IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

IT Security

Network Forensics – How to Prepare For and React to a Security Breach

Jay Botelho

Jay Botelho
Senior Director of
Products
Savvius

Biography

Jay Botelho is the Senior Director of Products at Savvius, Inc (www.savvius.com), a LiveAction Company, and a leader in actionable network visibility for network performance management and security investigations.

Jay holds an MSEE, and is an industry veteran with more than 25 years of experience in product management, product marketing, program management and complex analysis.

From the first mobile computers developed by GRiD Systems to modern day network infrastructure systems, Jay has been instrumental in setting corporate direction and specifying requirements for industry-leading hardware and software products.

He is based at Savvius' headquarters in Walnut Creek, California.

Keywords Network forensics, Network monitoring, Savvius, LiveAction, Security
Paper type Opinion

Abstract

Enterprise security teams have historically spent most of their time, human resources and money on defenses like firewalls and Intrusion Detection Systems (IDS) to protect and monitor the security of their networks. However, as the author of this article explains, a quick look at the news will tell you that these barriers are far from foolproof. With breaches becoming more common (and costly), enterprise teams are turning to tools that help them respond quickly to security incidents as soon as the attack has been discovered.

Introduction

Network forensics looks at information such as log data, network flow and packet data to answer the question 'How did the attackers get in?' It is similar to what you would expect a detective to do at a crime scene – look for clues to recreate the crime. The goal of network forensics is to identify the source of the breach faster in order to minimize the resulting damage, and to analyze them so that future attacks can be prevented.

Consider this example about port scans

Port scans are attempts to detect and penetrate open server ports from a remote location. Every enterprise is subject to attacks like these on a daily basis. In most cases, the security appliances shrug off unwanted scans.

But in this instance, a specialized scan hidden amongst the others detects a known vulnerability in a web server. The hacker then uses a known exploit to infiltrate the server and identify information like encrypted password files to retrieve and crack. Then they exfiltrate the data back to their attack server. The enterprises' IDS detects the exfiltration and signals an alert.

The alarm has been sounded, and the security team knows about the attack, right? Perhaps not. IDS devices typically produce many alerts per day – sometimes hundreds, if not properly configured. It is common to receive over 500 alerts every day marked as "severe/critical," yet a general lack of resources means that often they are only able to investigate and resolve 1% of those alerts. Most IT departments simply cannot respond to the deluge of alerts and false positives, which can allow real attacks to slip through unnoticed.

So what's the solution?

Examining network data such as network flow, TCP or IP events can help trained investigators eliminate false positives quickly. That leaves them with a reasonable number of potentially legitimate alerts to investigate. An effective network forensics tool will only capture network data associated with alerts, so investigators can easily focus on the data that matters.

Unfortunately, not all organizations are adequately equipped to investigate breaches. Access logs will indicate access attempts, but do nothing to highlight exploited vulnerabilities or malware-based attacks. System logs and network security logs (from a firewall, IDS, etc.) usually will not generate an urgent alert unless a login is preceded by several failed attempts, which clever attackers can easily avoid. The most useful information in network forensics is the original packet data.

In the above example, you may have noticed that the IDS only triggered once the stolen data was exfiltrated. The issue is that most tools today start capturing packet data only when the event has been triggered, which is too late to see which web server was attacked, which exploit was used and which port scan detected the vulnerability. Effective network forensics requires buffered data that can allow security investigators to examine the network activity immediately prior to and following the alert in question.

This brings us back to why network forensics is so important. Without the original packets to help piece together the cause of an alert, it takes significantly longer to find real breaches, meaning more stolen data and ultimately a greater cost to the company. It takes an average of 200 days to identify a breach and an additional 70 days to contain it. The average cost of a breach is almost £2.8 million.

The unfortunate truth is that no organization is safe from attack. With that in mind, here are some critical steps every organization should take to prepare for, and react to a security breach:

1. **Preparedness** – Employees are sometimes the weakest link in security. It is important that you conduct regular training with employees on basic security

best practices such as using strong passwords, how to identify phishing emails, and not plugging unknown devices into work machines.

2. **Identification** – Automate the process of data collection so that it is easier to investigate and identify security events.

3. **Containment** – Once a breach has been confirmed, determine exactly how far the problem has spread within the company's network and minimize further damage by disconnecting affected systems and devices.

4. **Eradication** – Resolve the root cause of the vulnerability and remove all traces of malicious code. Ensure that the flaw is completely resolved by running penetration tests and looking at server logs again to define whether other servers and devices might also be susceptible.

5. **Recovery** – Restore all data and software from clean backup files. Monitor systems for any sign of weakness or recurrence.

6. **Lessons learned and remediation** – Conduct a thorough post-mortem to analyze the incident and how it was handled. Identify prevention and response processes that can be improved.

In conclusion

The network analysis tools that organizations have invested in over the past decade or so are simply not able to keep up with today's high-speed networks. New tools and IT practices are necessary if IT organizations are going to keep new networks running as well and as securely as old ones.

Network forensics enables organizations to realize the full benefits of 10G and 40G networks: high performance with the control and security IT organizations take for granted on 1G networks. By investing in network forensics solutions and following the best practices listed in this paper, IT organizations can ensure that speed does not come at the expense of visibility, control, or security.