East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Monday 13th June 2020

This advice has been collated by EMSOU and is intended for wider distribution within the East Midlands Region to raise awareness among businesses and the public.

Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from reputable sources.

If you require any further information, assistance or guidance please contact the EMSOU Protect Team EMSOU Protect Team **or your local Force protect team.**

Today's topic is 'Incident Response' (IR)

In 1998, Robert Tappan Morris released the first Internet worm ('Morris Worm') shaping computer security history by: unleashing the first large scale denial-of-service (Dos) attack, impacting around 10 percent of computers on the Internet, being the first person prosecuted under the Computer Fraud and Abuse Act (CFAA).

The impact to the internet and the significant challenges in coordinating a response in such a wide scale environment led to the creation of the Computer Emergency Response Team Coordination Center (CERT). The goal of CERT organization is to provide a central hub for communicating and coordinating responses to security incidents. The UK-CERT forms part of the National Cyber Security Centre (NCSC).

As security measures evolve, so do the capabilities of our adversaries. As a result, no security can ever be perfect. Incidents can and will happen, so it's important to be prepared for them. Incidents can be opportunistic or targeted, and threats can originate from outside and inside your organisation. But, whatever the nature of the threat, ***only one thing can help you deal well with a cyber incident - good preparation.***

1. **Develop policy:** To outline the authority and responsibilities of the IR team. This might include; the revocation of access rights, taking systems offline, reconfiguring them, purchasing equipment and services, accessing sensitive information and conducting forensic investigations. Ultimately, any delays will hinder recovery so outline responsibilities and the means to settle disputes well in advance.

2. **Communication Plan:** Who should the IR team contact in the event of a problem? When is contact appropriate and how should it be made? How will messages be communicated vertically and horizontally across the organisation or to external agencies? How will you be contacted by customers and suppliers? A good communication plan facilitates a realistic appraisal of the ongoing situation and avoids unhelpful speculation during difficult times.

3. **Define critical functions:** Which systems have the highest impact if compromised and how quickly should they be restored? What data would be the most damaging to lose and where is it located? Once you know what the critical functions are, you can prioritise money, time and IR effort protecting them.

4. **Define roles:** Helps maximise efficiency. Who can lead the IR team, or facilitate purchases? Who will liaise with HR when there's an insider threat or an internal breach of policy? Who has the expertise to deal with applicable laws, regulations and contracts, or the skill and diplomacy to communicate across the organisation and to external entities?

5. **Rate the incident:** To understand the gravity of the situation and elicit the appropriate response across the organisation.

6. **IT hygiene:** Network diagrams, build documentation, recovery procedures, up-to-date inventories and change control documents should be in order to efficiently sanitise, recover or rebuild infected system and operations.

7. **Ensure network visibility:** Logs must be collated, synthesised and evaluated to identify and track problems across the network. Check - Windows event and security logs, anti-virus and firewall logs, as well as rogue accounts on the network. Alternatively, consider holistic solutions such as SIEM technologies.

8. **Business continuity:** Failing to prepare is preparing to fail. Develop work arounds for when there is a complete or partial loss of IT services. How will critical operations continue in the face of such difficulties?

9. **Train:** The identification and resolution of a problem needs an organised response. The IR team need to react to different situations calmly and with confidence which is why it is so important to practice IR by exercising or simulation.

An organisation can deploy many preventive controls as planning and finance permits, however, attackers will still slip through the net. It is the ability to detect and respond that determines how badly the business is impacted and why incident response (IR) preparation is so important.

Further advice on incident response, from the NCSC, can be found here

Hot topic

A recent study carried out by FICO Consumer Digital Banking, showed only 40% of people in the UK have separate passwords for their financial accounts. The research highlighted that just over 20% of UK citizens only use between 2-5 passwords. Using the same password for multiple accounts means that if the password is compromised, all accounts – and the sensitive data they protect – could be exposed and exploited.

To better protect your information, consider:

- A reputable credential manager to store all your passwords in an encrypted vault. Credential managers are downloadable apps that work across multiple devices such as your desktop, laptop or mobile phone. A good credential manager will not only help you create strong passwords tailored to the site, but also auto-fill these details when you wish to log in.

- Multi-factor authentication. For example, using a password as well as a pin sent to a mobile phone. To find out more about MFA see here.

Reporting

Please report all Fraud and Cybercrime to Action Fraud by calling 0300 123 2040 or online.
Forward suspicious emails to report@phishing.gov.uk.
Report SMS scams by forwarding the original message to 7726 (spells SPAM on the keypad).