Published on *The National Law Review* https://natlawreview.com

Verizon Releases 2016 Data Breach Investigations Report

Article By:

Ashden Fein

Verizon recently released its *2016 Data Breach Investigations Report* ("DBIR") that outlines cybersecurity threats, vulnerabilities, and trends from 2015. Verizon, with the assistance of more than 60 contributors, analyzed over 64,000 information security incidents (security events that affect the integrity of an information system) and 2,200 data breaches (incidents that result in the "confirmed disclosure of data to an unauthorized party") affecting organizations in 82 countries. Items of particular interest in this year's report include among others: (1) an analysis of attacks by industry; (2) an increase in breach discovery time; and (3) a list of the most prevalent attacks or types of threats. A brief description of each of these items follows.

Attacks by Industry

The majority of cyberattacks in 2015 targeted the financial services, accommodation, healthcare, information, and retail industries, along with the public sector. The targeting of the financial services, accommodation, and retail industries corresponds with Verizon's finding that monetary gain is the primary motive for attacks (75% of reported attacks appear to have been financially motivated). Also, while attackers generally did not target their victims based on an organization's size, organizations with fewer than 1,000 employees in the accommodation and retail sectors suffered more breaches than their larger competitors.

Increase in Breach Discovery Time

For more than 80% of the breaches analyzed in 2015, multiple days passed before a victim detected the compromise; the time it takes for an attack is shrinking and "is almost always days or less, if not minutes or less." Verizon attributes the increase in time to detect the attacker largely to improved phishing campaigns and other sophisticated methods that allow attackers to compromise networks and exfiltrate data before being detected. In contrast, as an indication of success in identifying attacks, the report notes that the number of long-term breaches — those that can last for months — have slightly declined.

Most Prevalent Attacks in 2015

The DBIR categorizes more than 90% of all the incidents and data breaches into nine types of attacks or threats. Listed below are these categories in order from the most to least prevalent for data breaches:

- **Web App Attacks:** The use of compromised websites, web-based applications, and web services to gain access and obtain data — 5,334 total incidents of which 908 involved the disclosure of data.

- **Point-of-Sale Intrusions:** Remote attacks against retail transactions requiring a card — 534 total incidents of which 525 involved the disclosure of data.

- **Miscellaneous Errors:** Unintentional actions that compromise data, including internal mis-delivery and disposal errors — 11,347 total incidents of which 197 involved the disclosure of data.

- **Privilege Misuse:** Unapproved or malicious use of elevated access by members of an organization to gather and exfiltrate data — 10,490 total incidents of which 172 involved the disclosure of data.

- **Cyber-espionage:** Persistent, unauthorized network or system access by state-backed actors for espionage purposes — 247 total incidents of which 155 involved the disclosure of data.

- **Payment Card Skimmers:** Physical implant of a device that reads magnetic stripe data from payment cards — 102 total incidents of which 86 involved the disclosure of data.

- **Physical Theft and Loss:** The loss or malicious theft of data or information systems (i.e. encrypted laptop) — 9,701 total incidents of which 56 involved the disclosure of data.

- **Crimeware:** Various forms of malware (e.g., primarily keyloggers and ransomware) that are injected via email attachments or links by criminal organizations or individuals with a financial motive — 7,951 total incidents of which 49 involved the disclosure of data.

- **Denial-of-Service Attacks:** Actions intended to overwhelm and compromise networks over a period of time, resulting in the interruption or degradation of service — 9,630 total incidents of which only 1 involved the disclosure of data.

National Law Review, Volume VI, Number 120

Source URL:https://natlawreview.com/article/verizon-releases-2016-data-breach-investigations-report