TELEWORKING UNDER COVID-19 THREAT

Posted on 13/04/2020

Category: Archive

This viral context, which forces teleworking, requires a special approach that most law firms and professionals are taking care of and, in turn, they are informing their clients and the general population about the precautions and recommendations to be followed, in this case, to

safeguard, among others, the health of computer systems

On March 19, the National Cryptology Center's Incident Response Team, CCN-CERT, warned of a surge in malware campaigns using Coronavirus/COVID-19 pandemic-related themes to infect individuals and organizations around the world through a statement.

“At the moment -said the statement- there are more than 24,000 domains registered on the Internet that contain the terms: 'coronavirus', 'corona-virus', 'covid19' and 'COVID-19'. Of these, more than half, 16,000, have been created in the month of March (10,000 in the last week). Some of them have legitimate purposes, and others are dedicated to spam campaigns, spear-phishing or as command and control servers, C2. It has also been detected that some Trojans like Trickbot and Emotet have evolved their TTP to evade detection, using the news related to the coronavirus."In this context, how is information security controlled? The coronavirus has forced teleworking not only in law firms but in all kinds of companies. "The coronavirus has made it necessary for companies to enable teleworking and mobility to the highest degree. Of course, ensuring the highest degree of safety and efficiency. It is comparable to the contingency situation of an unusable workplace and this will test all companies' business continuity plans; we have a difficult test ahead of us to pass and we must learn from it regardless of the results," says **Manuel Asenjo** (pictured bottom left), IT director at Eversheds Sutherland Nicea. **Jesús Yáñez** (pictured top left)**,** Risk & Compliance, Cybersecurity and Privacy & Data Protection partner at Écija Law & Technology, tells us that, for his part, "on Monday 16 March 2020, ÉCIJA activated the mandatory teleworking plan for all its professionals. However, it is worth mentioning that the firm has a free teleworking policy, that is, our professionals can telework every day they need to. In this aspect, we are one of the first firms that bet on teleworking in business law in Spain, therefore, our Cybersecurity systems already contemplate a system a relative amount of telework and we do not expect greater risks of cyberattacks out of the ordinary.

Our Cybersecurity team continues its normal activity and there are no known cases related to COVID-19. Another initiative is that we have made a helpdesk available to our customers; a multidisciplinary team formed by partners from different practices, to answer any questions that our customers may have. Finally, we have also prepared a Cybersecurity decalogue for teleworking that companies should take into account."Cybercriminals, who are aware of the vulnerabilities involved in teleworking, have already begun to take advantage of this situation, says **Francisco Pérez Bes** (pictured bottom centre)**,** Digital Law Partner at Ecix Group: "When we work outside the office, we are even more vulnerable to cyberattacks, so we have to be extremely careful about the type of information we send, as well as being cautious about accessing files or links. We are seeing this with the coronavirus crisis, where criminals (sometimes third parties seeking social destabilization, which can lead to a real national security problem), spread fake news and pages in order to take advantage of the users' concern, and the greater likelihood of them accessing compromised resources, for

criminal purposes. Such practices allow them to rapidly spread malware, such as - among others - the dreaded ransomware Emotet. This is where prevention and awareness are effective tools to ensure the Cybersecurity of companies and individuals."

The best thing is to be trained and prepared. **Joaquín Muñoz** (pictured top centre), head of IT & IP Law at Ontier explains it this way: "in these days in which the majority of professionals, also lawyers, are working in remote, there is a series of issues that we can remember to maintain a safe access to servers and a safe treatment of information. There are many measures to be implemented depending on each company s operation, but the first thing is to use only the equipment that the company makes available to the workers and that has the protection software. In this sense, it is advisable that all work activity is carried out in an environment controlled by the office, enabling a remote and direct access to the server being the easiest way, avoiding keeping documents locally. If it is necessary for the worker to access from a particular device, it will be advisable to determine unique credentials that identify him in the accesses to the corporate documentation and to create secure accesses to it, through VPN, for example. On the other hand, assigning roles and limiting access according to those roles becomes more relevant in remote access situations and it is always important to be able to keep access logs to monitor the activity. The above, without prejudice to many other security measures that can be implemented, may not work if the company does not invest time and resources in creating a culture in which all employees are aware of their responsibility and are committed to fulfilling the obligations that the company imposes in this area."But the dangers are not exclusive to the situation caused by COVID-19. Francisco Pérez Bes explains that "the lawyer, by the very nature of his profession, has to travel out of the office on numerous occasions, which means that the type of risks to be dealt with is different. Thus, law firms must let their lawyers know how to act during business trips, during which a great deal of information about operations and contracts will be managed, which can have great commercial value. And it is this professional s responsibility to protect the secrecy and confidentiality of such information.

Failure to protect our devices screens when working in public, revealing information in telephone conversations, using public Wi-Fi networks (which may have been breached), or losing a simple mobile phone or pen drive without the information being encrypted and protected by a password, are all negligence which, in addition to jeopardizing the client's trust, are legally and deontologically penalized. Teleworking is also common in this profession. For this reason, offices must have access to their systems from the outside, well protected (by means of strong passwords) and encrypted (preferably by means of VPN). They should also make those employees aware that they should be cautious about the information they include in their messages when they work out of the office, since there is a greater probability of suffering some kind of security incident (for example, a communications interception). Not necessarily because a cybercriminal gains access to the communication channel, but because the professional tends to lower his guard and use terminals that may have been compromised at some point (e.g., having some type of malware installed), or that have insecure applications installed. In such a case, a third party could access sensitive information before it is sent through the firm s systems, without being detected."In addition to all the above, **Noemí Brito,** partner and head of Technology area at Ceca Magán warns that: "it is important to consider the recent recommendations made to this effect by both the National Institute of Cybersecurity (INCIBE) and the National Cryptology Centre (CCN), which can be summarized as the need to adopt and implement a coherent and reasonable policy for secure remote access.

The solutions range from the implementation of a cloud-based solution with sufficient security to a system based on local, on-premise systems, in which the organization s limits are extended beyond its premises. The main objective of this policy would be, in any case, to provide the relevant security measures for this type of access, as well as the articulation of secure systems including videoconferences, connections with suppliers and customers. Without prejudice to the above, which

would be desirable, in any case, certain parameters should be ensured in teleworking situations (with company support if feasible or possible), in particular, if the equipment, network or device is provided by the worker."Aware of the added risks posed by the widespread situation of teleworking, the Incident Response Team of the National Cryptology Centre, CCN-CERT, has prepared a Good Practice Report: CCN-CERT BP/18 Security Recommendations for Teleworking Situations and Reinforcement in Surveillance and Security Measures for Remote Access.

Article by Desiré Vidal.

To read the article in full please download issue N.93 here