INTERVIEW

The dangers of safely working from home

ROMAN VAVRÍK
CEO, SWAN, a.s.

It's been more than a year since the Covid-19 pandemic has changed the way we work. Even companies which have managed to adapt well to these unprecedented conditions are dealing with practical issues related to cybercrime exposure. Roman Vavrík, the CEO of SWAN, a.s. shared some of his observations and recommendations related to this problem.

Do you think the amount of cybercrime has increased over the past year?
Cybercrime has grown by more than 100 % on a year-on-year basis. In fact, to be precise, over the last year it grew by more than 400 %. Last summer, the US Department of Homeland Security published information that showed a dramatic increase in the number of cyber-attacks from the beginning of the pandemic. This represents an important phenomenon and a threat that we shouldn't underestimate.

With the onset of strict lockdown measures most people have transferred their work to their domestic environment, which has created fertile ground for these types of attacks, as employees often access their company data using inadequately secured networks. Of course, these days it's possible to successfully handle almost any threat, but it's important that companies are well prepared. They should provide sufficient technological means and methods of protection. Likewise, employees should receive training on what they are allowed to do and how to handle sensitive information that they are suddenly allowed to bring home.

How can companies or their employees protect themselves?
They should start with the company's internal security, which needs to be at a high level. Companies should invest in services such as Managed Security that protects their network from the risks of today's IP world, such as viruses, spyware, spam, fraudulent emails, hackers, identity thieves, etc. These are complex services that include configuration, hardware lease and expert administration. Companies that decide to use these types of services are better prepared to face the cyber threats of today.

At the same time you have to think of the employees who are at home working from their living rooms. In order to eliminate the threat of cyber-attacks or leaks of important internal data, it's necessary to follow strict security measures. One of them is the use of antivirus, anti-spam and VPN technology, and if necessary data encryption, which is capable of creating an encrypted connection every time company data is accessed, thus eliminating the potential risk. The company network itself has to be adequately protected by a high quality firewall, antivirus and anti-spam system and a system designed to protect against distributed (DDoS) attacks.

Is it possible for a company to protect itself without outside help and leave these issues to the in-house IT manager?
It's a great advantage to have the person in charge of IT in-house because this person knows the internal systems and processes. Up to a certain degree it's possible to handle almost any attack. But more serious attacks can put the business out of operation for several days or even completely ruin it. DDoS attacks have become increasingly common in recent years. They can completely knock out an unprepared company for days or even weeks. During such attacks it's ideal to have the support of a strong professional IT partner with sufficient experience and a team of specialists, who can provide prompt technological and organizational help, which may prevent serious damage.

What is the best way to protect a company's data? Is a company's own server sufficient?
A company's data is its most precious asset and as such it deserves attention. Companies may have their own servers to manage, protect and regularly back up their data. There's nothing wrong with that. Problems begin when an adverse event takes place, such as a short circuit in the server room, an overload or power outage, or a weather event that causes damage that cannot be quickly and simply resolved. In such cases it's better to use a professional cloud service, which can eliminate a number of these risks as these systems are overseen by a team of specialists who operate 24/7, 365 days a year. The data is safely stored in a data center and nobody has access to it except authorized employees.

Another benefit is that large volumes of data can easily be shared. In some professions the employees regularly work with large quantities of data that they share and comment on. Sometimes it's more difficult to store or share such data when working from home and employees often seek freely accessible public solutions. This may seriously threaten not only the data in question, but also the very operation of the company, as a leak of precious data is unavoidable. A cloud solution provided by the employer would definitely help when processing such data in a secure way.

BIOGRAPHY

Roman Vavrík is a graduate of the Faculty of Management at Comenius University in Bratislava and Business at Webster University in Vienna. In 2007, he joined Slovak Telekom, where he held several key positions. In 2012, he was appointed head of the marketing department for the B2B segment. In 2014, he took up the position of Marketing and Sales Director at the subsidiary DIGI Slovakia. Since 2019, Roman Vavrík has held the position of CEO of SWAN, which is one of the largest telecommunication companies in Slovakia.

Do you have any advice for the management of work from home both for the employers and the employees?
Our health is the most important thing these days, which is why employers should be considerate of their employees and enable them to work from home, as far as the nature of their job allows it. But companies should also think about how to secure their applications and systems when accessed remotely so as to avoid exposure to threats.

Employees should bear in mind to use the tools provided by their employers – a laptop or a desktop – for work. If they have the option, they should connect via a VPN, keep their office and user software updated, as well as their antivirus and VPN clients, and never open any suspicious emails, download attachments coming from unfamiliar email addresses, or install programs unrelated to their work on their company equipment. All these actions reduce the degree of vulnerability to cyber-attacks and threats.