HE Update

Cyber Security

September 2015

Meet the New Threats, Same as the Old Threats

Technology is moving relentlessly forward, providing both increased opportunities and at the same time increased threats to security, privacy and availability. However on one level, the nature of the threats never changes – they rely on innate human and cultural factors such as our gullibility, carelessness and capacity for irrational behaviour. These will continue to be exploited by the 'bad guys' simply because they sometimes work.

We share some thoughts below arising from our continued close involvement in cyber security audits and events both within HE and the wider environment.

Social Engineering

Why go to the trouble and expense of using advanced hacking tools and techniques when a good old-fashioned con will work just as well? 'Social Engineering' has been around for years and simply means an attacker misleading us into doing something we shouldn't or divulging information by taking advantage of our better nature.

At a basic level it involves asking for passwords or other sensitive data or guesses based on known personal characteristics. More sophisticated practitioners will make use of advanced psychological techniques, perhaps establishing a rapport with reception staff to gain access to a building using an elaborate pretext which then allows all manner of network access. Universities, being generally open settings, are particularly vulnerable.

Social Media and Spear-Phishing

Our data does not just live within our organisational boundaries – it has a life of its own (a 'digital footprint') thanks to the net. By some reckonings, over 90% of organisations now use social media to screen recruitment candidates. This alone tells us how useful this information now is. And if it's useful to the good guys it's certainly going to be useful to the bad guys.

Many organisations will have policies on the use of Facebook or Twitter and most sensible employees will differentiate between their personal and professional lives. LinkedIn is different because by nature it is linked to professional experience and achievements. As a result the information it contains can be priceless. For example, IT staff will often log their technical credentials for networking or career progression reasons which could be extremely useful to hackers when linked with employer names.

This makes staff vulnerable to 'spear-phishing' – a highly targeted form of phishing. The aim is the same as any other type of phishing attack - to obtain personal information, passwords or bank details. But spear-phishing emails are designed to look like they are from someone you know – a colleague, friend or employer. They will address you by name and often contain personal information gleaned from social media.

How Can You Respond?

Focus on staff and HR Issues. Whilst technological resource will remain a crucial part of the defensive solution to cyber-attacks, there comes a point where this is a diminishing return. There is now a strong argument within the cyber-security community that, pound for pound, spending on 'HR' type factors such as education, and cultural awareness will be more effective. Our work with university senior management teams support this view that cyber security is a matter for all and not just an 'IT' problem.

Social Media Policies. These are now essential. Are staff trained in social media use? Is it clear what behaviour is allowed and what isn't and is this in employment contracts?

'Predict – Prepare – Respond'. To a degree, while attacks should be anticipated – 'stuff happens', inevitably. But the outside world will judge an organisation on the speed and effectiveness of their response. Cyber responses could certainly fall under the umbrella of a corporate business continuity planning framework. As such, plans should be systematic and include: identifying assets, types of threats/vulnerabilities and responses.

Cyber Liability Insurance has been available for a while but is still not widely taken up. It covers the expenses related to dealing with a cyber-attack, intellectual property rights (e.g. website) defacement and third-party damages resulting from a denial of service. It can be a very effective way to address the costs of a security breach by transferring the risk.

Wise Up. Sadly, we need to be less trusting to ensure systems are adequately protected. This means challenging strangers in buildings, using common sense and never revealing sensitive data such as passwords (which legitimate organisations will never ask for).

Get in Touch

If you would like to discuss how Uniac could help you provide assurance over cyber security risk, please contact:

Ian Musgrave
☎ 0161 247 4697
imusgrave@uniac.co.uk

Robert Foster
☎0161 247 2851
rfoster@uniac.co.uk

Certificate Number 13024
ISO 9001, OHSAS 18001, ISO 14001