

FORENSICS:

Staying Ahead of Hackers



The crux of forensic examination for regulators and for data center managers is examination of system logs for indications of security attacks and system issues.

BY PHIL BRITT

Virtually every regulatory mandate and security standard that IT organizations must comply with, including HIPAA, the HITECH, PCI, and NERC, require visibility into the forensic cracks and crevices of a data center-controlled network. This is easier said than done. Fortunately, advances in security information event management (SIEM) and other forensics technology can provide new levels of visibility and awareness across the entire data center stack. These new forensic capabilities can be used to empower and enrich the incident-response process and be used to gain new visibility into data center security and compliance management.

In addition to the regulatory demand, data centers have also increased their forensic capabilities in the last couple of years in order to try to thwart or at least minimize the impact of the growing number of security threats, to speed e-discovery requests and to better detect system issues that hinder network performance.

Increasing Threats

"The need for better forensic capability is significant," says Chris Petersen, chief technology officer and founder of LogRhythm. "Security is driving the need to purchase new forensic technology. There are persistent threats."

Not only do hackers continue to refine their attacks in attempts to find new ways to access data center files, insider threats are a growing concern, according to Petersen. For example, a disgruntled administrator who leaves a company may have compromised some systems prior to his departure. SIEM-powered forensics can detect an audit trail of his activities for a specified time period, depending on the company's preferences.

High employee turnover, particularly in the data center, is a growing concern,

though outsider attacks are continuing to grow in number and complexity, says Darren Hayes, CIS program chair at Pace University in NY.

"The primary challenge is that the number of threats has increased," says Rakesh Shah, director of product marketing and strategy for Arbor Networks, Inc. "The types of threats have changed significantly. Now they are targeting the application layer. These attacks require smaller bandwidths and are harder to detect. So data center managers need ways to detect these threats and to incorporate that into their incidence response process so they can not only detect these threats, but stop them."

"Security is driving the need to purchase new forensic technology. There are persistent threats."

**—Chris Petersen,
CTO of LogRhythm**

Arbor Networks' 2010 Worldwide Security Report says that data center operators are seeing significant outages, increased operating expenses, customer churn and revenue loss due to application level denial of service attacks. These attacks are targeting data center customers and their own ancillary supporting services such as DNS and Web portals.

Other types of attacks are increasing as well. Each type of attack targets different systems and requires different defense responses, so the data center forensics systems need to be able to distinguish between them.

"Auditing data center activity has become much more important as more

incidents occur," says Hayes. "Forensics provides you with a way to document the different types of trends and attacks, for example, a denial of service attack versus a port sniffing attack."

"I see a trend toward deeper data analysis," says Joe Gottlieb, president of SenSage. "The driver is that the attacks are more subtle and the insider threats are more prevalent. The biggest issue is illegitimate use of legitimate credentials."

The crux of forensic examination for regulators and for data center managers is examination of system logs for indications of security attacks and system issues. While some data centers have developed proprietary systems for examining log files, most are going to third-party providers for the technology and in some cases for the log analysis, according to Hayes.

"One size doesn't fit all. It's cheaper to hire a contractor when you need one for this service than to have this experience in house," Hayes says. "There are a lot of very competent companies providing this service."

Vendor Consolidation

The number of companies providing the technology has shrunk due to industry consolidation. There are some new players in the industry, but not as many as have left through recent mergers and consolidations, Roth says. He estimates that there were 57 companies in the industry just two years ago, a number that's shrunk to 25 now and will probably consolidate to about 15 companies in another year.

The forensics systems themselves range from relatively simple proprietary systems to sophisticated ones that use dashboards, alerts, remote reporting and other features to alert data center managers of issues as soon as possible.

“The types of threats have changed significantly. Now they are targeting the application layer. These attacks require smaller bandwidths and are harder to detect.”

*—Rakesh Shah, Director of Product Marketing and Strategy,
Arbor Networks, Inc.*



*Images courtesy of
Arbor Networks*

Though many of these systems provide the ability for deeper analysis, many users don't use many of the tools at their disposal, according to Gottlieb. "Most tend to be reactive rather than proactive."

Even though the volume of traffic has increased, these enterprise-wide systems reduce the time needed to locate the source of a problem from days down to minutes while also uncovering issues undetectable using older methods, says Bill Roth, executive vice president of Log Logic.

"For example, a consumer health care company started to receive threatening e-mails, but couldn't figure out where they were coming from. Typical forensics techniques didn't work. They installed a [enterprise-wide] data center forensics system and found out that the VPN access of a former employee hadn't been turned off. They turned it off, and police arrested him."

As in this case, most data center forensics today look for certain patterns rather than one-time instances of system anomalies in

order to uncover security threats or other issues, according to Roth. Data center managers need to know when a series of events is unusual or network traffic is out of normal ranges. For example, traffic might spike up on a particular day. While this might not be unusual for a data center supporting a short-term Internet sales promotion, it could signal a denial of service attack attempt if there are no other known reasons for the increase. The newer systems provide behavioral analytics as well as alerts to unusual events.

The more complex the attack or system issue, the more detailed the forensic analysis needs to be in order to resolve the matter, resulting in a two-fold approach, with initial analysis conducted quickly and deeper analysis conducted later.

Need for Speed

Data centers are producing and capturing data packets faster than ever before, adds Jay Botelho, director of WildPackets, Inc. Recording speed has jumped to 20 GB per second, up from 2 to 3 GB per second

only a couple of years ago as data center infrastructures have increased the throughput of their information, a trend that will continue.

"40 GB per second packet recording is just around the corner," Botelho says.

New appliances are capturing and storing the packets immediately, rather than recording them to a file system, which had been the previous practice, according to Botelho. "Storing in files is pretty slow. Now proprietary systems stream packets to disk as quickly as possible by avoiding the file system."

For such a system to work, the data center has to deploy network recorders to capture the data information, according to Botelho, who says that the need for these fast recorders will become more evident in the future as network throughput becomes even faster.

However, this method has its drawbacks as well, Botelho cautions. As data centers

record more packets, storage needs grow. And the sheer volume of data packet capture means real-time inspection is all but impossible. While some systems will show some trends immediately, deeper packet inspection has to wait until later.

Better Analysis

Moving to comprehensive systems with automated alerts enables data center managers to focus on security strategies and solutions rather than the minutiae of searching through mushrooming log files and packets.

“What we are seeing is a trend toward more SIEM technology, not so much for daily reviews of logs, but more for alerts and reviews of exceptions,” says Reema Parappilly, advisory manager for accounting firm Weaver & Tidwell LLP. “This enables users to spend their time improving and managing their security rather than spending all of their time looking for ‘a needle in the haystack’ in the daily logs. This way they can be more proactive with their security.”

For example, a data center hosting firm that is a Weaver & Tidwell client used to dedicate much of the time of the security staff to daily log reviews. Once the firm automated that task through SIEM, the staff spent its time analyzing trends so they could determine the precautions needed to protect against the most common threats.

“This eases the audit burden of the activities they had to perform in the past in order to gather the necessary information for a [regulatory or compliance] audit,” Parappilly added. “Now a central system maintains all of the log information.”

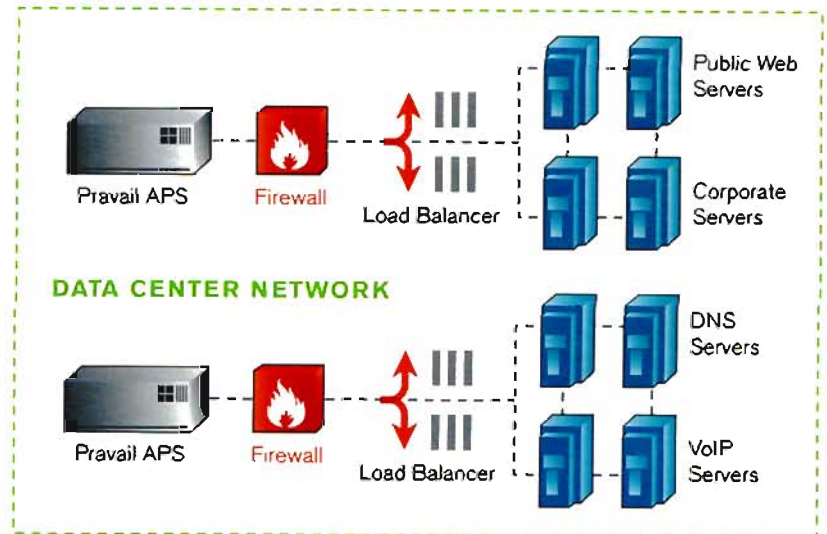
Cloud Considerations

Data center managers need to alter forensic strategies as they move more of their information into the cloud, advises Eddie Sheehy, CEO of Nuix, Sydney, Australia. “You have the benefits of scale, but you may

be using the same Exchange database as many other companies. When you have a private cloud, you can analyze everything to your heart’s content. In a private cloud, you can’t image that exchange server because it has your data, data from company b, company c and company d.”

based on having a particular technology infrastructure.

Another advantage of such homogenous systems is that they enable data center managers to develop repeatable processes to analyze information, rather than starting



“What we are seeing is a trend toward more SIEM technology, not so much for daily reviews of logs, but more for alerts and reviews of exceptions.”

—Reema Parappilly, Advisory Manager, Weaver & Tidwell LLP

Cloud environments are supposed to have “Chinese firewalls” to separate the data of different companies, but risk of data “leakage” across those firewalls is higher than if a company was maintaining all of its information on dedicated servers.

Cloud providers use a variety of hardware and software systems that may be different from what a firm uses in-house, so data center managers need to employ forensics systems that can work across different technologies, Sheehy says. Such agnostic forensics systems also enable firms to more easily move to a cloud provider based on business reasons rather than just simply

anew every time, says John Greaves, chief technology officer for Capathia Hosting.

Greg Adgate, general manager, global enterprise for Equinix, a collocation provider with 92 data centers around the world, adds that physical security should be the first step in a forensics strategy, particularly in shared environments. His firm uses mantraps and five levels of biometrics to positively identify each person accessing a company’s systems.

Business Applications

Better, more comprehensive, forensics provides better alerts for business issues

The Best Sealing Grommet on the Market

KOLDLOK
Wave



ENGINEERED TO MAKE A DIFFERENCE

USABLE AREA

Offers 169% more usable cable area than a leading brush competitor

ULTIMATE SEALING

Wave shaped thermoplastic elastomer is engineered to provide the best sealing against bypass airflow of any grommet on the market

VERSATILE

Split design allows edge-cut tiles to be removed without capturing cables

See it at
www.KoldLokWave.com



Request a free sample at
KoldlokWave.com/DCM

Sales - 888.982.7800 | www.KoldlokWave.com | Data Center Solutions from the **LOK** Family

KOLDLOK
GROMMETS

HOTLOK
BLANKING PANELS

ENERGYLOK
DATA CENTER SERVICES



as well, says Steve Shalita, vice president of marketing for NetScout Systems.

Companies are using appliances on the network that record all traffic in real time, then they can go back to these files for problem resolution of performance issues, Shalita explains. For example, if a user has problems with a VOIP system, the company can use the recorded information to review network traffic, patterns and other data at the precise time the problem occurred to see what caused it. It could be an increase in network traffic, configurations of policy items, or some other matter that can be corrected to avoid the same issue from occurring again, or before it affects others on the network.

"Having this type of data is invaluable in terms reducing the time needed to resolve issues," Shalita says. Dashboards linked to these systems can provide real-time alerts to issues such as dropped packets, enabling technicians to address issues as soon as they start occurring rather than waiting for an end user to report a problem.

"If you can see the subtle changes, then you can do something about it before there is a potential breach or a crisis," Shalita says. Some forensics systems also help rank system issues in terms of criticality, enabling a data center manager to more quickly prioritize resolutions.

"The operations team finds a lot of value in this data," agrees LogRhythm's Petersen.

The need for fast, complete insight into network events will continue to grow as will the amount of data that the forensic devices will need to review. Experts expect further installation of system-wide forensics systems and extensions of those that are already in place to expand to include an increasing array of appliances, smart phones and other devices that access the network. **D C M**

Phil Britt is a freelance writer based in South Holland, Ill.