telecomkh.com

http://www.telecomkh.com/en/internet/news/9117

Futuriom SysSecOps reports finds major gaps in security strategies

07/06/16

Date: ***Wed, 06/07/2017 - 12:48*** Source:

Futuriom

Endpoint security seen as key to more integrated approach

Debate session about security at the NetEvents European Media Spotlight "Innnovators in cloud, IoT, IA & Security", London. From left to right, Laurance Dine, Verizon; Guy Franco, Javelin; Paul Ferron, CA Technologies, Scott Register, Ixia; and Josh Applebaum, Ziften

Image credited to NetEvents

Futuriom's two-month study on integrated systems and security operations (SysSecOps) strategy, "Endpoint Security and SysSecOps: The Growing Trend to Build a More Secure Enterprise," reveals that many IT and security operations managers have challenges in delivering a comprehensive information security approach, including inter-department coordination, endpoint security technology integration, and resources.

The Futuriom survey of 149 IT specialists and executive managers found that 65% of respondents wanted "better management of budgets across department/silos" and 55% wanted "Better protection of endpoints." The top challenges included lack of time/resources (71%) and business unit resistance (35%).

When the survey results are put into the context of a review of the major cited causes of recent security breaches, it's clear that IT staff, security operations, and executive management need to work together better to create an integrated SysSecOps plan that starts with better endpoint protection, concludes the report.

"The findings show that it's not just about building better endpoint security technology -- which is certainly needed -- but it's also about executive leadership of an integrated SysSecOps plan," said Futuriom Founder and Principal Analyst R. Scott Raynovich, the author of the report.

Key Findings:
• **Integrated security visibility is a top challenge**. Fifty-three percent of the IT and security respondents (including IT system admins, security specialists, hardware specialists, network admins, executive managers, and others), indicated a “Challenge in integration of many security tools” as a major challenge of securing their endpoint environments.

• **Security starts at the endpoint**. Respondents to the survey see endpoint security technology as key, with 55% demanding better protection of endpoints as a top security goal.
• It’s a human problem -- many attacks can be stopped. A look at the major hacking events of the past five years shows that many breaches were flagged by technology – the failure came with human response.

• **Integrating existing tools is a major focus.** When asked, “What would be the most helpful in improving IT security in your organization?”, end users selected “Better integration between systems management and security operations tools,” as one of the most helpful approaches.

• **Time and resource are a big challenge**. A majority of the respondents to the survey (71%) said they lack time and resources to secure the environment. Thus, more efficient and prioritized operations would help.

• **Management isn’t always on the same page**. Thirty-seven percent of the survey end users say conflicting IT and security goals prevented them from achieving their goals.

• **Current endpoint tools may still be inadequate**. Many end users say despite the plethora of security and visibility tools at their disposal, better tools are needed.

• **Malware and Phishing remain major threats**. The Verizon Data Breach Investigations Report puts malware and phishing as the cause of 51% of cyberattacks, underscoring the importance of coordinated systems and security operations.