East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Thursday 16 April 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 **Cloud Services** and below are some tips on how to select a Cloud Provider.

For organisations whose hardware, software and data where the centre is located on site and directly under their control, organisations are free to determine their own security posture and policies. However, much of this oversight is lost when migrating to the Cloud. Most Cloud providers share a pool of resources between hundreds, if not thousands of other users.

- How does an organisation guarantee their data remains separate and secure?
- What sort of assurance should be sought before committing to cloud services?

Organisations may use the hardware and software provided - Software as a Service (SaaS).

Other organisations want hardware and IT infrastructure – Infrastructure as a Service (IaaS).

Some want something in between - Platform as a Service (PaaS).

Each model places different levels of responsibility on the customer. Organisations must be clear what security measures they are expected to take and where the responsibilities lie.

Check your security responsibilities

- **Does the cloud encrypt stored data?** Who has control of the encryption keys, if it's the cloud provider how do you know that they will be kept secure?
- **When your data travels over the internet, will it be encrypted?** A VPN gives a high degree of privacy when communicating with cloud applications.
- When changing providers, or leaving the cloud environment, organisations need to know that data will be removed from all hard drives. In the cloud these resources will be reallocated to other users. **Check how the provider intends to make data inaccessible to others and what guarantee they offer.**

- Many cloud providers offer self-service portals where you can access reports, logs. **Check with the provider what these show and whether they give you adequate visibility of security incidents**.
- **Check that any software used has been developed with security in mind.**
- Using the cloud is often seen as a way to provide business continuity and recovery. What if your cloud provider has problems? **Check what redundancy and resilience the Cloud Provider has.**

Staff training:

What is sensitive, private and confidential? Employees need to understand how valuable or sensitive data is, then it is more likely to be handled with the care and attention it deserves.

Most security incidents occur because of poor security policies. If employees are using poor passwords to connect to systems, or have access beyond that actually needed to do their job, then invest time and effort educating users.

Check that employee are trained to use applications correctly.

Hot topics

We are seeing a growing trend of so called 'sextortion' phishing emails. This is where the sender claims to have compromising images of the recipient and often the email will include a password that the victim has previously used, to add authenticity. Advice from Action Fraud can be found here.

These are fundamentally different to actual sextortion attempts where the sender does possess compromising images of the victim. The advice for this remains the same; anyone who is sent an email which includes compromising images and/or a request for payment should contact their local police force.

The free vouchers scam has moved to a new variant with phishing emails being sent to recipients claiming to be from Tesco, offering free vouchers. The email features a link for recipients to register and claim their free voucher which provides an opportunity for criminals to steal email logins, passwords and personal details.

A recent fraud involved the sale of a car where the suspect used the Covid19 lock down as a reason the victim could not see the vehicle and persuaded the victim to pay by bank transfer.

Reporting

Reporting is CRUCIAL. Please report all Fraud and Cybercrime to Action Fraud either online or by calling 0300 123 2040.