IT Security Basis for Corporates BY P3NGU1N

Inventory

🎯 Which is not one of the issues to be considered while doing hardening work?

Answer Format: X

A) Station handover procedures with prerequisite checklist

B) Audit of the secure configuration of the devices

C) Alert in case of configuration modification

D) Mouse movements of devices

ANSWER: d

Phishing Prevention

🎯 What is the simulation study done to raise awareness of corporate employees against phishing attacks?

ANSWER: phishing drill

Internet Browsing Protection

🎯 What should be done to block unwanted addresses to be accessed within the institution?

ANSWER: dns filtering

QUIZ:

🎯 **Which of the options should be in your IT inventory kept for security purposes?**

ANSWER: **The software installed with the exact version**

🎯 **Why is it important to restrict various software?**

ANSWER: **To prevent known malware from running**

🎯 **What is the main reason to keep an offline backup of backups?**

ANSWER: **To use in case of damage to online backups**

🎯 **How many days should the Minimum Retention Time be?**

ANSWER: **30**

🎯 **What does Phishing Drill do?**

ANSWER: **The company provides awareness to employees about phishing**

🎯 **Why is it important to use a password policy?**

ANSWER: **To standardize password security**

🎯 **What should be done to detect abnormal activities in the network?**

ANSWER: **Monitoring**

🎯 **Which of the following should be included in the scope of Hardening?**

ANSWER: **Audit of the secure configuration of the devices**

🎯 **Why should endpoint devices have EDR or at least AV?**

ANSWER: **To track and secure devices**

🎯 **Why is it important not to use end of life device?**

ANSWER: **Because they pose a security risk**