Learning from Real-World Access Control Breaches

Presenter Vasquez, John Paul S.

BSIT-3D

INTRODUCTION

Target (2013)

In 2013, Target Corporation suffered a massive data breach that exposed credit card and personal information of over 110 million customers. The attackers gained access through network credentials stolen from a third-party HVAC contractor.

CAUSE OF THE BREACH

Cause of the Breach

POOR ACCESS CONTROL

- Third-party had broad access to the internal network
- No network segmentation
- No Multi-Factor Authentication (MFA)

LESSONS LEARNED

Lessons Learned

- Restrict third-party access
- Enforce network segmentation
- Monitor access logs regularly
- Implement Multi-Factor Authentication (MFA)
- Use Role-Based Access Control (RBAC)

MITIGATION STRATEGIES

Mitigation Strategies

Apply RBAC for minimum privilege

1

Use MFA for all admin or sensitive access

2

Regularly audit and monitor access logs

3

Thank You