**Incident Response: concepts & step-by-step**

**Which is the primary goal of Incident Response?** The priority of any incident response is to protect life, health and safety. When any decision related to priorities is to be made, always choose safety first.

**How it works?** The Incidente Response Plan is composed of four parts:

|  |  |
| --- | --- |
| **Component** | **Example** |
| Preparation | Develop a policy approved by management, Identify critical data and systems, single points of failure, Train staff on incident response. |
| Detection and Analysis | Monitor all possible attack vectors, Analyze incident using known data and threat intelligence, Standardize incident documentation, Prioritize incident response |
| Contaiment, eradication and recovery | Isolate the attack, Identify the attacker, Choose an appropriate containment strategy, Gather evidence |
| Post-Incident Activity | Identify evidence that may need to be retained, Document lessons learned, Retrospective (preparation, Detection, containment, Post- Incident) |

**What does an incident response team do?**

Determine the amount and scope of damage caused by the incident.

Determine whether any confidential information was compromised during the incident. Implement any necessary recovery procedures to restore security and recover from incident- related damage.

Supervise the implementation of any additional security measures necessary to improve security and prevent recurrence of the incident.

**Disaster Recovery**

Disaster recovery refers specifically to restoring the information technology and communications services and systems needed by an organization, both during the period of disruption caused by any event and during restoration of normal services.

**Components**

Executive summary providing a high-level overview of the plan Department-specific plans

Technical guides for IT personnel responsible for implementing and maintaining critical backup systems

Full copies of the plan for critical disaster recovery team members

**Business Continuity (BC)**

The intent of a business continuity plan is to sustain business operations while recovering from a significant disruption.

**Components of a Business Continuity Plan (BCP)**

Firts, BCP is the proactive development of procedures to restore business operations after a disaster or other significant disruption to the organization.

List of the BCP team members, including multiple contact methods and backup members Immediate response procedures and checklists (security and safety procedures, fire suppression procedures, - notification of appropriate emergency-response agencies, etc.)

Notification systems and call trees for alerting personnel that the BCP is being enacted Guidance for management, including designation of authority for specific managers **How/when to enact the plan**

Contact numbers for critical members of the supply chain (vendors, customers, possible external emergency providers, third-party partners)

**Importante: The BCP should be tested** at predefined intervals (**Routinely**) as well as when significant changes happen within the business environment.

**Some terminologies and fundamental concepts**

**of IR, BC and DR**

**Terminology**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Breach | Unauthorized access or accidental disclosure of confidential information. |
| Event | Any observable occurrence in a network or system. |
| Exploit | A particular attack. It is named this way because these attacks exploit system vulnerabilities. |
| Incident | An actual or suspected security violation that affects the confidentiality, integrity, or availability of critical information. |
| Intrusion | Unauthorized access to a system or network. |
| Threat | A circumstance or event that could cause harm to a system or organization, such as a cyber attack or natural disaster. |
| Vulnerability | Weakness in an information system, system security procedures, internal controls or implementation that could be exploited by a threat source. |
| Zero-day | A previously unknown system vulnerability with the potential of exploitation without risk of detection or prevention because it does not, in general, fit recognized patterns, signatures or methods. |
| Adverse Events | Events with a negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, defacement of a web page or execution of malicious code that destroys data. |
| **Business Continuity (BC)** | **Actions, processes and tools for ensuring an organization can continue critical operations during a contingency** |
| **Business Continuity Plan (BCP)** | **The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.** |
| Business Impact Analysis (BIA) | An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. |
| **Disaster Recovery (DR)** | In information systems terms, the activities necessary to restore IT and communications services to an organization during and after an outage, |

|  |  |
| --- | --- |
| **Term** | **Definition** |
|  | disruption or disturbance of any kind or scale. |
| **Disaster Recovery Plan (DRP)** | The processes, policies and procedures related to preparing for recovery or continuation of an organization's critical business functions, technology infrastructure, systems and applications after the organization experiences a disaster. |
| Incident Handling | The mitigation of violations of security policies and recommended practices. |
| **Incident Response (IR)** | The mitigation of violations of security policies and recommended practices. |
| **Incident Response Plan (IRP)** | The documentation of a predetermined set of instructions or procedures to detect, respond to and limit consequences of a malicious cyberattack against an organization's information systems(s). |
| Security Operations Center | A centralized organizational function fulfilled by an information security team that monitors, detects and analyzes events on the network or system to prevent and resolve issues before they result in business disruptions. |
| Vulnerability | Weakness in an information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat source. |