ICT Security Update to Protocol Committee

Brian Curtis ICT Manager

Comhairle Cathrach Bhaile Átha Cliath
Dublin City Council

Introduction

- A range of High profile Cyber attacks have impacted on Government Agencies over the last twelve months.
- Presentation Contents
  - Recent Cyber attacks
  - DCC Response to these Attacks
  - Current Security profile in DCC
  - NIST Framework
  - Future Impact of Cyber Security
- This is a non technical and high level presentation

Comhairle Cathrach Bhaile Átha Cliath
Dublin City Council

Recent Cyber Attacks impacting on Government Agencies

- Note that there is a continuous attacks on all organisations at all times. More sophisticated with greater impacts now.
- The HSE suffered Ransomware attack
  - Impacted on business services
  - High Cost
  - Data loss
- Microsoft exchange mail for any organisation with email exposed to the internet.
- 2nd Microsoft Exchange weakness led to another critical patching
- Log4j major vulnerability

Comhairle Cathrach Bhaile Átha Cliath
Dublin City Council

DCC Response to these Attacks

- DCC not impacted by these attacks
- Incidents managed by
  - Security Team
  - Technical Teams
  - External support teams
  - SOC / SIEM managed service 24 x 7
  - Central government CERT team
- Attack vectors identified
- Scanning of Indicators of compromise
- Critical patches installed
- Staff awareness raised
- Exchange not a risk to DCC as design based on security did not allow direct connection to internet for mail

Comhairle Cathrach Bhaile Átha Cliath
Dublin City Council

Current Security Profile in DCC

- DCC has a dedicated security team
- DCC has a dedicated security budget
- Staff awareness key part of security profile
- Utilising external security companies for evaluation of new systems and existing systems
- DCC has an external managed SOC / SIEM (security operational and logging system)
- Enterprise grade backup
- Regular internal and External vulnerability scans
- Strong Patching policy
- LAN segmentation
- Security in depth by design
- Strong end point protection
- Upgrading of older software and hardware that cannot be secured

Comhairle Cathrach Bhaile Átha Cliath
Dublin City Council

NIST Framework

- DCC implements the NIST Framework
- Presumption that not all cyber attacks can be prevented
- Detection software and processes in place
- Incident response plan in place to respond
- Security profile of an organisation is linked to its business risk management approach

Comhairle Cathrach Bhaile Átha Cliath
Dublin City Council

Future impacts of Cyber Security

- Increased complexity of attacks expected
- Impact is now operational risk as well as data loss and Reputational risk
- Increased level of specialised Resources and Budget will be required into the future
- Availability of these resources in government is challenging
- EU NIS directive will add Government services to the security level of Essential services
- Increased use of cloud solutions adds to the resources required to secure DCC data and operations

Comhairle Cathrach Bhaile Átha Cliath
Dublin City Council