KCS Group Europe

On Trend: The Shape of Cyber-Security in 2017

11/08/2017

As we slide into August it is worth considering the current 'lay of the land' with regards to cyber-security and assessing what we might see in the second half of 2017. The year so far has been dominated by the twin ransomware hits of WannaCry and NotPetya, but these are far from the only emerging trends and evolving threats to contend with.

Data destruction just as big a threat as monetization of threat

Ransomware, if there was ever any doubt, is here to stay. While WannaCry and NotPetya continue to see the ramifications of their attacks across the world, a new report by cyber-security experts Kaspersky indicates that *'ransomware'* is the in-form vector of attack and warns that the true aim of the attacks is disruption, rather than blackmail.

"The real aim of the WannaCry attack", Kaspersky opines, *"was data destruction… disguised as ransomware".* This adds an unfortunate layer of complexity to a case: this is not ransomware in the strictest sense of the word, as there is little expectation from the criminals that they will receive payment: rather it is designed to cause large-scale damage as the means and the end of the operation. This might be purely for the thrill of it, or to test new variants of ransomware – or, occasionally be targeted by a foreign government as part of a campaign to damage interests in a rival country.

Certainly, this is not to disparage the damage that genuine ransomware can do – there are still few occasions in business more chilling than logging on to find all your data is locked behind a paywall – but for a program of data destruction to exist with the sole intention of just wiping everything puts the threat at a whole other level.

Criminals playing the pressure card

One of the reasons why ransomware is becoming so prevalent is that criminals understand that it poses a unique pressure challenge to the affected. Simply stealing money, or hijacking data, is of course serious but is a finite act which may then be resolved with the benefit of time. True ransomware relies on tying up not only the business of the affected company, but every other level of the supply chain in which it belongs – which can give one simple ransomware attack a significant reach. The schedule of one throws out the schedule of all, which can lead very quickly to damaged relationships. The pressure of

being responsible for the collapse of a complete supply chain, as well as the paralysis of your own business, the criminals adjudge, is enough to force companies to pay up.

Whether this is a reasonable assumption is up for debate, as governmental and expert authorities maintain a “do not pay” stance and for the most part it seems that entities abide by this. But on an individual, there is evidence to suggest that targeting chained companies in the manufacturing, energy and infrastructure sectors will ultimately bring the benefits.

Over-reliance on perimeter defence

It is believed that the two devastating ransomware attacks were propagated by a malicious email link and a USB stick respectively. Both were then in effect ‘enabled’ by the users (victims) rather than being the result of a brute-force hack. Still not enough is being done to educate and defend employees against the ‘internal threat’, compared to a brute-force hack or similar. Disruptive code, ransomware and malware is far better injected into a system if the victim willingly complies.

This brings us to one of the biggest continuing issues in cyber-security, that companies are still not doing enough to warn and educate users of the full nature of the threat that they themselves can unwittingly enable. To make matters worse, ‘cyber-insurance’ is still very much behind the times, almost exclusively focused on the damage done from a brute-force hack rather than through phishing, manipulation, and so on. To not move forward in this area is to invite disaster.

Secrets for sale from the Dark Web

The Dark Web continues to be a highly lucrative marketplace for the buying and selling of information, passwords, and malwares of all types but this year has seen an upswing in both the number of serious data breaches and their scale – most notably the exposure of the CIA’s ‘Vault 7’ knowledge base and the EternalBlue exploit. This is not a case of security around such bodies getting worse, it is a case of the hackers getting better. There has never been a more pressing need for companies to be aware of what data is ‘out there’, whether it is authorized or not, and who is looking at them for malign purposes.

With fake news and manipulation, the gloves are off

Evidence and allegations have emerged this year of campaigns of disinformation, deliberate deception and outright manipulation during the presidential elections of France, the United States, Kenya and South Korea, Sometimes, this has been through the propagation of ‘fake news’ by security services (South Korea’s NIS ensuring a 2012 conservative victory) but sometimes it has been a lot more direct (the Clinton and Macron email leaks). That what should in theory be among the most sacrosanct and

well-protected events in the world are reduced to sideshows while the world debates 'the leaks' is the continuation of a very worrying precedent: that there is no event which is now not subject to manipulation and attempts to create a favourable narrative. After all, if this happens at the very highest levels, then it is certain to be replicated at the corporate level.

What can be done?

Greater regulation is a must – in part this will be met by the introduction of GDPR in 2018 but needs to be equally met by the enshrining of proper cyber-insurance and an expansion in what constitutes a 'cyber-attack'. Companies too must be more vigilant in preparing their staff for incidents that seem out of place or suspicious.

Proactivity is the watchword here. With cyber-criminals constantly evolving their tactics, and becoming bolder, to stand still is to make yourself an easy target, and to focus exclusively on one or two areas of defence leaves you highly vulnerable. This is not an encouraging combination. The interconnectivity of the business world and the Internet of Things, two aspects of the connected world that are only going to get stronger, are proof enough that the cyber conversation must not only continue but seek to shout, rather than whimper. Keeping up with the developments, and considering the best responses to these, is but the first step.