Trend Micro Study Finds 39% of Employees Access Corporate Data on Personal Devices

Remote working has changed how business data is handled
Corporate data policies may need to be refreshed as workforce remains remote

DALLAS, Sept. 14, 2020 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), the leader in cloud security, today released survey results that show smart home devices and their apps represent a major weak link in the corporate cybersecurity chain as the lines between work and home life increasingly blur.

Trend Micro's *Head in the Clouds* study surveyed more than 13,000 remote workers across 27 countries to find out more about the habits of distributed workforces during the pandemic. It revealed that 39% of workers use personal devices to access corporate data, often via services and applications hosted in the cloud. These personal smartphones, tablets and laptops may be less secure than corporate equivalents and exposed to vulnerable IoT apps and gadgets on the home network. More than one third (36%) of remote workers surveyed do not have basic password protection on all personal devices, for example.

Dr Linda K. Kaye, a cyberpsychology expert said: "The fact that so many remote workers use personal devices for accessing corporate data and services suggests that there may be a lack of awareness about the security risks associated with this. Tailored cybersecurity training which recognises the diversity of different users and their levels of awareness and attitudes around risks would be beneficial to help mitigate any security threats which may derive from these issues."

More than half (52%) of global remote workers have IoT devices connected to their home network, 10% using lesser-known brands, the study revealed. Many such devices – especially from smaller brands – have well-documented weaknesses such as unpatched firmware vulnerabilities and insecure logins. These could theoretically allow attackers to gain a foothold in the home network, then use unprotected personal devices as a stepping-stone into the corporate networks they're connected to.

There's an additional risk to enterprise networks post-lockdown if malware infections picked up at home are physically brought into the office via unsecured personal devices at organizations with bring-your-own-device (BYOD) practices.

The research also revealed that 70% of global remote workers connect corporate laptops to the home network. Although these machines are likely to be better protected than personal devices, there is still a risk to corporate data and systems if users are allowed to install unapproved applications on these devices to access home IoT devices.

"IoT has empowered simple devices with computing and connectivity, but not necessarily adequate security capabilities," said Bharat Mistry, principal security strategist at Trend Micro. "They could actually be making hackers' lives easier by opening backdoors that could compromise corporate networks. This threat is amplified as an age of mass remote work blurs the lines between private and company devices, putting both personal and business data in the firing line. Now more than ever, it is important that individuals take responsibility for their cybersecurity and that organisations continue to educate their employees on best practices."

Trend Micro recommends employers ensure their remote workers are compliant with existing corporate security policies, or, if needed, companies should refine these rules to recognise the threat from BYOD practice and IoT devices and applications.

Companies should also reappraise the security solutions they offer to employees using home networks to access corporate information. Shifting to a cloud-based security model can alleviate many remote working risks in a highly cost-efficient and effective manner.

About Trend Micro
Trend Micro, a global leader in cybersecurity, helps make the world safe for exchanging digital information. Leveraging over 30 years of security expertise, global threat research, and continuous innovation, Trend Micro enables resilience for businesses, governments, and consumers with connected solutions across cloud workloads, endpoints, email, IIoT, and networks. Our XGen™ security strategy powers our solutions with a cross-generational blend of threat-defense techniques that are optimized for key environments and leverage shared threat intelligence for better, faster protection. With over 6,700 employees in 65 countries, and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to secure their connected world. www.trendmicro.com.

SOURCE Trend Micro Incorporated

For further information: Funda Cizgenakad, media_relations@trendmicro.com

https://newsroom.trendmicro.com/2020-09-14-Trend-Micro-Study-Finds-39-of-Employees-Access-Corporate-Data-on-Personal-Devices?fbclid=IwAR1kUmMw744pFaHUWL5giCtecDZBSkdQ3XGPmS2NLL5BxXxHagbr8P-I7us