|  |
| --- |
| **17. Integrated / Summative assessment Integrated situation**  KGL SOFT located in Gasabo district, is a medium-sized technology company that specializes in developing software applications. They store sensitive customer data, including personal information and payment details, on their servers. They have a headquarter and two branches, where the network, which is interconnecting them, is composed of different network devices such as (routers, switches, and servers,). The company implemented various cybersecurity measures to protect their data. However, the company is facing different challenges as follows:  ▪ Recently, some employees have been experiencing difficulties with their login credentials. They suspect that their accounts might have been compromised.  ▪ The company's firewall logs show an unusual increase in incoming traffic from a specific IP address located in a foreign country. This traffic is attempting to access the company's internal network.  ▪ The company is concerned about the security of data transmitted between their offices and data center. They suspect that data might be intercepted during transmission.  ▪ The IT security team notices an increase in phishing emails targeting employees. Some employees have fallen victim to these attacks, compromising their credentials.  ▪ The IT security team detects a suspicious login attempt on their core server. This login attempt was made by a user who should not have access to the server.  ▪ Further, the main company network security admin realized that the routers configurations are being modified by their co-admins without consulting him/her.  ▪ The system administrator was alerted by some system logs about unauthorized public IPs which are accessing systems devices and data.  ▪ Company suspects one of its employees of stealing proprietary source code and selling it to a competitor. They need evidence for possible legal action.  As cyber security expert, identify the cause of the above-mentioned issues, report them, and provide solutions in 8 hours |

ANSWER:

**Cybersecurity Incident Report and Solutions**

**Company:** KGL SOFT  
**Location:** Gasabo District  
**Date:** [Insert Date]  
**Prepared by:** [Your Name]  
**Role:** Cybersecurity Expert

### **1. Employee Login Credential Issues**

**Cause:** Employees' accounts might have been compromised due to phishing attacks, weak passwords, or credential stuffing attacks.  
**Solution:**

* Enforce multi-factor authentication (MFA).
* Implement strong password policies (length, complexity, expiration).
* Conduct security awareness training on phishing and social engineering.
* Monitor login activities for anomalies and reset affected accounts.

### **2. Unusual Increase in Incoming Traffic from a Foreign IP Address**

**Cause:** Possible brute-force attack, DDoS attack, or unauthorized scanning attempts.  
**Solution:**

* Block the suspicious IP address at the firewall.
* Implement geo-blocking to restrict access from untrusted locations.
* Deploy an Intrusion Detection and Prevention System (IDPS) to monitor malicious traffic.
* Review and tighten firewall rules.

### **3. Data Transmission Security Concerns**

**Cause:** Data might be intercepted due to lack of encryption or insecure communication channels.  
**Solution:**

* Implement end-to-end encryption (VPN, TLS, SSL) for data transmission.
* Use secure VPNs for remote office connections.
* Regularly audit network traffic to detect anomalies.

### **4. Increase in Phishing Emails and Credential Theft**

**Cause:** Employees are falling victim to phishing attacks, leading to compromised credentials.  
**Solution:**

* Implement an email filtering system to detect and block phishing emails.
* Conduct regular employee training on identifying phishing attempts.
* Set up Domain-based Message Authentication, Reporting & Conformance (DMARC) and Sender Policy Framework (SPF) records.
* Simulate phishing attacks to test employee awareness.

### **5. Unauthorized Login Attempt on Core Server**

**Cause:** Insider threat, credential compromise, or brute-force attack.  
**Solution:**

* Enable multi-factor authentication for server access.
* Implement strict role-based access control (RBAC).
* Monitor and log all access attempts with real-time alerts.
* Change server passwords and conduct a security audit.

### **6. Unauthorized Router Configuration Changes**

**Cause:** Lack of change management protocols and unauthorized admin access.  
**Solution:**

* Implement a centralized configuration management system.
* Require approval and documentation for network configuration changes.
* Restrict access to router settings using role-based permissions.
* Enable logging and alerts for configuration modifications.

### **7. Unauthorized Public IPs Accessing Systems and Data**

**Cause:** Misconfigured firewall, weak access control, or insider threat.  
**Solution:**

* Implement a strict firewall policy to restrict unauthorized public IPs.
* Use network access control (NAC) to limit access based on trusted devices.
* Conduct periodic security audits and penetration testing.

### **8. Employee Suspected of Stealing Proprietary Source Code**

**Cause:** Lack of proper data access controls and monitoring.  
**Solution:**

* Enable file integrity monitoring and track source code access logs.
* Implement data loss prevention (DLP) solutions.
* Restrict source code access to only authorized employees.
* Conduct a forensic investigation to gather evidence for legal action.

### **Conclusion**

By implementing the above security measures, KGL SOFT can significantly reduce the risk of cyber threats and data breaches. A proactive cybersecurity strategy, combined with continuous monitoring, will help safeguard sensitive information and maintain operational integrity.

**Recommendations for Future Prevention:**

* Regular cybersecurity training for employees.
* Routine penetration testing and security audits.
* Continuous monitoring using SIEM (Security Information and Event Management) tools.
* Strict access control policies with least privilege principles.

**End of Report**