Survey Highlights the Economics Behind Cyberattacks

February 1, 2016

Increasing the Time It Takes to Breach an Organization by Only Two Days Discourages Profit Motive for Attackers

SANTA CLARA, Calif., Feb. 1, 2016 /PRNewswire/ -- Palo Alto Networks® (NYSE: PANW), the next-generation security company, announced it published results of a survey sponsored by the company to explore the economics of cyberattacks. Available as a downloadable report titled "Flipping the Economics of Attacks," the survey analysis provides insight into topics like the average earnings of a cyberattacker, the amount of time attacks typically take, and how to prevent successful data breaches by increasing the cost of conducting them.

Key Findings

- **Cyberattackers are opportunistic and aim for the easiest targets first.**
  - 72 percent of survey respondents said they won't waste time on an attack that will not quickly yield high-value information.
  - A majority of the survey's respondents (73 percent) stated attackers hunt for easy, "cheap" targets.
- **Time is the enemy of cyberattackers.**
  - An increase of approximately 2 days (40 hours) in the time required to conduct successful cyberattacks can eliminate as much as 60 percent of all attacks.
  - On average, a technically proficient attacker will quit an attack and move on to another target after spending approximately a week (209 hours) without success.
- **The "big payday" is a myth.**
  - The average adversary earns less than $30,000 annually from their malicious activities, which is 1/4 of a cybersecurity professional's average yearly wage.
- **A strong security posture increases the time to execute an attack.**
  - It takes double the amount of time (147 hours) for a technically proficient cyberattacker to plan and execute an attack against an organization with an "excellent" IT security infrastructure versus 70 hours for "typical" security.
  - 72 percent of respondents believe attackers will stop their efforts when an organization presents a strong defense.

QUOTES

- "As computing costs have declined, so too have the costs for cyber adversaries to infiltrate an organization, contributing to the growing volume of threats and data breaches. Understanding the costs, motivations, payouts, and finding ways to flip the cost scenario will be instrumental in reducing the number of breaches we read about almost daily and restoring trust in our digital age."
  - Davis Hake, director of cybersecurity strategy at Palo Alto Networks
- "The survey illustrates the importance of threat prevention. By adopting next-generation security technologies and a breach prevention philosophy, organizations can lower the return on investment an adversary can expect from a cyberattack by such a degree that they abandon the attack before it's completed."
  - Dr. Larry Ponemon, chairman and founder, Ponemon Institute

Recommendations

- **Make yourself a "hard target" –** Adopting a security posture with a breach prevention-first mindset, instead of a detection and incident response approach, can slow down cyberattackers enough for them to abandon the attack in favor of an easier target.
- **Invest in next-generation capabilities –** Legacy point products present little deterrence to attackers. The use of next-generation security capabilities that automate preventive action and don't rely on signatures alone or static defenses are the best defense against today's advanced cyberthreats.
- **Turn your network visibility into actionable intelligence –** A prevention-focused security posture relies on natively integrated technologies like next-generation firewalls, network intelligence, and threat information sharing. This provides defenders with a clearer picture of what is happening inside their network, versus a confusing collection of uncorrelated point products.

Download the survey findings and analysis at: http://media.paloaltonetworks.com/lp/ponemon/report.html

To learn more about next-generation security capabilities, visit: https://www.paloaltonetworks.com/products/platforms.html

Methodology

Conducted by the Ponemon Institute, the survey queried 304 participants in Germany, the United Kingdom and the United States. 79 percent of respondents described themselves as involved with the attacker community.

About Palo Alto Networks

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets. Find out more at www.paloaltonetworks.com.

Logo - http://photos.prnewswire.com/prnh/20150527/218856LOGO

To view the original version on PR Newswire, visit:http://www.prnewswire.com/news-releases/survey-highlights-the-economics-behind-cyberattacks-300212638.html

SOURCE Palo Alto Networks

Jennifer Jasper Smith, Head of Corporate Communications, Palo Alto Networks, 408-638-3280, jjsmith@paloaltonetworks.com, or Tim Whitman, Voce Communications, 617-721-5994, twhitman@vocecomm.com