Prevent Insiders from Breaching Your Data

Devolutions

AND WHAT IF THAT THREAT WAS ACTUALLY COMING FROM THE INSIDE?

Companies like Yahoo, eBay and Equifax all learned the hard way that protecting your data from hackers is of the utmost importance. I mean, a data leak can ruin your company's reputation forever. But did you know that you might have a bigger problem than outsider threats?

And what if that threat was actually coming from the inside? Is your company ready for that?

Here's some food for thought: 8 out of 10 breaches require the assistance — intentionally or unintentionally — of internal users!

To turn a blind eye to the problem of insider threats would be a big mistake. It's time to take the bull by the horns, face the problem, and take the appropriate measures to protect your privileged accounts from any kind of attack.

THE REASONS BEHIND AN INSIDER BREACH

Here are some of the ways insider leaks most commonly happen.

THE ACCIDENTAL LEAKER :

These are users who fall victim to a phony "phishing" email, text, IM or social media message. Many of these campaigns are designed to deploy advanced persistent threats (APT), which means that nobody knows that devices/networks have been breached for quite a while. According to research conducted by the Ponemon Institute, it takes organizations an average of 6 months to detect a breach — and many take over a year, as was the case with the notorious Sony breach.

THE COMPROMISED INSIDER :

These are users whose identity and/or devices have been compromised by hackers. While all users are at risk of this, sysadmins, network engineers, database administrators, and other privileged users have a big (virtual) target on their backs at all times.

THE DISGRUNTLED EMPLOYEE :

These are users who are mad at their employer (or certain colleagues) and try to exact revenge. Often, these unhappy users work behind the scenes so they can wreak havoc and cause misery.

THE DOUBLE-AGENT :

These are users who act happy and compliant, but behind the scenes they're stealing data for rofit. And if that's not scary enough, the courts are starting to hold employers "vicariously liable" for the financial damage caused by rogue employees.

10 QUESTIONS TO HELP PROTECT YOUR ORGANIZATION FROM INSIDE THREATS

Without further ado, here are 10 questions to help your organization a avoid getting hacked due to accidental leakers, compromised insiders, disgruntled employees, and double-agents:

1. ARE YOU WATCHING YOUR PRIVILEGED ACCOUNTS?

It's critical to constantly monitor all privileged account activity through a centralized platform (instead of "one ring to rule them all", it's more like "one software to watch them all").

It's also important to get real-time alerts when any suspicious activity is detected, such as a sudden spike in data exiting your network to the outside world — which could mean that a disgruntled employee or double-agent is operating.

2. DO YOUR SECURITY POLICIES AND PROCEDURES COVER INSIDER THREATS?

It's not enough to have robust and comprehensive policies and procedures to guard against external threats — you also need to thwart internal threats, too. These policies and procedures should include the right mix of tools, technologies and workflows.

3. DO YOU REGULARLY AUDIT PRIVILEGED ACCOUNTS?

You should know who has access to privileged accounts, and why that access was granted. Remember: the more privileged accounts there are in your organization, the larger the threat surface that hackers can attack. Adopting the principle of least privilege is wise, as is using tools like security keys and biometric identification to augment passwords (which of course must be strong and unique!).

4. CAN YOUR CURRENT SECURITY TOOL DETECT A BREACH CAUSED BY INSIDERS?

Let's say someone inside your network is trying to leak sensitive data or compromise one of your privileged accounts at this very moment. Would you even know it? Would your current security tool detect the breach? If not, then upgrading to something safer should be your top priority.

5. IS YOUR SECURITY BUDGET PROPERLY BALANCED?

It's important to ensure that your security budget is sufficient to protect against external and internal threats — not just the former. If it isn't, then you need to boost the budget and re-balance your security profile.

6. ARE YOU USING A GOOD PASSWORD MANAGEMENT SOFTWARE?

Good password management software (like RDM and DVLS!) helps you control access to privileged accounts, generate strong passwords, vault end-user passwords, and securely store passwords in a centralized location. For a comparison of some popular password managers, click here.

7. ARE YOU DOING EVERYTHING YOU CAN TO AVOID PRIVILEGE CREEP?

It's really important to avoid "privilege creep." This is when a user accumulates different access privileges for the various roles they've held in an organization over the years. Make sure that everyone has the access they need for their current role: no more and no less.

8. ARE YOU LOOKING OUT FOR BEHAVIORAL SIGNS?

No, you don't have to start acting like Dr. Phil. The idea here is to pay attention to unusual behaviors that could point to potential trouble. For example, let's say that a user:

- Wants access to a privileged account that is not typically associated with their role.
- Starts taking home sensitive data.
- Starts working late and on weekends.
- Starts getting stressed out and nervous at the announcement of a security audit.

Now, all of the above may be perfectly legitimate and mean nothing. Truly, the stressed out and nervous employee may just be stressed out and nervous (hey, it happens to all of us). Or, the user who wants to work late or take data home may be part of a project where this is necessary. But then again, it might be a sign that something untoward is happening — or is about to happen.

It's important not to jump to conclusions, or accuse employees of doing something wrong without verified evidence. And even then, your organization must comply with prevailing human resources policies and labor laws, or else you could get in trouble (and your reputation could take a big hit).

9. DO YOU KNOW WHAT DOCUMENTS YOUR EMPLOYEES HAVE ACCESS TO?

Most employees have no idea the level of confidentiality of some documents; all they know is that they have access to the documents they need to work in. It's imperative to constrain permissions, control access and ensure that employees only have access to the documents they need based on the principle of least privilege.

10. WHAT TOOLS ARE YOUR EMPLOYEES USING TO SHARE FILES?

Do you know where your organization stores data? What tools are employees using when accessing data remotely? Is it through a VPN? Is it secure? And it they're copying files on their personal computer, is it safe and protected from outside threats? Make sure to know what your employees are doing when it comes to sharing files, and if necessary, provide training and coaching to enforce compliance.

PLAY IT SAFE

The business landscape is full of opportunities and innovations — but unfortunately, it's also full of risks and threats. Preventing insiders from intentionally and unintentionally breaching data will help your organization stay safe by reducing the chances of being victimized by accidental leakers, compromised insiders, disgruntled employees, and double-agents.

As always, please let us know your thoughts by using the comment feature of the blog. You can also visit our forums to get help and submit feature requests, you can find them here.