BSS/17/11
Corporate Infrastructure & Regulatory Services Scrutiny Committee
26th September 2017

CYBER SECURITY IN DEVON COUNTY COUNCIL
Report of the Head of Service for Digital Transformation and Business Support

Introduction

This report provides assurances to Scrutiny that the Defence, Detection and Recovery Process are in place to protect Devon County Council from Cyber Attacks.

1. The Threat

Cyber-attacks can be summarised into the four following areas:

1.1 Email

- "Phishing" to entice staff into opening malicious email attachments or visit malicious web sites
- "Spear Phishing" where information particular to the recipient is used to make attacks more likely to succeed
- "Whaling" where high profile staff with financial responsibility are targeted to secure large rewards.

1.2 Direct attacks on technical software vulnerabilities, both internal and across the Internet, known as Malware

- Operating system flaws
- ICT application flaws
- Vulnerabilities introduced through weak configuration

1.3 Social Engineering to gain unauthorised access or knowledge through impersonation, leaking of passwords or blackmail

- By telephone
- By email
- In person, at work or in leisure time

1.4 Communications Hijacking

- Intercepting supposedly secure communications by subverting encryption, a "man in the middle" attack. This is effectively breaking into the middle of a two way conversation.

2. Detection/Protection

2.1 Overview

DCC protect themselves against security threats by deploying high grade yet cost-effective technical protections to guard against attacks on infrastructure, data, and applications, and by training staff to better detect fraudulent emails and social engineering attacks. This protection is further enhanced by making use of the Windows 10 laptops for both Members and staff that has an automated and centrally managed anti-virus and security patching regime to ensure both PSN compliance and daily updates to guard against Cyber-attack. Should an attack break through this protection, an Incident Response Team will immediately respond to isolate and resolve the attack making use of data backups if required.

2.2 General Internet and Intranet Communications

Communication routes used by email, Internet and application data are scanned by advanced technology from a major supplier, which applies comprehensive firewalling and web filtering, and examines data for the presence of viruses, technical attacks against operating systems and applications, or attempts by staff to visit known malicious websites. The National Cyber Security Centre also monitors all outbound connections DCC and reports any observed malicious activity so that prompt and appropriate action can be taken.

2.3 Email, SPAM and Malware protection

Email is still the primary route for attackers. DCC Security Protection for email is provided by the anti-spam, anti-virus and anti-malware software as it enters the boundary of DCCs network. This is further enhanced by additional anti-virus software running on all Windows 10 devices.

All incoming email traffic is checked for authenticity by examining information about email originators. All outbound email complies with new central government guidelines, and is encrypted when travelling across the Internet if the recipient also supports encryption.

For those cases where further email protection is required, such as ensuring that only the intended recipient can read a sensitive email, DCC have licensed the "Egress Switch" product which tightly controls message encryption and requires the recipient to identify themselves before the message can be read.

2.4 Incident Preparation and Response

Currently one of the biggest threats to DCC infrastructure is that posed by "zero day" malware, especially that related to "ransomware" which quietly encrypts user data before demanding a monetary payment. The very nature of "zero day" malware means it is hard to detect as it passes through the layers of control as it has never been seen before. To defend against these latest problematic attacks, DCC’s ICT delivery arm ScoMIS monitor security newsfeeds throughout the day and so are alerted at an early stage when a major new security event is developing across the world.

ScoMIS ensure that all critical data is regularly protected via data backup solutions, and maintain formal Incident Response plans to be invoked as soon as a security or malware incident is reported. There is confidence that when the inevitable malware or security incidents do occur the impact on the operation of DCC services will be relatively low, as critical data can be quickly recovered from recent backups.

2.5 Security by Design

ICT systems and services are implemented with attention being given to ensuring they are robust and secure by their design and an ongoing operating system and application software patching policy ensures they remain secure through pro-active software fixes of identified security flaws.

The DCC ICT infrastructure is regularly scanned for technical weaknesses by both internal technology and an accredited external company to ensure we remain secure and protected. This proactive scanning combined with the technical protection described above, the modern Windows 10 devices and staff training and awareness ensure DCC is well protected and able to respond to any incident.

Rob Parkhouse
Head of Digital Transformation and Business Support

Electoral Divisions: All
Councillor Barry Parsons, Cabinet Member for Organisational Development and Digital Transformation
LOCAL GOVERNMENT ACT 1972:
Contact for Enquiries: Gary Dempster, ICT Strategic Commissioning Manager
Tel No: 01392 38 3000 Room: 122
Background Paper

Nil