Cyber Security

- ➔ Disaster Recovery
- ➔ Business Continuity
- ➔ Security & Testing

sebinbenjamin

What we'll do learn today

- Business continuity & Disaster recovery
  - Why
  - Some examples
- Penetration testing
  - Types of Pentests
    - Black Box Testing
    - White Box Testing
    - Gray Box Testing
  - Penetration Testing Teams
  - Tools used

Business Continuity & Disaster recovery

Practices that support an organization's ability to ***remain operational*** after an adverse event.

A fire, flood, ransomware attack or other malady can rack up financial losses, damage the corporate brand and, in the worst-case scenario, shutter a business permanently

BCDR ***minimizes the effects of outages and disruptions*** on business operations.

BCDR is broader than IT, encompassing a range of considerations -- including crisis management, employee safety and alternative work locations.

Business Continuity

BC is more ***proactive*** and generally refers to the ***processes and procedures*** an organization must implement to ***ensure that mission-critical functions can continue during and after a disaster***.

This area involves more comprehensive planning geared toward long-term challenges to an organization's success.

Considers various ***unplanned events***, from cyberattacks to human error to a natural disaster. They also have the goal of getting the business running as close to normal as possible, especially concerning mission-critical applications.

Business Continuity Planning (BCP)

Business Continuity Planning can be described as *putting procedures in place to* ***ensure that essential business functions are able to be carried out*** in the event of a disasters.

A Business Continuity Plan should answer the question, ***“How would my business continue to operate if we lost our building and all of our equipment?”***

- What do we need ***recovered first*** in order to stay in business?
- What do we need to do to ensure our customers that we are ***still operational***?
- What do our business partners, suppliers and vendors need in order to ***continue order fulfilment and delivery***?

Disaster Recovery

Disaster Recovery involves a set of ***policies, tools and procedures*** to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

An area of security planning that aims to protect an organization from the effects of significant negative events.

Disaster recovery focuses on the ***IT or technology systems supporting critical business functions***, as opposed to business continuity, which involves keeping all essential aspects of a business functioning despite significant disruptive events.

Disaster recovery service level

Tier 0 represents the least amount of off-site recoverability and tier 6 represents the most.

- Tier 0: **No off-site data**. Recovery is only possible using on-site systems.
- Tier 1: Physical backup with a **cold site**. Data, likely on tape, is transported to an off-site facility that doesn't have the necessary hardware installed.
- Tier 2: Physical backup with a **hot site**. Data, likely on tape, is transported to an off-site facility that has the necessary hardware installed to support key systems of the primary site.
- Tier 3: **Electronic vaulting**. Data is electronically transmitted to a hot site.

- Tier 4: Point-in-time copies/active secondary site. Vital ***data is copied across*** the primary and secondary sites, each site backing up the other. Disk is often used in this tier.
- Tier 5: Two-site commit/transaction integrity. Data is ***continuously transmitted*** across sites.
- Tier 6: Minimal to zero data loss. Recovery is instantaneous, often involving disk mirroring or replication.
- Tier 7: Automated Recovery. Represents the highest level of availability in disaster recovery scenarios.

Building a BCDR plan

Typically involves the following activities:

- Risk identification
- Infrastructure review
- Business impact analysis
- Plan design
- Plan implementation
- ***Testing/Audits***

Penetration Testing

A penetration test (pen test), or ethical hacking, is an ***authorized*** simulated cyberattack on a computer system, performed to ***evaluate the security of the system***.

It is method for ***gaining assurance*** in the security of an IT system by ***attempting to breach*** some or all of that system's security, using the ***same tools and techniques as an adversary might***.

Some of the common Pentest tools

A wide variety of security assessment tools are available to assist with penetration testing, including free-of-charge, free software, and commercial software.

Specialized OS distributions

Several operating system distributions contain pre-packaged and pre-configured set of tools so that penetration tester does not have to hunt down each individual tool. Common examples include,

- Kali Linux
- BackBox
- BlackArch
- Parrot OS

Phases of Penetration testing

The process of penetration testing may be simplified into five phases:

1. Reconnaissance
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Covering Tracks

Thank you