INFOPAPER:
HOW TO MANAGE IT SECURITY IN THE HOME OFFICE

Content

Introduction

The alarm clock rings later, you can have lunch at home and childcare is easier to arrange. Working in a home office can have many advantages. However, certain points should not be overlooked so that IT security can be ensured when working outside the company. Hornetsecurity has some recommendations to help with this.

HORNETSECURITY

Home office - but don't forget security precautions

The advance of digitalization and the development of new technologies have already brought about many changes for the economy worldwide: cloud computing, big data, robotics and artificial intelligence offer companies across sectors and industries advantages such as the optimization of processes, savings in resources and rapid data and information exchange.

New companies and jobs are created on the basis of these developments. In addition, the trend has led to **changes in the workplace:** many employees can perform their tasks regardless of location and still continue to communicate with their colleagues and employer. Companies make it possible for their employees to work from home.

Microsoft Office 365 is considered a major driver of collaborative work via the cloud, allowing important files to be stored and shared in real time from anywhere. This further simplifies work in the home office.

In times of crisis, such as the corona virus pandemic, telecommuting is often the only way for companies to ensure the safety of their employees while maintaining business operations. Both employers and employees, however, are constantly **raising questions about IT security:**

- How can the protection of the company-wide IT infrastructure be guaranteed from the home office?
- Do companies and employees have to take certain measures?
- Are protective mechanisms such as spam and virus filters also active in the home office?

In the following section, we explain security risks in the home office and possible precautions that will ensure the **protection of internal company data and remote communications.**

Train your employees and inform them about potential risks

First, employees should be informed about **possible security risks and protective measures to be taken** before they begin working from home.

Provide clear, unambiguous and **binding regulations on IT security** and the security of company data in written form so that the procedure is transparent and comprehensible for everyone.

It is particularly important to sensitize people to **potential dangers** such as phishing attacks, which are obviously still a threat in the home office.

In addition, make sure you communicate who employees can turn to if security-related problems arise, so that they can react quickly.

Secure your company data and use VPN clients

The WLAN at home, in a café or on the train can pose security risks. If employees access **sensitive data** or log into business accounts over such an unsecured network, the company is at risk from cybercriminals tapping into information in the event of a hacker attack. Companies must therefore establish security measures such as **virtual private network (VPN)** solutions for use in conjunction with WLAN.

The VPN service can also be supplemented with 2-factor authentication and when working via VPN, the employer should take care to limit access rights so that each person can only access the information relevant to them.

There is also a risk of data loss if an employee stores sensitive information on a laptop, which could be stolen. Sensitive data should ideally only be stored on **secure company servers or in cloud environments** that can only be accessed via VPN. Nevertheless, if data is stored on external hard disks, it is important to encrypt this information or access.

Prevent unauthorized access and viewing

In order to make effective use of travel time, **a lot of work is also done on the move**, for example at the airport or on the train. The problem with this is that people sitting next to you are given the opportunity to read internal company information. **Privacy filters** should therefore be used whenever sensitive company data is accessed outside the office. In addition, a **screen lock** must be activated immediately as soon as the employee leaves the computer - this should also occur when working from home. Of course, access to the computer should require a **password at startup**.

Provide company-owned hardware

The user's end device represents a major security gap. While it is relatively easy for company IT to enforce and ensure certain minimum security requirements for company devices, this is difficult for employees' private devices.

The protection of these end devices is only partially possible. Especially USB sticks and external hard disks are regarded as a **gateway for malware.** However, there are various approaches to get the risks under control. These include **device-specific policies** that ensure at least the most important security components are installed and activated on the clients — for example, automatic locking, unlocking by password only or malware scanners and firewalls.

Measures such as **network access control (NAC)** mechanisms also help. With these, only authorized devices have access to the company network, and it can be guaranteed that the relevant components are active. **However, the safest way is to use the company's own hardware.**

Install current security software

All corporate devices, including smartphones and laptops, should be protected by appropriate and **up-to-date security software.**

At best, this includes **features for data deletion of devices** reported as lost or stolen, separation of personal and professional data, and restriction of app installation options.

But security software is not just about securing devices; cybercriminals are also targeting **applications and services**. One of the most popular attack targets is **Microsoft Office 365**, which currently has around 180 million corporate customers internationally. Since Office 365 is cloud-based, it is ideal for home office work.

However, identifying an Office 365 user is very easy for an attacker, because the MX records and autodiscover entries are publicly accessible on the net.

Comprehensive security features are designed to ward off possible attacks from Office 365 accounts, but it must be remembered that the data in the cloud itself — even in the event of unauthorized access — can be accessed from anywhere. By using Office 365, companies eliminate an important security aspect: the firewall.

If an attacker succeeds in gaining unauthorized access to an Office 365 account, all data is available to him without restriction. Security experts therefore recommend not relying solely on Microsoft's protective mechanisms, but also to secure Office 365 accounts with **additional third-party solutions.**

For example, specialized vendors hide Microsoft DNS and MX records, making **Office 365 users difficult for attackers to identify and thus less likely to be targeted.**

Protect yourself from email communication failure

Contracts, important information and contact details are exchanged by email. However, if the company's own email server should fail for a longer period of time, this is catastrophic — especially for employees working from the home office, where support is not available as quickly as usual.

Vital business operations become vastly more complex with the long-term **loss of communication.** Therefore, it is particularly important that alternative solutions are available to help out in an emergency so emails are not lost and messages can still be sent and received.

A **continuity service is the solution here.** An autonomous monitoring system detects when the customer's mail server has failed, and **the Continuity Service is activated automatically and immediately.**

The delivery of the emails is carried out without interruption by alternative means (POP3/IMAP mailbox or webmail access).

Access to secure emails is thus maintained even during the outage, for example directly from Outlook.

Checklist

With the following checklist from Hornetsecurity you have an overview of the most important points to consider for **IT security in the home office:**

- ☑ **Employee training helps to raise awareness of potential risks**
- ☑ **VPN clients ensure secure access to sensitive data in the corporate network**
- ☑ **Unauthorized access to the equipment must be prevented**
- ☑ **Proprietary hardware minimizes security risks**
- ☑ **Latest security software and additional third-party solutions for Office 365 cloud services fend off cyberattacks**
- ☑ **Continuity Services prevent the failure of email communication in an emergency**