Ransomware attacks taking toll on security professionals as one in three organisations experience attacks weekly - Menlo Security report

Submitted by: Origin Comms Ltd
Wednesday, 3 August 2022

Ransomware attacks show no sign of slowing, according to a new research report, ‘2022 Impacts: Ransomware attacks and preparedness’ (https://info.menlosecurity.com/Assessing-ransomware-readiness-in-2022.html), published today by Menlo Security (https://www.menlosecurity.com/), a leader in cloud security. A recent survey found that a third of organisations experience a ransomware attack at least once a week, with one in 10 experiencing them more than once a day.

The research, conducted among 500+ IT security decision makers at US and UK organisations with more than 1,000 employees, highlights the impact this is having on security professionals’ own wellbeing. When asked what keeps them awake at night, 41% of respondents say they worry about ransomware attacks evolving beyond their team’s knowledge and skillset, while 39% worry about them evolving beyond their company’s security capabilities.

Their biggest concern, however, is the risk of employees ignoring corporate security advice and clicking on links or attachments containing malware (46%). Respondents worry more about this than they do their own job security, with just a quarter (26%) of respondents worried about losing their job.

According to the report, around half of organisations (61% US and 44% UK) have been the victim of a successful ransomware attack in the last 18 months, with customers and prospects the most likely entry point for an attack. Partners/suppliers and employees/contractors are also seen as serious security risks, although one in 10 admit they are unable to identify how the attacks got in. The top three ransomware attack vectors are email (54%), web browsers via a desktop or laptop (49%) and mobile devices (39%).

“Security professionals are coming under increasing pressure as organisations face an unprecedented number of highly sophisticated threats like ransomware,” comments Mark Guntrip, Senior Director of Cybersecurity Strategy at Menlo Security. “On the frontline of cyber defense, they are often coping with huge amounts of stress, worrying about what employees are doing, their team and whether they are getting the right support internally, so it’s no surprise they are prioritising the business over job security. Indeed, the burnout and high churn rate of CISOs is widely reported.”

Cost of recovery from ransomware attacks underestimated

The report also suggests that there is a growing disparity between the perceived cost and actual cost of recovering from a ransomware attack among security professionals. The survey shows that the average estimated cost is $326,531, with insurance payouts extending up to an average of $555,971 – although a significant minority (24%) admit they don’t know the value of their insurance policy or if they have cover. Industry figures (https://news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022/), however, show the average total cost of recovery from a ransomware attack in 2021 was $1.4 million.

Ransomware demands – to pay or not to pay?

There is also some debate about whether to pay a ransomware demand or not. One in three (32%) decision makers worry about the risk of paying a ransomware demand and not getting their data back. Yet nearly two-thirds of respondents would pay a ransomware demand. Almost a third (31%) say it's down to their insurance company to pay it, and nearly one in five say the government should pay. More than a quarter (27%) of respondents say they would never pay a ransomware demand.

Mark Guntrip adds: "Paying a ransomware demand depends on your level of preparedness – do you have the right processes and strong backup in place? If so, you won't need to pay it. If, however, your organisation is unable to function as normal, access data or the damage is likely to bring down the business, that's when you need to re-evaluate your options. With organisations adopting new ways of working and today's Highly Evasive Adaptive Threats (HEAT) (https://www.menlosecurity.com/blog/too-hot-to-handle-why-modern-work-has-given-rise-to-heat-attacks/), now is the time to re-examine your security structures to make sure you stop attacks before they even happen."

To download the full Menlo Security report, visit:
https://info.menlosecurity.com/Assessing-ransomware-readiness-in-2022.html

Additional report findings:
• Less than half (45%) of survey respondents implement a data backup or recovery plan as the first step in the event of a ransomware attack. While 37% inform their employees about an attack and 33% tell customers, only 29% will contact the CEO or Board in the first instance. One in 10 admit they don't know what step one is.
• Employees are seen as the 'weakest link' in terms of cybersecurity, with UK respondents (52%) more worried about them than in the US (33%). They rank well above customers (13%), technology suppliers (12%), contractors (11%), and suppliers and partners (6%).
• Just over half (56%) of respondents are confident in their solutions for remote worker protection, despite one in three (34%) admitting that vulnerable remote workers are one of the biggest challenges when protecting against ransomware.

Survey methodology
Commissioned by Menlo Security, the research was conducted by SAPIO Research in June 2022 using an email invitation and online survey. The company surveyed 505 IT Security Decision Makers working within organisations with 1,000+ employees across the US (251) and UK (254) – 61% at IT manager level and 39% at C-level. The top three business sectors were Software/Technology (18%), Healthcare (13%) and Government/Public Sector (11%).

About Menlo Security (https://www.menlosecurity.com/)
Menlo Security protects organisations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security's isolation-powered cloud security platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end user-experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies, eight of the ten largest global financial services institutions, and large governmental institutions. Menlo Security is backed by Vista Equity Partners, Neuberger Berman, General Catalyst, American Express Ventures, Ericsson Ventures, HSBC, and JP Morgan Chase. Menlo Security is headquartered

in Mountain View, California. www.menlosecurity.com.

For more information, access to graphs/charts and other graphics, please contact the Menlo Security PR team at Origin Comms: menlo@origincomms.com.