rb realbusiness

wavex
EXPERIENCE EXCELLENCE

Protection against cyber attacks – mitigation and response

If last year is anything to go by regarding the rate and sophistication of cyber attacks, 2017 is set to see a marked increase in both.

Remember – no cyber security approach is 100 per cent infallible

Practice into action

Taking a very high-level approach, once a plan is implemented and needs to be used to deal with an incident, businesses typically follow four broad steps:

(1) Identification

The first deals with the actual identification of the cyber security incident, which may in itself be a challenge. This can be done by monitoring, looking at log alerts, cyber intelligence and evaluating threat analytics, which can also assist in finding out exactly what happened. More often than not, working with a trusted IT or security provider could help in the identification process, as well as what followed.

(2) Definition

The second step looks at defining objectives and delving into what happened. Typically, this includes finding out who the attacker/s are, the scope of the attack, what was affected, what was taken, and the timescale of the attack.

(3) Elimination

From there, gathering that data allows an organisation to take the appropriate action — that includes tasks such as eliminating the cause of the incident, containing the damage, contacting law enforcement and gathering evidence.

(4) Recovery

The final area is recovery. Here an organisation needs to ensure that remediation has been carried out correctly, gaps closed, and vulnerabilities assessed. Depending on the type of incident and data affected, this could include things such as password resets, enhancing security and testing systems.

Conclusion

One of the most important aspects of cyber security is that organisations can rarely go it alone. While programmes, strategies and plans certainly do help in protecting valuable assets and the bottom line, expertise and advice from trusted advisors in the IT and cyber security space can be equally as valuable.

Cyber security is an ongoing endeavour — something that evolves and changes according to the threat landscape, the business itself and the risk it faces — and should address mitigation, protection and response to manage cyber attacks.

Link to the original article:
https://realbusiness.co.uk/protection-cyber-attacks-mitigation-response/