Verizon refocuses the cyber investigations spotlight on the world of Insider Threats
Monday, March 04, 2019 04:00:00 PM (GMT)

SAN FRANCISCO, March 04, 2019 (GLOBE NEWSWIRE) -- The Verizon Data Breach Investigations Report (DBIR) series opened the doors to the world of cybercrime – now, this dataset and caseload analysis has been refocused on the role of the insider - forming the Verizon Insider Threat Report.

Twenty percent of cybersecurity incidents and 15 percent of the data breaches investigated within the Verizon 2018 DBIR originated from people within the organization[1], with financial gain (47.8 percent) and pure fun (23.4 percent) being the top motivators. These attacks, which exploit internal data and system access privileges, are often only found months or years after they take place, making their potential impact on a business significant.

However, many organizations often treat insider threats as a taboo subject. Companies are too often hesitant to recognize, report or take action against employees who have become a threat to their organization. It's as though the insider threat is a black mark on their management processes, and their name.

The Verizon Insider Threat Report now aims to change this perception by offering organizations a data-driven view on how to identify pockets of risk within the employee base, real-life case scenarios, and countermeasure strategies to consider when developing a comprehensive Insider Threat Program.

"For far too long data breaches and cybersecurity incidents caused by insiders have been pushed aside and not taken seriously. Often they are treated as an embarrassment or just an issue for Human Resource departments," commented Bryan Sartin, executive director security professional services, Verizon. "This has to change. Cyber threats do not just originate from external sources, and to fight cybercrime in its entirety we also need to focus on the threats that lie within an organization's walls."

Defining the characteristics of the threat from within

Particular attention has been paid to the types of Insider Threats that organizations can face. Profiled within specific case scenarios from Verizon's own investigative caseload - from incident detection (and validation), to response and investigation, and then to lessons-learned (countermeasures) – five insider personalities have been identified:

1. **The Careless Worker** – These are employees or partners who misappropriate resources, break acceptable use policies, mishandle data, install unauthorized applications and use unapproved workarounds. Their actions are inappropriate as opposed to malicious, many of which fall within the world of Shadow IT (i.e., outside of IT knowledge and management).
2. **The Inside Agent** – Insiders recruited, solicited or bribed by external parties to exfiltrate data.
3. **The Disgruntled Employee** – Insiders who seek to harm their organization via destruction of data or disruption of business activity.
4. **The Malicious Insider** – These are employees or partners with access to corporate assets who use existing privileges to access information for personal gain.
5. **The Feckless Third-Party** – Business partners who compromise security through negligence, misuse, or malicious access to or use of an asset.

Eleven building blocks for an effective Insider Threat Program

The report provides practical advice and countermeasures to help organizations deploy a comprehensive Insider Threat Program, which should involve close co-ordination across all departments from IT Security, legal, HR, to incident response and digital forensics investigators.

Two factors hold the key to this success – knowing what your assets are and ultimately who has access to them.

"Detecting and mitigating insider threats requires a different approach compared to hunting for external threats," continues Sartin. "Our aim is to provide a framework that enables companies to be more proactive in this process and to slice through the fear, uncertainty and embarrassment that surrounds this form of insider cybercrime. Verizon sits between the sources and victims of cybercrime on a daily basis, and by sharing real scenarios from our caseload we hope that organizations can learn and adopt the countermeasures we recommend to implement their own programs."

These 11 countermeasures can help reduce risks and enhance incident response efforts:

1. **Integrate Security Strategies and Policies** – By integrating the other 10 countermeasures (listed below), or better yet a comprehensive Insider Threat Program with other existing strategies such as a Risk Management Framework, Human Resources Management and Intellectual Property Management can help strengthen efficiency, cohesion and timeliness in addressing insider threats.
2. **Conduct Threat Hunting Activities** – Refine threat hunting capabilities such as threat intelligence, dark web monitoring, behavioral analysis and Endpoint Detection and Response (EDR) solutions to search, monitor, detect and investigate suspicious user and user account activities, both inside and outside the enterprise.
3. **Perform Vulnerability Scanning and Penetration Testing** – Leverage vulnerability assessments and penetration tests to identify gaps within a security strategy, including potential ways for insider threats to maneuver within the enterprise environment.
4. **Implement Personnel Security Measures** – The implementation of Human Resource Controls (such as employee exit processes), Security Access Principles and Security Awareness Training can mitigate the number of cybersecurity incidents associated with unauthorized access to enterprise systems.
5. **Employ Physical Security Measures** – Employ physical methods for access such as identity badges, security doors and guards to limit physical access as well as digital access methods including card swipes, motion detectors and cameras in order to monitor, alert and record access patterns and activities.
6. **Implement Network Security Solutions** – Implement network perimeter and segment security solutions, such as firewalls, intrusions detection / prevention systems, gateway devices and Data Loss Prevention (DLP) solutions in order to detect, collect and analyze suspicious traffic potentially

associated with insider threat activities. This will help highlight any unusual out-of-hours activity, volumes of outbound activity as well as the use of remote connections.

7. **Employ Endpoint Security Solutions** – Employ established endpoint security solutions, such as critical asset inventories, removable media policies, device encryption and File Integrity Monitoring (FIM) tools in order to deter, monitor, track, collect and analyze user related activity.
8. **Apply Data Security Measures** – Apply data ownership, classification and protection, as well as data disposal measures in order to manage the data lifecycle and maintain confidentiality, integrity and availability with insider threats in mind.
9. **Employ Identity and Access Management Measures** – Employ identity, access and authentication management measures to manage limit and protect access into the enterprise environment. This can be taken to the next level by employing a Privileged Access Management (PAM) solution for privileged access.
10. **Establish Incident Management Capabilities** – Establishing an incident management process to include an Insider Threat Playbook with trained and capable incident handlers, will make cybersecurity response activities more efficient and more effective in addressing insider threat activities.
11. **Retain Digital Forensics Services** – Have an investigative response retained resource available which is capable of conducting a full-spectrum of deep-dive investigations ranging from the analysis of logs, files, endpoint and network traffic, in often delicate and human related (or user account related) cybersecurity incidents.

Download Verizon's Insider Threat Report or visit Verizon at RSA 2019 on booth #1541 in the South Expo Hall, Moscone Center, San Francisco (4-8 March 2019) to receive a copy from 6 March. Verizon will be discussing Insider Threats in more detail and showcasing its intelligent security solutions.

About Verizon's security services and solutions
Verizon is a leader in delivering global managed security solutions to enterprises in the financial services, retail, government, technology, healthcare, manufacturing, and energy and transportation sectors. Verizon combines powerful intelligence and analytics with an expansive breadth of professional and managed services, including customizable advanced security operations and managed threat protection services, next-generation commercial technology monitoring and analytics, threat intel and response service and forensics investigations and identity management. Verizon brings the strength and expert knowledge of more than 550 consultants across the globe to proactively reduce security threats and lower information risks to organizations.

Verizon Communications Inc. (NYSE, Nasdaq: VZ), headquartered in New York City, generated revenues of $130.9 billion in 2018. The company operates America's most reliable wireless network and the nation's premier all-fiber network, and delivers integrated solutions to businesses worldwide. With brands like Yahoo, TechCrunch and HuffPost, the company's media group helps consumers stay informed and entertained, communicate and transact, while creating new ways for advertisers and partners to connect. Verizon's corporate responsibility prioritizes the environmental, social and governance issues most relevant to its business and impact to society.

VERIZON'S ONLINE MEDIA CENTER: News releases, stories, media contacts and other resources are available at www.verizon.com/about/news/. News releases are also available through an RSS feed. To subscribe, visit www.verizon.com/about/rss-feeds/.

Media contacts:

Nilesh Pritam (APAC)	Clare Ward (EMEA)	Ilya Hemlin (US)
+65.62486599	+44 (0) 118 905 3501	+1.908.295.7677
nilesh.pritam@eg.verizon.com	clare.ward@uk.verizon.com	ilya.hemlin@verizon.com

[1] 'Privilege Misuse' category which is also classified as 'Insider and Privilege Misuse'.

verizon✓

Primary Identifiers: VZ-US
Related Identifiers: VZ-US
Subjects: Company Announcement, Trade Show