Virus protection in an SME environment

Virus protection is one of the basic provisions of any company, as malware poses a threat seriously on the rise in our digital world – and to SMEs in particular, too. Consistently applied technical virus protection and conscious human behaviour constitute the best remedies here.

The most important points to remember:

- Define and implement a **virus protection process** in your SME.
- Create an overview of channels for malware to intrude and **distribute itself** inside your company.
- Draw up a **virus protection concept** to establish where the most efficient checkpoints for your virus protection should be set up.
- **Sensitise** your employees to the dangers posed by malware.

The virus protection process

There are a variety of excellent antivirus protection systems offered by numerous suppliers nowadays, which can be adapted to the most variable of needs and circumstances inside SME networks. However, prior to this, you will have to undertake an analysis to evaluate the optimum solution, and then implement it in a professional manner.

Still, things don't stop there: The same way cyber criminality and malware keep evolving, you will have to continuously keep maintaining and updating your protective measures, too. Your virus protection for instance should always be updated with the latest virus patterns.

To do so, you will have to establish a virus protection process to safeguard not just the implementation of proper monitoring of your data flows, but also the detection and removal of malware (https://www.ebas.ch/en/malware-infection/) and the maintenance of your system. And it is just as important to regularly keep sensitising your employees to this kind of threat as part of this process.

The distribution channels

SME networks are becoming ever more complex. New software solutions are implemented, new data links created and infrastructure fine-tuned almost daily. Cyber-criminals abuse the resulting complexity to keep finding and exploiting ever new channels of intrusion and distribution.

To identify potential channels of malware intrusion and distribution as extensively as possible therefore forms the basis of your virus protection concept (#concept) . One established approach here is to think in scenarios:

1. "How and where could an attacker plant malware in the network?"
2. "How could this malware then spread through the network?"

The following channels are frequently abused to plant malware in a system:

- Internet, Wi-Fi and VPN connections
- Attachments to communications, e. g. e-mails
- Mobile devices owned by employees and visitors
- Remote Desktop (RDP) and terminal server applications
- Exchange of physical data carriers
- Insufficiently protected IoT enviroment

Once it has found its way into an internal network, malware can then exploit vulnerabilities to spread further, and can for instance also be activated by careless actions of your employees, to then do its destructive work. In such cases it is important to limit the resulting damage to the largest extent possible, and to prevent widespread distribution.

The virus protection concept

Based on the channels of intrusion and distribution identified, you can then determine where exactly inside your network your virus protection measures would be most effective.

Based on your exposure, you should screen incoming and outgoing network connections with the Internet for malware in particular. This can be implemented on your firewall or your proxy and communication servers. In this, it is important to note that content has to be checked before being encrypted or after being decrypted.

Mobile devices owned by employees and visitors also pose a great risk in this regard, since they are frequently used in unsecured environments, too. They should therefore never be accepted on the internal network unchecked. This especially applies to VPN connections from the outside, e. g. when working from home (https://www.ebas.ch/en/top-5-steps-to-work-securely-from-home/) . This is where centrally administered antivirus software on all terminal devices is a good idea.

And finally, all stationary devices where external data carriers are connected will have to be equipped with suitable virus protection, too.

Your virus protection concept should cover the complete virus protection system and its configuration.

Antivirus suites for companies

There are numerous suppliers offering antivirus solutions which are also suitable for larger networks. Roll-out, configuration and maintenance of your AV protection can therefore be administered cross-platform and cross-location from a single central point. This way you can ensure that compliance with your SME security policy can be safeguarded as soon as a device connects to the network.

Cyber criminality statistics are sending a clear signal: Malware attacks resulting in damage have increased considerably over the past few years. Ransomware in particular should be taking seriously as posing increasing risks to SMEs.