SME4DD: Your First Line of Defence Against a Cyberattack

Don't be fooled by the name. SMEs are anything but small. In Europe, they represent 99% of all businesses, employ nearly 100 million people and account for over half of Europe's GDP.

In other words, SMEs play a big part in the EU economy.

Unfortunately, they're also a big target for cybercriminals.

"SMEs are often considered 'soft targets' by cybercriminals," explains cybersecurity expert Vincenzo Turturro. "This vulnerability stems from a combination of factors, such as an SME's limited resources, that make them attractive and relatively easy to compromise compared to larger corporations."

Just how vulnerable are SMEs? In 2023, nearly 43% of all cyberattacks targeted SMEs, with the average cost of an attack ranging anywhere from EUR 110,000 to as much as EUR 1.14 million.

Yet despite this very real risk, a mere 14% of European SMEs are adequately prepared to defend themselves against a cyberattack.

This lack of preparedness doesn't just pose a threat to SMEs, it's a threat to Europe's global competitiveness. "Cybercriminals often target smaller, less secure businesses as a steppingstone to infiltrate the larger organisations they partner with," says Turturro. "By compromising an SME supplier, attackers can gain access to the data and networks of an entire value chain."

Finding – and fixing – the weakest link

As the saying goes, 'the best defence is a good offense'. In cybersecurity, that means understanding the risks and knowing how to adopt proactive strategies to mitigate those risks.

To help SMEs with both, SME4DD, an EU-funded project under the Digital Europe Programme, offers a dedicated course on cybersecurity and data protection. Taught by SME4DD partner Talent Garden, the course is designed to provide SMEs, SME professionals and jobseekers with the essential skills they need to protect and manage information.

The course starts by identifying some of the 'weak links' that cybercriminals look for in an SME. "Cybercriminals are opportunistic and look for the easiest path of entry," notes Turturro, one of the course's featured lecturers.

For SMEs, these weak points are often related to human error and basic security oversights.

According to Turturro, human error is a major contributing factor in 95% of all cybersecurity breaches. “Employees are often the first line of defence, but without proper training, they can be an SMEs weakest link,” he says.

To illustrate, he points to a typical ‘phishing’ attack where an employee receives an email that appears to be from a legitimate source, such as a CEO, a trusted supplier, or a bank.

The email usually creates a sense of urgency, instructing the employee to either click a malicious link, download an infected attachment, or transfer funds to a fraudulent account. If the employee clicks the link, they may be taken to a fake login page that steals their credentials or, if they transfer funds, the money is sent directly to the criminal.

Other common points of entry that are exploited by cybercriminals include outdated software and systems and weak or stolen passwords. Whereas unpatched vulnerabilities account for more than 70% of successful data breaches at SMEs, 81% of hacking-related breaches leverage stolen or weak passwords.

“Protecting yourself from a cyberattack doesn’t have to be complex, it could be as simple as updating your software and changing your passwords,” adds Turturro.

Adopt a security-first mindset

Speaking of protecting oneself from an attack, the SME4DD course covers that too. “SMEs must adopt a security-first mindset, one that includes prevention, mitigation and protection,” explains Turturro.

As to prevention, Turturro stresses the importance of regularly training all employees to recognise phishing attempts, understand the importance of strong passwords, and follow security protocols. He also recommends implementing a policy to routinely update all software and operating systems, as well as enabling multi-factor authentication (MFA) on all critical accounts.

On the mitigation side of the equation, SMEs should have a clear, documented plan for what to do in the event of a breach. This should include steps to isolate affected systems, identify the source of the breach, and notify relevant stakeholders. They should also maintain regular, isolated, and tested backups of all critical data and, when an attack does happen, immediately disconnect compromised machines from the network to prevent the attack from spreading.

Turturro also recommends taking steps to ensure data protection. This includes encrypting sensitive data, only giving employees access to the data and systems they need, and adhering to all data protection regulations. He also urges SMEs to adopt a recognised cybersecurity framework, conduct regular risk assessments and security audits, obtain cyber insurance and to vet the security practices of all third-party vendors who have access to one's data or network.

"At the end of the day, cybersecurity is a team responsibility," concludes Turturro. "While not every employee needs to be an expert, a baseline level of knowledge is essential to protecting the entire organisation."

Ready to up your cybersecurity game? Whether you're an SME looking to better protect itself from cyberattacks or an SME professional or jobseeker looking to add cybersecurity to their skillset, SME4DD is ready to help.

Learn more by visiting https://www.eitdigital.eu/eu-collaborations/sme4dd/ or contact us at professionalschool@eitdigital.eu.