FINANCIAL INTELLIGENCE & PROCESSING

Cybercriminals are also working remotely!

Placing the population in confinement to limit the spread of the Coronavirus has precipitated remote working for many businesses that were not necessarily prepared for it.

The adaptation of computer stations to allow for external connections to the companies' IT systems has, in many cases, been done in emergency rather than organically. Those that already had remote working procedures and suitable equipment in place prior to confinement were only required to increase capacity to cope with the increase in the number of remote workers using their IT systems. The situation is very different for companies which, following confinement, had to hastily improvise solutions to ensure the continuity of their operations.

The security flaws are, therefore, multiple. Some of the more serious examples include:

- Use of the employee's personal computer for personal affairs as well as work purposes;
- The use of a poorly secured WiFi connection, which may be shared with neighbours;
- The implementation of outdated computer communication protocols, which are unsecured and unencrypted;
- Staff untrained in computer security rules in ill-equipped conditions.

Cybercriminals are seeing this as a slice of luck, as they do not intend to pause their own «businesses» for a single moment.

They are already taking full advantage of the coronavirus outbreak by sending out fraudulent mailing campaigns or through the distribution of compromised applications (modified to include hidden malware), in order to gain control of computers. During any major national or global event, cybercriminals take advantage of the increase in people's fear and their increased interest in news to spread such malware. They use this opportunity to attack corporate information systems to either steal sensitive information, which they can monetise, or to install ransomware.

To reduce these risks, there are a number of good practices a company or individual can incorporate:

- Each employee must be provided with a laptop for professional use only. This computer must contain effective and regularly updated antivirus software as well as data encryption, in order to protect the equipment in the event of theft.
- Use a VPN connection. Employees' connection to a company's IT system must be secure. A VPN will hide business' online activity and protect it and its employees from cybercriminals by hiding data traffic through an encrypted tunnel. The hardware firewall will also tend to have a VPN function that you can activate. These solutions are generally inexpensive and affordable for all businesses.
- The IT department must ensure that operating systems and application updates are installed punctually. The main function of updates is to close the security holes that have been identified. Malware relies on the exploitation of these security vulnerabilities to function. Once these vulnerabilities are closed, the malware that exploits them is no longer a threat.
- Ensure the periodic backup of user data on removable hardware such as USB sticks.
- Ask employees to use unique passwords for professional purposes which differ in format to those they use for personal use. Some online sites or services store passwords associated with user accounts in clear text. Cybercriminals are well-versed in testing the login and password pairs they have collected on all online services in order to gain access to other systems.
- Ask employees to be even more vigilant than usual when receiving solicitations by email or telephone. Any unusual requests should go through a validation process with the requestor's superior through a different communication channel than that used by the requestor.
- If necessary, update your IT Security Charter listing the rules and responsibilities for the use of information system resources, making sure to include specific recommendations for remote working. This document acts as a reference manual for employees in case of doubt. It informs them what is permitted on the equipment made available to them and under which circumstances. Finally, it would be worth redistributing the charter, along with specific recommendations in the current unsettling period of time. ■

FIP Services

FIP was formed in 2005 as a risk intelligence agency specialised in anti-financial crime mitigation and investigation. We combined the skills of experts in corporate intelligence, financial engineering, fraud examination, and computer forensics, to undertake all forms of corporate investigation as required by our clients.

- Enhanced due diligence
- Pre-qualification and compliance of partners
- Evidence search – commercial or patrimonial litigation context
- Financial expertise in litigation or arbitration, damage valuation
- Fraud Risk Management process review
- Whistleblower claims review & other corporate internal investigation
- Forensic Accounting & related Fraud Investigation Services
- Computer Forensics and IT security audits
- Asset tracing and recovery