FEBRUARY 13, 2017

Legaltech® news

ONLINE

An ALM Publication

Can User Behavior Analytics Do a Better Job of Protecting Your Data?

The bulk of spending on cybersecurity in large organizations has been toward perimeter tools like firewalls. And yet the relentless pace of major data breaches has shown no signs of letting up.

By Jason Straight

IT security professionals will tell you that the bulk of spending on cybersecurity in large organizations in recent years has been toward perimeter tools like firewalls, antivirus systems and signature-based digital gatekeeping systems. And yet the relentless pace of major data breaches has shown no signs of letting up.

Why? In part it's because the perimeter itself is eroding. The benefits of mobility and round-the-clock productivity are simply too compelling for most organizations to ignore, and the result is that more and more devices are accessing enterprise networks. Organizations continue to outsource more functions to non-employee contractors and vendors, who often require network access to be effective. And the much-hyped "Internet of Things" (IoT) opens networks up to yet another huge class of "authorized devices," which can be exploited to orchestrate significant mischief, as the recent hacker attack on the Internet infrastructure company Dyn demonstrated so decisively, achieving sustained disruptions of service from some of the world's most prestigious online properties, including Netflix, Twitter, Amazon and Tumblr.

So, while spending at many organizations still tends to focus on perimeter defenses, security experts have begun to face the reality that it is nearly impossible to keep bad actors out of your network, and are turning their attention to better ways of mitigating threats posed by intruders once they've hacked their way in. Of course, it's not just hacker-instigated breaches from which we need to defend. Recent surveys suggest that insider threats — from trusted employees and other authorized users in possession of legitimate credentials — account for somewhere between 20 percent and 60 percent of today's data breaches, and perimeter defenses are not equipped to stop them. Awareness of the potential danger of insider attacks, in fact, is an important factor in an upsurge in interest among cybersecurity professionals in user behavior analytics (UBA).

How User Behavior Analytics (UBA) Works

UBA is a promising adaptation of an array of "big data" science techniques known as data analytics. UBA performs real-time monitoring, correlation and analysis of event data and activity logging that digital systems routinely and constantly record as a matter of course. Given that even mid-size companies typically have tens of thousands of devices communicating with their networks every day, such activity

generates massive amounts of data that may contain clues leading to detection of an attempted incursion or attack. Relying on human labor and expertise to sort through and interpret the security implications from such massive volumes of information would be impossible, but UBA combines powerful computer systems, advanced applied mathematical models, and business and behavioral intelligence to analyze the data, ferret out anomalous activity that would otherwise go undetected, and alert security professionals to issues that may warrant immediate attention.

UBA also has the capacity to "learn" from ongoing inputs, so over time its ability to distinguish normal patterns of usage from potentially dangerous signals becomes more robust and discriminating. UBA does require careful management — a topic we will explore in more detail later — but, unlike perimeter defense tools, it has the unique ability detect unusual or suspicious activity carried out by malicious or careless insiders who have access privileges to the network and may be using those privileges in unauthorized and harmful ways.

When properly configured and deployed, UBA's ability to identify and flag potentially dangerous insider activity can add a very powerful weapon to the enterprise-level cybersecurity arsenal. Think about what would happen in your own organization if, say, a trusted mid-level staffer logged into your network through a VPN connection at an unusual time — 2:00 a.m., perhaps — and spent a few hours accessing various servers and dozens or hundreds of files. What if many of the accessed files were in locations that person had never visited before, and at the end of the session the files were saved in a compressed and encrypted folder? If no malware were detected and the IP address was clean, would your security system be able to identify this activity as anomalous and potentially devious? Would the activity ever come to light? In most organizations, the answer would be no — unless they already had a well-managed UBA program.

Profiling Users and Setting Alert Thresholds

A UBA system's ability to detect anomalies and issue alerts when there are reasonable indications that something might be amiss depends in part on the system's understanding of what is "normal" behavior on the part of a user. To work properly, the system must have accurate information about individual users' roles and responsibilities, including attributes like job title, position in the organizational structure, peer groups or teams the individual routinely works with, normal work hours, work locations, network access permissions and so on. With UBA, that information is correlated with automatically compiled data about an individual's computer-based activities, such as IP address, log-in and log-off times, server access attempts, files opened and downloaded, website visits, print jobs, etc.

A major task in managing UBA involves setting appropriate alert thresholds. A typical approach is to assign individual users to peer groups comprising colleagues who have similar functions and access permissions. Each user is also assigned a baseline risk score. At the lowest end of the risk spectrum would be someone like a part-time administrative staff member with very limited access to the network. At the highest-risk end would be a network administrator with virtually unlimited access to the entire IT infrastructure. An individual's risk score determines the sensitivity of anomaly detection and the degree to which an anomaly is considered critical. The threshold for triggering an alert would, accordingly, be much higher for a low-risk employee.

Typical Use Cases

We've already presented a scenario in which a malicious insider might use authorized access to an organization's network to covertly gather information for potentially harmful purposes. Insiders who engage in unauthorized activities inside the network represent a range of motivations and tactics. An employee who is about to leave the organization may decide to take information she considers her own property without realizing she is violating company policy. On the other hand, you may have an employee who has a financial motive to steal and sell large quantities of proprietary information to a competitor, appropriating relatively small chunks of data over an extended period of time in order to avoid detection. In both cases, UBA can help identify suspicious activity early and limit the damage. For example, a common application for UBA would be to input a daily list of employees who have submitted resignations and look for correlations with higher-than-usual file access, download or print activity over a specified period prior to the resignation.

Other use cases for which UBA is especially well-suited include:

- Monitoring third-party activity: If a user working for a vendor one day pivots from the vendor portal to other parts of your network, a properly configured UBA should detect that activity and issue an immediate alert.

As more non-core business functions are delegated to outsourcers, UBA's ability to mitigate the consistently underestimated risk of granting outsiders access to the network will become increasingly important.

- Monitoring the exfiltration of sensitive data: UBA can be configured to monitor the movement of an organization's most valuable data assets, including intellectual property, trade secrets, customer lists, forecasts, pricing info and sensitive employee data.
- Detecting the use of compromised credentials: UBA is very good at detecting subtle changes in user behavior that may indicate an outsider has gotten access to legitimate account credentials. Changes in "normal" activity that may indicate a problem may be revealed by the timing of log-ins and log-outs, connection from an unrecognized IP address, unusual Internet browsing and visits to network locations that are a departure from the user's typical activity.
- Preventing the misuse of high-privilege accounts: These cases represent some of the highest-risk incursions an organization can face. UBA is uniquely suited to monitor "super users" with broad privileges and high levels of technological sophistication. For example, UBA systems can be set up to profile masking behavior, such as the deletion or modification of logs and event data, and create alerts to detect it. In this case, UBA monitoring is most effective when combined with smart policy controls that set strict limits on the number of high-privilege accounts and establish highly specific limitations on how those accounts can be used.

Human Judgement and Business Context Still Matter

UBA is a very powerful tool, but it is not a panacea. Companies that adopt it must understand that a UBA program requires significant investment — not just in the technology itself, but in the resources required to train staff to implement and continuously manage it. A hasty rollout and a plethora of false positives have the potential to adversely affect an organization's overall security culture. False positives in particular need to be handled with extraordinary sensitivity so that valuable and committed employees don't reach the conclusion they are no longer trusted. Organizations should be encouraged to be transparent with their employees from the beginning about the implementation of UBA and how it will be used. User awareness training is almost always a good idea when deploying security technology and can be a powerful deterrent in itself to careless or malicious behavior. Security staff should be required to complete a thorough training program that teaches them to examine the full business context of any alert-triggering behavior before jumping to conclusions and to closely follow pre-determined escalation paths and communication protocols involving supervisors, HR and legal staff as they investigate potential incursions. Organizations considering UBA should also be aware that privacy laws in other parts of the world may impose strict limitations on how it is used.

These caveats aside, for organizations who already have a strong security culture and a range of fundamental security basics in place — like solid access controls, mature event logging, end-point encryption, secure remote access, intrusion detection and a detailed incident response plan — UBA can represent a significant step up in your cybersecurity program, allowing you to detect and respond to even the most subtle and sophisticated attacks quickly and decisively.

Jason Straight *is the Senior Vice President and Chief Privacy Officer of Cyber Risk Solutions at UnitedLex. Prior to joining UnitedLex, Straight held numerous leadership positions at a leading global investigations and cyber security company, most recently as a managing director in the cyber investigations practice. He began his career as an attorney at Fried, Frank, Harris, Shriver & Jacobsen in New York. As a recognized domain expert and Certified Information Privacy Professional (CIPP), Straight is a frequent speaker and author on topics relating to data privacy, cyber security, data breach response and computer forensics.*