Survey: 48% of organizations attacked by ransomware over 12-month period

Bradley Barth[1]

In a SentinelOne survey, 22 percent of cybersecurity decision-makers whose organizations suffered a ransomware attack said that senior IT staffers lost their jobs as a consequence.

In an international survey[2] of 500 cybersecurity decision-makers, 48 percent of respondents said that their organizations suffered a ransomware attack over the past 12 months. Of that group, 80 percent said that their organizations had to defend themselves against ransomware at least three times during that same period.

Moreover, 54 percent of those who encountered an attack over the past 12 months said that their organizations had to defend themselves against ransomware as many as five or six times, while 32 percent faced seven to 20 such threats, according to the study, conducted in October by technology market research firm Vanson Bourne on behalf of endpoint protection software provider SentinelOne[3].

On average, organizations had to defend against six ransomware attacks over a year's period. "We can say the average today is six, but the average going up and up because the growth rate of ransomware is staggering," Jeremiah Grossman, chief of security strategy at SentinelOne, said in an interview with SC Media.

As a direct result of these attacks, 67 percent of respondents' organizations increased spending on IT security, while 52 percent changed their strategy to focus on mitigation. "This comes down to normal human behavior – we're reactive in nature," said Grossman. "You don't buy your first pair of running shoes until you've had your first heart attack."

Fortunately, the affected digital assets were rarely unrecoverable. Recounting the worst ransomware attack they experienced in the past 12 months, 45 percent of respondents said the malware encrypted some files or data, but the organization was able to decrypt them without paying an extortion fee. Another 27 percent said the attacker wasn't able to encrypt anything, and 25 percent said some assets were encrypted, but ultimately replaced with back-ups.

Still, even if no ransom was paid, the damages were sometimes costly in terms of wasted personnel hours. On average, it took 33 total employee hours for affected companies to replace their encrypted data with clean back-up data. Moreover, some companies experienced major negative repercussions post-attack: 37 percent of respondents said their company's reputation was damaged, while 22 percent said that senior IT staffers lost their jobs.

In light of the ransomware epidemic, 54 percent of respondents at least somewhat agreed that their organizations have lost faith in traditional cybersecurity solutions.

Links

1. https://www.scmagazine.com/author/bradley-barth-3635/
2. https://go.sentinelone.com/rs/327-MNM-087/images/Data%20Summary%20-%20English.pdf
3. https://www.scmagazine.com/search/SentinelOne/