T2_ans

Type of Attack : Based on the detail/scenario given its safe to assume that there was a combination of phishing and a ransomware attack.

Reason For Belief : This is so because the email that was supposedly from HR that was urging employees to update their timesheet led to a site which gave same error for everyone on entering their credentials. This means it was a malicious url by attacker impersonating as HR(someone who is known and trusted by the victims).

Also later IT Desk received calls and mails that files shares and multiple Word Documents are not opening which was opening/working before they went to the malicious site which is a indicator that the files may have been encrypted by the attacker in order to get ransom . Hence it's highly probable that its a ransomware attack.

NEXT STEPS TO TAKE

Some Immediate Actions are:

- Isolate Infected Systems:
- Alert All Employees:
- Reset Compromised Credentials:
- Notify Incident Response Team:

Next steps to Contain , Resolve and Recover are :

- Identify the scope of damage by scanning the network to see how many systems have been affected/compromised.
- Segment the affected network and isolate critical systems to protect them even further
- Block malicious domains ,URL's via firewall,IPS,etc.
- Then Eradicate the malware via anti-malware (ransomware tools) to prevent further encryption.
- Then patch the system with latest updates and try to decrypt the encrypted files.
- If the encrypted files can't be decrypted then restore those files from backup systems.
- For high compromised systems consider wiping out.
- Monitor the restored systems carefully to look for any signs of residual malware.

Post Incident Activities to be performed are :

- Incident Report:
- Root Cause Analysis
- Improve Security Measures

- Review and Update Policies