Data breaches becoming more complex, pervasive and damaging, finds Verizon's 2017 Data Breach Digest
Tuesday, February 14, 2017 09:00:00 AM (GMT)

SAN FRANCISCO, Feb. 14, 2017 /PRNewswire/ -- RSA 2017 -- Data breaches are becoming more complex and are no longer confined to just the IT department, but are now affecting every department within an organization. Each breach leaves a lingering, if not lasting imprint on an enterprise, finds the 2017 Data Breach Digest.

As we found in the Verizon 2016 Data Breach Investigations Report (DBIR), the human element is again front and center this year. Humans continue to play a significant role in data breaches and cybersecurity incidents, fulfilling the roles of threat actors, targeted victims and incident response stakeholders.

Now in its second edition, Verizon's Data Breach Digest details 16 common breach scenarios, inviting the reader to take a behind-the-scenes look at cyber investigations that tell the stories behind the company's annual Data Breach Investigations Report (DBIR). The cases are each told from the perspective of the various stakeholders involved, such as corporate communications, legal counsel, or the human resources professional.

"Data breaches are growing in complexity and sophistication," said Bryan Sartin, executive director, the RISK Team, Verizon Enterprise Solutions. "In working with victim organizations, we find that breaches touch every part of an organization up to and including its board of directors. Companies need to be prepared to handle data breaches before they actually happen in order to recover as quickly as possible. Otherwise, breaches can lead to enterprise-wide damage that can have devastating and long-lasting consequences such as a loss of customer confidence or a drop in stock price."

"The Data Breach Digest is designed to help businesses and government organizations understand how to identify signs of a data breach, important sources of evidence and ways to quickly investigate, contain and recover from a breach," added Sartin.

2017 Data Breach Digest scenarios based on type, industry, incident pattern and stakeholder involvement

The report once again confirms that there is a finite set of scenarios that occur with data breaches but many permutations occur within each, leading to an expansive range of damage that can be observed in the aftermath of a data breach. Breaches in the Digest are defined by type of breach, industry, one of nine DBIR incident patterns, and by stakeholder involvement.

This year's 16 data breach scenarios are also classified according to their prevalence and lethality in the field. Ten of the cases represent more than 60 percent of the 1,400 cases investigated by Verizon's Research, Investigations, Solutions and Knowledge (RISK) Team over the past three years, while the other six are less common but considered lethal or highly damaging to an organization.

For each scenario, you go through a detailed analysis of how the attack occurred, level of sophistication, threat actors involved, tactics and techniques used and recommended countermeasures. Content is derived from the RISK Team caseload and categorized according to the standardized VERIS (Vocabulary for Event Recording and Incident Sharing) Framework used to compile the DBIR.

The report groups the 16 scenarios into four different types of breaches and gives each a personality, including these select examples:

- **The human element**
  - Partner misuse – The Indignant Mole
  - Disgruntled employee – The Absolute Zero
- **Conduit devices**
  - Mobile assault – The Secret Squirrel
  - IoT calamity – The Panda Monium

- **Configuration exploitation**
  - Cloud storming – The Acumulus Datum
  - DDoS attack – The 12000 Monkeyz
- **Malicious software**
  - Crypto Malware – The Fetid Cheez
  - Unknown unknowns – The Polar Vortex

This year's report points to five actions an organization should take in the aftermath of a breach:

- Preserve evidence; consider consequences of every action taken
- Be flexible; adapt to evolving situations
- Establish consistent methods for communication
- Know your limitations; collaborate with other key stakeholders
- Document actions and findings; be prepared to explain them.

Verizon's Data Breach Digest series

To preserve anonymity, Verizon has modified/excluded certain details of each real-world situation including changing names, geographic locations, quantity of records stolen and monetary loss details. Everything else has been imported straight from Verizon's case files.

The Verizon RISK Team performs cyber investigations for hundreds of commercial enterprises and government agencies across the globe. In 2016, the RISK team investigated more than 500 cybersecurity incidents in more than 40 countries. In 2008, the results of this team's field investigations were the genesis of the first Data Breach Investigations Report, an annual publication that dissects real-world data breaches with the goal of enlightening the public about the nature of threat actors behind the attacks, the methods they use, including the data they seek and the victims they target.

To access the full digest, visit: http://verizonenterprise.com/databreachdigest

Verizon Communications Inc. (NYSE, Nasdaq: VZ), headquartered in New York City, has a diverse workforce of 160,900 and generated nearly $126 billion in 2016 revenues. Verizon operates America's most reliable wireless network, with 114.2 million retail connections nationwide. The company also provides communications and entertainment services over mobile broadband and the nation's premier all-fiber network, and delivers integrated business solutions to customers worldwide.

Verizon's Online News Center: Verizon news releases, executive speeches and biographies, media contacts and other information are available at Verizon's online News Center at www.verizon.com/news/. News releases are also available through an RSS feed. To subscribe, visit www.verizon.com/about/rss-feeds/.

Verizon Enterprise Online News Room: News releases, blog posts, media contacts and other information are available at *Verizon Enterprise Solutions News & Insights (news.verizonenterprise.com)*. News from Verizon Enterprise Solutions is also available through an RSS feed at http://www.verizonenterprise.com/rss-options/.

Media contact:

Janet Brumfield
+1.614.582.9636
janet.brumfield@verizon.com
Twitter: @janet_brumfield

Nilesh Pritam - APAC
+65.9277.9048
nilesh.pritam@intl.verizon.com
Twitter: @Nilesh_pritam

Clare Ward – EMEA
+44.118.905.3501
clare.ward@intl.verizon.com
Twitter: @ClareWSpeaks

To view the original version on PR Newswire, visit: http://www.prnewswire.com/news-releases/data-breaches-becoming-more-complex-pervasive-and-damaging-finds-verizons-2017-data-breach-digest-300406846.html

SOURCE Verizon

Countries: United States
Industries: Telecommunications, Computer Electronics, Hardware & Software, High Tech Security, Multimedia, Internet & Wireless Technology
Languages: English
Primary Identifiers: VZ-US
Related Identifiers: VZ-US