COVID 19: CRISIS MANAGEMENT

IT security & data protection in times of Corona (CoVid19)

DEKRA

In most companies, the current Covid 19 crisis is leading to a rapid increase of people working from home. Obviously, home office has a lot of advantages such as ensuring the continued operation of administrative business processes. At the same time, working from home creates new challenges in the area of IT security and data protection for those organizations and their employees.

For your convenience, we have compiled some recommendations for business owners, entrepreneurs and employees.

2. IT SECURITY IN THE HOME OFFICE A QUICK GUIDE FOR SMES AND THEIR EMPLOYEES

Implemented information security systems e.g. according to ISO 27001offer excellent protection

The foundation of efficient information security lies in the implementation, establishment and continuous improvement of an information security management system (ISMS). Among others, this prescribes information security guidelines, regular training of employees regarding data protection and information security or provides guidelines for mobile working such as in the home office.

The latter is particularly necessary in the current situation of Covid-19.
The following overview is meant as an initial guide.

Use of VPN (Virtual Private Network)

To enable secure communication in the home office, employees should only connect to the employer's network via a secure VPN connection. The VPN enables encrypted communication between the sender and receiver and thus ensures a secure communication process.

Evaluation of employee's home network

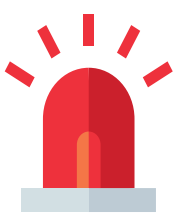
Employees should evaluate their own home network and connected devices. The weakest link in a network determines its security. Here are some examples:

- Does everyone's computer have the latest anti-virus update installed? This includes children, partners and anyone else connecting to your network.
- Is the router up to date?
- Is work and private usage strictly separated?
- Is a separate device is used for this exceptional situation?

Carrying out a security check

Even while a large number of employees are in the home office, employers should ensure that:

- Software updates and patches are regularly installed,
- Configurations, user and administrator rights are regularly checked and, if necessary, adjusted,
- Processes in response to cyber-attacks can be also steered, controlled and handled remotely and, if not, adjusted accordingly.



Sensitization of employees

In the current situation employers should once again urgently sensitize all employees in home office to the associated risks around information security.

This includes among others:

- Covid-19 leads to heavily increasing numbers of phishing emails
  > Do not open messages or attachments from unknown senders
  > Remain vigilant and check URLs and sender addresses

- Covid-19 leads to heavily increasing numbers of social engineering attacks
  > Be particularly cautious if:
  - Emotionality and urgency is addressed,
  - Exclusivity is stated by an unknown sender,
  - Spelling and grammar mistakes are apparent

- Educating the family
  A computer for work should only be used for work purposes and cannot be used by children or partners in parallel. A strict separation must be ensured!

- Examination of the working environment in order to protect company privileged information
  Employees should find a protected working environment at home in which confidential conversations and the exchange of sensitive information can be carried out undisturbed. This ensures that crucial information does not leave the company and is not made accessible to unauthorized persons.

- Social networks
  Employees should not log into social networks via their work equipment. Furthermore, they should only share generally accessible information in their profiles.

- Protect carefully work-related passwords
  Employees should protect passwords from unauthorized access and should not write them down or share them with family members.

- Opening a separate account when using private devices for business
  Employees who access company software via private devices should at least create a separate account for these activities.

- Reporting of data protection and IT security incidents
  Just like working from the office, so too in times of home office data protection and IT security incidents should be reported by employees immediately. Employers must ensure that the contact persons are known and that a functioning process has been established. The employee is obliged, without any exceptions, to immediately inform the employer if suspicious activities are noticed. It is advisable for employers to set up a hotline.

- Hygiene
  Employees should always ensure a high level of (personal and) device cleanliness. IT equipment that is used should be cleaned regularly. Always follow the device manufacturer's advice on cleaning. Using a damp microfiber cloth with soap and water may be all you need.