MICRO FOCUS

Flash Point Paper

Security

Advanced Persistent Threats: Insider Credentials at Risk

Can You Shut Down a Security Threat Before It's Too Late?

These days having an identity and access management solution is a must. Businesses cannot operate without knowing who their employees are and granting them appropriate access. However, this begs the question: are you sure the identity credentials used to access your systems are being used by the correct individual?

Most organizations work hard to ensure that they're compliant with corporate security policy and governance requirements. But that doesn't necessarily mean that they're protected. With most cyber-attacks, the damage is done long before any corrective actions can be taken. Managing identities is essential—but it can also lead to a false sense of security if you can't track the behavior of that identity. Specific log-in credentials may look fine, and certain behaviors may be appropriate, but do the credentials and the behavior make business sense? If you can't interpret activity in the context of identity, your organization may be at risk.

This sort of behavioral tracking may make obvious sense for highly regulated industries, such as government or finance. In order to continue to operate, these organizations must maintain a high level of trust from their constituencies, who want to know that their information is protected. This need for public trust is why these industries are regulated in the first place. But increasingly, businesses in any industry can be the subject of attacks, and those attacks don't always target the things you'd expect. Any sensitive information can be at risk if you don't know what people are doing with their access.

Crippling and Hard-to-Notice Threats

Security was once focused on securing and "walling off" key data, but today's cyber threats follow a less linear path. "Advanced Persistent Threats" (APTs) consist of teams of attackers who work day and night to infiltrate a network by compromising insider credentials, and continuously extract data while remaining undetected. These attacks are frequently focused on meticulously expanding access so that they can infiltrate deeper or reach further into other companies.

In 2009, an email account belonging to a Twitter administrator was compromised. Usually, this wouldn't be a corporate problem, but that personal breach was used to infiltrate the employee's Google Apps account. Twitter was using Google Apps as a way to share sensitive documents and information. The challenge for Twitter was that the employee had a known, trusted identity. Accessing the documents was not suspect behavior. Twitter lacked the ability to apply policy to the activity, and because of this, they were unable to see if accessing sensitive documents (and forwarding them) was appropriate for that user. In fact, Twitter didn't even realize the extent of the breach at first.

The Twitter breach was more embarrassing than damaging, but these types of attacks are increasingly common. Recently, the U.S. Department of Homeland Security identified a coordinated campaign of cyber intrusions targeting the energy industry. The intent of the hackers is unclear—as there is no evidence that data was compromised or that malicious action was taken. However, the attacks provided access to critical control systems, including those for major natural gas pipelines*.

Questions to Ask Yourself About Identity and Access Solutions:

- *Do you have an identity and access management solution? (If not, stop reading this paper and go get one.)*
- *Can you monitor activity on your network?*
- *Can you link activity to an individual?*
- *Do you know which individual is responsible for which activity?*
- *Can you take immediate action when the users' actions don't match what the individual should be doing?*

---

* Written testimony of NPPD for a House Homeland Security Subcommittee on Cybersecurity hearing titled "Facilitating Cyber Threat Information Sharing & Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities." **www.dhs.gov/news/2013/05/16/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity-hearing**

93.6%

of 1,551 CISMs (Certified Information Security Managers) & Information Security Professionals feel APTs are a serious threat.

Source: ISACA Advanced Persistent Threat Awareness Study 2012

As was the case with the Twitter incident, the breach was not catastrophic. However, had the hackers intended harm, reactive analysis and response would not have prevented a potentially serious problem.

The reality is that the nature of security threats has changed. A firewall protecting information is not enough anymore. There are too many indirect routes to sensitive information and systems. But at the same time, you can't just completely shut things down; people still need access. In the new paradigm, security is not just about preventing access but also actively monitoring it. How can you maintain security and compliance before the damage is done? The key is to figure out where the threats are and take appropriate preventative action.

Automating Real-Time Threat Response

Taking preventative action is easier said than done. Critical breaches can happen so fast that you can't rely on human intervention to respond in a timely manner. The key is to have an automated system in place that is ready to respond.

Automation makes real-time threat response possible. Ideally, a set of policies can be established so that a system can constantly monitor behavior and immediately identify and alert on suspicious activity. For example, a typical financial transaction may need to touch an identity management system, an end-user terminal and a transactional database before it is complete and funds are disbursed. The identity management system verifies the user's identity. The database generates log data, and a Security Information and Event Management (SIEM) system tracks every action that the user executes on these applications. If, however, an employee has administrator access to the database, and their account is compromised, that account could conceivably circumvent the established process—the process that external customers are forced to follow—and initiate an unauthorized transaction, the result of which could be theft. In an ideal world, your system should be able to identify these actions as suspicious and shut them down automatically, in real time.

Some businesses today are adopting an approach to security that is similar to that of a Las Vegas casino. Casinos let anybody come in the door, but they monitor their activity. While most businesses would want to maintain a certain level of credentialing, automation allows for a similar concept. You want to be able to keep critical information safe without impeding user activity. Policies establish expectations and thresholds for a breach in protocol. This can be transparent but effective security. This approach to security can be particularly valuable for universities or other institutions that need to have a significant amount of data sharing while still shutting down activity that violates a defined set of parameters.

Identifying and Selecting Solutions for Modern Security

Security threats have changed, and organizations must change their mindset and approach accordingly. You have to adopt a more comprehensive approach to not only security but activity as well. As you look for solutions, there are some important things to consider. Make sure that the solution you choose can:

1. **Link to your identity and access system—and, in a perfect world—link to your Security Information and Event Management solution**

2. **Allow you to establish a granular level of policies around behavior**

3. **Enable tiered, automated responses.** As security threats evolve, your response should rise to the challenge. Like a vector, your security direction and speed need to change to meet the pace at which our increasingly tech-oriented world is moving.

Find out more by visiting here.