How to take care of cybersecurity while working remotely in the new reality

Sebastian GOSCHORSKI
Business Development Partner at RSM Poland

The situation with which we are currently dealing calls for an entirely new approach to the management of business organisations and their assets. Whether these changes will be successful, and thus the business organisation will survive, strongly depends on our ability to agilely organise business processes and help employees switch to the new way of working. Due to constant changes and companies' inability to plan the entire process in detail, organisations have become exposed to cyber risk to much higher degree than it was possible in the past.

New reality – learning to work differently

Faced with the need, or even forced by the COVID-19 pandemic, to work from home, we have changed many of our habits and existing schemes. Plenty of business processes have been transferred from offices to our homes. Video conferences, working on company software (e.g. accounting software) have immediately become part of our daily routine. Working from home has many benefits, such as availability, flexibility, no need to commute to work, being able to better focus on work, working on own devices, especially appreciated by the users of Apple products, the truth is, however, that it also increases cyber risk. The reason is quite simple – the number of potential and easy targets detected by hackers has soared, and many users are still unaware of the threat and ways to avoid it.

Reorganisation of digital routine – essential rules

At the time of the crisis, when most of us work from home and participate in online meetings, it is crucial to review and reorganise our new digital reality. Below you will find some rules that will help you increase your company's cybersecurity while working remotely.

1. Company systems should be accessible only via VPN, upon 2-step authentication (e.g. app password and verification code).
2. The choice of VPN software provider should be deliberate. The cheapest or the most popular solution is not necessarily the best.
3. Remote access for a limited time. It is recommended to set up a remote connection for a limited time (minutes / hours).
4. Update the operating system and software version – it is recommended to update organisational operating systems and software to the latest versions, since many times newer versions are offered to businesses due to security breaches detected in older versions.
5. Antivirus software should be updated to the latest version and have full security package, i.e. possibility to test emails for malicious programmes or protection in the form of a simple firewall.
6. Backup – backup must be carried out for all relevant devices and information, and should be performed periodically to verify backup integrity.
7. Any incidents that occurred on computers used at home must be immediately reported and verified by authorised persons or IT support servicing the company.
8. Any suspicious emails must be checked and, if it is likely that they are a cyber-attack, reported to right persons or companies, especially if these are payment orders.
9. Employers must be aware of the obligation to protect information, this concerns especially sensitive data.
10. It is important to hold a cyber risk policy that will be helpful in the event of losing important personal data and will cover the cost of reaction and emergency management.
11. Follow closely all GDPR procedures.
12. Buy adequate insurance that will cover the loss in the event of hacking and provide PR support.

We have to remember that working from home using VPN usually entails slower access to our company resources stored on, e.g., shared drives. As a result, some employees may want to have these drives on their own, less protected computers. In such case, apart from the risk of losing data (e.g. due to some drive damage) we are much more exposed to the risk of having it stolen. It would be safer to allow for automatic synchronisation of data on the personal computer at home with the company network drive.

To sum up – what is new for us and often neglected when it comes to cybersecurity may be a golden opportunity for potential thieves. Lack of proper preparations, planning and audit of the ways in which we (and our employees) work remotely may expose us to huge losses. Thus, the currently binding working rules and systems should be verified and tested for potential risks. We should protect ourselves in advance or change our strategy for working remotely as well as the rules of functioning in the new reality.