Five Best Practices in Security Awareness Training for Small-Medium Enterprises

Executive Summary

Small and medium-sized enterprises (SMEs) are increasingly becoming prime targets for cybercriminals. The FBI reports that hackers consider SMEs, typically businesses with 25-150 employees, as "soft targets." As large organizations allocate significant budgets to enhance their cybersecurity defenses, cybercriminals are turning their attention to SMEs, which are often ill-equipped to deal with sophisticated attacks. This white paper presents five best practices for security awareness training in the SME market, helping these businesses protect themselves more effectively.

Introduction

SMEs are at a heightened risk of cyberattacks and face unique challenges that set them apart from larger organizations. The top five security challenges for SMEs include:

1. A lean security team:
Many SMEs lack a Chief Information Security Officer (CISO) or dedicated security teams, leading to knowledge gaps and security vulnerabilities.

2. Over-stretched resources:
SMEs often operate with limited resources, causing security alerts to go unnoticed or unaddressed.

3. Outdated technology:
A reliance on legacy security protocols can leave SMEs vulnerable to modern threats, as adopting new technology is seen as expensive and complex.

4. Supply chain risk:
SMEs frequently rely on outsourcing with a complex supply chains, making them susceptible to supply chain attacks that can have devastating consequences.

5. Human error:
Employee skills gaps and a lack of cybersecurity training contribute to SMEs' vulnerability to attacks, as many fail to provide adequate training compared to larger companies.

Best Practices for Security Awareness Training

1. Compliance is King

While compliance doesn't guarantee immunity from cyberattacks, maintaining compliance allows you to prove that you haven't been negligent and prepares you for potential audits. To achieve and exceed compliance. What to do? Assign a Compliance Officer: an individual responsible for understanding industry regulations and tailoring compliance efforts to your specific business context.

2. Look for Autopilot

SMEs often avoid adopting new security tools due to the perceived complexity of onboarding and management. Opt for technologies that offer an autopilot feature, that runs in the background and actively contribute to your security posture with minimal intervention, ideally requiring less than 1 hour of IT time per quarter.

3. Don't Skip Employee Training

Recognize that your employees are your weakest link, especially with the rise of remote work. Investing in continuous and automated security awareness training can significantly reduce the risk of human error. What to do? Implement ongoing, automated security awareness training programs that operate behind the scenes to educate and empower your employees, and select a training solution that provides regular progress Key Performance Indicators (KPIs) and advanced analytics to track your training program's success and identify areas for improvement.

4. A Security Strategy Built for SMEs

SMEs can optimize their resources by adopting a lean security strategy and leveraging the right tools. What to do? Focus on essentials and prioritize security and compliance while optimizing resources, Investing in security tools that work in the background to protect your organization, reducing the burden on your IT team.

5. Measure ROI with Definite Results

To gain support and buy-in from management, opt for security solutions that yield measurable results. Demonstrating a clear return on investment (ROI) that can justify your cybersecurity expenditures and show the value of your security awareness training program. What to do? Select solutions that provide quantifiable metrics, such as reduced incident rates, faster incident response times, and lower incident remediation costs. Generate regular reports that showcase the tangible benefits of your security awareness training program, making it easier to communicate your security successes to management.

Conclusion

As cybercriminals increasingly target SMEs, these businesses must take proactive measures to enhance their cybersecurity defenses. By following the best practices outlined in this white paper, SMEs can protect themselves effectively, despite limited resources. Remember, it's not about the size of your organization but the quality of your security strategy and the tools you choose to safeguard your business.

SOFTPROM