COMPUTER SECURITY 34NTI
<MR ETUDIAYE>

TOPIC TREATED.

1. What is backup.
2. ~~Several~~ Several Importants of backup
3. What is Recovery Point Objective <RPO>
4. What is Recovery Time Objective <RTO>
5. Important of disaster recovery plan. Alarming stat
6. Mention the most common techniques or technologies of data backup options
7. What is 3-2-1 backup strategy.
8. Your three copies Are?
9. What is server backup.
10. Features of server backup.
11. Backup storage technology.
12. What is social networking.
13. Popular social networking sites.
14. Features of social networking.
15. Four main objective of social networking.
16. Different types of social networking.
17. ~~Security~~ Saftey tips of social networking
18. What is ~~Antivirus protection~~ / Antivirus software
19. Effects of virus on a computer.
20. Advantages of antivirus software
21. What is disaster recovery
22. Disaster includes what?
23. What is disaster recovery plan.
24. Benefits of disaster recovery.
25. What is Internet security.
26. Mention some Internet security threats and explain.

Scanned with CamScanner

26. What is log analysis.
27. Examples of logs
28. List and explain categories of logs
29. When to do log analysis techniques
30. Tools of log analysis
31. What is cyber attack.
32. Aims of cyber attack.
33. Why do cyber attacks happen.
34. Objective of cyber attack
35. What is nation strike attackers
36. Types of cyber attacks
37. How do we prevent a cyber attack
38. Mention 3 broads categories of a defensive action.
39. What is incident response.
40. Who handles incident response.
41. List and explain six steps 4 effective incident response.
42. What is Network traffic analysis.
43. Importance of network traffic analysis
44. Network traffic analysis implementation
45. What is encryption
46. Reasons why data and file are encrypted.

GROUP

Scanned with CamScanner

What is Data Backup?

- The importance of a Disastery Recov Plan: Alarming statistics.
- 6 Data Backup option.
- Backup storage Technology.

What is Data Backup.

Data Backup is the practice of copyi data from a primary to secondary locatio to protect it incase of a disaster, accider or malicious action. Backing up your data is critical for all businesses, Large and small.

What does Backup data means?

Backup data means all necessary data for the workloads your server is running. This can includ.. documents media files, configuration files, mach ne images, operating system and registry files.

dCMor
m²dcoR

REINVIGORATION CREW
Led by:
JC. Comr. Abdulganiyu Toyeeb Kayode
President 2020/2021

Scanned with CamScanner

RPO - is the amount of data an organization is willing to lose if a disaster occurs and is determined by the frequency of backup. If system is backed up once per day the RPO is 24 hours

NACOS | THE FEDERAL POLYTECHNIC EDE CHAPTER P.M.B. 231, Ede, Osun State.

Data Backup Includes Several Importants.

- Backup solution and tools. B3R2 st
- Backup Administrator.
- Backup scope and schedule. ss
- Recovery Point Objective (RPO) is the amout of data an organization is willing to lose if a disaster occurs and is determined by the frequency of backup.
- Recovery Time Objective (RTO) is the time it takes for an organization to restore data or system for backup and resume normal operation. 4
- RPO (Recovery Point Obj) is the time takes for an organization to restore data or system for backup and resume normal operation.

THE IMPORTANT OF A DISASTER RECOVERY PLAN: ALARMING STATISTICS

* Cost of downtime.

According to Gartner, the average cost of downtime to a business is $5,600 per minute.

* Survival Rate. Another Gartner study found only 6% of companies affected by a disaster that did not have

IGORATION CREW
Dr. Abdulganiyu Toyeeb Kayode
2020/2021

Scanned with CamScanner

disaster recovery in place survived and continued to operate more than two years after the disaster.

CSC

* Causes Of data Loss

The most common causes of data loss are hardware /system failure (31%) human error (29%) and viruses and malware of ransomeware (29%).

Data Backup Option.

There are many ways to back up your file. Choosing the right option can help you ensure that you are creating the best data back up plan for your needs. "Below are six of the most common techniques or technologies.

- Removable media.
- Redundancy.
- External hard drive.
- Hardware appliances.
- Back up software.
- Cloud Backup Services.

REINVIGORATION CREW
Led by:
JC. Comr. Abdulganiyu Toyeeb Kayode
President 2020/2021

R²EHBC

Scanned with CamScanner

- Removable media.

A simple option is to backup files on removable media such as CDs DVDs newer Blu-Ray disks or USB Flash drives.

- Redundancy

You can set up an additional hard drive that is a replica of a sensitive System's drive at a specific point in time or an entire redundant system. Redundancy is a powerful technique but complex to manage

- External Hard drive.

You can deploy a high volume external hard drive in your network and use archive software to save changes to local files to that hard drive. or hard disk

- Hardware Appliances

Backup appliances come with a large storage capacity and pre-integrated backup software.

- Back up Software.

VIGORATION CREW
Mr. Abdulganiyu Toyeeb Kayode
2020/2021

Scanned with CamScanner

Software - based backup solutions are more complex to deploy and configure than hardware appliances but offer greater flexibility.

- Cloud Backup services.
  Where you can push local data to public or private cloud and in case of disaster, recover data back from the cloud

WHAT IS A 3-2-1 BACKUP STRATEGY?

A 3-2-1 backup strategy is a method for ensuring that your data is adquately duplicated and reliably recoverable. In this strategy, three copies of your data are created on at least two different storage media and at least one copy is stored remotely.

* Three copies of data - Your three copies include
- Your original data
- Two duplicate.

REINVIGORATION CREW
Led by:
JC. Comr. Abdulganiyu Toyeeb Kayode
President 2020/2021

Scanned with CamScanner

Scaling
scaling
scaling

(2) two different storage type. It ~~stores~~ include internal and external hard drives. removable media or cloud storage.

(3) One copy off-site.

✓ Server Backup: Backing up critical Business System.

Server Backup solution are typically designed to help you backup server data to another local server, a cloud server or a hybrid system.

Features of Server Backup:

1. Support for diverse file types.
2. Backup location.
3. scheduling and automation.
4. Backup management
5. Partition selection. B3S3PD
6. Data compression.
7. Scaling 8. Backup type selection

B3S2Pd

BACKUP STORAGE TECHNOLOGY unique Adv

1. Network share and NAS (Network attached storage)
2. Tape Backup.

IGORATION CREW
r. Abdulganiyu Toyeeb Kayode
2020/2021

Scanned with CamScanner

3. Cloud-Based Object storage. ⟨NTC⟩

Social Networking.

Social Networking is the pratice of using a dedicated online platform to maintain contact, interact and collaborate with like-minded individuals, peers, friends and family. PF2

POPULAR SOCIAL NETWORKING SITES

1. Facebook.
2. Yelp
3. Twitter.
4. Instagram
5. TikTok.
6. Snapchat.
7. Quora ⟨FYTIT⟩
8. Youtube

Features of Social Networking Sites

* Enable Individuals to maintain social connections.
* Stay Informed and access. ⟨ES²T⟩
* Share a wealth of Information.
* These sites enable marketers to reach their target audiences

FOUR MAIN OBJECTIVES OF SOCIAL NETWORKING

1. Sharing.
2. Learning

Scanned with CamScanner

NACOS | THE FEDERAL POLYTECHNIC EDE CHAPTER
P.M.B. 231, Ede, Osun State.

3. Interacting.
4. Marketing. <SLIM>

THE DIFFERENT TYPES OF SOCIAL NETWORKING.

1. Social connections.
2. Proffessional connections.
3. Sharing of multimedia.
4. Informational
5. Educational. <SPSIE> OR <S²PIE>

SECURITY ISSUES IN SOCIAL NETWORKING.

To avoid been victims of social network the following are safe practice to deploy

SAFETY TIPS FOR SOCIAL NETWORKING.

1. Manage your privacy setting
2. Remeber: once posted always posted protect your reputation on social network.
3. Build a positive online reputation.
4. Keep personal information personal
5. Protect your computer
6. Know what action to take

IGORATION CREW
r. Abdulganiyu Toyeeb Kayode
2020/2021

Scanned with CamScanner

7. Use strong password.
8. Be cautious on social networking sites.

ANTIVIRUS PROTECTION

A virus is any unwanted program that enters a user's system without their knowledge. It can be self replicate and spread. A computer virus can be thought of as an illness to computer, just like human viruses that causes diseases in humans

Antivirus software is a data security utility which is installed in computer system with a purpose of protection from viruses, spyware, malware, rootkits, Trojan, phishing attacks, spam attack and other online cyber threats.

EFFECTS OF VIRUS ON A COMPUTER.

1. Slow down the computer.
2. Damage or delete files.
3. Reformat hard disk.
4. Frequent computer crashes.
5. Data loss

SDRFDI
SD²FIR

Scanned with CamScanner

NACOS | THE FEDERAL POLYTECHNIC EDE CHAPTER
P.M.B. 231, Ede, Osun State.

6. Inability to perform any task on the computer or the Internet.

Advantages of antivirus software.

a. Protection from viruses and their transmission.
b. Block spam and ads.
c. Defense against hackers and data thieves.
d. Ensure protection from removable devices.
e. Protect your data files.
f. Firewall protection from spyware and phishing attack.

DISASTER AND DISASTER RECOVERY

Disaster can strike a business at any moment. Research shows that without preparation and data protection over 50% of business will not survive a major disaster.

DISASTER RECOVERY.

Disaster recovery is the pratice of anticipating, planing for surviving and recovery from a ~~business~~ disaster that may affect a business

VIGORATION CREW
Mr. Abdulganiyu Toyeeb Kayode
2020/2021

Scanned with CamScanner

Disaster Include:

1. Natural events like earthquakes or hurricanes.
2. Failure of equipment or infrastructure, such as a power outage or hard disk failure.
3. Man made calamities such as accidental erasure or data or loss of equipment
4. Cyber attack by hackers or malicious insiders.

Disaster Recovery Plan

A disaster recovery plans enables businesses to respond quickly to a disaster and take immediate action to reduce damage, and resume operation as quickly as possible.

BENEFITS / IMPORTANT OF DISASTER RECOVERY.

1. Minimize interruption. MI
2. Limit damages. Ld
3. Traning and preparation. TP
4. Restoration of services. RS

MLTR

REINVIGORATION CREW
Led by:
JC. Comr. Abdulganiyu Toyeeb Kayode
President 2020/2021

Scanned with CamScanner

INTERNET SECURITY:

Internet Security is a term that describe security for activities and transactions made over the internet.

SOME OF THE INTERNET SECURITY THREATS WE CAN ENCOUNTER.

1. Hacking.
2. Phishing.
3. Hacking and remote access. AR
4. Malware and malverising. M2
5. Ransomware. R
6. Botnets. B

HPHMRB
H2 BPMR.

Hacking

is when an unauthorized users gain access to computer systems, email accounts or websites.

* Viruses or malicious software (known as malware) which can damage data or make system vulnerable to other threats.

- Phishing.

Phishing is a cyber attack involving emails. The goal's is to decieve people into handing over their personal information or downloading malware.

IGORATION CREW
r. Abdulganiyu Toyeeb Kayode
2020/2021

Scanned with CamScanner

- Hacking and Remote access.

Hackers are always looking to exploit a private network or system's vulnerability so they can steal confidential information and data.

- Malware and malversting.

Malversting is a portmanteau of "malicious" and software". It's a brand term related to viruses, worms, trojans and other harmful programs that hackers used cause havoc and steal sensitive information.

- Ransomeware.

Ransomeware is type of malware that prevents you from using your computer or accessing specific files on your computer unless a ransome is paid.

- Botnets.

The term botnets is a contraction of "robot network" A botnets is a network of computers that have been intentionally infected by

REINVIGORATION CREW
Led by:
JC. Comr. Abdulganiyu Toyeeb Kayode
President 2020/2021

Scanned with CamScanner

malware so they can carry out automated tasks on the internet without the permission or knowledge of the computer's owners.

THEY CAN USE IT TO CARRY OUT MALICIOUS ACTIVITIES WHICH INCLUDES

- Generating fake internet traffic on third party websites for financial plan.
- Emailing span to millions of interest users.
- committing fraud and identity theft.
- Attacking computers and servers.

Wi-Fi threats, in public and at home.

Public Wi-Fi carries risks because the security on these networks - in coffee shops, shopping, malls, airports, hotel, restaurants and so on.

- PACKET SNIFFING.

Attackers monitor and intercept unencrypted data as it travels across an unprotected network.

- Man-in-the-middle attack.

GORNTION CREW
: Abdulganiyu Toyeeb Kayode
2020/2021

Scanned with CamScanner

Attackers compromise a Wi-Fi hotspot to insert themselves into communications between the victim and the hotspot to intercept and modify data in transit.

LOG ANALYSIS:

Log analysis is the process of interpreting computer generated records called logs. Logs can contain a variety of information about how a digital product or service is used.

EXAMPLES OF LOGS MIGHT INCLUDES:

1. Sign in and sign-out request on a website
2. Transactions made on a currency exchange.
3. Calls made to informational API
4. Various other industry-specific actions

Applications:

Logs are often used for monitoring, auditing or debugging purposes. As a result, the applications

Scanned with CamScanner

of log analysis will usually fall under one of these categories.
- Maintoring.
- Auditing.
- Debugging.

MAD

- Muntoring.
Logs can be used to monitor the usage of a product service, often for security reasons

- Auditing.
Log may also be used for auditing purpose as in especially common in the finance industry.

- Dubugging.
Logs are especially popular for debugging computer processes, which is one of the reasons they are so frequently used.

WHEN TO DO LOG ANALYSIS TECHNIQUES.

In Log analysis, five common techniques (also know as processes) are.

IGORATION CREW
Abdulganiyu Toyeeb Kayode
2020/2021

Scanned with CamScanner

* Normalization.
* Pattern recognition.
* Classification and tagging
* correlation analysis
* Artificial Ignorance. NPC²A

* Normalization.
Normalization is the process of cleaning logs so that they adhere to the same standard or formats.

* Pattern Recognition.
Pattern recognition is the process of identifying patterns in logs, so that individual log entries can be handled appropriately.

* Classification and tagging.
Classification and tagging is another process that involves categorizing individual log entries.

* Correlation analysis.
correlation analysis is the process of finding

REINVIGORATION CREW
Led by:
JC. Comr. Abdulganiyu Toyeeb Kayode
President 2020/2021

Scanned with CamScanner

Splunk
Re sum

log entries that are correlated. This may refer to identifying which entries pertain to specific event, or identifying which entries are correlated.

* Artifical ~~intelligent~~ Ignorance

- Artifical ~~int~~ Ignorance is the process of "ignoring" entries which are not useful for analysis. Artificial ignorance may be used to identify which logs relate to intended usage partterns.

TOOLS

There are plenty of log analysis tools on the market, which allow you to quickly and easily import, normalize, and process data.

- Splunk
- Retraet.
- Sumologic
- Graylog
- Go Access
- Logz.io.

SRSGGL
S²G²SL

Scanned with CamScanner

CYBER ATTACKS.

A cyber attack is any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage.

Aims of Cyber attack

1. To disable.
2. To disrupt.
3. To destroy.
4. To control computer system.
5. To alter.
6. To block.
7. To delete.
8. To manipulate or steal the data held within the system.

WHY DO CYBER ATTACKS HAPPEN?

Cyber attacks are designed to cause damage. They can have various objectives, including the following.

1. Financial gain.
2. Disruption and revenge.
3. Nation-state attackers are behind some of these.

Scanned with CamScanner

types of attacks. Others called hacktivists might launch these types of attacks as a form of protest against the targeted entity.

Insider threats are attacks that come from employees with malicious intent

Cyberwarfare: Governments around the world are also involved in cyber attacks, with many national government acknowledging or suspected of designing and executing attack against other countries as part of ongoing political, economic and social disputes. These types of attacks are classified as cyberwarfare.

HOW DO CYBER ATTACKS WORK?

Threat actors use various techniques to launch cyber attacks, depending in large part on whether they're attacking a targeted or an untargeted entity.

WHAT ARE THE MOST COMMON TYPES OF CYBER ATTACKS.

Scanned with CamScanner

Cyber attacks most commonly involve the following: Read more

* Malware is malicious software that attacks information systems. Ransomware, spyware and Trojans are examples of malware.

* Phishing occurs when hackers socially engineer email messages to entice recipients to open them.

* Smishing (also called SMS phishing or smishing) is an evolution of the phishing attack methodology via text (technically known as short message service.

* Man-in-the middle or MITM occur when attackers secretly insert themselves between two parties such as individual computer

* DDOS take place when hackers bombard an organization's servers with large volumes of

Scanned with CamScanner

simultaneous data requests, thereby making the servers unable to handle any legitimate requests.

SQL Injection occurs when hackers insert malicious code into servers using the structured Query Language Programming Language to get the sever to reveal sensitive data.

Zero-day exploit happens when hackers first exploit a newly identified vulnerability in IT infrastructure.

HOW CAN YOU PREVENT A CYBER ATTACK?

There is no guaranteed way for any organization to prevent a cyber attack, but there are numerous cybersecurity best practices that organizations can follow to reduce the Risk.

* Reducing the risk of a cyber attack relies on using a combination of skilled security professionals, processes and technology.
* Reducing Risk also involves

Scanned with CamScanner

three broad categories of a defensive action.

1. Preventing attempted attacks from actu entering the organization's IT systems;
2. Detecting intrusions; and.
3. Disrupting attacks already in motion

BEST PRACTICES INCLUDE THE FOLLOW

* Implementing perimeter defenses, such a firewalls, to help block attack attempts and to block access to known malicio domains; [AUCT²

* Adopting a zero trust framework, which requires every attempt to access an Organization's network or systems.

* Using software to protect against malware, namely antivirus software, thereby adding another layer of protecti against cyber attacks

* Having a patch management progra to address know softwa vulnerabilities that coul

REINVIGORATION CREW
Led by:
JC. Comr. Abdulganiyu Toyeeb Kayode
President 2020/2021

Scanned with CamScanner

* Threat hunting program

be exploited by hackers.

* setting appropriate security configurations, password policies and user access controls.

* Maintaining a monitoring and detection program to identify and alert to suspicious activity.

* Creating incident response plans to guide reaction to a breach.
* Train and educate users.

Materials 2.

A Definition Of Incident Response

Incident response is a term used to describe the process by which an organization handles a data breach or cyberattack, including the way the organization attempts to manage the consequences of the attack or breach (the "incident").

Who Handles Incident Responses?

Incident response is conducted by an organi

Scanned with CamScanner

zation's computer incident response team (CIRT), also known as a cyber incident response team. CIRTs usually are comprise of security and general IT staff along with members of the legal, human-Resources, and public relations departments. As Gartner describes, a CIRT is a group that "is responsible for responding to security breaches, viruses and other potentially catastrophic incidents in enterprises that face significant security risks. In addition to technical specialists capable of dealing with specific threats it should include experts who can guide enterprise executives on appropriate communication in the wake of such incidents.

SIX STEPS FOR EFFECTIVE INCIDENT RESPONSE.

The SANS Institute provides six steps for effective incident response

1. Preparation.
2. Identification
3. Containment
4. Eradication.

Scanned with CamScanner

5. Recovery
6. Lessons Learned

PICER

1. Preparation

The most important phase of incident response is preparing for an inevitable security breach. Preparation helps organizations determine how well their CIRT will be able to respond to an incident and should involve policy, response plan/strategy.

2. Identification

Identification is the process through which incidents are detected, ideally promptly to enable rapid response and therefore reduce costs and damages.

3. Containment.

Once an incident is detected or identified, containing it is a top priority. The main purpose of containment is to contain the damage and prevent further damage from occuring (as noted in step number two, the earlier incident

GORATION CREW
Abdulganiyu Toyeeb Kayode
2020/2021

Scanned with CamScanner

are detected, the sooner they can be contained to minimize damage).

4. Eradication.

Eradication is the phase of effective incident response that entails removing the threat and restoring affected system to their previous state ideally while minimizing data loss.

5. Recovery.

Testing, monitoring and validating systems while putting them back into production in order to verify that they are not re-infected, or compromised are the main tasks associated with this step of incident response.

6. Lessons Learned.

Lessons learned is a critical phase of incident response because it helps to educate and improve future incident response effort

Scanned with CamScanner

500

NETWORK TRAFFIC ANALYSIS

Network traffic analysis is a method of tracking network activity to spot issues with security and operations and other irregularities.

Network trafic analysis solutions are used to monitor enterprise networks. Network traffic analysis tracks network availability and activity and identifies irregularities in operations and security.

IMPORTANCE OF NETWORK TRAFFIC ANALYSIS and

1. Automatic anomaly detection.
2. Stellar network availability.
3. Strong network performance.
4. Robust visibility.
5. Enhanced security posture.

NETWORK TRAFFIC ANALYSIS IMPLEMENTATION.

STEP 1

Identify data sources within your organization.

GORATION CREW
Abdulganiyu Toyeeb Kayode
020/2021

Scanned with CamScanner

Step 2
Choose the best approach to map data sources.

Step 3
start with a diverse data sample.

Step 4.
Set up continuous monitoring and choose the appropriate destination for collected data

Step 5
configure the right alerts for your IT teams.

done with a tools 2 check & weakness, the challenges so as 2 prevent it

VULNERABILITY ASSESSMENT.

Risk that comes problems

Types of vulnerability
1. Host vulnerability

Vulnerability is a tools that use to check & weakness, the challenges so as 2 prevent it.

REINVIGORATION CREW
by:
omr. Abdulganiyu Toyeeb Kayode
ent 2020/2021

Scanned with CamScanner