KCS Group Europe

Cyber-Psychology: The Underestimated Threat

22nd October 2021

Cybercrime has only of recent years, been recognised for the seriousness of its capabilities of harm to businesses and individuals. This is due in part to the lack of visual impact perceived by the public in terms of the effect it has on businesses, individuals, and communities; until that business or individual had become the victim of cybercrime. This is largely due to the way in which cybercrime is reported in the media.

On the 29th of April 2021, the Colonial Pipeline; the largest in the US (Houston Texas) was hit by ransomware. The perpetrators known as Darkside (familiar to law enforcement, intelligence, and cyber risk-management agencies) had gained access to a staff members' VPN remote account password. The password was compromised with a single vector. Attack vectors are a means (or a path) by which a bad actor can gain access to a computer or network to deliver the ransomware.

In this instance, the ransomware found its way into Colonial Pipeline's infrastructure through the login credentials of an employee. Other examples of vector attacks may find their way through email attachments. The ransom demand was $5m. The hack attack had cost Colonial Pipeline $4.4m – although they later recovered $2.3m.

Darkside performed their 'hat trick' three days prior, the organised crime group (OCG) used the same format (single vector) on a compromised employees account. Brenntag, a German chemical distribution company operating in over 70 countries, paid a ransom of $4.4m. (The demand was $7.5m).

Infrastructure and big business are an attractive source of income for cyber criminals. Such businesses are vulnerable targets for hackers, simply because, when compromised, this impacts their community, their brand and therefore their reputation. A speedy solution involves a speedy payment. When Colonial Pipeline were hacked, the fall out caused a knock-on effect of panic buying and fuel shortages.

The OCG known as Darkside, have recently tried to change their image. Flooding the internet with their 'Robin Hood' style fake persona of stealing from the "rich" to give to the needy. Make no mistake, these individuals are extortionists, thieves, and blackmailers of the most dangerous kind – manipulating public opinion and seeking approval for their crimes. Darkside have extorted millions from organisations (and individuals) around the world and have recently (since 2020) occasionally donated to some charities, the bitcoin equivalent of up to $40,000 in total. The charities were Whale Alert, The Water Project and Children International. Whilst there are charities that state they will refuse to accept the donation; others have declined to comment on how they will proceed with their donation.

No matter how tight an organisation feels its cyber security is, or what policies and procedures they issue to employees – a significant percentage of breaches to organisations are inadvertently caused by employees. Whilst most businesses have cyber security policies in place, most often, these security and policy documents are of a basic, generalised format.

Enough only to cover that which is required of them by law. How many businesses drill down into their security and organisational policies? How many smaller businesses have a data controller tasked to monitor that procedures are being effectively followed? How many businesses effectively carry out periodic Continuous Personal Development (CPD) training for their employees?

Organisations benefit from building strong cybersecurity policies for their employees on the use of company data, and the way with which they access this data. An example would be guidelines that employees must follow whilst at work. These would include policies on using company computers, internet, and systems only for business needs and not for personal use. Personal use constitutes mail order shopping, booking vacations online, and using social media. Similarly, their corporate emails must be limited to the use of business needs only.

Corporate emails must not be used to sign up to social media, mail order shopping, or applications and software not related to the needs of the organisation. Corporate emails are best kept in-house and not shared with family and friends. This in turn will minimise the risk of a domino effect of viruses and malware spreading from personal emails to corporate infrastructure.

Strong policies on cyber security and risk compliance organisation wide, significantly restricts access for bad actors. Individuals and OCG's use email (and images attached to email) as a host for their phishing and ransomware attacks on organisation infrastructure. Similarly, for those employees who work remotely, it would be prudent to provide them with secured company laptops. The work around (although not as effective) for this latter element of security, would be to provide education for employees on cybersecurity at home. However, organisations cannot guarantee employee home networks or hardware and software have not been compromised. Logging into company servers on a device that may be compromised with spyware, ransomware, and keyloggers leaves the employee's corporate login information wide open to attack.

Cyber Organised Crime Groups have become sophisticated enterprises. They have adapted their skillset to take advantage of the human psychology of vulnerability. Examples of this include phishing and 'reply-to' emails sent to inboxes. phishing is designed specifically for the intended target.

A medical institution for example, may receive phishing emails disguised as a regular supplier of devices for that organisation. 'Reply-to' emails consist of an email sent to an organisation requesting 'clarification' of an order the organisation had purportedly made.

The sender constructs a convincing email with a call to action *"click here to confirm your order"* which in turn activates malware. These emails are targeted at busy reception desks such as hotels, general practices, hospitals, construction companies, and help desks.

There is no such thing as a "general cybercriminal". Therefore, security and policy must be designed specifically to meet the needs of the individual organisation.