IDC ANALYZE THE FUTURE

IDC ANALYST CONNECTION

Sponsored by: Micro Focus

At the heart of a cyber-resilient organization is an adaptable approach to security that leverages artificial intelligence/machine learning, automation, and analytics.

Protection Strategies for a Cyber-Resilient Organization

November 2020

Questions posed by: Micro Focus

Answers by: Curtis Price, Program Vice President, Infrastructure Services

Q. How has COVID-19 changed business and therefore the requirements of cybersecurity strategy?

A. COVID-19 has been very disruptive to business and IT operations as organizations have had to adjust their supply chain, switch to new channels to interact with customers, and shift their IT architecture to accommodate work from home for their employees. These business shifts have also exposed organizations to new security threats that were previously unidentified but potentially expose businesses to new vulnerabilities.

Even companies that thought they had a solid and comprehensive business continuity plan in place have had to transform their security strategy and pivot from a static view of risk protection to a more dynamic approach with the ability to react to changes in the business in a more agile way.

Q. How should organizations embrace cyber-resilience to be more secure, but in a way that minimizes business friction and supports business acceleration?

A. In many organizations, the negative effects of cybersecurity threats on the business can be an inhibitor to innovation and growth. However, as organizations pursue digital transformation (DX) initiatives, cyber-resilience must be an integral component of a DX strategy. Designing cyber-resilience into the transformation strategy allows organizations to pursue growth initiatives while minimizing security risk. Risk assessments have become an important component of an organization's cyber-risk management strategy. In a rapidly changing IT environment, organizations must continuously reassess their risk posture to ensure their most critical assets are adequately protected.

Being cyber-resilient starts with a strategy for risk protection that minimizes disruption to the business. Implementation of advanced technologies such as artificial intelligence/machine learning (AI/ML), analytics, and automation enables organizations to accelerate their time to detect and remediate security threats, thus minimizing disruption to the business.

Q. How can organizations transform their cyberprograms to build a layered, adaptive, and business-aligned protection (cyber-resilient) strategy?

A. Traditionally, companies have invested heavily in security controls that provide a defense-in-depth strategy for the protection of critical business assets. This strategy has made it more costly and difficult for adversaries to launch successful attacks. Operationally, the traditional defense-in-depth approach can be a costly and complex strategy for enterprises that are looking to manage an array of different security controls and procedures.

Multilayered defense is still an essential cyberdefense strategy; however, companies must shift away from today's static approach to an approach that utilizes artificial intelligence and automated response to support a more flexible and adaptable strategy that anticipates potential threats to the business and executes an automated and orchestrated response.

Q. What challenges come with deploying adaptive layered defenses for organizations embracing cloud at scale? How should organizations address a cyber-resilience strategy with emphasis on protection?

A. While cloud has fast become the core of the enterprise architecture, providing a consistent approach to managing on premises and cloud infrastructure and assets has increased complexity for cybersecurity protection. The lack of visibility across security controls, the heavy use of manual security processes, and the need to monitor ever-changing access privileges can slow an organization's ability to act quickly when a breach occurs.

Given the dynamic nature of cloud and the movement of enterprise workloads to and from cloud, establishing an effective change management strategy for security is critical. The use of automation to monitor changes in the environment, identify suspicious behavior, and take action to remediate vulnerabilities allows for an adaptable hybrid cloud security strategy.

As organizations embrace multicloud strategies and operate an IT environment where business assets are highly distributed and at risk to various security threats, an adaptable security architecture that allows for continuous evaluation of the security posture is an essential component of a cyber-resilient strategy.

Q. How do organizations prioritize the investments needed to protect against potential cybersecurity threats?

A. As organizations execute digital transformation initiatives, they must think holistically about the risk inherent in their strategy and develop a cyberfocused investment strategy that addresses potential vulnerabilities early in the DX strategy formulation process. A detailed understanding of the assets that drive value for the business is essential to identifying where investments for cybersecurity protection should be prioritized to minimize security risk.

At a time when IT budgets are tight and chief information security officers (CISOs) are being asked to do more with less, making sound investments in cybertechnologies that minimize the business impact of a security breach is a strategic imperative. Building resilience into the security strategy means developing a cyberfocused investment strategy that enables continuous assessment of the IT environment, which allows for changes to be made to controls, policies, and procedures in an automated fashion.

About the Analyst

Curtis Price, *Program Vice President, Infrastructure Services*

Curtis Price is the Program Vice President of IDC's Infrastructure Services group. He oversees all research efforts within IDC's Network Life-Cycle Services, Wireless Infrastructure Services, and Software and Hardware Support Services programs. Mr. Price provides expert insight and analysis of the trends and market dynamics impacting the network services market within the enterprise and telecommunications sectors.

MESSAGE FROM THE SPONSOR

About Micro Focus

Cyber resilience is the ability of an organization to enable business acceleration (enterprise resiliency) by preparing for, responding to, and recovering from cyber threats. A cyber-resilient organization can adapt to known and unknown crises, threats, adversities, and challenges. The ultimate goal of cyber resiliency is to help an organization thrive in the face of adverse conditions (crisis, pandemic, financial volatility, etc.).

Micro Focus develops integrated cybersecurity solutions to enhance your intelligence and cyber resilience and protect against advanced cyberthreats at scale. To learn more about becoming cyber resilient, please take our 360-degree assessment at ***www.cyberresilient.com***.

IDC Custom Solutions

IDC Research, Inc.
5 Speen Street
Framingham, MA 01701, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com