ELEARNINGNEWS ARTICLE

Year 4 - number 120 Wednesday 8 july 2020

The world of smart working: cyber security

Let's find out the cybersecurity implications that the l nimble work he brought with him.

We talked in this article about the psychological and physical implications associated with the massive use of **smart working** during the months of quarantine.

But the phenomenon of mass and "hasty" adoption of home working has revealed critical issues and best practices also in terms of **cyber security** and defence against cybercrime.

Smart working and cybercrime

The haste with which companies and professionals have had to change the way they work, converting everything that could previously be done in the office or in person to online and remote, has created new **IT security risks**.

All the main cyber security experts - including those of Clusit, the Italian cyber security association - have launched alarms: the sudden spread of smart working has increased the risk of hacker attacks in search of money and confidential data.

"The smart worker runs greater dangers online. He is not in the office, where he can count on the direct support of technicians if he runs into malware, for example. He may lack many of the corporate protections that worked well in the office, but not at home," explains Alessio Pennasilico, an expert and member of the Clusit's board of directors.

The problem is exacerbated by the context: "We work more hours online, we manage more emails, we are always in video conferencing: as a result we are more tired and more prone to security errors," he adds. Basic cyber security errors: how to click on links or open phishing email attachments; downloading apps or programs from unreliable sites potentially full of malware that can steal personal data, passwords, login credentials.

If "home PCs" are used in smart working to connect to the company network, the consequences are even more disastrous: they carry infections everywhere. If you save everything on your home PC and malware blocks the disk, you can't count on corporate backup. The theft of the email password, the videoconferencing system now cuts you completely off from the world, as all relationships with colleagues, customers and suppliers have to go through the internet," continues Pennasilico, cyber security expert.

Giorgio Sbaraglia, IT consultant, confirms: "Smart working significantly increases the risk of cyber attack and data breach and theft. For those who work remotely, the greatest risks are - once again - linked to the human factor and social engineering. And most threats (about 90 percent, as also confirmed by a recent report by Yoroi) come through email," he says.

We may receive an **email** that seems to be sent from the personal address of the boss or a colleague. Given the smart working situation, we won't be so suspicious that the boss doesn't use corporate email (also in smart working). "But if the email address has been forged for malicious purposes, clicking on the link or attachment will result in malware intrusion into the victim's computer. This risk would have been much less likely if the employee had been in the office, where - among other things - he would have had the opportunity to ask the IT department for advice on what to do when faced with such an email", says Sbaraglia.

Moreover, cyber criminals are adept at grasping the trends of the moment. For this reason, phishing emails use the most current topics: in about 230 thousand spam and phishing campaigns detected in recent months (6% hit Italy), the most frequent keywords were: Covid-19, coronavirus, WHO (World Health Organization) and the different videoconferencing platforms.

Fortunately, after the most emergency phase, now workers and companies can set up better defences against cyber risk.

Experts agree: user awareness of cyber risks is the nodal point of **cyber security**. "The human factor is the cause of over 95% of all cyber attacks," says Sbaraglia. "The company must also provide its employees with an adequate level of training and awareness of the use of cyber tools. Awareness that can be summarized in the Zero Trust model (trust is good, not trust is better), to avoid that a hurried or distracted click blocks a company".

For this purpose, the one-hour online " **Cyber Security - Company information protection**" course is very useful.

To prevent attacks, in a basic way, everyone should activate two-factor authentication for all services where it is possible to do so (social, Google account, email). "Even if companies were to provide fully armored devices, they would still have to guarantee secure and secure wifi and routing systems at the employee's home at the same time. All governed by policies and procedures for the proper use of the systems and company equipment," says Iezzi. And he adds: "But that wouldn't be enough. The home network can also be put at risk by the behaviour of other members of the employee's household. For this reason, the training activities that are periodically carried out for employees could also be extended to family members".

In the opinion of experts, the most technical policies that companies should adopt are those aimed at:

- determine the company's videoconferencing and chat system;
- make periodic technological risk analyses;
- constantly conduct asset and software inventory activities in order to identify non "corporate" hardware or software objects;
- adopt network monitoring systems in order to identify anomalies in company network traffic through early warning systems;
  have an adequate disaster recovery system or at least an effective cloud backup system;
- activate a separate partition on the home PC to manage and store company data.

It would be even better to opt for "**cloud based**" solutions and applications: the application is in the supplier's cloud and you only need an internet connection and a connection interface (a browser). In this way the employee can use the computer without installing any software and minimizing the risks mentioned above. However, this solution cannot be improvised: it requires time and programming. It will be advisable to adopt products from reliable suppliers, avoiding improvised and free solutions even when choosing **VPN** (Virtual Private Network). The advice is to prefer VPNs that use encryption of transmitted data, so as to have a secure communication. Finally, if you use the Remote Desktop (RDP) connection, it will be essential to set strong passwords and - as additional security - enable two-factor authentication.

Translated with www.DeepL.com/Translator