ELEARNINGNEWS ARTICLE

Year 4 - number 114 Wednesday 27 may 2020

COVID-19: smart working, video conferencing and cybersecurity

Digital reality is a resource and an opportunity, but it also brings vulnerabilities and critical issues that should not be underestimated.

During Phase 1 and 2 of the **Coronavirus** pandemic management, telematic resources (from **smart working** to **eLearning**, to **videoconferencing**) were crucial to allow professionals to manage the situation in the best possible way, not stopping the work or preparing for the restart.

Digital reality is a resource and an opportunity, but it also brings vulnerabilities and critical issues that should not be underestimated. First of all, those related to the **cybersecurity** of your computer devices or main stream videoconferencing platforms that, thanks to their notoriety, often appear as completely secure.

This is certainly not the time to let your guard down: a research commissioned by Check Point shows an increase in the risk of **cyber attacks** and data theft beyond the usual, already high in itself. The results of the research report a worldwide increase in attack attempts for 71% of companies and security problems related to telework for 95% since the outbreak of the pandemic. In this historical phase that bets everything on digital, cyber criminals have exploited the fears and mechanisms triggered by the covid-19 pandemic.

As mentioned, out of a sample of 411 professionals employed by companies worldwide, 71% of respondents reported an increase in threats or attacks targeting their company since the outbreak of the pandemic: phishing attempts (55%), malicious websites claiming to offer information or advice about the pandemic (32%), increased malware (28%) and ransomware (19%).

As far as **smart working** is concerned, 95% of respondents say that IT security problems have increased as a result of the need to adopt teleworking en masse. The three main challenges cited are the difficulty of ensuring secure remote access to applications (56%), the need for scalable solutions for remote access (55%) and the proliferation of "shadow IT" solutions used by employees without the company's consent (47%).

IT security must be a key priority. Tomá? Foltýn, content writer at ESET Security Community, explained in a recent article how the continuing demand for people-to-people and business-to-business videoconferencing is highlighting many privacy and security issues, particularly in terms of overloaded platforms such as Zoom.

Videoconferences and criticalities: the Zoom case

"At a time when most people are confined within their homes in an attempt to contain the COVID-19 pandemic - the expert's paper says - the popularity of video conferencing software for work, education and leisure is exploding. Among the various communication tools that have suddenly been pushed into the limelight, probably the one that stands out most is Zoom". A very famous digital platform that, lately, has had to face a great demand from individuals and companies that has brought to light issues related to privacy and security. "The developer of the app - continues the cybersecurity specialist - is facing a storm of criticism from various fronts, including privacy advocates, security experts, several senior US officials and the FBI. Criticism has continued to accumulate over the last few days, prompting the company to respond. A few weeks ago, the company's founder and CEO, Eric S. Yuan, apologized for the problems that had arisen and outlined measures to strengthen Zoom's security and privacy. "He also announced," Foltyn continues, "a 90-day stop to development activities, pointing out that the company is dedicating all its engineering resources to "solving trust, security and privacy issues.
What are the problems Zoom has stumbled upon? "Zoom's privacy policy - points out the IT security professional - did not mention that the iOS version of its app sent analytical data to Facebook even of users who did not have a Facebook account, according to a report by Vice at the end of March. The company recognized the problem and removed Facebook's Software Development Kit (SDK) for iOS, and is currently in the middle of a class action lawsuit in California over this issue. Despite the

claims, the application's video and audio meetings do not support end-to-end encryption, according to research by The Intercept. The company made it clear that it uses the Transport Layer Security (TLS) encryption transmission protocol. The main difference is that it does not guarantee that users' communications are invisible to the company. In addition, the app also revealed several security vulnerabilities, although they were all resolved in a short time. A UNC path injection vulnerability was found on its Windows client that could expose users' Windows login credentials and even lead to arbitrary commands being executed on their devices. Two other bugs, this time involving Zoom's MacOS client, could have allowed an attacker to take control of a vulnerable computer. As if that wasn't enough, then: "The FBI - Foltyn adds - also highlighted the "Zoom-bombing" phenomenon following multiple reports of trolls sneaking into private meetings and school lessons to show images that didn't fit the context".

The risk was very high for a huge number of people, as the platform has seen the number of daily users multiplied by at least twenty in recent months. By Yuan's own admission, Zoom was overwhelmed by an unexpected success. "We now have a much larger set of users who are using our product in a myriad of unexpected ways, presenting us with challenges we had not foreseen when the platform was conceived.

So the cybersecurity expert's question is: "How do we stay safe?". Also, and most importantly, at this time of remote working (whether it's smart working or video conferencing), we should never overlook the importance of our privacy and security. For example, with regard to the case in point, "The most effective measures to be taken to protect security and privacy include: password protection of meetings and control of meeting participants; limitation of screen sharing to the organiser; abstention from sharing links or meeting IDs on social media".

Translated with www.DeepL.com/Translator