Cyber criminals are taking advantage of the COVID-19 crisis

With all eyes on the coronavirus, another type of virus is spreading – a virus that cyber criminals are using against companies that are particularly vulnerable due to the COVID-19 crisis and the large number of employees who are currently working from home.

By Tine Olsen, cyber insurance expert, Willis Towers Watson

The widespread fear of the coronavirus (COVID-19) and the extraordinary need for employees to work from home – as well as other business-specific initiatives – have created a new opportunity for hackers who are adept at identifying IT infrastructure and virus defense vulnerabilities to infect IT systems with ransomware and malware and to launch other cyber threats.

Malicious infections in the name of Wuhan coronavirus have already been reported to be in circulation in the U.S. and U.K. with similar threats on the horizon. The IT security firm Kaspersky has found malicious pdf, mp4 and docx files disguised as documents relating to the coronavirus. Although the file names suggest that they include virus protection instructions, current threat developments and virus detection techniques, they actually contain a number of malware samples, such as Trojans and worms that could damage or encrypt data.

»Do not expect the hackers to show community spirit. On the contrary, the COVID-19 crisis represents a particularly favorable opportunity for cyber criminals to attack Danish IT networks,« says Thomas Lund-Sørensen, head of the Center for Cyber Security under the Danish Ministry of Defense.

The Danish Ministry of Defense has sent a general warning to Danish companies with advice – in Danish – on how to maintain high security standards when working from home. Read the advice

Willis Towers Watson would like to emphasize the importance of focusing on the cyber threat during the corona crisis and would recommend companies to follow two particular tips:

- Communicate clearly with all employees. Make sure that all employees know which communication channels are used for official management/company announcements.
- Be aware that criminals are trying to exploit the current situation. IT criminals will e.g. try to spread ransomware and send phishing e-mails and text messages, so encourage your employees to be extra careful about opening e-mails and clicking on links.

Would cyber insurance apply?

There will undoubtedly be cyber incidents during and following the COVID-19 crisis, and with the expanding breadth of coverage available under traditional cyber insurance policies coverage should be available. Therefore, as a general rule, a COVID-19 ransomware attack should be covered in the same way as other ransomware attacks. The coverage, however, will always be individually assessed.

Willis Towers Watson is monitoring the situation as it develops, and our experts are available for further discussions on specific cyber insurance.