RCA: Fault Tree Analysis (FTA) for Bright Utility Company

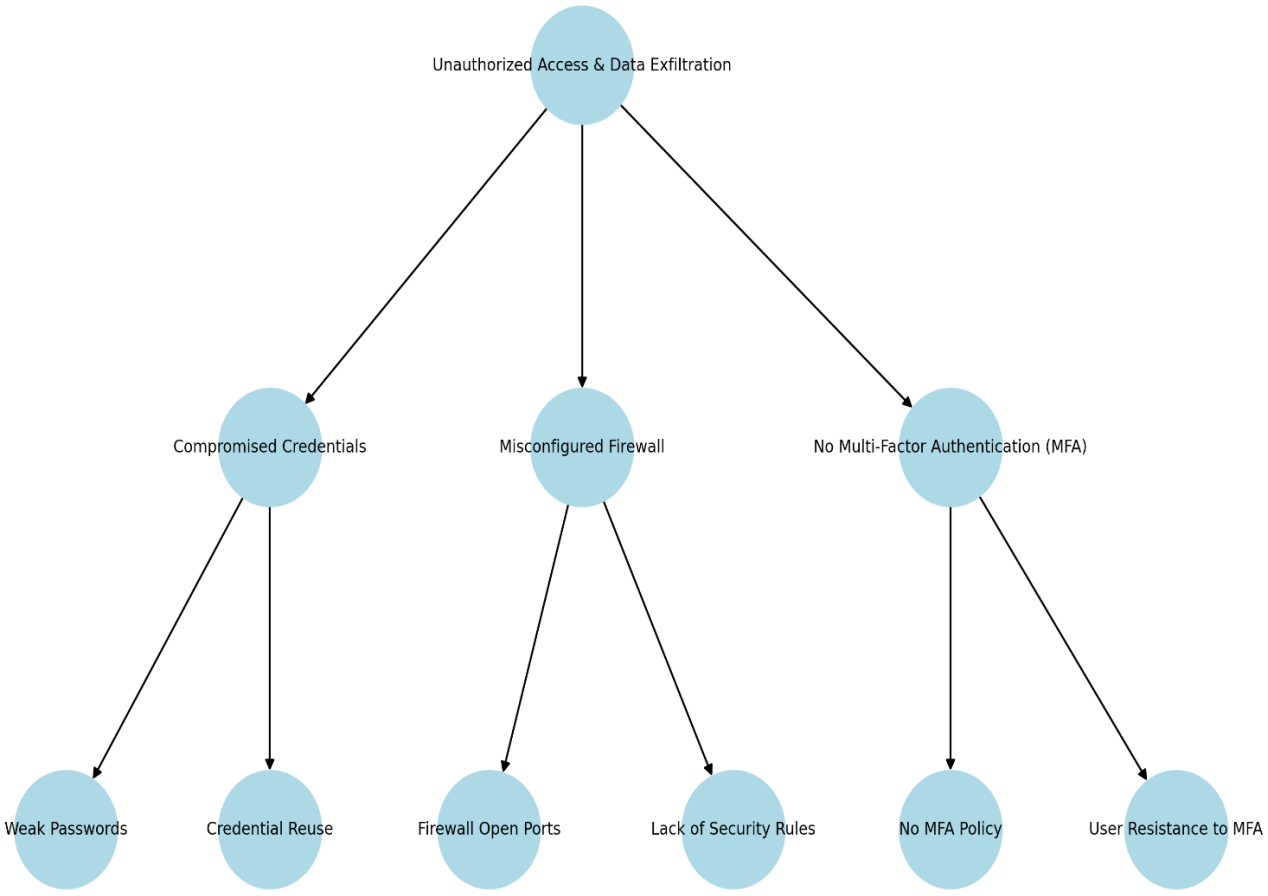
Scenario: Unauthorized Access to Critical Infrastructure Systems

BUC has experienced unauthorized access to its cloud-based Supervisory Control and Data Acquisition (SCADA) system, which manages power distribution. The breach leads to data exfiltration and potential non-compliance with the Alberta Reliability Standards (ARS) – Critical Infrastructure Protection (CIP) requirements.

FTA Breakdown

Top Event: Unauthorized access & data exfiltration leading to potential ARS non-compliance.

Fault Tree Analysis: Unauthorized access in BUC's Cloud System



Primary Causes

- Compromised Admin Credentials (*Violation of ARS-CIP-007: System Security Management*)
- Misconfigured Firewall Rules (*Non-compliance with ARS-CIP-005: Electronic Security Perimeter*)
- Lack of Multi-Factor Authentication (MFA) (*Non-compliance with ARS-CIP-004: Access Management*)

Sub-Causes & ARS Implications

- Weak credentials: Admin passwords were stored in plain text, violating ARS-CIP-007 (requiring strong authentication).
- Firewall misconfigurations: No enforcement of Electronic Security Perimeter (ESP), violating ARS-CIP-005.
- Ineffective access controls: Some high-privilege accounts bypassed MFA, violating ARS-CIP-004.

Outcome & ARS Compliance Mitigation Plan

- Implement MFA for all accounts, including legacy ones, ensuring compliance with ARS-CIP-004.
- Reconfigure firewall rules to follow least privilege principles, aligning with ARS-CIP-005.
- Deploy a password management system with auto-rotation and encryption, meeting ARS-CIP-007 requirements.
- Establish a continuous compliance monitoring framework to track adherence to ARS requirements.
- Train personnel on CIP compliance to prevent human error and improve security awareness.

By addressing these vulnerabilities and aligning with Alberta Reliability Standards (ARS-CIP), BUC will reduce regulatory risks, improve security posture, and ensure compliance with the Alberta Utilities Commission (AUC) and NERC standards.