Comhairle Cathrach
Bhaile Átha Cliath
Dublin City Council

Roinn um Chórais Faisnéise
Bloc 1, Urlár 9, Oifigí na Cathrach, Baile Átha Cliath 8
Tel. +353-1-222 2240 Fax. +353-1-2222229 E. isdept@dublincity.ie

Information Systems Department
Block 1, Floor 9, Civic Offices, Dublin 8

Finance Strategic Policy Committee

Cyber Security

Introduction

There have been a range of high profile Cyber-attacks recently which have impacted on government agencies and it is appropriate to brief the Finance SPC in DCC on the current position.

Recent Cyber Attacks impacting on Government Agencies

There have been a number of high profile attacks recently but it should be noted that there is a continual Cyber-attack on all organisations at all times.

The HSE suffered a major ransomware attack that is still being remediated at the time of this report. This attack had a significant impact on the business services and will have a large cost to the HSE. This impacted on all of the key systems of the HSE.

A major security weakness in the Microsoft Exchange mail system had significant potential impacts on many organisations worldwide. This weakness would have allowed for total access to organisations systems if email was enabled from the internet directly.

A second Microsoft Exchange weakness was the subject of an urgent patching policy to again stop a major attack vector.

DCC Response to these Attacks

DCC has not been impacted by these attacks. These incidents are managed by our Security team, Technical teams and our external managed service providers. This includes a 24x7 Security operation centre and SIEM(logging) solution that is contracted to DCC. We are also supported from the Central Government CERT team.

We have identified the potential attack vectors and scanned for the associated indications of compromise. All critical additional patches would have been installed.

Staff awareness was raised through a number of channels.

The exchange attack was not a risk to DCC as our design for over twenty years does not include a direct connection from the Internet to our mail systems. This was a security feature that shows the need to include security requirements in the systems design phase.

Current Security profile in DCC

DCC has a security profile suitable to a major public body. The following points illustrate the high level of security applied to our systems.

- DCC has a dedicated security team
- DCC has a dedicated security budget
- Staff awareness is a 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 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

NIST Framework

DCC implements security on the NIST framework which includes additional functionality beyond prevention. This framework presumes that not all cyber-attacks can be prevented and so it is important to detect and respond to incidents that are not prevented. An incident response plan is utilised in DCC following the detection phase.

It should be noted that the security profile of an organisation is also linked to its approach to its business risk management approach.

Future Impacts of Cyber Security

Looking forward there is going to be increased complexity in terms of the attack profile expected. The impact of a security incident is now both operational risk as well as data loss and reputational risk. This is likely to increase the level of specialised resources and budget that will be required into the future. The availability and cost of such resources is challenging for government bodies.

This will also increase with the proposed EU directive on NIS being extended from the current operator of essential services to include government services in the coming years.

The increased use of cloud solutions also adds to the resources required to secure DCC data and operations.

Brian Curtis
ICT Manager

1st September 2021