simeio
Identity, intelligently managed.

Check Your Armor

WHAT'S YOUR MOST VULNERABLE CYBERSECURITY SPOT?

CHAPTER 1:

Check For Common Mistakes

CHAPTER 2:

Check Your Perimeter

CHAPTER 3:

Check For Infection

When a company experiences a data breach, hack or other compromise to infrastructure or assets, a post-mortem is usually conducted to look at what went wrong. More often than not, senior leaders are surprised and dismayed by what they hear — the processes or policies that were overlooked, or the risks they didn't realize existed.

Acknowledging errors is merely table stakes, however. CISOs and their colleagues need to get one step ahead by offering better education and training, addressing areas of vulnerability and building a "security-first" culture.

That's why we have put together this comprehensive checklist of all the questions, gaps and mistakes you need to talk about...before a disastrous incident can happen!

CHAPTER 1:

Check For Common Mistakes

Is your company making the following mistakes? If you're not in IT or security yourself, print this out and march it over to your IT department now.

The '1, 2, 3, 4, Open Door' Mistake

It's one of the oldest security blunders in the book, but too many companies fail to enforce strong password policies. The right tools and technology will ensure passwords are better than "admin" or "1234," but think about how you can make the job easier early on. It could be a lunch n' learn that demonstrates how cyberattacks can begin by guessing an easy password, or information during employee on-boarding about how to create and update passwords.

The 'But I Didn't Know They Could Do That!' Mistake

You wouldn't give the same degree of access and control over information to a junior employee as you would the CEO. Would you? Establishing policies that spell out the degree of access and authorization up front is one of the best ways to ensure insider threats, such as disgruntled employees, don't blow up into data loss, business interruption or worse.

CHAPTER 1: CHECK FOR COMMON MISTAKES

The 'I Thought They Still Worked Here' Mistake

Employees may get an exit interview where they talk to HR and hand over their key fob, but system credentials can be left untouched long after staff depart in some cases. That's a huge trap door that can be easily remedied by tools to monitor and close off access where it's no longer necessary.

The 'But It Looked Legit!' Mistake

Phishing schemes, where employees open an email message and click on attachments they shouldn't, seem to trip up at least one company a year. Use an intranet, lunch n' learn and any other opportunity to explain to your team what genuine communication from the company will look and sound like, and the kind of links they should report as soon as they spot them. Help the lessons stick by performing phishing awareness tests. But make sure they go beyond assessing employees' knowledge of traditional scams — such as emails purporting to be from Paypal, Wells Fargo and UPS. On tests, emails from these sources get much lower click-through rates (1-5% range) than "spear phishing" campaigns, showing click-through rates upwards of 40-50%.

CHAPTER 1: CHECK FOR COMMON MISTAKES

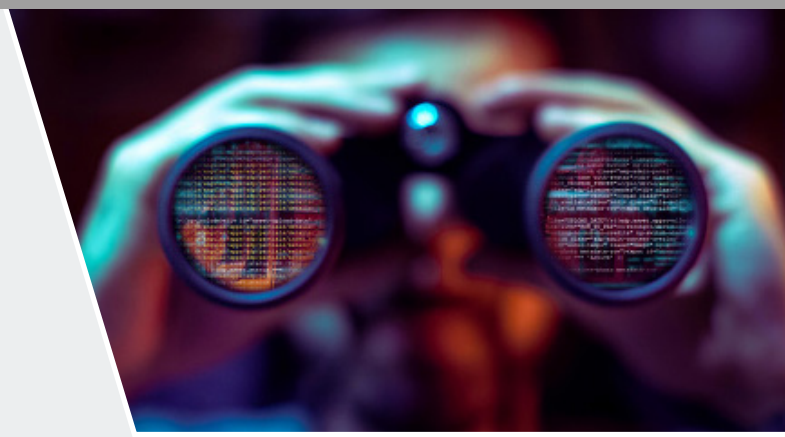
The 'I Just Left It For A Second' Mistake

Mobile devices are great ways to empower employees to be productive outside the office — until they put them down unwittingly and let others tamper with the applications. Even desktop systems can be compromised with offices that are left unlocked. Strong identity management strategy factors in here. It can help ensure that your access is safe from third parties who may happen to wind up with it.

WHAT'S IN A WORD?

If this list seems overwhelming, it's a lot easier to tackle with a partner who can help address all these mistakes, and more.

SIMEIO OFFERS THE IDENTITY ORCHESTRATOR PLATFORM, designed to simplify the operation of complex, multi-vendor IAM and security infrastructures. Identify users, behavior patterns and bring more security to your perimeter.



CHAPTER 2:

Check Your Perimeter

Physical boundaries, firewall boundaries, security domains, forests, realms and virtual networks... none of those matter if a single logon credential that can access multiple domains is compromised.

The statistics bear this out. In fact, the recently released 2017 Verizon Data Breach Investigations Report (DBIR) showed 81% of data breaches were only possible because hackers were able to get their hands on stolen and/or weak passwords. In other words, identity is the perimeter.

HERE ARE A LIST OF QUESTIONS FOR YOU TO POSE TO YOUR CISO:

How should we authenticate?

Every mission-critical system should require proof of the user requesting access and employ methods such as Single Sign-on (SSO), federated and multi-factor authentication. Determine how strict these controls need to be, based on the data you're protecting. The best solutions need to be frictionless for the end users to avoid shadow IT.

What authorization level is required?

Not every employee should have the same degree of access. Determine what's most needed by particular job functions or levels of authority. Eliminate shared accounts and restrict admin access to least privilege principles.

Where can we ease administration & auditing?

IAM should safeguard data without hindering business processes. It's important to continuously monitor and review access to ensure end user access is granted based on the rules you've established.

CHAPTER 2: CHECK YOUR PERIMETER

In a world of permeable borders, Identity is the key foundation for security in the cloud, but it needs to be implemented correctly. A sound IAM strategy means your organization will not only be able to keep cybercriminals and insider threats at bay but can also deploy new enterprise applications to remote teams with peace of mind. Reinforcing identity means your perimeter will be better protected, ensuring employees have access only to the data that is relevant to their job.

Backed by Simeio Identity Intelligence Center, Simeio Solutions delivers Identity as a Service (IDaaS) and expertly managed IAM services to reinforce your perimeter. Simeio is the first and only solution designed to protect corporate resources and information by monitoring the use of digital identities and access privileges and leveraging IAM data to deliver actionable business intelligence.

Ready to talk to one our experts about your identity management needs? Book your free consultation today.

CHAPTER 3:

Check For Infection

There's good reason security experts refer to hackers "infecting" corporate IT systems with a "virus." Like almost any illness, cybercrime is a largely a process of getting past the victim's initial defenses, spreading as far as possible and finding a way to stick around permanently.

As the recent 2017 Trustwave Global Security Report shows, cybercrime is becoming nearly as prevalent as the common cold. The study said that 43 percent of security incidents that its researchers tracked involved corporate or enterprise environments. More than half involved payment card data, and 86 percent of the malware used by hackers could obfuscate or encrypt itself to try and avoid detection.

While those stats could leave companies feeling overwhelmed about how to protect themselves, there's one symptom that stands out: insufficient security around privileged credentials. These include SSH keys and certificates, of course, but also admin credentials that offer cybercriminals the power to take over entire networks.

According to a recent research report, 80% of data breaches involve privileged credentials, and the latest Verizon Data Breach Investigations Report found 81% of incidents were caused through stolen or weak passwords.

Fortunately, we can approach cybercrime in much the same way that we combat common illnesses: by gaining a better understanding of how they work and bolstering our defenses. In this case, that means privileged identity management (PIM).

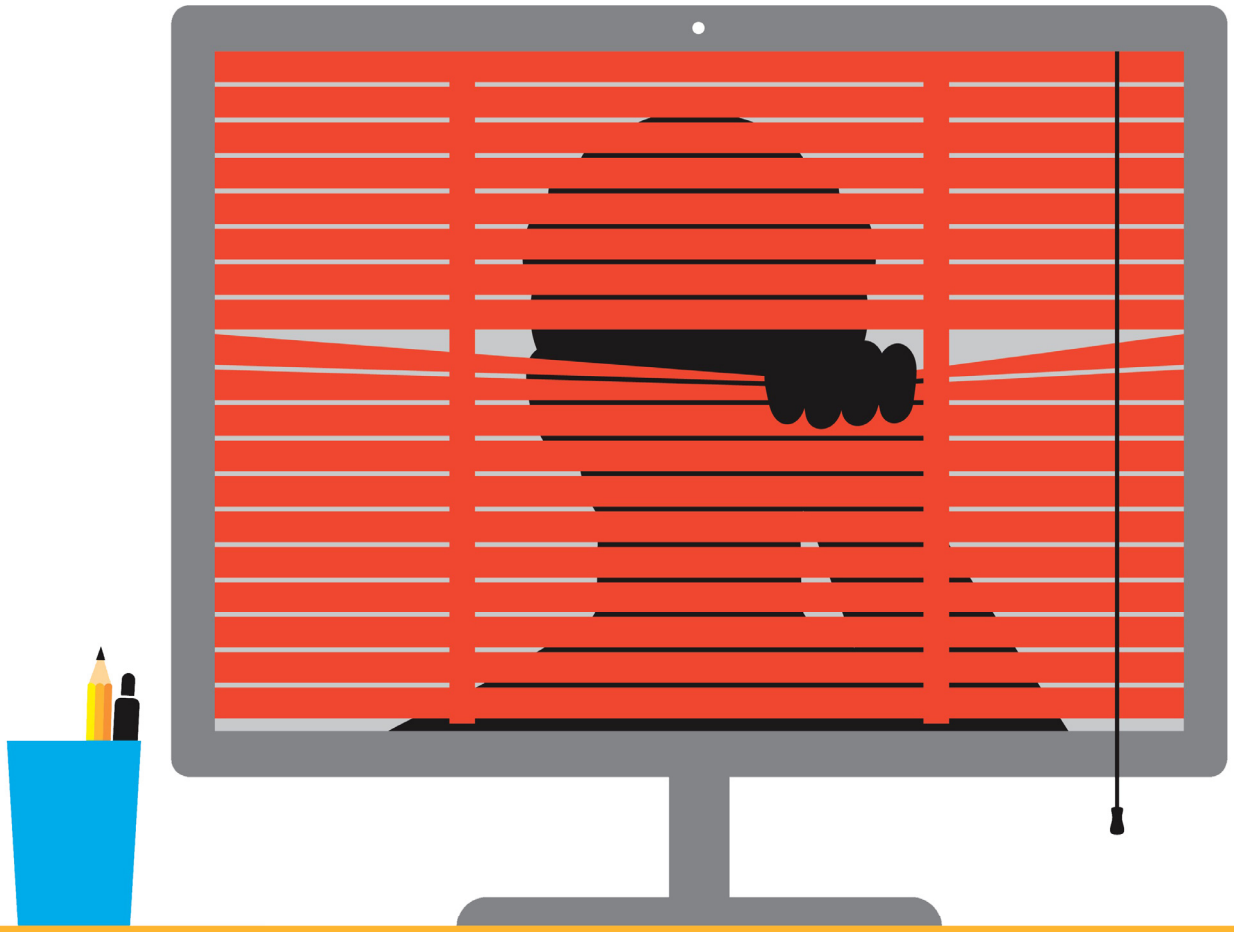
CHAPTER 3: CHECK FOR INFECTION

Take the "temperature" of your superusers

When humans get sick, the effects are often highly visible, from watery eyes to sneezing or coughing.

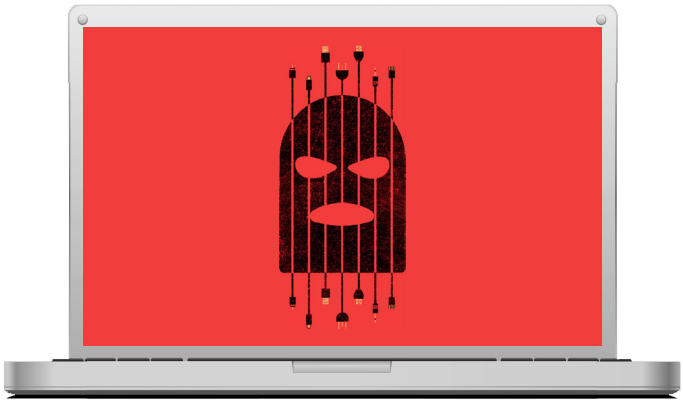
Cybercriminals use social engineering tricks such as bogus e-mail messages with links that lead to exploit kits or zero-day attacks. When you don't even know you're getting infected, it can become difficult to ward off an illness. Enterprise IT is no different. **There can be an extremely small window of opportunity to batten down the hatches before hackers discover credentials that let them open doors to more critical areas of the network.**

Early adopters of PIM have already discovered that the right technology can not only monitor important credentials on a regular basis but, in the event of suspicious behavior, ensure they can be randomized or replaced with a unique value.



CHAPTER 3: CHECK FOR INFECTION

Take the "temperature" of your superusers



What sometimes feels like a simple cold can turn into the flu almost without warning. Of course, viruses are hard at work behind the scenes, making sure they find any avenue possible to battle our immune systems. So it goes with cyberattacks, where compromised machines are systematically mined for as many passwords and other credentials as possible. This means it's possible for an initial breach to become far worse, with increasing tiers of critical data throughout the network potentially exposed to bad actors.

Think of PIM solutions in this scenario as a sort of law enforcement official patrolling the IT environment. Its role could include changing SSH keys or moving them to a more secure location where necessary. The same technology can isolate interdependencies between and make sure they are updated so hackers can't escalate their attacks. From a policy perspective, PIM limits the use of certain credentials to minimize the propensity for abuse from third parties.

Shut it down!

There's sick, and then there's really sick - like a long-term disease with little hope in sight. That's the scariest scenario in an IT security context; when cybercriminals attempt to take over ticket granting services to maintain their place in the network and become ever more difficult to remove.

The best PIM play here includes wiping out the memory of hashes and passwords on systems infected through an automated, "chained" reboot. Another option could involve copying passwords when they're being changed to stop tickets that aren't legitimate before further damage can be done.

Simeio is a complete Identity and Access Management (IAM) solution provider that engages securely with anyone, anywhere, anytime, with an unparalleled “service first” philosophy.

Contact us now to set up your free consultation.

simeiosolutions.com