McAfee Study on Big Security Data Reveals Businesses Unable to Harness Its Power to Protect against Threats
Monday, June 17, 2013 06:37:00 PM (GMT)

Study Finds Only 35 Percent of Businesses Can Quickly Detect Security Breaches and 58 Percent Store Big Security Data for Three Months or Less

McAfee today released a study revealing how organizations around the world are unable to harness the power of Big Data for security purposes. According to the report '*Needle in a Datastack'* , businesses are vulnerable to security breaches due to their inability to properly analyze or store big data.

The ability to detect data breaches within minutes is critical in preventing data loss, yet only 35 percent of firms stated that they have the ability to do this. In fact, more than a fifth (22 percent) said they would need a day to identify a breach, and five percent said this process would take up to a week. On average, organizations reported that it takes 10 hours for a security breach to be recognized.

"If you're in a fight, you need to know that while it's happening, not after the fact," said Mike Fey, executive vice president and worldwide Chief Technology Officer. "This study has shown what we've long suspected -- that far too few organizations have real-time access to the simple question 'am I being breached?' Only by knowing this, can you stop it from happening."

Misplaced security confidence putting organizations at risk

Nearly three quarters (73 percent) of respondents claimed they can assess their security status in real-time and they also responded with confidence in their ability to identify in real-time insider threat detection (74 percent), perimeter threats (78 percent), zero day malware (72 percent) and compliance controls (80 percent). However, of the 58 percent of organizations that said they had suffered a security breach in the last year, just a quarter (24 percent) had recognized it within minutes. In addition, when it came to actually finding the source of the breach, only 14 percent could do so in minutes, while 33 percent said it took a day and 16 percent said a week.

This false confidence highlights a disconnect between the IT department and security professionals within organizations, which is further highlighted when the *Needle in a Datastack* findings are compared with the with a recent Data Breach Investigations report of security incidents. The study of 855 incidents showed that 63 percent took weeks or months to be discovered. The data was taken from these organizations within seconds or minutes in almost half (46 percent) of the cases.

Organizations increasingly exposed to Advanced Persistent Threats

Needle in a Datastack found that on average that organizations are storing approximately 11-15 terabytes of security data a week, a figure that Gartner Group predicts will double annually through 2016. To put that in perspective, 10 terabytes is the equivalent of the printed collection of the Library of Congress. Despite storing such large volumes of data, 58 percent of firms admitted to only holding on to it for less than three months, thereby negating many of the advantages of storing it in the first place.

According to the McAfee Threats Report: Fourth Quarter 2012, the appearance of new advanced persistent threats (APTs) accelerated in the second half of 2012. This type of threat can lay dormant within a network for months or even years, with numerous recent high profile examples including attacks on major U.S. newspapers. Long term retention and analysis of security data to reveal patterns, trends and correlations is crucial if organizations are to spot and deal quickly with these APTs.

Realizing the Value of Big Security Data

To achieve real-time threat intelligence in an age where the volume, velocity and variety of information have pushed legacy systems to their limit, businesses must embrace the analysis, storage and management of big security data. These ever-growing volumes of events, as well as asset, threat, user and other relevant data have created a big data challenge for security teams. To overcome this challenge, successful organizations have moved from traditional data management architectures to systems that are purpose-built to handle security data management in the age of APTs.

With this need to identify complex attacks, organizations should go beyond pattern matching to achieve true risk-based analysis and modeling. Ideally, this approach should be backed by a data management system able to create complex real-time analytics. In addition to the ability to spot threats in real-time, organizations should have the ability to identify potentially sinister long-term trends and patterns. Beyond just finding a 'needle in a datastack', organizations should move to a longer time horizon with risk-based context to find the right needle, so they can proactively deal with today's threats.

Notes to editors

The study, conducted by research firm Vanson Bourne, interviewed 500 senior IT decision makers in January 2013, including 200 in the USA and 100 each in the UK, Germany and Australia.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence network, McAfee is relentlessly focused on keeping its customers safe.
http://www.mcafee.com

Note: McAfee is a trademark or registered trademark of McAfee, Inc. in the United States and other countries. Other names and brands may be claimed as the property of others.

--30-- JAR/SF

Contact:

McAfee
Sal Viveros, +44 1753 513 200
sal_viveros@mcafee.com
or
Hotwire PR
Alice Crook, +44 207 608 4654
alice.crook@hotwirepr.com

1.2

Industries: Data Management, Internet, Security, Technology
Languages: English
Primary Identifiers: 002WNN-E, INTC-US
Related Identifiers: MFE-US, INTC, US458140100
Source: McAfee Inc.
Subjects: Survey