GuardiCore
InfoSec Island Article

http://www.infosecisland.com/blogview/24835-Minimize-Dwell-Time-to-Cut-the-Cost-of-Data-Center-Breaches.html

Minimize "Dwell Time" to Cut the Cost of Data Center Breaches

Not a day goes by, it seems, without a high-profile data breach in the news. The incessant, daily drip of leaked emails from the Democratic National Committee is only the latest sobering reminder: in spite of the millions that organizations spend on preventive security measures, no one is invulnerable to breaches.

Not only are breaches occurring with stunning frequency, but their costs are going up as well. The Ponemon Institute's 2016 study of 383 organizations found that the average cost of a data breach rose from $3.79 to $4 million over the previous year.

If enterprises are serious about curtailing those costs, it's time to shift their focus to one of the chief culprits driving up the cost of breaches: dwell time.

What is "dwell time"?

Dwell time refers to the length of time a threat actor lingers in a victim's environment before it is detected. While dwell time may be tricky to quantify, most cybersecurity researchers estimate that it averages around 150 days. In its seventh annual M-Trends report, Mandiant measured it at 146 days. A recent global Ponemon study put the average at 98 days for financial institutions and as much as 197 days for retailers. However varied these numbers may be, they all tell us the same thing: attackers are being allowed too much time to do their dirty work.

In the highly publicized Target breach of 2013, where over 100 million customers were exposed — and cost the retailer over $500 million — the actual theft of credit card data went undetected for around two weeks. But the real news was that the attackers lurked inside the company's network for months before they started ex-filtrating the actual credit card data.

Today's data centers are particularly vulnerable to dwell time. The movement to

software-defined data centers and cloud technologies has created a security gap that includes both lack of visibility into and lack of controls of network data flows, enabling malware to move laterally within data centers undetected once it has breached perimeter defenses. Traditional security measures focused on prevention around north-south traffic are not designed for scaling and securing internal data center traffic. They have difficulty keeping up with the pace of change in these dynamic, virtualized environments, allowing attackers to lurk undetected for days, weeks or months.

Dwell time and cost

It stands to reason that the longer it takes to detect and contain a data breach, the more damage it can inflict and the costlier it becomes to resolve. As noted in the Ponemon Institute's 2016 Cost of Data Breaches study, "Time to identify and contain a data breach affects the cost…(and) our study shows the relationship between how quickly an organization can identify and contain data breach incidents and financial consequences." More specifically, the study found that when a breach was identified within 100 days, the average cost was $5.83 million per breach. However, when a breach went undetected for 100 days or more, the average cost went up to $8.01 million, or nearly 40% higher.

So how will minimizing dwell time help contain costs? Consider all the direct and indirect costs of a data breach – notifying customers, regulatory disclosures, setting up customer hotlines, offering credit monitoring for victims, professional fees for crisis management, legal costs, lawsuits and settlements. Breach investigation and remediation by outside experts is also a big expense. And that's not to mention the value of the assets or intellectual property that has been stolen or compromised.

Virtually all of these costs are exacerbated by dwell time – which means that curtailing dwell time should help cut costs in a variety of ways. For example, detecting and stopping a breach before a lot of data has been ex-filtrated will reduce the losses from IP theft. If relatively few customer records are compromised, it will cost less to notify, accommodate and settle with customers. If the internal security team detects a breach before much damage is done, the need for external experts to scope, investigate and repair the damage may be reduced if not eliminated. And a company that beats the media to the story about the breach, proactively explaining clearly the measures it has taken to minimize the impact, will likely see less damage to its reputation.

Minimizing dwell time needs to be a priority of security teams. One could argue this is the most important metric for incident response. As a recent SANS Institute survey of security professionals pointed out, "IR teams should be evaluating themselves on metrics such as incident detection or dwell time to determine how quickly they can detect and respond to incidents in the environment. Through well-crafted assessments, teams should find weaknesses in responsiveness and focus on strengthening those areas."

What will it take?

There's no question that strong perimeter defenses are essential, but it's clearly time to place equal if not greater emphasis on earlier breach detection and faster incident response within the data center.

Technology exists today that can dramatically reduce the time it takes to detect, confirm and contain a breach from months to minutes, thereby minimizing dwell time and the resulting costs. To prevent attackers from moving freely within the flow of east-west traffic, the ability to create security policies at the application level is essential. Security teams can then leverage automation to monitor all data center traffic and investigate anomalies that indicate a potential breach.

Distributed deception is a technique that employs a variety of lures throughout the environment, including decoy workstations, servers, infrastructure, devices, applications and other elements, to automatically engage any suspicious activity detected. It is a powerful tool for identifying threat actors without them realizing it, allowing teams to instantly distinguish actual attacks from false positives and prioritize incidents based on severity. Automation can also help quickly identify systems impacted by a breach without the need for outside investigators.

Give security teams the upper hand

In-house security teams often say they lack the resources or staff to monitor everything that goes on inside the data center. They don't have time to chase down every incident, which more often than not turns out to be a false positive. New technologies that leverage automation can multiply the effectiveness of security personnel, enabling them to monitor the environment and detect more live breaches with fewer people and resources.

Enterprises may not be able to prevent every breach, but they can minimize the impact of those that break through. A solution that minimizes dwell time and accelerates remediation will go a long way towards mitigating the ever-increasing cost of today's inevitable data breaches. Because in incident response, time truly is money.