HOW TO OVERCOME THE SECURITY CHALLENGES OF TODAY’S HYBRID ENTERPRISE IT ENVIRONMENTS

Article by- Tony Velleca, CEO of CyberProof and CISO of UST Global. California

With an analysis of approximately 1.5 billion data points in 86 countries, the recently released 2019 Verizon Data Breach Investigation Report (DBIR) highlights several important trends in cyber security. Let’s have a look at some of these trends in cyber security and explore how they may be linked to the move to the cloud and the widespread adoption of hybrid IT environments.

A Year That Saw a Shift in the “Why” and the “How”

According to the Verizon report, attacks related to cyber espionage are dropping as compared to attacks that are financially motivated, which are growing across the board.

One expression of this trend toward financially motivated attacks is the increase in ransomware documented in the report. Ransomware was seen in 24% of incidents where malware was used. Moreover, ransomware ranked #2 in most-used malware varieties.

A second trend uncovered in the report is that cybercriminals are more focused on finding the easiest targets providing the greatest returns.

An indication of this is the increase in cloud-based compromises. According to the DBIR, compromised email accounts and cloud misconfiguration (“Miscellaneous Errors”) led to the exposure of at least 60 million records this past year.

TONY VELLECA

What's Behind This Year's Trends?

These shifts in the patterns and activities of threat actors gain greater significance viewed against the background of the recent transformation of the IT environment. While organizations that are smaller have adopted cloud-based solutions faster than enterprise organizations, we've now reached a stage where enterprises are rapidly transitioning to hybrid IT environments. Most enterprise IT environments today have adopted a mixture of deployment models. There's the on-premises infrastructure – including legacy systems that are still in use – and there are systems and services in the cloud or multi-cloud.

This is recent; and it's a change that has a notable impact on approaches to cyber security. This creates a lack of control. It becomes easier for threat actors to attack – and it's harder for organizations to maintain visibility, monitoring, control, and response.

The Challenges of Hybrid Security Operations

Hybrid IT environments have a wide array of security challenges:

• Disappearance of an on-prem perimeter: Development of IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service) creates an environment with microservices and platforms to secure, which are not fully visible to your security monitoring.

• Growth of shadow IT: Information technology systems and solutions are used within the organization without explicit organizational approval – and the downloaded software can put an organization at risk. According to industry analyst firm Gartner, by 2020, a third of successful attacks experienced by enterprises will be on their shadow IT resources.

• Increase in the number of screens: An enterprise's highly distributed environment lacks a centralized management view; each system comes with a separate management console and requires additional time and human resources to manage.

• Regulatory challenges: When data is moved to the cloud, it becomes harder to prove what an organization is doing with PII (Personally Identifiable Information) and to meet the requirements of GDPR, HIPAA, PCI DSS, SOX, federal government regulations in the U.S., and other regulations regarding privacy and data ownership, which are becoming increasingly stringent.

• Scarcity of talent: Complex IT environments requires high-level expertise. There's an international shortage of people with the right skill set and the demand for cyber security professionals continues to grow.

Maintaining a Strong Security Posture

These challenges make it that much harder for IT teams to provide effective protection. The increased complexity of hybrid systems may mean that they cannot eliminate the possibility of attack.

They should, instead, shift focus; rather than trying to avoid attack, they could aim to respond to attack more quickly.

> The unique complexity of a hybrid IT environment can be managed most effectively by working with a next generation security service provider, who connects all systems within your organization and provides flexible hands-on expertise

What's necessary is the reduction of mean time to detect (MTTD) and mean time to respond (MTTR). Speed is the name of the game.

How? That's where new technologies and processes come in. Leveraging the advanced use of AI-learning protocols like machine learning or User and Entity Behavior Analytics (UEBA) make it possible to sift through gigabytes of enterprise data in real time.

Security Service Providers Offer the Tools and Expertise You Need

The unique complexity of a hybrid IT environment can be managed most effectively by working with a next generation security service provider, who connects all systems within your organization and provides flexible hands-on expertise. Combining the efforts of an in-house security team with the experience and expertise of a managed detection and response provider allows you to address the new levels of risk – without compromising your security posture. CR