Incident Response Plan (IRP)

Are your employees aware and prepared for a cyber threat?

Do you conduct hands-on cyber exercises for your employees?

When it comes to evaluating technology in preparation for a potential disaster or cyber incident, IT and security departments typically conduct multiple tests, playing out different scenarios to see how applications, systems, devices, and interfaces will respond in the event of an outage or attack.

But what about testing your people? For example, how would your IT or security team respond to a ransomware attack, or to a strategic DDoS assault?

The reality is that a team's security preparedness – or lack of it – is often the real problem.

Conducting hands-on cyber exercises can improve your incident response plan

5 Scenarios

that you should be prepared for

1 Phishing Emails

The frequency of phishing emails and overall business email compromise (BEC) has gained momentum, especially as ransomware attacks have been on the rise.

2 Malicious Attachments

If malicious attachments make it through your filters and into your employee's inboxes, you need a plan in place – one that has been practiced – to be able to respond quickly and limit the damage.

3 Password and Other Suspicious Requests

Cybercriminals can pose as employees, contractors, or third-party vendors to bait employees into divulging sensitive passwords and other access controls. Conduct exercises to simulate password requests from familiar sources such as the help desk or even executives, who are often spoofed.

4 Unauthorized Computers and Devices on Network

Computers and devices that haven't gone through proper authentication processes before joining your corporate network are perfect targets for attackers. Can your IT team not only identify attempts to connect to your network, but also block them? Have you tested how quickly they can do this?

5 Data Breaches

Create a data breach and test the incident response plan. Make sure that the incident response protocol works for all cases. Ensure that an incident response team (IRT) responses in a timely manner, notifications are sent out to clients, authorities are notified, a forensics team is contacted and other processes are on alert five.

entreda

entreda.com | sales@entreda.com | 650.308.4269

Entreda Inc. | 3211 Scott Blvd Suite 204, Santa Clara, CA 95054