SENTIS
Managed Solutions

Seven Essential Steps for SMEs to Combat Cyberattacks

w: sentisms.com
t: 0345 862 2930

Cyberattacks can be devastating for small and medium-sized businesses – and they're becoming increasingly sophisticated.

Having a well-defined response plan is crucial. Here are seven key steps you should take to protect your business in the event of a cybersecurity breach.

1 Incident Response Team

Establish an incident response team so you know who's responsible for doing what if your business is the subject of a cyberattack, preventing confusion in the crucial early stages.

This team will consist of key people in your organisation with clearly defined roles and responsibilities.

2 Incident Classification and Reporting

Incidents should be classified by severity. Outline criteria for incident severity classification and procedures for reporting incidents.

Timely and accurate reporting is essential to ensure a rapid response. Having the right protocols in place means staff know who to report to, saving valuable time.

3 Containment and Eradication

Once an incident is confirmed, containing and eradicating the threat is paramount to ensure other parts of your business aren't affected.

Staff training can mitigate attacks such as phishing attempts, but for other, more complex attacks – such as certain types of malware – you'll need to restrict access to infected networks.

4 Detection and Analysis

Detection and initial analysis are the first steps in responding to a cyberattack. You must have methods not just for incident detection but also verifying the nature and scope of an attack.

A Managed Security Service Provider (MSSP) can handle detection and analysis for you. Sentis Managed Solutions recommends that SMEs appoint an MSSP to deal with these threats.

5 Communication and Documentation

Effective communication is key during a cyberattack. Relevant stakeholders, including employees and third-party cybersecurity teams, must be kept informed and updated.

Make sure everyone involved in your response knows which channels to use, and that everything relating to the attack is documented so you can learn from what's happened.

6 Legal and Regulatory Compliance

Clear guidelines can ensure that your business is able to ensure compliance throughout the incident response process and handle any subsequent legal ramifications.

Data breaches can be seriously costly, especially in the age of GDPR. A third-party cybersecurity specialist can advise you on how to respond and stay fully compliant with legislation.

7 Post-Incident Analysis and Improvement

It's important to learn the right lessons following a cyberattack. Look at your response procedures and how effective they were, then use this knowledge to make continuous improvements.

Sentis Managed Solutions has extensive cybersecurity expertise to help you protect your business and an array of tools to help you recover more quickly in the event of an attack. Get in touch with us to arrange a full security audit of your IT assets