How to set up an effective cybersecurity strategy

Guide for Small and Midsize Businesses

Digital Security
Progress. Protected.

In large businesses, there are usually whole departments that oversee the company's cybersecurity and set up effective strategies. But what about small and midsize businesses (SMBs) with just a few internal IT specialists? How should they proceed to make sure the business is protected accordingly, without getting overwhelmed by all the possible measures?

Here are a few tips from **Michal Jankech, vice president of the SMB & MSP segment at ESET**.

ESET
Digital Security
Progress. Protected.

Where to start?

In most cases, SMBs only have a limited workforce that takes care of digital security strategy, if any at all. Therefore, it is crucial for them to focus on the biggest threats and invest their energy into areas that are substantial for their business continuity.

"**They should adopt a risk-based approach that includes identifying the most crucial vulnerabilities**," explains Jankech, who adds that SMBs should address the following areas first.

- **Data protection and encryption**
- **Multilayered endpoint protection and user access restrictions**
- **MFA and regular updates**
- **High-quality email providers and employee education**
- **EDR or MDR for the mature and thorough**

Data protection and encryption

Are all your devices locked with a username and a strong password? Great. But still, there is more you should do if you want to have your devices hardened as much as possible. "**All endpoints should be encrypted**. Imagine someone steals your computer. Well, they can't get inside since they don't know the password and username, but still, they can access the data by taking out the hard drive. Make sure that not only portable devices but also desktop computers are properly encrypted," suggests Jankech.

"I once visited a health institution and saw that they had a computer placed right at the kiosk, and the device was not secured with a password. Someone could easily break in and steal the PC, gaining access to all patient data. Such scenarios can be prevented by implementing effective data protection and encryption measures."

Multilayered endpoint protection and user access restrictions

"It is crucial to limit admin user accounts. In many cases, it's people who might cause the most damage. If a saboteur gains access to the admin account, they can potentially install anything on the device," says Jankech.

Also, be aware that one layer of protection is not enough. "It's like securing a family house. In that case, you would also use measures that multiply your defenses – a gate, security doors, an alarm, a fence, and windows. ... A lot of people say that **the age of antivirus is over**. Yes, the age of standard antivirus that only works with signatures is over. Such solutions are not able to cover the huge range of current threats," continues Jankech.

Instead, **multilayer endpoint security software** that is based on the principles of machine learning and that offers behavior–type protection is recommended, blacklisting dangerous websites and blocking access to risky domains, including protection against network attacks or vulnerabilities in remote desktop protocol that might be misused.

> **For SMBs, it makes sense to invest in prevention the most. Hardening your systems, keeping them up to date, and using good endpoint protection software is key.**
>
> **Michal Jankech**,
> VP of the SMB & MSP segment at ESET

"It's not only about having protection in place but also about having it correctly configured and updated," adds Jankech. For example, making sure that the endpoint protection software can't be uninstalled, or have its configuration altered, should be a must.

Next, **use a management console for endpoints**. "Many companies think it's enough to use an endpoint protection client. But you never know if it is working correctly if you don't manage it via a console that lets you oversee the whole network. Even if you only have 10 computers in the company, you won't be able to check them properly, especially nowadays, when people increasingly work from home and travel," Jankech offers. At the same time, the console should provide you with reports you can check to be 100% sure your systems and network traffic are in ideal condition.

MFA and regular updates

Multifactor authentication (MFA) should be in place on all work as well as private devices. Also, keep all operating systems running on their latest versions. “Most breaches appear due to identity and password theft or a commonly known vulnerability in the operating system that can be misused,” explains Jankech.

With every new version of the operating system, the vendor fixes the possible gaps, and you raise the chance cybercriminals won’t find their way into company devices. **Automatic updates are recommended.** “When it comes to SMBs, zero-day attacks are only seen rarely. If you’re using purpose-built software, the chances that cybercriminals conduct such a targeted attack are rather low. In most cases, widespread vulnerabilities in commonly used or open-source software are the door into your business,” says Jankech.

Doctors, architects, PR agencies … all of them need a cybersecurity strategy. For example, many people aren’t aware that certain documents are protected by copyright and should thus be protected accordingly.

Michal Jankech,
VP of the SMB & MSP segment at ESET

High-quality email providers and employee education

Reliable email providers are key as well. “Also, employees should know how to detect a phishing email. You can also let every recipient know that the message arrived from outside the company – even Office 365 lets you mark emails with the tag ‘external,’” recommends Jankech. From time to time, it’s worth investing in cybersecurity employee training to boost awareness. **You can read a few tips** on how to make education effective and fun on ESET Digital Security Guide.

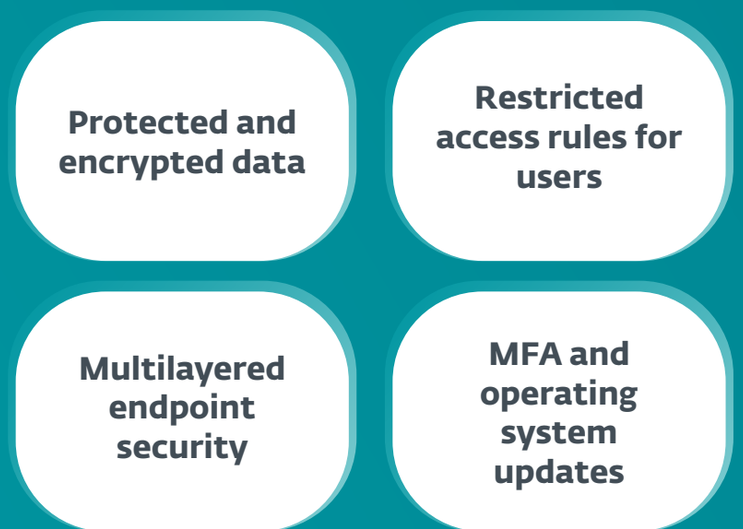
Jankech stresses that most companies don’t have these basic measures implemented, and sometimes, there are even more significant gaps in the digital security of large businesses. “Some companies still hesitate to invest in cybersecurity solutions or think they wouldn’t become a target since their business area is rather unattractive. But usually, cyberattacks are not targeted. Anyone can fall victim,” the cybersecurity expert points out.

EDR or MDR for the mature and thorough

Once you have all the basic cybersecurity building blocks firmly in place, it's time to consider **advanced cybersecurity tools – such as endpoint detection and response (EDR) solutions.** "It's a whole new submarket, built on the premise that prevention always fails. This part of the product suite is mostly applicable to large enterprises that can afford the luxury of numerous internal IT departments and an in-house SOC [security operations center] with 24/7 operations. Following this approach usually means taking the stance that eventually, cybercriminals will successfully attack your system," adds Jankech.

The EDR solutions identify anomalies and suspicious behavior in the network and ideally let you react by blocking the process – or the systems handle these tasks via custom automated rules. "While they are usually used in larger companies, they can be beneficial to smaller businesses too.

Essential building blocks in the SMB cybersecurity strategy

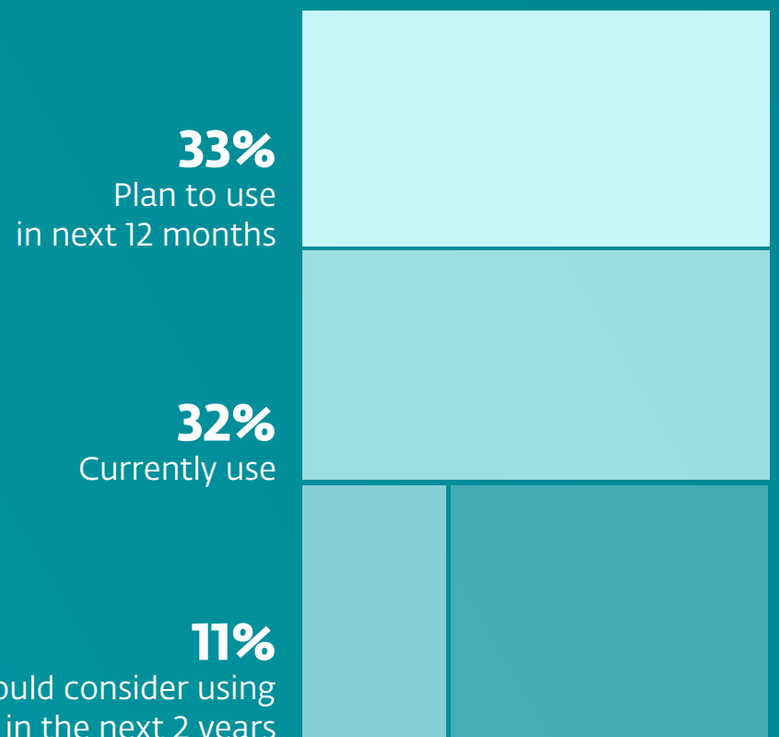


Regardless, since you need staff to manage your EDR platform, it's recommended that smaller businesses with a use case look at outsourcing such services," adds Jankech.

This is where so-called MDR – managed detection and response – steps in. MDR is EDR that is managed by a third party. "From one monitoring center, tens or even hundreds of customers are supervised, and there is usually a 24/7 hotline you can reach out to too," says Jankech.

Nonetheless, EDR or MDR should only be considered if you already have the basics covered. When you're ready, using EDR or MDR raises the chance that your business can withstand any cyberattacks, with your company safe but always still alert.

Usage of EDR / XDR / MDR solutions



Source: 2022 ESET SMB Digital Security Sentiment Report

ABOUT ESET

For more than 30 years, **ESET®** has been developing industry-leading IT security software and services to protect businesses, critical infrastructure, and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit **www.eset.com** or follow us on **LinkedIn**, **Facebook**, and **Twitter**.

Digital Security
Progress. Protected.