Ten Cybersecurity Misconceptions That Could Become Very Expensive.

Cybercrime has become such a ubiquitous topic that we hardly notice the numerous reports of ransomware attacks, data breaches, and other scams anymore. This, however, is a big mistake. Cybercrime has become a lucrative business sector generating billions in revenue. We are all affected by this and it is therefore important that we assess the risk correctly. Mistakes could become very expensive.

Misconception Number 1_
Ransomware is the worst that can happen - if we survive this we will be safe.
Ransomware, in the vast majority of cases, is just the point at which the attackers alert the victim that they are present and show them what they have done. The attackers have probably been in the network for days, if not weeks, before activating their ransomware. During that time, they have explored the network, disabled or deleted backups, found computers with important information or applications, removed information, and installed additional payloads or backdoors. Remaining on victims' networks allows attackers to launch a second attack - whenever they want.

Misconception Number 2_
Ransom payment will restore our data.
Paying the ransom - even if it seems to be the easiest option - is not a quick solution to get back on your feet. According to the 2021 State of Ransomware survey, companies that paid a ransom had a data recovery success rate of only about 65 percent. Only eight percent got all of their data back, and 29 percent recovered less than half. Furthermore, recovering data is only part of the recovery process - in most cases, the ransomware completely cripples computers, requiring software and systems to be rebuilt from scratch before any data can be restored. These recovery costs are, on average, ten times higher than the ransom demand.

Misconception Number 3_
We have a firewall. This means that our IT is well secured.
The firewall's task is to continuously check and filter data traffic between internal and external networks. At the same time, it is meant to alert key IT personnel in the company or at the external IT service provider in the event of malfunctions or cyberattacks. However, a firewall alone is not enough to effectively secure your organization. For example, data that users load onto computers via USB drives is not covered by the firewall. This makes such devices a potential gateway for malware. Improper handling of login data (for example, in a phishing attack) cannot be prevented by a firewall either.

Misconception Number 4_
Security is up to our IT department.
Far too often, the issue of security is delegated to those responsible for IT. Or the company relies on their IT partner to somehow get it right - without clearly defining responsibilities. It is not uncommon for serious attacks to occur at the interfaces because they are not clearly defined or are misunderstood. In the event of a cyberattack, the company is liable. The board of directors and possibly also the management could be held responsible in the event of damage due to a cyberattack because of inadequate protective measures. This responsibility cannot be delegated to IT managers and certainly not to external parties. IT security should therefore be treated by management as a strategic topic of the highest importance.

Misconception Number 5_
I don't want to outsource security; it is too important for me.
For SMEs in particular, it is hardly possible to deal with all aspects and the most recent findings of cyber security on an ongoing basis. As a result, immediate action cannot be taken in the event of a change in the threat situation. Monitoring their own IT infrastructure and reacting quickly to incidents is only possible for a few SMEs with their own protection organization. Even if the company has its own IT team, it is worth working with an external IT security partner - this allows the in-house IT department to focus on business-relevant IT projects.

Misconception Number 6_
We are not interesting for hackers and have no secrets anyway.
Many victims of cyberattacks consider themselves too small, too uninteresting, or financially not sufficiently attractive to be threatened. Criminals pay little heed to this. Any person or small business with a digital presence and use of computers is a potential victim. Most hacker attacks happen in a less than spectacular fashion, but are carried out by opportunists looking for easy prey. Among the most popular targets are companies with unpatched security holes or misconfigurations. Even if you think you are too insignificant a target you should scan your network for suspicious activity as soon as possible.

Misconception Number 7_
We are ready; we have an emergency plan.
An emergency plan is indeed quite essential. It ensures that you and your IT department will be able to take the appropriate security measures and respond quickly in the event of a cyberattack. Such a plan may include instructions on how to quickly disconnect a server from the network should you be attacked. In the event of a cyberattack, responding quickly is one of the most important factors in minimizing the consequences. Still, having an emergency plan in place is not enough protection on its own. Rather, it‘s a safeguard to prevent greater damage. Protection must be proactive. An emergency plan is always reactive.

Misconception Number 8_
We have insurance.
Unfortunately, insurance alone will not protect you. It typically only pays for the monetary damage at most. Proactive cyber security measures are like brakes on a vehicle. Just because the vehicle is insured you wouldn‘t want to do without brakes.

Misconception Number 9_
Our employees are trained on a regular basis, which is sufficient.
According to the State of Ransomware 2021 study, 22 percent of organizations fear they may fall victim to ransomware in the next 12 months. Social engineering tactics such as phishing emails are increasingly difficult to detect. The messages are often so specific, persuasive and carefully written that it is nearly impossible for employees to detect them. Of course, many attacks can be thwarted through regular employee awareness campaigns. Nevertheless, employee training should be integrated into a comprehensive cyber security strategy.

Misconception Number 10_
Each employee is responsible for the safe operation of IT systems.
Many companies make their employees responsible for the safe use of e-mail and the Internet. However, making employees aware of safety risks falls to the company, just like safety shoes or a helmet for the construction site. It is the employee‘s duty to use these provided tools correctly and at all times. But it does not rule out misconduct and safety breaches.

UMB Cybersecurity

Thanks to modular cybersecurity services UMB creates permanent protection in an increasingly digital and complex world. Only balanced organizational and technical measures will protect your company effectively and holistically. To achieve this, new security dimensions must be introduced that are designed to complement classic prevention (network and perimeter protection). On the one hand, this includes the ability to detect an attacker at an early stage. On the other hand, it is critical to initiate the appropriate countermeasures quickly.

IBM Platinum Business Partner

Sounds exciting? Contact us!

We‘re happy to answer your questions about cybersecurity and more.

Contact
Markus Kaegi
Senior Security Consultant
markus.kaegi@umb.ch
+41 44 805 14 47
www.umb.ch