Peace
EUROPEAN UNION
Northern Ireland - Ireland
European Regional Development Fund

Special EU Programmes Body
Gina McIntyre

Surviving a Major Cyber Attack




Special EU Programmes Body
Foras Um Chláir Speisialta An AE
Boord O Owre Ocht UE Projecks

The ‘Incident’ from a Business Administration viewpoint

- Do you think you are prepared?
- The Perfect Storm !
- Containment , investigation, scrub , recover, restore,
- Need an incident team/ experts to support you
- ICO countdown - 72 hours
- Prioritise your needs & requirements– stick to the Plan
- You only know what you know !

Some of the Lessons Learned……

- Fully functional again and have emerged stronger than before
- We are very aware of the risks and will never take that for granted – EVER!!!

Recommendations :

- KEEP A LOG OF EVERYTHING DURING AN INCIDENT – incident log and book
- ICO – have the templates ready –completed forms - Insurance
- Consider what the most valuable items for your org would be in a crisis
- Stand alone source of the most important information for handling any incident
- Increasing security in every way possible, using encryption more
- Train staff and keep that regularly updated
- Call crisis meeting and see what the response is.
- Business Continuity Plans – revisit regularly / keep updated/ Keep them short

……Lessons Learned

- Test everyone and everything randomly
- Vigilance is more important as people working in isolation and more likely to be a bit casual
- Off site Back ups – remote working may mean some processes are not operational
- Revisit risks to your organisation regularly – keep up to date with emerging risks
- Contact lists for staff and stakeholders up to date eg all the staff without email urgently
- SEUPB was able to procure services from an external organisation to provide expertise in managing the incident. Smaller organisations and businesses may find it difficult to obtain the same support due to cost
- Get your support contracts and call of lists in place before you need them
- Don’t expect anything !

SEUPB Solution

Actions taken to date

Engaged with a Cyber Security Specialists, Cyphra.

Replaced legacy firewalls with **Next Generation firewalls**

- Advanced threat protection and network visibility.
- Web Access controls.
- Threat controls.
- DNS Security.
- Geographical access controls.

End Point Protection and Visibility

- PAN Cortex XDR.

Appointed CISO advisory Role Chief Information Security Officer- threat assessment

A new cloud based **remote access solution**

- Enhanced security and availability for remote clients.
- Threat controls.
- Efficient route services such as Microsoft Office 365 and Microsoft Teams.
- An always-on VPN.

Central Management solution

- solution to control policy consistent levels of acce

SIEM solution

- Providing advanced visibility and notification of threats.

Ongoing Improvements and vigilance

- Completion of a Business Impact Assessment to identify information assets- give the time as you really need to consider this
- Soon to undertake a Cyber Maturity Assessment on systems- to identify any system gaps to improve on protecting our information assets
- Security Information & Event Monitoring (SIEM)solution collecting and correlating events from multiple SEUPB network sources including the firewalls, remote access, clients and authentication servers.
- Providing advanced visibility and notification of threats.


Malicious
Activity

Recent Attempt

- Multiple attempts to connect to the network - reconnaissance scans.
- Reconnaissance scans to look for vulnerabilities to exploit - general knowledge gathering attacks.
- Predominantly from China, Vietnam and Russia.
- Multiple events taking place over a short period.
- Contained by the firewall rules
  Rule base mitigates unwanted connections and possible attacks.

Geographical attempts to connect to SEUPB network

- **Result:**- Preventative measures in place reduced the chance of impact and updated security policies prevented any breaches – all identified, managed and reported.

Still To Do

- The SIEM recently picked up persistent access attempts from addresses in China. The visibility from both the firewall and SIEM platforms provides SEUPB assurance that all attacks were identified, alerted on and prevented.

- STILL TO DO , and DO and DO and DO:
- Duo 2 Factor Authentication solution
- Procurement of Security Awareness Training and Phishing simulation testing, to keep SEUPB staff vigilant.
- Encryption of database systems which store Personal Data.
- Procurement of Penetration Testing for both SEUPB Firewalls and our external project system – eMS……

We all face the same threat !

SEUPB is one of the 6 cross border bodies setup under the 1998 Good Friday agreement, this means we as a body have a close affiliation to the Northern Ireland Civil Service specifically Department of Finance (DoF) and understand for normal day to day processes IT Assist should not have to support us,

However, in certain incidents a Public Sector body such as SEUPB should be able to avail of some of the extensive resources within IT Assist.

Some arrangements should be put in place for not only SEUPB but other cross border bodies or NDPBs.

Thank you




Special EU Programmes Body
Foras Um Chláir Speisialta An AE
Boord O Owre Ocht UE Projecks