Anatomy of a Breach

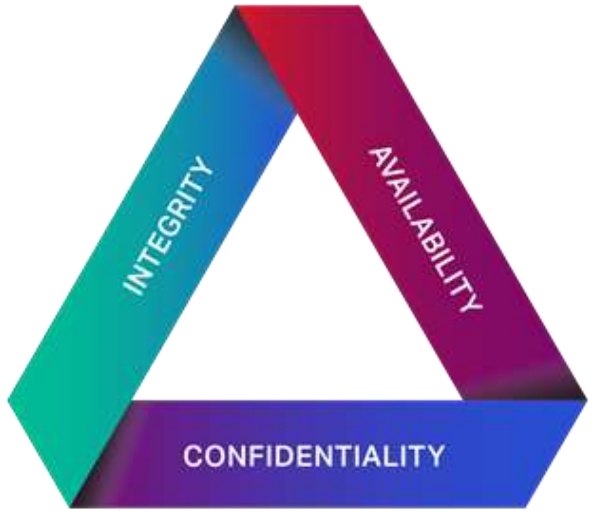
Alex Loffler
Principal Security Architect
Information Security Branch
November 2021

BRITISH COLUMBIA | Ministry of Citizens' Services

What is a Breach?

An attack that degrades or bypasses any of the following controls:

- **Confidentiality**
  - Protects resources from unauthorized access
- **Integrity**
  - Protects resources from unauthorized alteration
- **Availability**
  - Protects timely and uninterrupted access to resources



Breach Lifecycle

- **Reconnaissance** – Gather information about the target
- **Attack** – Use this intelligence to compromise the target
- **Expansion** – Gain a deeper foothold and increased access
- **Obfuscation –** Cover ones tracks to avoid detection

Reconnaissance

- Attackers need to understand their targets **attack surface**
  - Email addresses
    - @work, @home, @play
  - Social media accounts
    - Relationships, Friends, Hobbies, Interests
  - Technology stack
    - iOS, Android, Linux, Windows, OSX
    - ISP, FW, VPN, WIFI networks
    - IoT Devices
      - Smart TV's, Home Automation

Attack

- Exploits
  - Social Engineering
  - Technical

- Attacks
  - Ransomware
  - Coin Mining
  - Botnet Zombie
  - Identity Theft

Expansion

- Attackers will often attempt to pivot to more valuable assets
- Blast Radius

Obfuscation

- Sometimes, attackers will attempt to mask the origins of an attack in order to avoid detection
- By covering their tracks, attackers make it more difficult to determine how the attack started and how much information has been compromised

Takeaways

- Reduce your attack surface
  - Evaluate your online profile & behaviour
- Reduce the blast radius
  - Segment all of your networks
    - Should this entity be in this ‘circle of trust’
- Continually Re-Evaluate
  - From the perspective of an attacker

Thank you

Questions?