Read this post online

Covid-19 and Telework: Data protection

The Covid-19 pandemic has prompted many companies to implement teleworking solutions. The implementation of this type of working method requires that rules be duly followed to guarantee the security of information systems and processed data.

The French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés* or "CNIL") has published recommendations to help secure personal data in this context.

The Covid-19 global health crisis required the implementation of lockdown measures and strict travel restrictions allowing only travels for essential reasons. Companies, associations, administrative authorities or communities that had the possibility to do so had no other choice but to implement telework in order to preserve at the very least the continuation of essential activities that this working method can allow.

Some were already prepared to cope with telework but assuredly not on such a massive scale and over such a long period. Others had to implement it urgently, perhaps even "remotely". In some cases, and because it has not been possible to deploy the necessary means, telework is even carried out from employees' personal equipment (within the framework of the Bring Your Own Device (BYOD) practice), the level of security of which cannot be assessed, let alone guaranteed. And the use of this equipment makes it more difficult to draw a clear line between private life and professional life.

At the same time, cybercrime has increased since the start of the COVID-19 pandemic as cybercriminals are seeking, like in any exceptional situation, to make the most of it.

Employers are responsible for the security of their company's personal data, including when stored on terminals over which they have no physical or legal control but that they have authorized to be used to access the company's IT resources.

The risks against which it is essential to take precautions range from a one-off attack that impacts the availability of the system or the integrity and confidentiality of the data, to the general compromise of the company's information system (intrusion, viruses, Trojan horses, etc.).

How to reduce such risks? This article outlines the best practices to be followed to set up and manage telework.

Securing the information system

Opening up a company's information system to the outside world can create serious security risks that could jeopardize the company, and even threaten its survival in case of a cyberattack. It is therefore essential for every company to secure its information system by implementing the following recommendations:

- publish a telework security policy or, in the current context, at least a minimum set of rules to be followed, and circulate this document to your employees in accordance with the internal rules and regulations. As far as possible, favor for teleworking purposes the use of means that are made available, secured and controlled by the company. When this is not possible, give clear instructions concerning equipment use and security to employees but be aware that their personal equipment can never have a verifiable level of security;
- if necessary, amend the management rules of the information system to allow teleworking (change the authorization rules, remote administrator access, etc.), measure the risks involved and, if necessary, take the necessary measures. In particular, provide external or remote access (Remote Desktop Protocol (RDP)) only to essential persons and services, and strictly filter such access through the firewall. To preserve systems for which remote access is not necessary, isolate them, especially if they are sensitive for the company's business;
- equip all employee workstations with at least one firewall, antivirus software and a tool for blocking access to malicious websites;
- set up as soon as possible a Virtual Private Network (VPN) to avoid direct exposure of services on the Internet, and activate, if possible, a two-factor authentication processes. In addition to encrypting external connections, this device also makes it possible to strengthen the security of remote access by limiting such access to authenticated devices only.

Internet Services

For the Internet, it is recommended to:

- use protocols that guarantee the confidentiality and authentication of the receiving server, e.g. HTTPS for websites and SFTP for file transfers, using the most recent versions of these protocols;
- apply the latest security patches to the equipment and software used (VPN, remote desktop solution, messaging, videoconferencing, etc.), and regularly consult the CERT-FR News Bulletin[1] to get to know the latest software vulnerabilities and how to protect against them;
- implement two-factor authentication mechanisms on remotely accessible services to limit the risk of intrusion;

- regularly check access logs for remotely accessible services to detect suspicious behaviors;
- refrain from making unsecured server interfaces directly accessible. In general, limit the number of services made available to the strict minimum to reduce the risk of attacks.

---

[1] The news bulletin of the National Cybersecurity Agency of France: https://www.cert.ssi.gouv.fr/actualite/