User Threats Vs. User Privacy

Striking the Perfect Balance

Dimitri Vlachos is the vice president of marketing at ObservelT. He has more than 15 years of experience as a marketing leader in both start-ups and established corporations. He has extensive experience with industry analysts in the security, network performance and application performance markets.

On the one hand, user-based attacks—whether from hackers using stolen credentials, careless third-party vendors, or negligent or even malicious insiders—represent the largest IT security threat to organizations. On the other hand, no one wants to work in an environment where their activities are constantly being monitored. So, should companies watch everything their employees are doing? Or, should they blindly trust them to safeguard company data? The answer is: Neither.

Disponible également en français
www.isaca.org/currentissue

THE NATURE OF USER-BASED ATTACKS

Typically, user-based attacks come in two flavors: a disgruntled employee or a hacker using stolen credentials. These attacks are usually the fault of an employee, knowingly or unknowingly; 82 percent of data breaches are caused by employee error.[1] Regardless, these individuals are able to bypass infrastructure-level defenses with their authentic login credentials. Once inside the system, these users begin to execute on their agenda.

User-based activity monitoring solutions were designed to provide insight on these threats from the perspective of the user. This technology can track every action taken by authenticated employees, vendors and partners, regardless of how they connect or which applications they access. And, it aggregates screen captures throughout the process to collect video footage on exactly who did what and when.

As it turns out, more than 67 percent of data breaches involve stolen credentials.[2] Even those hackers who start with information from low-ranking employees or vendors are capable of finding ways around internal roadblocks, disabling firewalls, extracting data and installing malware.

Analytics are the best defense against this type of attack. Comparing user actions against their known user profiles, job descriptions, usage patterns and other intelligence helps security teams quickly sniff out anomalous, suspicious and out-of-policy behaviors. For example, companies can quickly see if an employee or trusted vendor changed a firewall setting, executed a DROP command from a database or ran a screen-sharing application while looking at CRM records. Today's solutions are extremely sophisticated; they can even notify a hospital when a nonattending physician accesses the files of a patient or flag a vendor attempting to access a point-of-sale (POS) system.

THE IMPORTANCE OF IT FORENSICS FOR INCIDENT RESPONSE AND COMPLIANCE AUDITS

One of the most difficult tasks security professionals face is reconstructing what a hacker did once inside. Many IT departments rely on system log files to provide the details. Unfortunately, this approach is both time-consuming and full of knowledge gaps. System logs were not designed to provide a full accounting of user activity. Because they were created to provide developers with much needed intelligence on software defects, it is extremely hard for the average person to distinguish meaningful user information from system details. Not every application provides log files, which means that even those companies that aggregate all their log-based data using a central security information and event management (SIEM) system will have trouble piecing together a seamless, 360-degree view of user activity.

On the other hand, user activity monitoring solutions follow authenticated users as they travel the network, access files and use applications while also recording every keystroke, preference and option they select. Forensic investigators can simply play back video footage of exactly what a user did to gain empirical evidence of illegal activity. More important, companies can quickly identify the culprit—or at least the user whose credentials were compromised—and quickly shut

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:

down the account. And, they can see exactly what was stolen, which customer records were comprised and which systems are still vulnerable. Armed with this level of information, companies can more quickly rectify the situation.

As an added benefit, user activity monitoring solutions provide irrefutable evidence as to a company's compliance with Payment Card Industry (PCI), North American Electric Reliability Corporation (NERC), US Federal Energy Regulatory Commission (FERC), and US Health Insurance Portability and Accountability Act (HIPAA) regulations, among others governing the access and use of sensitive data.

WHAT TYPES OF ACTIVITY SHOULD BE MONITORED

For the most part, companies are not concerned about the personal lives of their employees. The exception, of course, is when that personal behavior can adversely affect corporate security. For that reason, every action a user takes after authentication—and while on the corporate network—should be monitored, recorded and stored. Hackers are extremely adept at covering their tracks and maintaining a low profile once inside. If the monitoring system were to stop monitoring while users went on Facebook or only track activity across specific programs, the gaps could provide key escape hatches for obscuring illegal behaviors. Although every action is being recorded, only suspicious activities should trigger alerts.

HOW TO COMMUNICATE MONITORING POLICIES

Companies must notify employees and any third-party users that their actions are being monitored. To start, organizations need a policies and procedures document that clearly defines what the company monitors, how that information is used and what constitutes acceptable behavior. Users should fully understand that all actions, including individual keystrokes, are recorded, but only those actions with security implications are scrutinized.

All users should be given policy information along with their login credentials. Depending on the size of the organization, human resources (HR) departments can include a review of this information during the employee orientation process.

Companies should also remind users that they are being monitored. Notifications and important policy messages can be built into the monitoring software and presented at user login. Requiring users to confirm before continuing ensures that policy messages have reached their targeted users.

THE CONCEPT OF IT DETERRENCE

Informing employees, vendors, partners and other users trusted with authentic credentials that they are being monitored goes a long way toward deterring abnormal, illegal and out-of-policy behavior. After all, someone is much less likely to commit an illegal act in front of a video camera.

FINDING THE RIGHT BALANCE

When it comes to security, companies need to use every available defense to protect valuable assets and sensitive information. While user activity monitoring is the best protection against the threat within, companies need to be smart about it. The key is communicating openly with employees and trusted third parties to ensure that they fully understand corporate initiatives, policies and procedures. Such a system is best used for incident response, compliance audits and, in fact, protecting a company's users themselves from being held accountable for actions a hacker may take with their account. Employees and partners should understand that this system is not designed for monitoring their day-to-day activity, snooping on their browsing history or making them feel scrutinized. With a balanced approach to monitoring and privacy, companies can deploy user activity monitoring solutions to protect themselves and their users.

ENDNOTES

[1] Fogarty, K.; "82% of Data Breaches Due to Staff Errors; 4% of IT Trusts Users; IT Is Still to Blame," *ITWorld*, 19 April 2012, *www.itworld.com/article/2729066/security/82--of-data-breaches-due-to-staff-errors--4--of-it-trusts-users--it-is-still-to-blame.html*

[2] Verizon, *2014 Data Breach Investigations Report*, March 2014, *www.verizonenterprise.com/DBIR/*