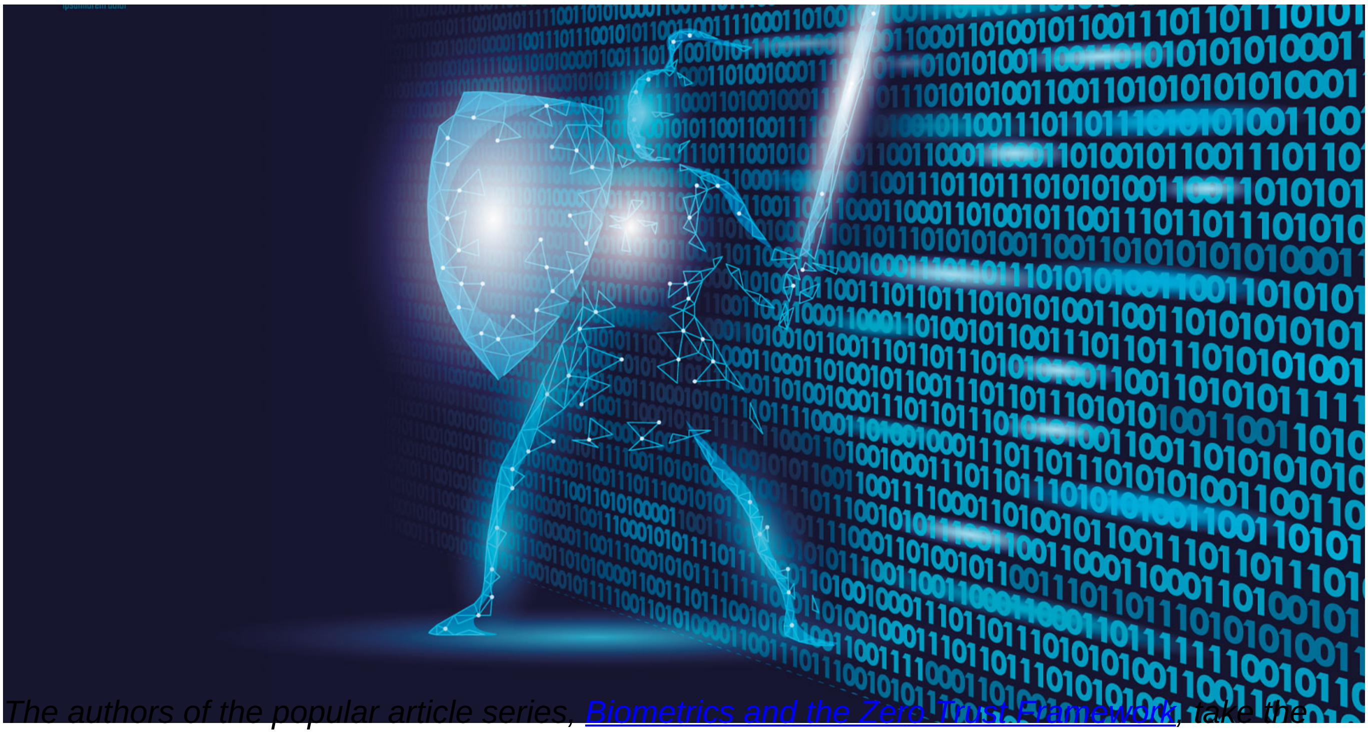
ZTF: The Secret to Seamless Authentication: Part 4

Author :



The authors of the popular article series, Biometrics and the Zero Trust Framework, take the topic to the next level in their new book, ZTF: The Secret To A Seamless Authentication Experience (on Amazon). In a previous excerpt from the book, the authors introduced the concept of Privileged Access Management (PAM). Here, they explain why PAM is well-suited for Cloud based deployments. They also outline PAM best practices—and common mistakes to avoid.

The Advantages of Using PAM In the Cloud

Obviously, deploying a PAM based solution in the Cloud is far better than doing it On Prem. The benefits can be detailed as follows:

> **Centrally store and manage passwords**. In today's business world, passwords are amongst the biggest nemesis that is faced. For example, the cost to reset a password is pegged to be at about $100.00 per employee. If you are a smaller SMB, this may not come to a lot of money in the end. But if you are a Fortune 100 company with thousands of employees worldwide dispersed globally, this cost can add up quickly, and take a toll on the bottom line. Sure, there are other tools you can use out there, such as the basic Password Manager. But there are inherent security flaws with those as well, especially when it comes to overseeing those employees that have privileged access accounts. What makes PAM unique in this sense is that it brings to the Cloud a high powered "Password Vault" which allows to you manage and assign administrative privileges from a single dashboard, in a very safe and secure environment. Nobody else but you will be involved in this process, unless you have other IT Managers that you want to grant this kind of access to.

Easier to enforce the Concept of Least Privilege. One of the cardinal rules in Cybersecurity is to give employees just enough access to shared resources for them to do their job on a daily basis. Although this sounds simple in concept, enforcing it and keeping of what employees have is another story. For example, the IT Security team may give out admin level credentials to a contractor only for the time that they are at your business. Once they are done with their work, this account should be immediately disabled, but many times it gets forgotten about. Or employees may share their passwords behind your back. Whatever the situation is, you need a tool that can oversee and execute the concept of Least Privilege on a real time basis. This is where PAM will play a crucial role. Once deployed in a Cloud environment, it can automatically assign privileges on a needed basis, following the rules and permutations that you have set forth. But best of all, it will terminate those accounts which no longer need those privileges for certain applications. In other words, you don't have to go from through every computer and wireless device to make sure that the baseline rights and permissions have been assigned and/or deleted. The PAM can store all of the employee profiles and decide when to allocate and disable permissions automatically. This reduces the risk of forgotten accounts still being activated, which could create a potential backdoor for a Cyberattacker. This is also known as "Just In Time Access" and can even be used for members of the IT Security team in order to reduce probability of misuse of admin level privileges.

Control Remote Access. With the COVID-10 pandemic still upon us to varying degrees, the Remote Workforce is here to stay permanently. While many of the initial security issues were worked out when WFH was first launched a couple of years ago, many of the traditional security tools have been stretched beyond their breaking points. A prime example of this is the Virtual Private Network (VPN). Before the pandemic hit, it did an excellent job of encrypting and securing the network lines of communications. But this was when only 15% - 20% of all employees were working from home, not the near 100% capacity we are seeing now. Thus, Cyberattacker now has greater ease in which to penetrate into the VPN, gain access to privileged credentials, and even hijack a remote session. But by implementing a PAM solution into your Cloud environment, you can make use of the Zero Trust Framework and implement what is known as the "Next Generation Firewall" which far surpasses the security thresholds that are offered by the VPN. Not only will this prevent the hijacking of privileged access credentials, but you will have logging activity recorded on a real time basis, which makes auditing far easier and simpler.

Protecting Interconnectedness. As the digital world is coming together, so are the objects that we interact with on a daily basis, which include those in the physical and virtual worlds. This is technically known as the "Internet of Things," or the "IoT." The Cloud has also made it to a great extent these objects to interact with one another, but the problem is that the end users still have the security set to the default level, which also includes making use of a very weak password. When PAM is implemented into IoT infrastructure you have deployed into the Cloud, it can manage the creation and assignment of appropriate privileges to the end users on an automatic basis. It will even assign passwords that are far most robust than what a traditional Password Manager can create.

Secure DevSecOps In The Cloud. This was a concept that was introduced in the last article. This is a merging of three distinct teams:

Software development
Operations
IT Security.

One of the central themes of DevSecOps is automation. While PAM can be used here once to protect privileged access to the source code, it can even do much more than that, for example:

Secure developer accounts
Secure Encryption Keys
IT Security.

One of the central themes of DevSecOps is automation. While PAM can be used here once to protect privileged access to the source code, it can even do much more than that, for example:

Secure developer accounts
Secure Encryption Keys
Secure Digital Certificates.

A Best Practices Guide for Deploying a PAM based Solution
Just deploying the Zero Trust Framework, deploying a PAM based solution takes careful planning, and testing before releasing it into the Production Environment. Here are a few tips to help ensure a smoother deployment:

Understand why you need PAM in the first place. You simply should not deploy a PAM solution just because you think you need to. You first need to think carefully why you need one in the first place, and if you decide to have one, then you need to map it very carefully how it will fit into your IT and Network Infrastructure. You need to fully ascertain which systems, processes, and technologies will be requiring this. Then you need to figure out who will have access to the PAM solution these are keys to the proverbial crown jewels of your organization.

Create a PAM password policy. You should already have a password policy in place, but the one for PAM will be different in the sense that you need to craft it so that it addresses the needs of those that have managerial or IT admin titles. Having such a policy in place will help to avoid any misuse of credentials, as Cyberattackers love to go after these kinds of passwords. Therefore, it is recommended that you follow the guidelines from entities as SANS, NIST, and ISO. Remember to change out passwords on a regular basis, and just like for your regular employees, they should be made long and complex and just a little bit more, as these credentials will give access to the most sensitive areas of your business. Also, make sure you implement Multifactor Authentication (MFA) to make sure 100% that only the legitimate employees have access to privileged accounts. Some of these second and third layers of authentication can include the use of passphrases, RSA tokens, Smart Cards, Biometrics, etc.

Change out default passwords. Once you have created a privileged account, make sure that the person to whom it is assigned immediately changes the password. Even though the default password may be long and complex, it is always a good practice to make sure it is changed out when the account it is first activated. Make sure you put into your PAM security policy as to what these passwords need to contain. This will be an alphanumeric string, but to what detail it needs to contain needs to be spelled out to avoid any confusion or mistakes. Remember, your employees do not have to create these kinds of passwords. The PAM functionality should take care of all of this on an automatic basis. But it is always a clever idea to conduct an audit from time to time as to who has what access when it comes to privileged accounts.

Keep tabs as to what is going on. Just as much as the IT Security team has their eye on the Cyber Threat landscape, you also need to keep an eye as to what is happening to the privileged accounts that you assigned. For example, you need to make sure that those employees who have these kinds of accounts are abiding by every letter of the PAM password policy. Of course, you will not be able to keep track of all of this on a 24 X 7 X 365 basis, so this is where you can use the tools of both Artificial Intelligence (AI) and Machine Learning (ML). They can keep an eye for you on these accounts on a real time basis, and alert you in case there is any type of anomalous or suspicious behavior that is transpiring. Keeping track of all this will give you the essential metrics that other members of the C-Suite will ask for, and even the Board of Directors. Keeping track of this will also be very advantageous to you in case you are ever faced with an audit by regulators from the GDPR, CCPA, HIPAA, etc.

Make use of Least Privilege. This was reviewed in one of the previous articles. With this, you are assigning the minimal amount of permissions that are necessary for your employees to conduct their daily job tasks. But this holds true also for those employees that have privileged accounts. Just because they are technically at a higher plane because of the level access, you still need to follow the concept pf Least Privilege here as well. For instance, you would grant your IT Security Manager access to all of the devices in your company, so that they can install the needed software patches and upgrades and perform other troubleshooting tasks. For your Network Administrator, you would assign those rights and permissions that are needed to gain access to the network, the servers, etc. These are privileges that your IT Security Manager would not need, and vice versa.

Deletion of temporary accounts. At times, it may be necessary for you to set up a privileged account for an outside third party, especially if you hire a vCISO. Rather than assigning an original, privileged account for them, create a cloned account, and from there, you can then specifically configure the privileged access this individual will need, based upon their contractual obligations to you. Set this account to be inactive on their last day. This way, you will not have to worry about forgetting about this task, it will be done automatically for you.

The Mistakes That Are Made When Deploying PAM Solutions & How to Fix Them

Even despite the care that you and your IT Security take, mistakes are always inevitable. Here is the common list of mistakes made and how to correct them:

1. **How up to date are your systems?** The PAM solutions of today are mostly compatible with the latest technologies. For example, deploying a solution for Windows 10 will not work for Windows 8, as it is a much more out of date system. Before you deploy a PAM

configuration, it is very important to make sure that it will work with all of the digital assets in your business. The best way to do this is to take an inventory of all of the hard wired and wireless devices that you have. If anything is outdated, then it is time to discard and upgrade ASAP. This is not just from the standpoint of launching PAM, but it is a rule of thumb in Cybersecurity that any outdated device can pose a serious risk, as this is one of the first items that the Cyberattacker will go after.

2. **Not applying passwords properly.** This has been a widespread problem for decades, and it is only getting worse. Many employees are given admin passwords, whether it is intentional or not. By doing this, they will be able to login into the most sensitive areas of your business, and cause any type of havoc, such as data leakage. Or worse yet, they can accidentally give out these passwords to a Cyberattacker in a Social Engineering attack. Password sharing still remains a huge problem as well, and this is one of the leading causes for Insider Attacks to precipitate. To avoid all of these problems, you need to separate out the normal, everyday employees from those that are eligible to have privileged access. The former group should have its own set of security policies, whereas the latter should have its own as well. While both should be enforced equally, the group of employees with privileged access needs to have further scrutinization. In other words, you don’t want to have password misuse here, as the effects can be far more serious. You are dealing with privileged accounts. In order to make sure that all is airtight, it is imperative that you check for any types of suspicious behavior on these types of accounts. This can include multiple login attempts that have failed, or trying to login to a resource to which they have no business in doing so. You can keep a daily watch on all of this by implementing AI tools, and having any alerts or warnings transmitted to the SIEM, where a dedicated member of the IT Security team can proactively tirage them.
3. **Create the right kinds of profiles in Active Directory.** One of the primary benefits of AD is that you can create as many user groups as you need, and from there, assign privileges on ad hoc basis. For example, you can create a user group for all of the accountants that work in your company, and import into that all of the individual usernames. From there, you can create all of the privileges for that profile, and deploy all of the privileges and permissions in a simultaneous fashion. While this is certainly advantageous, it can also prove to be a serious mistake from the standpoint of the privileged user groups. You do not want a help desk specialist to have network administration privileges assigned to them by accident. So, in this manner, you are probably better off assigning rights and privileges to privileged accounts manually, rather than on ad hoc basis. True, this will take more time, but at least you will have confidence that the appropriate permissions have been applied. This is where having a separate list created for the privileged accounts will be very useful, as described earlier in this article.
4. **The move to the Cloud.** The movement to the Cloud is now happening at a pace than it was ever imagined. A lot of this has been fueled by the COVID-19 pandemic, and in this rush, security is now a forgotten topic here. When you move all of your applications to the Cloud, you need to take an inventory of what you have just moved, and from there, determine which of those assets need the highest level of protection. Of course, you will need some sort of PAM architecture here, but this too will need to protect as well. In other words, you simply cannot assign privileged accounts and merely trust your IT Security team will not run off with them. There could be a malicious threat actor here as well. Therefore, you will even need to keep a careful eye here, because in today’s world, you simply cannot trust anybody anymore, even those employees that have been around for a long time. In other words, the days of having implicit trust even in the most

minute degree is now over, it is time for the Zero Trust Framework.

5. **Outside vendors.** As the world becomes more interconnected partly fueled by the Internet of Things (IoT) revolution, businesses are becoming more dependent now upon hiring third party contractors to help meet customer demands and expectations. It is highly recommended these days that you have a deep vetting process in place before you make a selection. But this is where most companies make their mistake. They don’t continually monitor the hired third party after the fact. It is very important that you do audits on a regular basis, in order to confirm that there are no leakages of your datasets, and that all privileged accounts that have been assigned are not being misused in any way.

This concludes our series of articles based on excerpts from ZTF: The Secret To A Seamless Authentication Experience (on Amazon).

Sources/References:

See: *ZTF: The Secret To A Seamless Authentication Experience (on Amazon)*

Join the conversation.

GO

Visit Keesing Technologies