HealthManagement.org
Promoting Management and Leadership

4 ways to protect data beyond endpoint

Data collection is accelerated by the Internet of Things (IoT) with the use of both onsite and remote IT systems, apps and devices. Cloud computing, on the other hand, makes it easier for organisations and business entities to store, use and share information. With data increasingly moving across endpoints and in the cloud, it is important for security teams to develop a **strong data protection strategy** for this so-called hybrid infrastructure.

You might also like: Part 1: Cyber security key obstacles and addressing tech personnel shortage

"If you're just focusing on **device protection and not data protection**, you're missing a lot," according to Shawn Anderson, executive security advisor for Microsoft's Cybersecurity Solutions Group. "You could put 15 pieces of software on an endpoint, but if you don't have a data protection strategy, [attackers] win," he points out. Instead of adding multiple endpoint security products to corporate machines, security teams should be thinking more broadly about protecting data wherever it resides.

To help IT and security pros build this kind of data strategy, Anderson urges them to take note of these **"four pillars" of infrastructure security.**

1) Identity and access management. Anderson says that when an attacker gets hold of an employee's laptop that's one thing; if they have credentials to access a corporate network, that's another. He recommends these steps: 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. As he points out: "Our admins internally do not have 100% access, 100% of the time, across the network."

© For personal and private use only. Reproduction must be permitted by the copyright holder. Email to copyright@mindbyte.eu.

2) Threat protection. This pertains to the organisation's capability 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**?

3) Information protection. Data must be protected in use, in transit, and at rest. It's important for organisations to 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 organisation before the data is retired and deleted. Anderson notes that organisations may have to adjust their strategy depending on what they observe as they monitor sensitive data and its effect on users.

4) Security management. Visibility, which is often cited as a key challenge among security pros, is core to the fourth pillar of security management. Organisations therefore must build their security posture with visibility, control, and guidance across identities, **devices, apps and data, and infrastructure** to manage their security strategy across the organisation and improve security practices over time.

Source: Dark Reading

Image credit: Pixabay

Published on : Tue, 28 May 2019

© For personal and private use only. Reproduction must be permitted by the copyright holder. Email to copyright@mindbyte.eu.