SevenC

Incident response planning

ICT or security incidents can happen without warning and will often go undetected for long periods of time.

Many organisations struggle to identify incidents because they often work in silos or because the sheer volume of alerts is overwhelming and hard to determine.

Let SevenC determine and manage a relevant incident response plan for your business.

Key aspects of an incident response plan from SevenC.

- Prioritisation of your companies' assets
- Identification of potential risks
- Establishment of procedures
- Response team assembly
- Buy in from company decision makers

Our skills and expertise will enable us to set up an incident response plan that addresses the breach or incident, in the following phases:

1. Preparation

- Ensure employees are properly trained regarding their incident response roles and responsibilities in the event of the disaster or breach
- Develop incident response drill scenarios and regularly conduct mock disasters or breaches to evaluate the response plan
- Obtain business approval for all aspects of the incident response plan in advance

2. Identification

- When did the incident happen?
- How was it discovered?
- Who discovered it?
- Have any areas been impacted?
- What is the scope of the compromise?
- Does it affect operations?
- Has the entry point been discovered?

3. Containment

Contain the breach and ensure it doesn't spread to other areas of the business, and not cause further damage.

4. Eradication

- Once the issue has been contained, we will find and eradicate the root cause
- After eradication, systems will be hardened and patched, and relevant updated applied

5. Recovery

Manage the process of restoring and returning affected systems and devices back into the business environment, without the fear of another breach.

6. Lessons learned

- After action meetings will be held to determine what has been learned from the breach
- Analyse and document all aspects of the breach
- Determine what worked well in the response plan
- Address the following questions
    - What changes should be made to the environment or security?
    - Should employees be trained differently?

SevenC Computing (Pty) Ltd.

Unit 36, Sunninghill Office Park
Peltier Drive, Sunninghill
Johannesburg, South Africa

+27 (0)11 467 3388
info@sevenc.co.za