OCIO | Office of the Chief Information Officer

The Cyber Huns are at the Wall!
… and the "Arms Race" that ensues

Presented By:
Dale Land, Manager IT Security Operations

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer

BC Government “Cyberscape”

- Large network that serves many Public requirements
  - ~70,000 Devices on ~ 2,000 subnets
    - Data Centre with ~5,000 public facing systems.
  - ~ 1 million public IP addresses.
  - Access for Staff, Citizens, Schools/Colleges
  - Operated by several partner organizations

In the Early Days

Evolution of the threat

The 90's

- Vulnerable Software abounds
- Low sophistication annoyances
  - 88' Morris Worm was a wakeup to the danger.

The 00's

- Sniffing clear text traffic and brute force attacks.

First attempts at institutional security.

Firewalls

- Firewalls were added at the border to provide access (and sometimes egress) controls for the corporate internet.
- Block stuff you do not trust or proved to be untrustworthy.
- *Generally no "whitelisting". Too hard.*
- The interior remained undifferentiated (i.e. Production servers right next to desktops, maybe on different subnets).

Additional Protections added

Intrusion Detection/Prevention Systems

Anti-Virus Software on Computers

- Good at protecting against well known virus and types of misuse attacks.

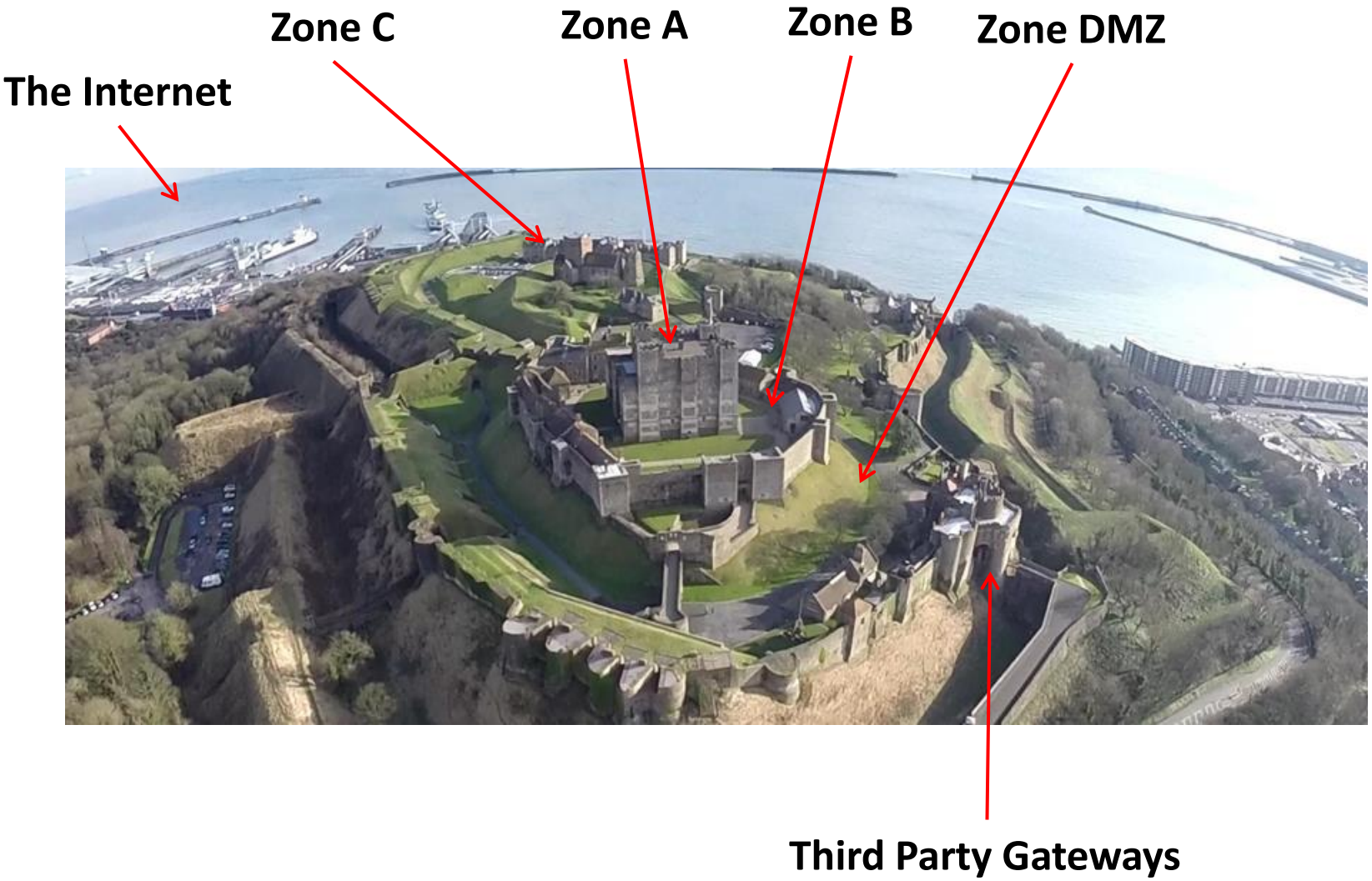
Anti-DDOS

- Required by any type of public business that cares about Availability.

What if they are “Inside the Wall”?

- Identify value of assets
- Segment assets by value “class”
- Restrict access based on business requirements.
- Implement additional controls for B2B interfaces into network.
- Implement software to give greater visibility into networked devices.

Multi-Layer Defense Layout



Today's BC Government Threat Landscape

- Ransomware / Advanced Malware
- Phishing/Spear Phishing attacks
- Denial of Service (DOS, DDOS)
- Advanced Persistent Threats (APTs)
- Reconnaissance scans

Why stop these threats?

- Protect Information
- Prevent breaches and harm to reputation
- Keep the business functioning
- Prevent harm to stakeholders
- Preserve “trustworthiness”
- Enable electronic service delivery

What are we doing?

- **Hygiene level controls**
  - Network: Anti-DDOS, Firewall, IPS, URL/App filtering
  - Host: hardening, patching
- **Security Awareness**
- **Threat Intelligence / Advanced Threat Analytics**
- **Vulnerability Management**
- **Security Information and Event Management**
- **SOC / Incident Response / Investigations**

What else can we do for future threats?

- Advanced Threat Prevention.
  - analyzing any file that comes into the environment.
  - Check hyperlinks on email (all HTML links?)
- Advanced threat detection, forensics on end devices.
  - Be able to detect what is going on with the device.
  - Be able to gain visibility into actions that take place on the end device.

What about no more border!!! Devices and Data are self protecting.

Q&A