computer
FRAUD & SECURITY

whiteoaks

FEATURE

Building better data protection with SIEM

David Howell

David Howell, ManageEngine

In today's data-rich enterprises, information is currency. This makes the requirement to protect it against external security threats more acute than ever. Already, the exponential increase in sophisticated data breaches seen in recent years has prompted IT and security administrators to move from simply being aware of the most up-to-date security solutions to proactively building their own internal security policies. Increasingly, they are also deploying security information and event management (SIEM) tools to help mitigate threats.

Proactive security

Following recent large-scale attacks, Gartner has forecast that business security is about to become much more proactive. By 2018, it predicts that 40% of large enterprises will have formal plans to address aggressive cyber-security business disruption attacks – up from none today.[1]

Instead of blocking and detecting attacks, this is likely to mean that, increasingly, businesses will devote more attention to actively detecting and responding to security threats.

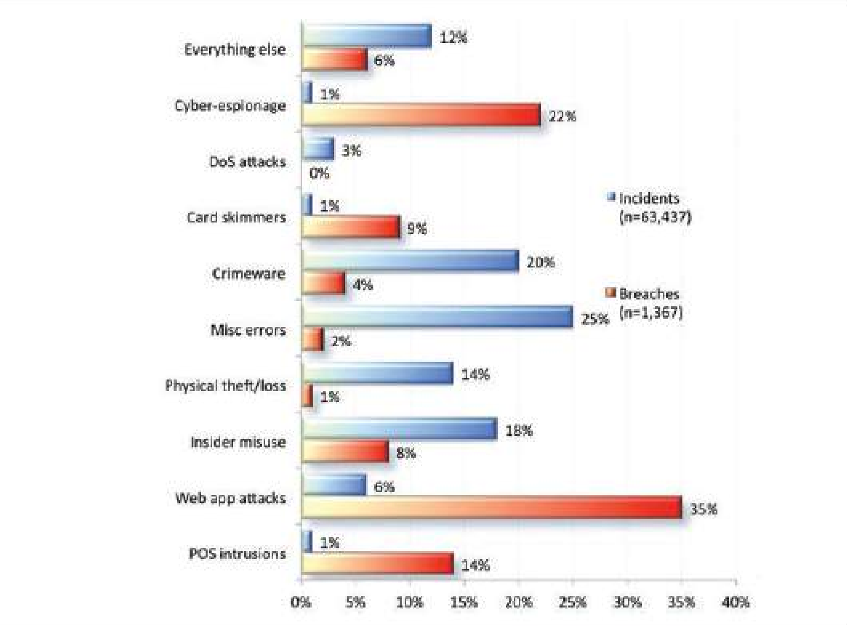

Figure 1: Breaches and incidents in 2013 broken down into nine major attack patterns. Source: Verizon Data Breach Investigation Report 2014.

Rather than the current approach of collecting and analysing logs from critical log sources in a central location, the only way that security administrators can hope to foresee, prevent or react immediately to a security breach is to adopt a different mindset – and begin to think like a hacker.

This change of approach requires distinct skills and capabilities. In particular, security admins need to be able to predict a suspicious event, treat it as a potential data threat and defuse it before it causes any damage.

Attack patterns

The Pareto principle that, for many events, roughly 80% of the effects come from 20% of the causes is evident from common global attacking patterns used to steal data. According to Verizon, as few as nine attack patterns have given rise to as many as 80% of the security breaches in recent years.[2]

For these reasons, it makes sense to understand how common attack patterns unfold. In turn, this can provide insight into how a data breach may occur in an organisation's network, as well as highlighting any potential security loopholes.

Continued on page 20...

...*Continued from page 19*

Paying close attention to the industry, the type of confidential data the enterprise deals with, its network infrastructure and other contextual information are all crucial when narrowing down the most likely attack pattern. For example, a healthcare provider should be alert to internal and malware threats. To counteract security threats and protect confidential patient records, it might consider monitoring privileged user activity, monitoring user activities on critical servers and applications, and checking compliance with data security regulation.

In a retail environment, the potential vulnerability of point of sale (POS) devices should mean being alert to RAM scraping, as well as payment card skimming and web app attacks. Essential risk-mitigating steps should include compliance with PCI DSS and other regulations, ongoing monitoring of point of sale devices and analysis of POS logs for unusual activities.

For a bank or credit card provider, the risk of insider security threats, phishing and attacks on POS or operating systems should all be considered. Steps that could be taken to mitigate these attacks might include an audit trail of privileged user activity, constant monitoring of critical web servers and applications, and compliance with PCI DSS.

Time to discovery

Realistically, not all security breaches can be proactively anticipated or discovered. Too often, organisations do not even know an attack has happened until they are informed about it by an external vendor.

For this reason, getting to grips with the various factors limiting faster speed of discovery means developing a thorough understanding of the various stages a security attack will go through before it is discovered. Commonly, these steps consist of an examination of the network, network intrusion, and then exploiting data or a critical source before escaping the network undetected.

Before choosing their attacking technique, hackers will typically explore the business type as well as the nature of the data they want to breach. Once they have carried out this evaluation, they will attempt to invade the network infrastructure.

Rather than allowing the attack to progress, security administrators should look to contain the incident at this stage. One of the biggest challenges, however, is that administrators rarely have detailed visibility of security incidents that could indicate network intrusion. Likewise, hackers often carry out slow intrusions of the network over time that make it virtually impossible for security administrators to correlate events. In turn, they can easily be missed.

For these reasons, a real-time detection system with a powerful correlation engine can provide an essential defence mechanism. By capturing events and analysing them as soon as they happen on the network, a truly real-time SIEM engine will improve the speed of discovery by analysing and correlating incidents, giving security administrators more time to cope with the unfolding incident, contain it and neutralise the damage.

About the author

David Howell is the European director of ManageEngine (www.manageengine.com) and has been with the company for over 14 years. He was part of the team that created the worldwide channel for ManageEngine and established the European operation. Howell is a highly experienced sales and marketing specialist with extensive knowledge in industries such as IT, telecommunications and electronics.

References

1. 'Gartner Says By 2018, 40% of Large Enterprises Will Have Formal Plans to Address Aggressive Cyber-security Business Disruption Attacks'. Gartner, 24 Feb 2015. Accessed Jul 2015. www.gartner.com/newsroom/id/2990717.
2. 'Data Breach Investigations Report 2014'. Verizon. Accessed Jul 2015. www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf.

EVENTS

8–10 September 2015
International Conference on Information Security and Digital Forensics
Kuala Lumpur, Malaysia
http://sdiwc.net/conferences/isdf2015/

13–18 September 2015
Hacker Halted USA
Atlanta, Georgia
www.hackerhalted.com

14–15 September 2015
Gartner Security & Risk Management Summit
London, UK
www.gartner.com/technology/summits/emea/security/

22–25 September 2015
OWASP AppSec USA
San Francisco, US
https://2015.appsecusa.org/c/

28 September–1 October 2015
(ISC)^2 Security Congress
Anaheim, CA, US
https://congress.isc2.org/

28–30 September 2015
Cyber Intelligence Europe
Bucharest, Romania
www.intelligence-sec.com/events/cyber-intelligence-europe-2015

29 September 2015
Government IT Security & Risk Management
London, UK
www.whitehallmedia.co.uk/govsec

8–9 October 2015
BruCON
Ghent, Belgium
http://brucon.org

20–21 October 2015
(ISC)^2 Security Congress EMEA
Munich, Germany
http://emeacongress.isc2.org/