EBOOK

simeio

Privileged Access Management VS Healthcare Supply Chain Attacks in 2023

Introduction

Cybersecurity is often likened to the defense of a medieval castle. Strong barriers manned by watchful sentinels, challenges of "who goes there," and the occasional pouring of boiling substances (be they tar or coffee) onto the heads of underpaid minions who would rather be at home. And, like the siege of a castle, one of the most effective means of making life difficult for the occupants is preventing people who should be getting in from ever passing the gate.

Before this metaphor becomes even more convoluted (what would the diseased cows launched by trebuchets be?), let's all agree that Denial of Service (DoS) attacks are frustratingly effective. Few sectors feel this more acutely than healthcare professionals. High profile incidents like the 2014 Boston Children's Hospital attack demonstrate the vulnerability of even high-profile medical institutions.[1]

Brute force hacking serves bad actors just as well in slowing web resources to a crawl as they do for trial-and-error password cracking. DoS attacks sour customers, impede employees, and gimp your services. What's more, these results can be achieved without ever actually breaching your perimeter. With DoS attacks increasing by 74% in 2022 over 2021,[2] your enterprise needs to prepare.

Then you have instances when the invading Normans...er, hackers, actually breach your walls and expose your patients' data. A fair number of enterprises, either through arrogance or (much more commonly) ignorance do not institute remediation methods until after they have been breached. Unless you want to be standing in the smoldering ruins of your keep, proudly declaring that next time you'll remember to have a fallback, you need to focus on intelligent defense now.

Fortunately, a hero has appeared, and her name is PAM. Privileged Access Management systems, and their users, serve as the first and last line of identity defense. This access system applies the principles of role-based access control to enforce the principle of least privilege. From directing and monitoring the functions of your identity fabric to detecting and isolating bad actors, a strong PAM solution forms the core of your IAM apparatus.

Your enterprise can build that core from the ground up. Assess your identity fabric, close the gaps in your infrastructure, bolster your tracking and remediation, educate your users, and automate as much as you can. Follow these steps towards proper implementation, and your walls shall stand tall and strong against all attackers.

[1] DDoS Attacks: In the Healthcare Sector
[2] 2022: DDoS Year-in-Review, InfoSecurity Group

1 GET A FULL ASSESSMENT OF YOUR OWN IDENTITY FABRIC

Like an absent vaccination, so long as you have a single gap anywhere in your security, you are counting down to your next breach event. Without comprehensive consideration of every aspect of your identity, you cannot claim to have a strong risk posture. Take a hard look at your AM, CIAM, IGA, and PAM, but pay special attention to PAM.

If possible, do a full audit. There are strong advantages to using an external assayer instead of trying to measure the whole process in-house. Between bias and lack of experience, attempts at internal audits seldom provide results worth the investment. Dedicated IAM experts deliver delineated budgets, timeframes, and objectives.

When you begin your assessment, either through an internal committee or a skilled firm, bear a few pointers in mind. Make sure to emphasize to the assayers that cybersecurity is a top priority of your identity investments.

Let them know to pay special attention to monitoring and remediation, both what you have and may build in the future. Clarify that you want to know which of your security gaps are coming from third parties and have the assessment team advise you on how to make those avenues secure.

Request a specific section in the final report on the state of your PAM and how it can be improved. Ask for a detailed to-do list of what software, hardware, or policy changes need to be implemented to make your PAM as powerful as possible. If your budget forces you to pick and choose your upgrades, prioritize PAM over the other pillars if need be.

Beyond just the status of your systems, you also need to heed their words about personal practice. Have your assessment cover potential attack scenarios (DDoS, compromised credentials, hardware failure, etc) and how you can counter them.

2 PLUG UP YOUR INFRASTRUCTURE GAPS

Once you've gotten back the diagnosis, you'll have a much better idea of what needs to happen within your organization to prevent data breaches and DoS attacks. While the specifics of your situation will be unique, you likely will have a few common points you can improve on. All these suggestions flow out of PAM.

> **Protect your patients from data breaches and DoS by embracing PAM, automating access control, securing third-party tools, hardening systems, and following audit recommendations."**

2 PLUG UP YOUR INFRASTRUCTURE GAPS CONT.

Provisioning and de-provisioning accounts is likely to be a major concern. Joiners, movers, and leavers are a stumbling block to good identity defense, as their actions constantly shift the perimeter you must defend. Automating your infrastructure to enforce the principle of least access is a major step in the right direction. Your system can regularly audit itself and ensure that users only have the access they need. This prevents orphan accounts from accumulating and removes individualized role-based privileges enforcement.

Be wary of how your organization implements outside tools. Bringing in an external application can open byways to your patients' sensitive information, especially if the application is maintained by another company. Simply put, if third party vendors are not linked to your systems via secure APIs, your patients are going to be at risk of attacks. An estimated 16% of all breaches come from third party vendor vulnerabilities.[1] Be prepared to cut out access to some sensitive data. A supply chain attack can't steal secrets from a vendor if you never give them any.

Harden your systems against DoS by instituting countermeasures ahead of time. When an attack comes, make sure you have a plan ready to set in motion. The saving grace against brute force attacks is that they can only adapt as fast as their instigator. If you can bottleneck their attempts to overwhelm your service, you can stop their attack in its tracks.

Above all else, follow the directives of your audit even if they are difficult to implement at first. If you've placed particular emphasis upon PAM, DoS, and breach protection, then their recommendations should be exactly what you need to fulfill your security goals. Better still, the same company that performed your assessment service may be able to implement your solutions directly.

3 ENSURE YOU HAVE POWERFUL DATA TRACKING & REMEDIATION AVENUES

Now that the immediate threats to your identity fabric are addressed, turn your attention to active prevention. Make sure you have adequate data protection and breach detection on your own systems. Traditional perimeter-based security leaves you vulnerable to covert focused attacks. Identity-based security erects a barrier around each individual target. PAM oversees all subordinate sectors of IAM, and the strength of those domains contributes to your overall security posture.

Of course, this assumes that your baseline infrastructure can support such protocols. Tightening up security is going to be tougher if your basic systems are not properly integrated. A seamless system of applications is much easier to keep secure. Plug-ins to various applications need to be centralized and modular enough to scale up as needed. Your enterprise is not static, and your security cannot be either.

> **"STRENGTHEN YOUR SECURITY POSTURE BY IMPLEMENTING PAM, INTEGRATING SYSTEMS, EXTENDING PROTOCOLS TO VENDORS, AND ANSWERING THE 6 KEY IAM SECURITY QUESTIONS."**

[1] Cost of a data breach 2022, IBM

3 ENSURE YOU HAVE POWERFUL DATA TRACKING & REMEDIATION AVENUES CONT.

As before, automatic de-provisioning for leavers, good governance based on minimum and role-based access, MFA, and SSO should be your baseline. Take special care to follow through with your auditors' suggestions about building out your IGA infrastructure and integrating it with your PAM. Anything that contributes to your ability to trace what users are doing with your resources should be on the table. This includes on-call experts, either internally or through an identity service, able to swoop in on a problem.

Once you have a strong baseline, extend those processes and policies to your vendors. Monitor all outgoing data requests and keep tight control over any data called up. Zero-trust methods can greatly help in cases where sensitive data is needed for a specific system function.

As always, PAM is how you achieve these goals. Build up your PAM with the understanding that it is both command center and security checkpoint. Nothing digital should happen within your enterprise that PAM does not keep track of. Do not trust that data leakage software will keep your systems secure; 69% of companies with a DLP still experience insider data breaches.[1]

The best rule of thumb is to ensure you can always answer the 6 identity access and management security questions. Make sure you can always answer who has access, when did they get access, how did they get access, who authorized their access, is their access privileged, and how are they using their access?

80% OF ALL DATA BREACHES CAN BE TRACED BACK TO COMPROMISED CREDENTIALS

4 EDUCATE USERS ON IDENTITY HYGIENE... AND ENFORCE IT.

PAM can serve as a safety net against human error, but that doesn't mean your users can grow lax and leave themselves and your systems open to attack. 80% of all data breaches can be traced back to compromised credentials.[2] Make sure your staff and partners know what to avoid and what information should never be disclosed outside of narrow situations.

Your PAM infrastructure should give you good metrics and reliable feedback on which users are causing the most problems. When your privileged administrators review this data, they must be committed to rectifying it.

[1] 6 Unusual Data Behaviors That Indicate Insider Threat, Code42

[2] How Compromised Passwords Lead to Data Breaches, IDX

4 EDUCATE USERS ON IDENTITY HYGIENE... AND ENFORCE IT CONT.

This opens the door to CISOs having considerable sway over employees, perhaps even to the point of abuse. Make sure that, while your CISOs can shut off access, the reprimand of staff still falls to direct superiors and the human resources department.

Also remember that your vendors are beholden to your needs, including those of your risk posture. If you are entrusting them with any kind of sensitive user data, they must be accountable for its misuse. Make sure they are holding on to as little of your data as possible. Don't be afraid to push hard for security measures in initial contract signings. Be even more aggressive when overhauling existing contracts. If a vendor is unable or unwilling to make the changes needed, shop around for another.

The same applies to your employees. Be very serious and clear in precisely what constitutes a security violation. Do not back down from reprimanding employees who make avoidable mistakes, but also recognize when honest errors are made. In the latter case, be prepared to place extra security features on that employee until they learn how to use company resources safely. If they don't learn, you might need to let them go.

5 AUTOMATE AS MUCH AS POSSIBLE

Instituting advanced automatic systems enables all aspects of the previously discussed steps. Several of these, such as SSO and adaptive MFA, have already been covered. However, these solutions only improve your enterprise if they are enabled on all levels and are fully integrated across your entire identity fabric. That means administrating all those domains from a single source: PAM. How you implement the automation of PAM will ultimately determine the success of your digital transformation.

PAM is predicated on giving you control over who has access to what, yet too often can become a source of friction. By instituting role-based access control and other criteria checks for potential users, you get the benefits of gated access without the strain of continual human authorization. You enhance accessibility and security in a single stroke.

Zero-trust methods that rely on automation are also much more palatable to users and help enterprises not have to worry about growing friction. As previously mentioned, automation is key to systems such as adaptive MFA, role-based access, and most of all quick threat detection.

Automation also aids in scaling up your infrastructure. Application onboarding services can provide your enterprise with a clear protocol for building out additional functionalities without compromising security. Besides maintaining your strong risk posture, such services can reduce the cost of onboarding by up to 80%.[1]

Build out a strong self-service apparatus. Beyond enhancing your data monitoring capabilities, self-service provides a more frictionless interface, providing greater efficiency for your employees and a smoother experience for your clients. It can also give considerable savings from reduced help-desk incidents.

Human-centric security runs a high risk of being too little, too late. By enabling your PAM to automatically shut off and isolate access as soon as it detects something fishy, you get continuous “eyes” on your data and close to instant responses against bad actors.

Empower your digital transformation with advanced automation in PAM. From seamless integration across your identity fabric to frictionless access controls, automation ensures success. Embrace zero-trust methods, scale your infrastructure, and unleash the power of self-service. With automated threat detection and instant response capabilities, fortify your security and stay ahead of evolving risks."

[1] Application Onboarding, Simeio

? ARE YOU READY TO PUT THESE STEPS INTO PRACTICE?

Simeio can perform your assessment, create your action plan, implement your improvements, and maintain it all for years to come.

PAM with Simeio

- 60% faster deployment - Simeio partners with leading PAM vendors with best-in-class technologies and tools. Thus, with the expertise and experience to manage and operate PAM tools and technologies we enable reduction of deployment time.
- 95+ PAM certified experts effectively monitor and protect users with the highest access.
- Reduce risks related to privileged accounts and secure critical assets.
- Improve policy to ensure policies are continuously followed.
- Align compliance to improve the audit process and meet compliance guidelines.
- Improve visibility to identify and monitor both privileged accounts and usage.

IGA with Simeo

99.99%
Uptime Achieved

60%
Reduction in Help Desk Requests

85%
Time Savings in Provisioning

MANAGING IDENTITY MAY BE A CHALLENGE FOR YOU.
WE SIMPLIFY IT.