Accelerating Access Management to the Speed of Hacks

Chris Sullivan is vice president of advanced solutions at Courion. He is responsible for developing and bringing new products and solutions to market as well as cultivating and innovating new ideas that effectively address the industry's ongoing challenges. Previously, Chris has been vice president of EMEA Operations, Advanced Solutions, Customer Solutions and Professional Services. Chris also serves as chairman of the Access Risk Benchmarking Committee for ISACA and is a frequent speaker at industry conferences including European Identity Conference, Gartner Catalyst Conference, MIT International Science and Technology Initiatives (MISTI), IT GRC Forum and the ISACA ISRM conference.

Organizations grant network access nearly every minute of every day. Hackers frequently try to get inside networks using co-opted access credentials. Yet most IT departments still review access privileges only quarterly or semiannually.

Even organizations that review access privileges monthly, which is diligent by today's standards, are not keeping up with hackers who are on the job and working around the clock. It is easy for network security staff, who toil daily to keep intruders out of systems, to lose track of the fact that they are under constant siege. Certifying access on even a monthly basis leaves large open periods of time for intruders or nefarious insiders to sneak in, do their damage and cover their tracks before the next certification comes along.

The attack that penetrated an Anthem database of 80 million customers and employees is a classic example. The breach occurred in May 2014 but was not discovered until early 2015. In many, if not most, data breaches, a delay such as this is the case. According to the Verizon 2015 *Data Breach Investigations Report* (DBIR), 60 percent of compromises took only seconds or minutes.[1] Nearly 50 percent of those tested in the investigation opened emails and click on phishing links within the first hour, according to the report, which surveyed 70 global organizations from 61 countries.

By comparison, 75 percent of detection took weeks, and it was not always because of anything the company did. "We need to close the gap between sharing speed and attack speed," the report concluded.

A similar report showed that attackers were present on victim networks for an average of 229 days before they were discovered.[2] Realities like these are a clear call for a new approach to identity and access management (IAM).

FRAGMENTED SECURITY

The need for open access fuels the big data crush that is overwhelming today's access certification processes. Consumer access models are firmly entrenched in the business world. Employees, contractors and vendors expect access through every online and mobile channel: web sites, direct logins and mobile applications. With every new access point comes another opportunity for intruders to exploit their favorite vehicle into companies' vital assets: legitimate network access credentials.

Also available in Korean

한국어로도 가능

Data thieves are getting into networks by using the same tactics they have been using for years—phishing, malware attachments, and stolen or compromised credentials—to infiltrate networks. New access options have made those tactics even easier to use and more effective.

Email phishing, for example, is easier now because legitimate email addresses are posted in more locations. Mobile apps may not have gone through the usual security vetting, yet they provide direct network access. Once inside with a legitimate login identity or email address, an intruder can request access to vital systems. Or, they can use malware or fake web sites to steal manager credentials, give themselves access and then cover their tracks once they have taken what they want.

With so many more doors opening to the network, most organizations are under almost constant attack from the inside. Effectively defending against intruders or malicious insiders means eliminating orphan accounts, pinpointing unusual behavior and identifying privileges that do not match an employee's role. That requires a new microcertification model of network management.

Microcertifications continually validate access privileges against business policies when they are triggered by questionable activities and events. If violations are found, notifications immediately go to the relevant managers for remedial action. Managers react only to anomalies, not constantly recertify compliant user accounts.

The problem with microcertifications is that most companies today do not have an enterprisewide IT security framework or the technology tools required to support them. Solutions common in IT environments today automate compliance reviews, but provide only periodic or interval audit checks. That leaves large windows of vulnerability between 90-day and even 30-day review cycles. Reviewing access privileges more frequently is prohibitively expensive, largely due to the manual processes dominant today and almost impossible logistically. Certifying all of their reports every few days would take managers so much time that they would not be able to do much else. The pace of business productivity would be severely reduced.

Intelligence, in the form of embedded data analytics optimized for identity and access management, can reduce the number of certifications that managers must perform by reporting only anomalies that require a sign-off. In an intelligent system, managers do not have to compare and contrast access privileges to determine if there are high-risk combinations or if a privilege is outside an employee's role. The system identifies the risk and calculates how much accepting the exception will increase the employee's risk rating. The manager is left only with the decision of whether the exception is necessary and the risk is warranted.

> “Security is a strategic priority, and COBIT enables organizations to translate it to frontline action.”

COHESION THROUGH COBIT

Implementing microcertifications requires two elements: a unified IT security infrastructure and big data analysis tools. The information security program architecture,[3] addresses the current patchwork nature of most identity and access management systems.

COBIT® integrates security into a cohesive framework that encompasses risk, resource and performance management, in addition to business considerations (e.g., strategic alignment of IT with business goals). With the risk posed by IT breaches so significant, creating this connection between strategic goals and IT is essential. Security is a strategic priority, and COBIT enables organizations to translate it to frontline action.

COBIT provides the common language for defining goals and objectives essential for executing strategic goals. It also defines objectives and metrics for IT security. Metrics serve as the parameters for reconciling access management functions into a cohesive process for identifying the patterns of behavior that can expose an intruder.

COBIT addresses the fragmentation that exists in much of IAM. Access management vendors have developed a broad array of tools to automate tasks. Generating intelligence to detect intruders, however, is still left to manual processes and to management tools without native data intelligence.

“Generating the data to feed effectiveness metrics is not easy,” says Gartner analyst Brian Iverson. “Most products in the IAM space do not yet possess a mature understanding of the basic process elements that are needed to demonstrate control over user access. Furthermore, such products also vary in the robustness of their support for analytics, reporting and dashboards. Even if there is a desire to use a product's internal dashboards, there may be a need to process data externally to produce some desired metrics.”[4]

AUTOMATION GAP

The lack of intelligent, automated data analysis tools in most corporate IT environments forces companies to make do with manual access management. IT teams present reports to each business manager with lists of permissions granted to each of their direct reports. Managers attest to whether the permissions are appropriate or should be modified. System owners do the same. That means manually parsing large data sets that multiply exponentially with each level of detail.

Usually, IT staff extracts user data from databases and applications into unorganized flat files. Another set of IT staff, usually the security team, has to reconcile those masses of data into formats that can be dissected by spreadsheet applications. The difficulty and expense of this process are primary contributors to the higher risk of credentials being used to improperly access key systems. It is simply too laborious a process to go through more than a few times per year. The problem is even more acute for organizations that want to detect unusual usage patterns that could indicate an intruder.

A manager with 10 direct reports can be taken as an example. Each direct report has access to at least 10 systems. Within those 10 systems, each employee could have dozens of entitlements. The team has to parse that much data for each manager, and the manager must attest to each data point. Some managers might require a specific breakdown.

Shifting that scenario to the company level illustrates how data volumes quickly multiply to outstrip manual analysis. A company with 10,000 employees, each with access to 10 applications, has 100,000 accounts. Take a conservative view and assume the users log in twice per day. That creates 200,000 login activity records per day. One month generates 4 million login activity records.

To detect improper usage, a company must also know what employees are doing within each application. Assuming those same 10,000 workers access 50 data assets per day, there would be 500,000 activity records per day and 10 million per month. With the login records, there are 14 million data elements to analyze per month.

Manually analyzing entire data sets that are that large is impossible. Without automation, IT organizations are left to monitor only select risk areas, leaving many gaps in the security fabric for intruders to exploit.

THE BIG DATA APPROACH

The development of big data management and automated analysis tools makes it possible to close those gaps by constantly analyzing tens of millions of data points to detect suspicious activity. As recently as two years ago, these tools did not exist for IT, even though almost identical tools were common in areas such as sales, marketing and customer service. Big data analysis tools continue to gain a foothold in IT.

Massachusetts (USA)-based health care provider Harvard Pilgrim is among the early adopters to apply identity analytics and intelligence to IAM. With more than 1.2 million subscribers, the company manages tens of millions of records per month. The company implemented a solution to monitor all significant risk areas. Among the key areas the IT staff focused on were detecting unused accounts and closely monitoring privileged accounts that had the ability to change systems and perform maintenance.

Harvard Pilgrim's intelligent IAM solution enables managers to report accounts that have not been accessed in a set amount of time so they can be deactivated before a hacker can exploit them. It also regularly analyzes privileged accounts to determine what access they have as compared to what access they should have. The analysis is automated to run constantly and detect any behavior outside of norms that are determined by managers and expressed in the access management solution. Harvard Pilgrim has used that intelligence to reduce the number of privileged access accounts and eliminate those with unnecessary access.

In another example, Miami (Florida, USA) Children's Hospital implemented the same approach to constantly scan its access environment. Analyzing millions of data points, the automated scan revealed hundreds of orphaned accounts and several user groups with no members. Each represented a data theft risk that would have been difficult, if not impossible, to detect until after damage had been done.

In both cases, adding identity analytics to the IAM equation enabled IT and business managers to instantly identify high-risk individuals and groups by answering questions such as:

- Are there domain administrator accounts whose passwords have been changed?
- Which nonsales systems have sales people accessed?
- Is anyone accessing patient medical information without a genuine need to know?
- Which accounts with at least five entitlements have not been used in more than 30 days?
- Does this account have a suspicious number of privileged entitlements?
- Should part-time employees receive all the access rights they are routinely granted?
- Do contractors continue to access resources after their projects end?
- Are system administrators routinely assigned rights they do not need to perform their jobs?
- Does this business unit have an abnormal number of accounts with unnecessary entitlements?

There are no technical restrictions preventing companies from taking this approach. In the consumer realm, Amazon.com has been doing something very similar for years to track shopping habits. It knows what product a customer views and when they view it so that the company can offer promotions and incentives to purchase. The same practice occurs with credit card companies. They can detect almost instantly when a purchase looks out of character, alert the customer and cancel the card within minutes of detection to prevent losses.

Similarly, there are already IAM solutions on the market that eliminate manual data extraction by working through application programming interfaces (APIs) or scripting. They automatically cleanse the data for analysis and automatically apply analytical intelligence to answer the vital questions for determining who is doing what on the network and when.

TOWARD INTELLIGENT ACCESS MANAGEMENT

The pace of business today demands an increasing degree of open access to IT resources. With that access comes greater risk of data theft or corruption through intruders who use legitimate access points, credentials and user accounts to attack sensitive data sources.

Constantly monitoring access privileges to identify improper use of those resources to remediate risk is nearly impossible with the access management solutions dominant in most corporate IT environments today. Built around the native access management and security tools integrated into key applications and databases, IT security infrastructures are fragmented. This fragmentation contributes to a reliance on manual processes to analyze security data and certify access privileges. Slow and expensive, they cannot scale to accommodate the enormous data volumes generated by today's consumer-inspired open-access environments.

The same consumer models, however, also contain the answer to the problem. Big data analytical tools, comparable to those used in consumer applications, provide the capacity to constantly, quickly and economically analyze access data to support a microcertification access management model. Microcertification systems identify unusual behaviors and ask business managers to react only when there is a potentially risky situation. This allows for constant diligence without bogging managers down with excessive, redundant, unnecessary certifications.

> "IT organizations must adopt automation and intelligence strategies if they hope to stay ahead of hackers."

IT organizations must adopt automation and intelligence strategies if they hope to stay ahead of hackers. Otherwise, as the demand for wider access grows and opens more doors into the network, companies will continue to measure their response times in weeks while data thieves attack in minutes, disappear in seconds and cause years' worth of damage.

ENDNOTES

[1] Verizon, 2015 *Data Breach Investigation Report, www.verizonenterprise.com/DBIR/2015/*

[2] Mandiant, *M-Trends 2014: Beyond the Breach, http://connect.mandiant.com/m-trends_2014*

[3] Frisken, John; "Leveraging COBIT to Implement Information Security," *COBIT Focus*, ISACA®, USA, 4 May 2015, *www.isaca.org/cobitfocus,* figure 2.

[4] Iverson, B.; *Demonstrate Control Over User Access With IAM Effectiveness Metrics*, Gartner, 5 February 2015, *www.gartner.com/doc/2978217/demonstrate-control-user-access-iam*