BeyondTrust

Managing Passwords & Local Administration Rights: a Two-Step Approach to a Secure Workflow

BY ABE SMITH
PRINCIPAL AT MSH CONSULTANTS

As a strategic director in the field of enterprise IT infrastructure and information security management, Abe Smith is dedicated to sharing his expertise in vulnerabilities management, configuration analysis, and IT operational strategy and implementation.

Information security starts with employee education. By now, most everyone knows the importance of security training and walking every employee through the dangers of phishing scams, ransomware, and other online threats. They must learn to use email, the web, and online tools safely, thus reducing the chances of a breach. But that's only part of the solution.

An informed workforce and robust IT policies are a strong line of defense, but you still need to establish winning conditions on the other side of the fence. To protect your infrastructure, you have to start by equipping your InfoSec team with multifaceted network management and security tools that reduce or eliminate security breaches—before they happen.

FROM FIREFIGHTER TO FIRE MARSHAL

I'm an independent information security professional. I ran a consultancy for 15 years, and I spent the last six years working in-house for a string of high-tech companies before going solo again.

My last position was really a dream job for me. Our CISO hired me as the company's Director of InfoSec. Everyone else who worked under him had clearly defined roles, but their sole focus was on putting out fires. There were issues left, right, and center, but nobody was looking at the bigger picture.

I didn't want to work in the trenches. Instead, I decided to take a holistic approach and was able to carve a niche for myself. It was apparent that stamping out one blaze after another was inefficient. We could never allocate enough people or time to plugging every security hole. It was a waste of resources, and it wouldn't take much for our costs to spiral out of control.

Instead of everyone being firefighters, I told our CISO that he needed a fire marshal. Rather than solving a specific security issue, I took a step back and analyzed everything that was going on. From this vantage point, I was able to spot patterns among the fires. I transformed my observations into insights that informed my strategic planning around countermeasures.

BeyondTrust

> Local admin rights, privileged access management, and password rotation are the basic foundation on which security is built. You can erect the most concrete steel-reinforced pillars, but they'll come tumbling down if the foundation on which they are built is weak. BeyondTrust ensures that your foundation is built on a rock instead of on sand.

PRIORITIZING PREVENTION

They say that "an ounce of prevention is worth a pound of cure," and that's exactly how InfoSec works. If you're trying to repair a breach after the fact, it's too late. The best approach is to figure out potential attack vectors and find ways to reduce the attack surface within the infrastructure.

We needed to set our priorities. To do this, our InfoSec team ran a penetration test to identify internal and external vulnerabilities. We analyzed the results, and our CISO then listed our top 10 security priorities. I went through his list and decided to focus on resolving those concerns that had the most impact, narrowing my scope to address our two biggest security holes: password vulnerabilities and local administration rights.

If you talk to any InfoSec expert, they will tell you that 8 out of 10 security breaches start with compromised passwords. If you tighten security around employee login credentials—and make it mandatory for them to use hard-to-guess passwords that they change regularly and two-factor authentication— you've solved the bulk of your problem.

Managing local admin rights is the other crucial issue. I believe 95% of people don't need or understand this level of control over their computer. They should never be granted permissions to perform unauthorized software installations or upgrades on their equipment.

A SOLUTION WITH PRIVILEGED ACCESS MANAGEMENT

The answer to our problems was privileged access management (PAM). PAM is a way to ensure that security managers maintain control over their sensitive data and systems. I was well-versed in this technology, but was really able to take the strategy to the next level once I found BeyondTrust.

I had seen BeyondTrust in action a few years back, but had gone with a competing product. My decision made sense at the time because I was dealing with a different set of issues. I kept an open mind this time around and decided to put their platform to the test. I set up a two-week "bake-off" to compare both solutions. We ran dozens of trials and simulations. After the dust settled, I was ready to make my choice, but I wanted a second opinion.

I asked my lead engineer whether he thought BeyondTrust was just as good as the other platform. He said it was not just as good—it was actually far better in terms of implementation, professional support, GUI, and functionality.

DEALING WITH THE HUMAN ELEMENT

I could have used brute force and pulled the plug on our existing password and permissions setup right away, rolling out BeyondTrust to everyone in the company at once, but that approach rarely works. No one wants to walk in on a Monday morning to discover that their computing environment has suddenly changed.

My CISO was nervous about the rollout, and rightfully so. He'd tried to implement similar measures before, but had trouble getting people to adopt a new system. I explained to him that we needed to start by acknowledging a basic fact: folks aren't always comfortable around new technology. You can't always be the all-or-nothing sheriff, threatening to lock up everyone who doesn't come on board. In order to drive

> I was lucky to get the nod of approval from these technical teams at the start of the process. They set up a BeyondTrust PoC in a sandboxed environment, ran a series of benchmarks, and confirmed the effectiveness of the PAM solution. They helped me speed its adoption by showing everyone that it worked.

long-term adoption, I find it more effective to take a softer, gentler approach. I like to start by working with those who are open to change and converting them into evangelists for the transformation.

First, I got everyone in our C-suite to buy into the platform. I then deployed BeyondTrust to everyone on my team, followed by early-adopter system administrators. There are always some glitches that arise during deployment, and it's beneficial to get people on board early who are not only enthusiastic about the platform, but who are technically capable of troubleshooting any problems. Once they'd found and fixed those early issues, they started encouraging other IT teams to embrace BeyondTrust.

I was lucky to get the nod of approval from these technical teams at the start of the process. They set up a BeyondTrust PoC in a sandboxed environment, ran a series of benchmarks, and confirmed the effectiveness of the PAM solution. They helped me speed its adoption by showing everyone that it worked.

Everything went smoothly from a technical standpoint, but my main concern with these rollouts is always the human element. It's only natural for people to resist when you mandate a particular approach to an activity or limit their access to previously available functions.

Getting everyone to adopt BeyondTrust's credential management features was one thing. You log in, follow instructions, and update your privileged passwords regularly. That small behavioral change meets with little resistance.

Changing local access privileges was another matter. Even though probably less than 5% of employees typically need or use full local admin access privileges, many of them will balk at the idea of someone robbing them of the freedom to make changes to their machines. Some people may even feel that you're revoking privileges as a type of punishment.

This second transition is not technological, but cultural. To successfully navigate it, you must advance slowly and socialize your workforce so that everyone understands the stakes. Start by explaining the new approach. Tell your employees why you're adopting new security rules and elaborate on the pros and cons. Most importantly, remind your people that you trust them and are restricting their access privileges so they don't have to worry about securing their machines.

IT WASN'T JUST BLACK AND WHITE

Our next step was to work with employees to establish a hierarchy of access privileges. BeyondTrust allows you to whitelist, blacklist, and graylist applications, thereby marking them as safe, unnecessary, or dangerous, or requiring more investigation, respectively. It also allows you to monitor the applications and upgrades your employees are installing on their computers.

Through this monitoring, we were immediately able to see how many people were putting new applications on their computers, and we started to understand their logic. We realized that, in most instances, users didn't fully grasp the implications of their software choices, so we made it our job to educate them.

When a user tried to install a whitelisted application, there was no security risk, so we let them proceed uninterrupted. If we'd graylisted the application, we received an alarm. We were then able to generate a pop-up window asking the user to explain

why they needed that application. If they provided a use case, they were allowed to install it immediately, while we received a daily report to review.

We were much stricter with blacklisted apps. If we received such a request from a knowledgeable worker—for example, a senior developer or an InfoSec analyst—we would approve its installation and generate a report explaining our authorization. If the request came from someone who didn't have an obvious need or the right qualifications to use the blacklisted app, we would ask them to justify it and then forward this information to the security team and the requestor's immediate superior.

Every night, we generated a report documenting all such requests. In this way, we could track employee demand for software that posed a moderate risk and evaluate the need to expand its availability or recommend alternative solutions.

We never shamed or accused our employees of wrongdoing. In most cases, they put in their requests because they didn't have all the facts they needed to make an informed decision. Often, their request was something as simple as trying to install an older version of a browser that was compatible with a particular plugin, but had known security issues. In such cases, an explanation was sufficient.

DOING YOUR HOMEWORK CAN TURN THINGS AROUND

At project completion, I knew I had helped them turn around their InfoSec culture and processes. Their infrastructure was much more secure, and their people were now taking password management and local access privileges seriously.

If anything, the restrictions imposed by adopting PAM freed everyone in the company to focus on using IT to improve business practices instead of worrying about potential breaches. In all my years in the InfoSec space, I have learned one thing: Do your homework. Evaluate threats, protect yourself against breaches, and adopt products and processes that protect your company's IT assets.

Also—and this is key—your InfoSec team's number one job is to make everyone's life easier, not to punish people. Local admin rights, privileged access management, and password rotation are the basic foundation on which security is built. You can erect the most concrete steel-reinforced pillars, but they'll come tumbling down if the foundation on which they are built is weak. BeyondTrust ensures that your foundation is built on a rock instead of on sand.

BeyondTrust provides the tools you need to stop security breaches before they happen. Its robust PAM tools protect you by securing passwords and managing access privileges. It blocks the most common intrusion vectors and frees your InfoSec team to be proactive instead of reactive.

Firefighters are everyday heroes, but IT professionals shouldn't have to be. In the end, wouldn't you rather prevent fires instead of putting them out?

“

BeyondTrust provides the tools you need to stop security breaches before they happen. Its robust PAM tools protect you by securing passwords and managing access privileges. It blocks the most common intrusion vectors and frees your InfoSec team to be proactive instead of reactive.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering companies to secure and manage their entire universe of privileges. The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Learn more at beyondtrust.com