequent basis and stored in an encrypted vault. The key to privilege access management is understanding the accounts that you have, what they have access to, and keeping them secure both internally and externally.

Bibliography

Alic, M., PhD. (2018). HIPAA. In J. L. Longe (Ed.), The Gale Encyclopedia of Nursing and Allied Health (4th ed., Vol. 3, pp. 1734-1739). Farmington Hills, MI: Gale. Retrieved from http://dbproxy.lasalle.edu:5066/apps/doc/CX3662600548/GVRL?u=phil31439&sid=GVRL&xid=8707a1df

Baldwin, H. (2012, November 05). Passwords are the weak link in IT security. Retrieved from https://www.computerworld.com/article/2493184/security0/passwords-are-the-weak-link-in-it-security.html

Beilfuss, L. (2015, Apr 15). Target reaches $19 million settlement with MasterCard over data breach; funds to reimburse financial institutions for costs after 40 million credit and debit card accounts were compromised. *Wall Street Journal (Online)* Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/1673165230?accountid=11999

Burnette, M. (2017, February 9). Are your administrators using admin accounts for everything? Retrieved from https://www.lbmcinformationsecurity.com/blog/are-your-administrators-using-admin-accounts-for-everything

Burnett, Mark. Perfect Password : Selection, Protection, Authentication, William Andrew, 2006. ProQuest Ebook Central, https://dbproxy.lasalle.edu:5967/lib/lasalle-ebooks/detail.action?docID=254851. Pg. 94

Bjorhus, J. (2014, Feb 12). Target breach started with email phishing attack, report says. *McClatchy - Tribune News Service* Retrieved from http://dbproxy.lasalle.edu:2048/login?url=https://dbproxy.lasalle.edu:6033/docview/1497276719?accountid=11999

Butterfield, A., & Ngondi, G. E. (2016). *A dictionary of computer science*. Oxford: Oxford University Press.

Campbell-Miller, S. (2017). As data breach costs rise, cyber insurance looks good. *Arkansas Business, 34*(47), 12. Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/1986312553?accountid=11999

Czagan, D. (2018, May 21). Quantitative Risk Analysis. Retrieved from https://resources.infosecinstitute.com/quantitative-risk-analysis/

ValueWalk: Deloitte suffers catastrophic data breach (2017). . Chatham: Newstex. Retrieved from http://dbproxy.lasalle.edu:2048/login?url=https://dbproxy.lasalle.edu:6033/docview/1942664232?accountid=11999

Cordell, David M, PhD, CFA,C.F.P®, C.L.U®, & Langdon, Thomas P, JD, LLM,C.F.A., C.F.P®. (2017). Curbing client risk with cyber insurance. *Journal of Financial Planning*, *30*(2), 34-35. Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/1875325187?accountid=11999

Curran, J. (2014). TARGET: DATA BREACH HURT SALES IN QUARTER. *Cybersecurity Policy Report,* , 1. Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/1506141975?accountid=11999

CyberArk Wins Security Innovation of the Year Award at the UK IT Industry Awards 2012. (2012, November 19). Retrieved from https://www.cyberark.com/press/cyberark-wins-security-innovation-year-award-uk-industry-awards-2012/

Target breach fallout shows CEOs, CIOs share cybersecurity stakes -- WSJ blog. (2014, May 05). *Dow Jones Institutional News* Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/2077801218?accountid=11999

dictionary attack. (2013). In D. Downing, *Barron's business guides: Dictionary of computer and internet terms* (11th ed.). Hauppauge, NY: Barron's Educational Series. Retrieved from http://dbproxy.lasalle.edu:2048/login?url=https://search.credoreference.com/content/entry/barronscai/dictionary_attack/0?institutionId=2839

Cyber-ark gets security innovation of the year award. (2012). *Entertainment Close - Up,* Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/1218634183?accountid=11999

Deloitte security consulting earns rank from Gartner. (2013). *Entertainment Close - Up,* Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/1398358396?accountid=11999

Federal Deposit Insurance Corporation. (n.d.). Retrieved from https://www.fdic.gov/consumers/consumer/alerts/glba.html

Ferraiolo, D. F., Kuhn, D. R., & Chandramouli, R. (2007). Role-based access control. Retrieved from https://dbproxy.lasalle.edu:5967 pgs. 57-58

Ferrillo, P., & Singer, R. (2015). Is employee awareness and training the holy grail of cybersecurity? The Corporate Governance Advisor, 23(3), 10-13. Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/1679423689?accountid=11999

PCI DSS Quick Reference Guide [Pamphlet]. (n.d.). PCI Security Standards Council. Pg.13

Plett, C., Schonning, N., Poggemeyer, L., & Conlin, C. (2016, October 11). Securing Privileged Access. Retrieved from https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access

Ponemon institute survey: Data breaches can cause lasting and costly damage to the reputation of affected organizations. (2011). *Entertainment Close - Up*, Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/902304462?accountid=11999

Hodgman, R. (2017, September 28). The Attacker's Dictionary. Retrieved from https://blog.rapid7.com/2016/03/01/the-attackers-dictionary/

Huston, T. (2017, May 28). Cost of Target's Data Breach Nearing $300 Million. Retrieved from https://www.breitbart.com/tech/2017/05/28/cost-targets-data-breach-nearing-300-million/

Ince, D. honey pot. In (Ed.), A Dictionary of the Internet. : Oxford University Press,. Retrieved 17 Nov. 2018, from http://dbproxy.lasalle.edu:2190/view/10.1093/acref/9780191744150.001.0001/acref-9780191744150-e-1523.

40,000 yahoo! user names and passwords stolen. (2012, Jul 13). *Irish Times* Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/1024594176?accountid=11999

Isaac, M., & Frenkel, S. (2018, September 28). Facebook Security Breach Exposes Accounts of 50 Million Users. Retrieved from https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html

Krebs, B. (2014, May 06). Krebs on Security. Retrieved from https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

ManageEngine. (n.d.). Integrated Active Directory, Office 365, Exchange, G Suite & Skype/Lync Management & Reporting solution. Retrieved from https://www.manageengine.com/products/ad-manager/

Marriage, M. (2017, September 25). To read: Financial Times Accounting group Deloitte hit with cyber attack. Retrieved from https://www.ft.com/content/7c52fe88-7bf1-3798-9d55-2d5498b53c20

Matthews, N. (2011, Nov 06). Helpware: KeePass password safe. *Telegraph - Herald* Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/902308775?accountid=11999

Malcolm, H. (2014). Target Sees Drop in Customer Visits after Breach. Retrieved January 31, 2017, from http://www.usatoday.com/story/money/business/2014/03/11 /target-customer-traffic/6262059/.

Peterson, A. (2014). eBay asks 145 million users to change passwords after data breach. Washington: WP Company LLC d/b/a The Washington Post. Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/1526748031?accountid=11999

Plachkinova, M., & Maurer, C. (2018). Security breach at target. *Journal of Information Systems Education, 29*(1), 11-19. Retrieved from http://dbproxy.lasalle.edu:2048/login?url=https://dbproxy.lasalle.edu:6033/docview/2018608701?accountid=11999

New research shows cyber criminals focused on credential theft; WatchGuard's latest internet security report reveals rise of mimikatz, finds that 47 percent of all malware is new or zero day and offers comprehensive analysis of WannaCry. (2017, Sep 28). *M2 Presswire* Retrieved from http://dbproxy.lasalle.edu:2048/login?url=https://dbproxy.lasalle.edu:6033/docview/1943536736?accountid=11999

Ristuccia, H. (2015, January 21). Security Attacks: A Lead Driver of Reputation Risk. Retrieved from https://deloitte.wsj.com/riskandcompliance/2015/01/21/security-attacks-a-lead-driver-of-reputation-risk/

Roberts, J. J. (2017, September 25). Deloitte Gets Hacked: What We Know So Far. Retrieved from http://fortune.com/2017/09/25/deloitte-hack/

Rouse, M. (2010, November). What is privilege escalation attack? - Definition from WhatIs.com. Retrieved from https://searchsecurity.techtarget.com/definition/privilege-escalation-attack

Shaer, M. (2014, Mar 14). Target missed important warnings before security breach: Report. The Christian Science Monitor Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/1507493051?accountid=11999 pg.14

Suleman, K. (2014, Dec 08). Biggest hacks of 2014: From apple to eBay, no-one is safe. *IT Pro,* Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/1634613731?accountid=11999

Todd, S. (2014). Target security personnel raised the alarm before data breach: WSJ. *Credit Union Journal, 18*(7), 45. Retrieved from http://dbproxy.lasalle.edu:2048/login?url=https://dbproxy.lasalle.edu:6033/docview/1501453976?accountid=11999

Urrico, R. (2015). KnowBe4 automates security training. Credit Union Times.Breaking News, Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/1697746978?accountid=11999

Veysey, S. (2014). CYBER INSURANCE IN THE SPOTLIGHT. *Business Insurance, 48*(4), 20. Retrieved from

http://dbproxy.lasalle.edu:2048/login?url=https://dbproxy.lasalle.edu:6033/docview/1500461500?accountid=11999

Weiner, R., & Hawkins, D. (2018, June 19). Hackers stole federal workers' information four years ago. Now we know what criminals did with it. Retrieved from https://www.washingtonpost.com/local/public-safety/hackers-stole-feds-information-four-years-ago-now-we-know-what-criminals-did-with-it/2018/06/19/f42ff2b2-73d3-11e8-805c-4b67019fcfe4_story.html?noredirect=on&utm_term=.0822a8a21a7d

Woody, Aaron. Enterprise Security : A Data-Centric Approach to Securing the Enterprise, Packt Publishing Ltd, 2013. ProQuest Ebook Central, https://dbproxy.lasalle.edu:5967/lib/lasalle-ebooks/detail.action?docID=1103988. Pg. 165

Wright, S. (2011). *Pci dss : a practical guide to implementing and maintaining compliance*. Retrieved from https://dbproxy.lasalle.edu:5967 Pgs. 18-21

Ziobro, P. (2014, Feb 06). Target breach began with contractor's electronic billing link; fazio mechanical services says it was 'a victim of a sophisticated cyber attack'. *Wall Street Journal (Online)* Retrieved from http://dbproxy.lasalle.edu:2048/login?url=https://dbproxy.lasalle.edu:6033/docview/1495162524?accountid=11999