Financial Services Firms Operating Under False Sense of Security

Trend Micro research finds most are over-confident about ability to withstand ransomware

DALLAS, Oct. 25, 2022 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today revealed that financial services firms are more confident they're protected from ransomware than any other sector. Yet at the same time, they're exposed by supply chain risk and sub-par detection capabilities.

To find out more, please visit: https://www.trendmicro.com/explore/glrans

Trend Micro commissioned Sapio Research to poll over 355 financial services IT and business leaders across the globe, as part of a wider cross-industry report into ransomware.

It found that 75% believe they're adequately protected from ransomware, far higher than the average of 63% across all sectors.

This confidence is partly justified: 99% say they regularly patch servers, 92% secure remote desktop protocol (RDP) endpoints, and 94% have rules in place to mitigate risks from email attachments.

> Financial services firms are exposed to cyber risk via their supply chains and sub-par detection capabilities.

However, 72% of respondents admitted their organisation has been compromised by ransomware in the past, and 79% see their sector as a more attractive target for threat actors than others.

This awareness of current threat levels in the financial services sector does not always translate into action.

Around two-fifths do not use network detection and response (40%) or endpoint detection and response tools (39%), and half (49%) don't have extended detection and response (XDR) in place.

This may account for poor detection rates for activity connected with ransomware. Only a third (33%) say they can accurately spot lateral movement, and 44% initial access.

Trend Micro also uncovered significant third-party cyber risk for financial services organisations:

- 56% have had supplier compromised by ransomware, mostly partners (56%) and subsidiaries (29%)
- 54% believe their suppliers make them a more attractive target
- 52% say a significant number of their suppliers are SMBs, who may have less resource to spend on security

"Greater collaboration and information sharing with third parties could help to improve the security posture of the overall supply chain," said Bharat Mistry, Technical Director at Trend Micro. "However, without adequate detection and response capabilities, they may not have the intelligence to hand in the first place. Financial services leaders recognise they're a top target for ransomware actors. It's time to turn that awareness into action."

A quarter (24%) of financial services firms don't share any threat information with their partners, 38% do not do so with suppliers, and even more (42%) don't engage with the broader ecosystem, according to the research.

About Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

https://newsroom.trendmicro.com/2022-10-25-Financial-Services-Firms-Operating-Under-False-Sense-of-Security