Trend Micro

Financial services under fire:

How overconfidence in security could be undermining ransomware mitigation.

Financial services firms play a unique role in society, which makes them an attractive target for ransomware. As providers of critical national infrastructure (CNI), there's tremendous pressure to ensure any service disruptions are avoided or kept to an absolute minimum. That might force business leaders to accede to ransom demands, threat actors reason. These organisations are also the custodians of highly regulated personal and financial information, which can provider further leverage for extorters if stolen.

From the US to Zambia, financial institutions have been finding out the hard way that the sector is increasingly in the crosshairs of a growing group of profit-driven criminal gangs. But how high are awareness levels? And is this translating into stronger security posture?

To find out more, Trend Micro commissioned Sapio Research to poll 355 financial services IT and business leaders from across the globe.

In the crosshairs

Nearly three-quarters (72%) of global financial services firms have been compromised by ransomware at least once over the past three years, according to our research. The vast majority (87%) of these had their data encrypted and leaked (83%) as part of extortion attempts – the latter figure significantly higher than the 74% average across all sectors. Most (92%) also had operations impacted by the compromise, which took days (53%) or weeks (21%) to fully resolve.

That's testament to the increasingly attractive target the sector represents to financially motivated cyber-criminals. Respondents agree, with 79% of them arguing financial services is a more popular target than other verticals, much higher than the 67% average across sectors. Perhaps unsurprisingly given their experience of previous breaches, 87% think they're a target going forward, more than any other sector.

A false sense of security

With this kind of awareness about the scale of the threat, and of previous experience on the receiving end of ransomware attacks, it could be assumed that financial services leaders are laser-focused on mitigating cyber risk. In fact, the majority (75%) we spoke to believe their organisation is already adequately protected. That's the most of any vertical polled for this study and significantly higher than the average (63%) across sectors.

Is this confidence justified? In some respects, yes. Financial services respondents seem to be following best practices to mitigate risk across the main threat vectors for ransomware: phishing, vulnerability exploitation and RDP compromise. To that end, 99% say they regularly patch externally facing servers, 94% have controls in place restricting email attachments, and 92% protect remote desktop protocol (RDP) endpoints.

However, in other respects, security strategy is still lacking. Whilst high, use of network and endpoint detection and response (NDR/EDR) and extended detection and response (XDR) tooling is certainly not ubiquitous. Half (49%) of respondents don't use XDR, 40% don't have NDR in place and 39% haven't deployed EDR. That's a major oversight in a world in which threat actors are increasingly capable of breaching perimeter defences, or outsourcing the work completely to initial access brokers (IABs).

The number of respondents capable of detecting data exfiltration (57%), initial access (44%) and lateral movement (33%) is also disappointingly low.

Tackling supply chain risk

Financial services firms are also exposed by their third-party business relationships. Over half (56%) say a supplier has been compromised by ransomware in the past, most of which were partners (56%) and subsidiaries (29%). A similar number (52%) say their customers and suppliers (54%) make them a more attractive target. The risk of threat actors "island hopping" from these third parties into financial service providers' networks is real.

An additional concern is that most (52%) respondents have a "significant" number of suppliers that are SMBs, who may have fewer resources to spend on cybersecurity. They could improve the security posture of the entire ecosystem by sharing more threat intelligence with these parties, but many don't do so with partners (24%) or suppliers (38%).

It's clear that financial services organisations are on the right track to improving resilience against ransomware. But many lack the critical detection and response capabilities that sound the alarm about suspicious behaviour inside the network. With such tools in place, organisations would get a crucial head start on their adversaries, and be able to contain risk before it spreads. Even better, they'd also have the intelligence to share with and improve the security of the entire supply chain.

TREND MICRO™

Securing Your Connected World