Action Taken and Remediation Report

Reference Number:	AT-2024-001
Date of Report:	2024-06-10
Reported By:	Jane Doe
Department:	IT Security

Description of Issue

On 2024-06-08, an unauthorized external access attempt was detected on the corporate email server. The intrusion was prevented by the firewall, but several suspicious login attempts were logged.

Root Cause Analysis

The attempts were traced to a vulnerability in the email login interface, which allowed for multiple brute-force attempts without rate limiting. The lack of sufficient monitoring also delayed immediate detection.

Action Taken

- Blocked the suspicious IP addresses at firewall level.
- Increased monitoring of login attempts for all email accounts.
- Informed all users about the incident and recommended password changes.

Remediation Steps

- Implemented rate limiting on email login attempts.
- Updated the security patch for the affected system.
- Scheduled user awareness training on phishing and account security.
- Enhanced alerting processes for critical security events.

Follow-Up & Monitoring

The system will be monitored closely for the next 30 days. A follow-up audit is scheduled for 2024-07-08 to verify the effectiveness of the remediation efforts.

Important Notes

- Clearly document all actions taken and individuals involved.
- Ensure all remediation steps are tracked to completion.
- Regularly update stakeholders on progress and new developments.
- Store this document securely as it may contain sensitive information.
- Review and revise the format as needed based on incident learnings.