Mimecast Research: 80% of Organizations Surveyed Have Been Attacked by Ransomware in the Past Two Years

November 9, 2021

“State of Ransomware Readiness: Facing the Reality Gap” finds surveyed organizations are confident in their ransomware preparedness despite consistently being the target of attacks

LEXINGTON, Mass., Nov. 09, 2021 (GLOBE NEWSWIRE) -- Mimecast Limited (NASDAQ: MIME), a leading email security and cyber resilience company, today announced the publication of its new report, “State of Ransomware Readiness: Facing the Reality Gap.” Over the past year there has been a dramatic rise in ransomware attacks, and while all organizations are a target, large enterprises are bearing the brunt - experiencing an average of 10,000 attacks over the past two years. This new research report is based on a global survey of 742 cybersecurity professionals.

Resource Gaps
Cybersecurity leaders are facing challenges related to technology, people and processes. The shift to remote work brought on by the COVID-19 pandemic has resulted in numerous new devices to protect, leaving organizations more vulnerable to ransomware through unsecure networks. “State of Ransomware Readiness” found:

- Respondents cited phishing emails with ransomware attachments (54%), web security (47%), and phishing emails leading to a drive-by download (45%) as primary sources of ransomware attacks.
- Only 45% reported they have file backups that would allow them to avoid having to pay the ransom, or to mitigate damage from an attack.
- 45% would like budget to fund more up-to-date data security systems.
- 46% of executives want more frequent security awareness training for end-users.
- 40% of respondents want greater sharing of threat data.

Preparedness vs. Confidence
Mimecast research has shown that ransomware attacks are widespread and prevalent: 80% of organizations have been targeted and experienced an average of 3,000 attacks over the past two years, or four per day. Yet, “The State of Ransomware Readiness” found that 77% of executives are confident in their company’s preparedness for ransomware attacks. The contradiction may be a result of:

- 83% of executives believe they can get all their data back without paying the ransom.
  - Directly contradicts the fact that 39% of organizations paid the ransom.
- 77% of executives believe they can bring their company back to a state of normalcy within two to five days.
- 78% have received incremental budget to help address the ransomware problem.
- 60% of organizations train their employees to recognize email threats that could lead to an attack.

“Ransomware attacks have never been more common, and threat actors are improving each day in terms of their sophistication and ease of deployment,” said Jonathan Miles, head of strategic intelligence & security research. “Preparation is key in combating these attacks. It’s great to see cybersecurity leaders feel prepared, but they must continue to be proactive and work to improve processes. This report clearly shows ransomware attacks pay, which gives cybercriminals no incentive to slow down.”

Ransoms Vary Widely Across the Globe
Responding executives were evenly split when it comes to paying the ransom, 41% did not pay, while 39% did. Thirteen percent of organizations negotiated their payments down. “The State of Ransomware Readiness” found the average ransom to be:

- Australia – AU$ 79,857 ($59,066 USD)
- Canada – C$ 6,666,220 ($5,347,508 USD)
- Germany - € 171,203 ($197,727 USD)
- South Africa - R 3,261,352 ($213,884 USD)
- United Kingdom - £ 628,606 ($848, 377 USD)
- United States - $6,312,190

Ransomware Consequences Reach C-Suite Executives
Successful ransomware attacks can have devastating consequences for organizations. In fact, companies that fell victim to a ransomware attack noted that they saw disruption to their operations (42%), faced significant downtime (36%), lost revenue (28%) and lost current customers (21%). “The State of Ransomware Readiness” found that these attacks are now also causing reverberations on an individual level:

- 39% of executives feel they could lose their jobs over a successful ransomware attack.
- 24% saw changes to their C-suite.
- Two-thirds of executives would feel very or extremely responsible if a successful attack occurred.
- When asked why they feel responsible, 60% said it’s their job to protect the company, and 48% said it would be because
they underestimated the risk of a ransomware attack

To download Mimecast's full "State of Ransomware Readiness: Facing the Reality Gap" report, click here.

Mimecast: Relentless protection. Resilient world.™

Mimecast (NASDAQ: MIME) was born in 2003 with a focus on delivering relentless protection. Each day, we take on cyber disruption for our tens of thousands of customers around the globe; always putting them first, and never giving up on tackling their biggest security challenges together. We are the company that built an intentional and scalable design ideology that solves the number one cyberattack vector – email. We continuously invest to thoughtfully integrate brand protection, security awareness training, web security, compliance and other essential capabilities. Mimecast is here to help protect large and small organizations from malicious activity, human error and technology failure; and to lead the movement toward building a more resilient world. Learn more about us at www.mimecast.com.

Mimecast social media resources:
LinkedIn: Mimecast
Facebook: Mimecast
Twitter: @Mimecast
Blog: Cyber Resilience Insights

Press Contact
Tim Hamilton
Press@Mimecast.com
617 393 7122

Investor Contact
Robert Sanders
Investors@Mimecast.com
617-393-7074