KCS Group Europe

The Global Threat facing the corporate world in 2018 – Cyberspace, the new battlefield

02/01/2018

Throughout 2017, it became clear that the risks and threats to organisations and businesses and, in some cases individual company executives, is rising at a significant pace all of which is of increasing concern to those we work with and their clients. With the abilities and tools of the bad actors and criminals becoming more and more sophisticated, we must plan for the worse in 2018.

The answer is clear we can expect to see an increase in the growth and intensity of cyber-attacks and these will no longer be carried out in isolation. In discussions with clients pre-Christmas concerning the levels of sophistication of bad actors throughout 2017 it became clear that the risks and threats are worsening and that we can expect an increase in the growth and intensity of cyber-attacks but that these attacks will no longer be carried out in isolation.

KCS Group Europe has identified many shared concerns with its clients regarding the intensifying and evolving cyber threats and there is a clear recognition that the time of thinking ‘I have nothing of interest’ has passed. Going forward, the attacks we anticipate may very well be carried out by script kiddies, but the information employed by the cyber attackers is most likely to be obtained by other means, mainly by criminal elements employing Cold War tactics.

In 2017, contract cleaners, security staff, interns, pretext phone calls, fake interviews, telephone engineers, executive car hire drivers, social media engineering and journalists have all been employed to provide the relevant background information. Without doubt this will increase.

This year also saw a significant increase in the number of industrial espionage, major frauds, long cons and unfair market competition cases. The methodology employed invariably included the monitoring of social media platforms to secure more rounded inside information.

Employees often pass information to their co-workers via social media platforms little realising the value of an innocuous comment. Regular monitoring is now going on externally. It is being read and analysed by fraudsters, conmen and scammers prior to being utilised by the cyber hacker.

Social media is not per se creating new threats but amplifying the risks connected to the existing ones. These platforms are exploited by cyber criminals to better target and adjust the strategy and improve the efficiency of the attack.

KCS Group Europe

The Global Threat facing the corporate world in 2018 – Cyberspace, the new battlefield

Social platforms are also being employed for propaganda purposes to badmouth competitors and to tarnish the reputation of key individuals that the bad actors need to reach and/or undermine. Social engineering will be a major issue in 2018 more than it has been during recent years.

Phishing has proved to be the simplest and most profitable technique as it exploits the vulnerability of the human component. Employees should be better educated in order to increase their level of awareness.

Without doubt 2018 will see the level of sophisticated cyber-attacks and fraud increase on a major scale, we will also see competitors being undermined and individual reputations being attacked. Ransomware will remain the most preferred type of attack, employed as a cyber espionage technique as well as a target to disrupt operations.

These attacks will come from State actors, recently we have seen state intervention from North Korea, China, Iran Russia, USA, UK, but in many cases, it will be subcontracted out. As we have seen with the recently disclosed information regarding the perpetrator of WannaCry, States tend to be involved more and more often, initiating what could be defined as a cyber war, where the cyberspace will become the new battle field.

What is also disconcerting is the number of major multinational companies, using cut-outs to employ bad actors and others to carry out propaganda attacks to improve their own position in the market. Indeed, with corruption and bribery being a major concern and under the spotlight there are companies in certain sectors that are joining together to form cartels with a view to reducing a competitor's effectiveness when pitching for major tenders. Utilising social engineering to bring into question the competitors reputation and to tarnish the competitors' products, effectiveness and value will happen on a far greater scale in the coming year.

There was never a greater time to forewarn, allowing you time to forearm.