GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Sheridan, Kelly

"Data Security: Think Beyond the End Point."

Darkreading.com

Informa tech Technology Group

21 May, 2019

The URL: https://www.darkreading.com/endpoint/data-security-think-beyond-the-endpoint/d/d-id/1334770

Accessed: 30 July 2019

Synopsis: A strong data protection strategy is essential as data moves across endpoints and in the cloud.

Endpoint security is a common concern among organizations, but security teams should be thinking more broadly about protecting data wherever it resides.

DARKReading

5/21/2019
02:00 AM

Kelly Sheridan
News
Connect Directly

Data Security: Think Beyond the Endpoint

A strong data protection strategy is essential as data moves across endpoints and in the cloud.

INTEROP 2019 – LAS VEGAS – Endpoint security is a common concern among organizations, but security teams should be thinking more broadly about protecting data wherever it resides.

"If you're just focusing on device protection and not data protection, you're missing a lot," said Shawn Anderson, executive security advisor for Microsoft's Cybersecurity Solutions Group, at the Interop conference held this week in Las Vegas. Rather than add multiple endpoint security products to corporate machines, he urged his audience of IT and security pros to think about protecting their data.

An estimated 60% percent of data is leaked electronically, Anderson said, and 40% is leaked physically. When an organization is breached, the incident costs an average of $240 per record. The average cost of a data breach was $4 million in 2017, a year when hackers stole more than 6 billion records.

As more devices jump online, the risk to businesses and their information continues to grow. An estimated 9 billion devices equipped with microcontrollers are deployed in appliance, equipment, and toys each year. Fewer than one percent are now connected. But that number will grow, and "highly secured" IoT devices require properties many devices don't have: certificate-based authentication, automatic security updates, hardware root of trust, a computing base protected from bugs in other code.

All computers within an organization – laptops, smartphones, tablets, a rapidly growing pool of IoT devices – are collecting larger amounts of data. Some of it is kept on the machine but more of it is moving to the cloud, which is powering the number of alerts companies handle. Microsoft analyzes 6.5 trillion threat signals daily, Anderson pointed out, up from 1.2 trillion a few years ago.

The cloud is accelerating how companies can collect, process, store, and use information. As companies transition to hybrid infrastructure, and their data moves across cloud-based and on-prem systems, they should evaluate their endpoint security strategies to make sure data is protected where it resides.

In his talk, Anderson discussed what he called the four pillars of infrastructure security: identity and access management, threat protection, information protection, and security management.

Securing Data Wherever It Resides

Companies should have a strategy in place to secure hybrid infrastructure and protect data from internal and external threats. "I always tell customers to assume compromise," Anderson said, emphasizing the importance of protecting identities. If an attacker has an employees' laptop that's one thing; if they have credentials to access a corporate network, that's another.

Identity protection is a critical component to threat protection, he explained. Businesses should strengthen users' credentials by enabling MFA, block legacy authentication to reduce the attack surface, increase visibility into why identities are blocked, monitor and act on security alerts, and automate threat remediation with solutions like risk-based conditional access. "Our admins internally do not have 100% access, 100% of the time, across the network," he said.

Threat protection describes the organization's ability to detect suspicious activity on the network and address problems on-prem and in the cloud. Ask yourself the following questions: Do you know if your credentials are compromised? How quickly can you remediate advanced threats? Do you have a system in place? How do you protect users from email threats?

"You could put 15 pieces of software on an endpoint, but if you don't have a data protection strategy, [attackers] win," Anderson noted.

Data must be protected in use, in transit, and at rest. Businesses should discover and classify sensitive data as it enters the environment, apply protection based on policy, monitor and remediate threats, and remain compliant as data travels throughout the organization before it's retired and deleted. Information should be tracked and monitored throughout its lifecycle.

Anderson listed a few key steps in the process of building this strategy: define sensitive data, establish a label taxonomy, and customize protection policies based on objectives and compliance requirements. As data is classified and labeled, organizations may adjust their strategy depending on what they observe as they monitor sensitive data and its effect on users.

Visibility, a commonly cited challenge among security pros, is core to the fourth pillar of security management. Businesses should build their security posture with visibility, control, and guidance across identities, devices, apps and data, and infrastructure to manage their security strategy across the organization and improve security practices over time.

Related Content:

- Effective Pen Tests Follow These 7 Steps
- 97% of Americans Can’t Ace a Basic Security Test
- When Older Windows Systems Won't Die
- The Data Problem in Security

Kelly Sheridan is the Staff Editor at Dark Reading, where she focuses on cybersecurity news and analysis. She is a business technology journalist who previously reported for InformationWeek, where she covered Microsoft, and Insurance & Technology, where she covered financial ... *View Full Bio*