Ensuring Business Continuity Management Capabilities

Strengthening cybersecurity risk management during the COVID-19 outbreak

Businesses and citizens across Asia Pacific are responding to help contain the spread of the novel coronavirus (COVID-19) outbreak. A large number of people are purchasing their daily necessities and staying in touch through mobile devices and applications. Meanwhile, many have donated money and supplies via the internet to support affected areas.

As a large number of businesses employ remote working policies during the outbreak, ensuring data security and privacy has become an increasingly relevant topic of discussion for enterprises. In this article, we discuss various types of “phishing” scams and other cybersecurity risk that firms face during times of crisis and provide recommendations to help mitigate potential threats.

What is “phishing”? Phishing is the fraudulent attempt to obtain users’ personal information or steal money by sending attachments or links which contain malicious software (known as “malware”) to users through email, SMS or other channels, and enticing users to open the attachments and links.

Phishing scams exploit system vulnerabilities and users’ lack of knowledge or awareness about data security. Since the start of the outbreak, various types of sophisticated phishing attacks have surfaced.

Phishing was listed as a top concern for cybersecurity professionals in KPMG’s latest Consumer Loss Barometer survey, ahead of other threats such as ransomware attacks or misuse of information by business partners, suppliers, or internal employees*. During an outbreak, such attacks may cause greater economic losses as users become increasingly reliant on digital platforms.

Since the COVID-19 outbreak started, KPMG has seen a consistent rise in the amount of associated phishing attacks globally. Various formats and methods seen in phishing attacks associated with the outbreak include the following:

**Recommended from KPMG’s Cybersecurity team**

To ensure that employees are aware of the risks of phishing attacks associated with the outbreak, here are some recommended tips to communicate to your teams:

### Don’t rush to check information about the outbreak

Remain vigilant about suspicious files or messages received via email or through other channels which claim to have details on COVID-19 treatment or related precautionary measures. Don’t readily download or open executable files (such as *.exe, *.csr and *.vbs files) whose names contain hot words such as “information on Wuhan pneumonia” or “novel coronavirus”. Email programs should also be set to disable macros.

### Be wary of SMS messages

When receiving SMS notices or emails related to returning or changing tickets, users should exercise caution when opening links contained in those messages. Do not enter bank account information, passwords, account passwords and other confidential information if a link appears to be suspicious. Instead, confirm through official channels whether the information is genuine and ensure that all transactions are completed via official apps or websites.

If sensitive information has been inputted in the phishing link, it is recommended that you should change your personal password immediately through the official website and, if necessary, contact related customer service personnel to temporarily lock your user account.
Buy hygiene products through trusted e-commerce channels

Individuals and businesses should only purchase outbreak prevention products (such as masks, hand sanitizer, alcohol wipes, etc.) from proper online shopping channels, and should not trust unknown sales websites. Here are some handy tips we recommend:

- Only buy supplies through trusted e-commerce channels
- Check whether the email address of the e-commerce website belongs to a trusted e-commerce vendor, and be alert to fake email addresses that look very similar to official email accounts
- Check whether you can access other parts of the website, in addition to the landing page from the phishing link
- Exercise good judgment when making payments. When making a payment an online platform, if users notice the payee is an individual’s name as opposed to a company name, they should exercise caution before proceeding

As this situation continues to develop, KPMG will continue our research on strategies that individuals and enterprises affected by COVID-19 can adopt with regard to cybersecurity risks and provide professional comments and suggestions.

KPMG’s team of professionals comprises emergency response specialists and cybersecurity professionals with substantial expertise and extensive practical experience. In the event of a cybersecurity incident, in addition to helping clients to restore normal operations, we can isolate and eliminate attacks and assist legal teams to prepare filings to relevant regulators.

During this difficult time, we strive to keep close communication with our clients to jointly tackle challenges. If you would like more information or would like to discuss these points in further detail, please contact us.

For more information:

KPMG has compiled a series of Business Continuity Insights to provide guidance to businesses across all sectors during difficult times. Further guidance can be found by visiting https://home.kpmg/cn/en/home/topics/business-continuity-insights.html.