Authentication Attacks, Web Application Exploits Are Among Most Likely Threats Organizations Will Face in 2013, According to Verizon DBIR Researchers
Wednesday, December 19, 2012 01:30:00 PM (GMT)

Other Threats Such as Cloud Exploits and All-Out Cyber War Seen as Much Less Likely

BASKING RIDGE, N.J., Dec. 19, 2012 /PRNewswire/ -- Although many security experts predict that the most likely data breach threats organizations will face in 2013 include cloud exploits, mobile device attacks and all-out cyber war, "Verizon Data Breach Investigations Report" researchers have reached a far different conclusion: The most likely threats involve authentication attacks and failures, continued espionage and "hacktivism" attacks, Web application exploits and social engineering.

The findings of the researchers -- members of the company's RISK (Research Intelligence Solutions Knowledge) Team – are based on data that spans eight years and thousands of cases and is contained in the 2012 data breach report, released earlier this year.

"Many security experts are using anecdote and opinion for their predictions, whereas Verizon's researchers are applying empirical evidence to help enterprises focus on what will be truly important in the coming year -- and also what isn't," said Wade Baker, principal author of the data breach report.

"First and foremost, we don't believe there will be an all-out cyber war, although it's possible," he said. "Rather, an enterprise's 2013 data breach is much more likely to result from low-and-slow attacks."

Verizon's RISK team has identified the following most likely data threats:

- Topping the list – with a 90 percent change of probability -- are attacks and failures related to authentication, including vulnerable or stolen usernames and passwords, which often represent the initial events in a breach scenario. "Nine out of 10 intrusions involved compromised identifies or authentication systems, so enterprises need to make sure they have a sound process for creating, managing and monitoring user accounts and credentials for all of their systems, devices and networks," Baker said.
- Web application exploits which are most likely to affect larger organizations and especially governments, rather than small to medium-sized businesses. The chances of such attacks occurring are three in four, according to the data compiled by the RISK Team. "Given these odds, organizations that choose to take their chances and ignore secure application development and assessment practices in 2013 are asking for trouble," said Baker.
- Social engineering, which targets people rather than machines and relies on clever -- and sometimes clumsy -- deceptions to be successful. "The use of social tactics like phishing increases by a factor of three for larger enterprises and governments," said Baker. "It's impossible to eliminate all human error or weaknesses from an organization, but vigilance and education across the employee population help to control and contain such schemes."

Baker also said that targeted attacks from adversaries motivated by espionage and hacktivism -- breaking into a computer system, for a politically or socially motivated purpose -- will continue to occur, so "it's critical to be watchful on this front."

In addition, the RISK team does not foresee the failure of an organization's cloud technology or configuration as being the root cause of a breach. However, an organization's service provider could inadvertently increase the likelihood of a breach by failing to take appropriate actions or taking inappropriate ones.

As for mobile devices, the Verizon researchers believe that lost and stolen – and unencrypted -- mobile devices will continue to far exceed hacks and malware.

The RISK Team also projects that attacks on mobile devices by the criminal world will follow closely the push to mobile payments in the business and consumer world. "There's a good chance we'll see this shift in 2013, but our researchers think mobile devices as a breach vector in larger enterprises will lag beyond 2013," Baker said.

Large organizations tend to pride themselves on their security strategy and accompanying plans, but the

reality is that a large business is less likely to discover a breach itself than to be notified by law enforcement. "And if you do discover it yourself," Baker said, "chances are it will be by accident." He concluded:

"Keep in mind that all of these breaches can still be an issue for enterprises. However, what we're saying is that they're over-hyped according to our historical data and are far less likely to factor into an organization's next breach than is commonly thought."

Verizon Communications Inc. (NYSE, Nasdaq: VZ), headquartered in New York, is a global leader in delivering broadband and other wireless and wireline communications services to consumer, business, government and wholesale customers. Verizon Wireless operates America's most reliable wireless network, with nearly 96 million retail customers nationwide. Verizon also provides converged communications, information and entertainment services over America's most advanced fiber-optic network, and delivers integrated business solutions to customers in more than 150 countries, including all of the Fortune 500. A Dow 30 company with $111 billion in 2011 revenues, Verizon employs a diverse workforce of 184,500. For more information, visit *www.verizon.com*.

VERIZON'S ONLINE NEWS CENTER: Verizon news releases, executive speeches and biographies, media contacts, high-quality video and images, and other information are available at Verizon's News Center on the World Wide Web at *www.verizon.com/news*. To receive news releases by email, visit the News Center and register for customized automatic delivery of Verizon news releases.

SOURCE Verizon

Contacts: Media, Janet Brumfield, +1-614-723-1060, janet.brumfield@verizon.com, or Nilesh Pritam, +65 6248 6599, nilesh.pritam@sg.verizonbusiness.com, or Maria Rodriguez, +1-305-961-3181, mrodriguez@terremark.com, or Clare Ward, +44 118 905 3501, clare.ward@uk.verizonbusiness.com
Countries: United States
Industries: Telecommunications, High Tech Security, Multimedia, Internet & Wireless Technology
Languages: English
Primary Identifiers: VZ-US
Related Identifiers: VZ-US, 0040FQ-E