ABERDEEN GROUP

CYBER SECURITY: FOR DEFENDERS, IT'S ABOUT TIME

June 2017

Executive Summary

In multiple areas of cyber security, time is currently working in favor of the attackers — and time is the strategic advantage that the defenders need to regain.

In a recent report, Aberdeen Group leveraged Verizon *Data Breach Investigations Report* data to uncover the distribution of attacker "dwell times," i.e., the total time in days from attacker compromise to defender detection.

The median attacker dwell time for data breaches between 2014 and 2016 was about 38 days. This means that in half of the successful data breaches, detection by the defenders took five to six weeks or less. In the other half, detection took as long as *four years!*

How does such a time lag affect risk? Risk, properly understood, involves the likelihood of a particular event, such as a data breach, and its potential business impact. Aberdeen has developed a simple Monte Carlo analysis to assess risk in a number of security categories.

Aberdeen's report used this analysis to provide four illustrative examples showing how recapturing an advantage of time can help defenders reduce risk.

Time and Data Protection

Aberdeen's model found that the business impact of a data breach is greatest at the beginning of the exploit. Capabilities for faster detection and response reduce the business impact of a successful breach.

Indeed, by incorporating this assumption into Aberdeen's Monte Carlo analysis, it turns out that responding twice as fast to data breaches can lower the business impact by about 30%.

Time and Threat Detection / Incident Response

Data loss is not the only consequence of a security incident. Sophisticated attacks on enterprise networks and network-based services can also result in substantial business impact involving both the availability and performance of enterprise systems.

Based on insights from empirical data on DDoS attacks, Aberdeen discovered that the business impact from a sustained disruption in availability grows continually from the time of compromise to the time of remediation.

Incorporating this assumption into the Monte Carlo analysis shows that being twice as fast at threat detection and incident response lowers the business impact of such an attack by about 70%.

Time and Data Center / Cloud Security

The impact of time on data center and cloud security can best be understood by considering the time, cost, and complexity of a traditional vendor patching approach to databases and applications.

Based on its Monte Carlo analysis, Aberdeen estimates that such an approach requires between 220 and 660 vendor patches per year, with a median value of about 410. This approach also involves a median of about 910 hours per year of disruption to enterprise databases and applications.

Looking at the impact of this disruption on revenue and user productivity, and factoring in the cost of administrative staff, Aberdeen estimates the business impact of a traditional, vendor patching approach to be between 1% and 8% of annual revenue, with a median value of about 4%.

There is an alternative to this approach: virtual patching (sometimes known as external patching or vulnerability shielding.) When using a virtual patching approach the window of vulnerability — i.e., the time from public disclosure to eventual mitigation — is substantially shorter. This significantly reduces the likelihood that enterprise databases and applications may be compromised at all.

Virtual patching also substantially reduces the time that enterprise databases and applications are disrupted for traditional vendor patching processes. This minimizes the two biggest contributors to the total annual business impact of patching: lost revenue and lost user productivity.

Time and Endpoint Security

The importance of time in the realm of endpoint security is amplified by the volume of vulnerabilities and exploits to which users are subjected, not to mention the increasing sophistication and targeted nature of attacks.

One critical issue here is the alarming fact that the availability of vendor patches frequently lags zero-day vulnerability disclosures by days or weeks. Even when patches are made available, it may be weeks or months before enterprise systems are actually updated.

Security professionals are reducing the likelihood of endpoint security incidents through faster identification and containment of zero-day malware. They are also reducing the business impact of such incidents by adopting flexible approaches to response that

sustain the productivity of users and improve the productivity of responders.

Moving Forward

Enterprises need to recapture the advantage of time when it comes to cyber security risk. To this end, security organizations should prioritize investments in capabilities that are aligned with the current reality of threats and vulnerabilities.

Specifically, they should focus on capabilities designed to:

- ➔ **Reduce the likelihood and business impact of attacks** while shortening detection and response times.
- ➔ **Maintain the productivity of users** (e.g., *minimize friction* in workflows).
- ➔ **Increase the productivity of defenders** (e.g., detect and resolve *more threats and incidents, faster*).

Author: Derek E. Brink, CISSP, Vice President and Research Fellow, Information Security and IT GRC