3rd Annual Penetration Risk Report Reveals Surprising Trends, Offers New Recommendations

Top Vulnerabilities Persist and Cloud is More Secure

- *Enterprises are 46% more vulnerable than large cloud providers*
- *New threats are on the rise with remote workforce, Internet-of-Things*
- *Application security is twice as secure as last year*

WESTMINSTER, CO – September 10, 2020 – Coalfire, a provider of cybersecurity advisory and assessment services, released its 3rd Annual Penetration Risk Report, based on over 800 penetration tests that emulate cyberattacks to identify vulnerabilities. The tests were performed by Coalfire Labs, the company's threat modeling, attack simulation, and pen testing division, and findings show that organizations continue to struggle with many of the same vulnerabilities and systemic weaknesses year over year.

"Our data shows companies undergoing rapid digital transformation into more complex, multi-cloud environments," said Mike Weber, Vice President of Innovation for Coalfire Labs. "But in this extraordinary year of 2020, it also tells a story of repeating flaws across similar attack vectors over time. This creates an opportunity for holistic cybersecurity solutions that address those systemic weaknesses once and for all."

The report found that company size has a direct bearing on how effectively they are able to fend off would-be attackers. Large and small companies see more than 3x the year-over-year improvement of medium-sized companies.

While many industry verticals saw little to no improvement in year-over-year findings, the technology industry continues to dominate the race toward strong security posture, while threat actors continue to find new ways to breach defenses.

The report's most encouraging finding is that large cloud service providers (CSPs) have dramatically improved security postures when compared to the large, private enterprise category. Signaling the drawdown of on-premise IT systems in favor of the dominant cloud paradigm, the report highlights important trends and tipping points:

2020 penetration risk findings

- *Large cloud providers saw tremendous security gains over the last year, and are 46% less likely to suffer a breach than large enterprises.*

- *As more workloads and supply chains move into cloud environments, top vulnerabilities remain in place: security misconfiguration and cross-site scripting.*

- *Phishing continues to dominate as the easiest breach: 61% of phishing attempts result in full compromise of access credentials.*

- *In a major turnaround toward safer systems, applications doubled their security posture during 2020.*

- *Insecure protocols dominated (22.7%) our top vulnerabilities across all verticals except technology.*

- *Companies are moving from point-in-time to continuous, on-demand compliance monitoring.*

- *Strategies for common frameworks are targeted. Phishing tops the list of issues leading to compromise for our FedRAMP clients - focus on the human side and social engineering attacks. For PCI, attackers looking to compromise data attack the corporate infrastructure where the cardholder data environments are attached rather than through point-of-sale.*

- *Mid-size companies hit the cybersecurity sweet spot in 2018, scrambled to keep up last year, and in 2020, improved only 4% year-over-year in fending off attackers compared to their large and small counterparts.*

“As more companies migrate to the cloud and new dynamics of the remote workforce emerge, executive leadership needs to prioritize a comprehensive programmatic approach to threat and vulnerability management to improve outcomes,” said Mark Carney, executive vice president, Cybersecurity Services. “Our research definitively shows that while some companies are adapting to fast-moving technology, bad actors and systemic weaknesses both persist.”

Since Coalfire’s inception two decades ago, adversarial tactics have evolved from breaking into wireless networks, to preying on vulnerable points of sale, to today’s direct attacks on corporate infrastructure. “Cyber has become a business-oriented corporate objective,” said Carney. “A key leadership takeaway from our research is that Chief Information Security Officers (CISOs) must act as change enablers with increasing authority and accountability to align cybersecurity strategy with business value, performance management, and controls discipline.”

About Coalfire
Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps and effectively manage risk. By providing independent and tailored advice, assessments, technical testing and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe.

###

For media inquiries:
Mike Gallo
(212) 239-8594
luminacoalfire@lumninapr.com