CIONET

DISCUSSION SUMMARY

USING INTELLIGENCE TO COMBAT CYBER ATTACKS

This article was written by Roger Camrass, director of CIONET UK and a visiting professor of the University of Surrey. It is based on the conversations during a dinner in London which was sponsored by FireEye.

According to Lt General Kevin McLaughlin, former Deputy Commander of U.S. Cyber Command who attended this round table, the last decade has seen a rapid increase in hostile attacks from states such as China, Iran, North Korea and Russia. In his own words "we are engaged in global warfare that involves persistent and corrosive attacks that will last for decades". The use of malicious software such as WannaCry has caused western governments to heighten defenses and support private sector organisations in the constant fight against such criminal activity.

But the current situation may only get worse with the widespread adoption of new technologies such as sensors and IoT, public cloud, 5G, autonomous vehicles and connected buildings. Rogue operators are constantly testing our defenses as the 'attack surface' expands into civilian as well as corporate life. Russia has now established itself as the super power of crime. Iran is piling all its resources into a concentrated attack on Israel and Saudi Arabia. These states employ cyber-criminal teams to conduct much of their work and such governments are prepared to invest billions of dollars to achieve their disruptive goals.

To discuss these developments the round table focused on the UK public sector. However much of the dialogue and its conclusions are as relevant to the private sector. Here is a summary of the discussion that took place.

Intelligence by design

Many of the delegates attending the round table are engaged in infrastructure and workplace modernisation, enabled by recent advances in technologies such as sensors/IoT in the case of Smart Metering (as deployed by the Department of Energy) and public cloud in the case of digital workspace (relating to major projects in the Department of International Development).

The consensus amongst these executives is that security and related cyber defenses must be an integral part of the design process. This has been the case in the UK smart metering programme where some 16 million homes have been equipped with intelligent devices. Security has been designed into the end-points (the sensors) rather than the public networks that connect them to energy companies. This makes penetration more difficult, but not impossible given that Chinese companies supply the sensors.

Much concern was voiced about similar developments taking place in the deployment of Building Information Management (BIM) systems which now assist in the design, build and operation of all government buildings. Such information could provide criminals with detailed plans and occupancy patterns of such facilities, enabling them to shut down vital assets. The prospect of connected homes, cars and cities offers further opportunity for criminal activity. In the words of one delegate "imagine sitting in an autonomous car that has just received a signal to accelerate to 100 mph".

Use of intelligence to combat cyber crime

Much of cyber defence has been reactive to date – responding to attacks such as the NHS, Target and Sony incidents. ISIL was a trigger to adopt a more proactive approach, especially within the USA where the NSA and Cyber Command have acquired 6,000 specialist staff to enhance their Cyber defence capability. This represents a new era of 'persistent engagement'.

This proactive approach has been adopted by FireEye who maintains hundreds of agents out in the field to generate intelligence on hostile states such as Russia, North Korea and Iran. By focusing on the largest adversaries FireEye informs its global clients about areas of future vulnerability and helps them to devise effective defence strategies.

Each year FireEye publishes its M-Trends Report that informs the global security community about changes in cyber-attacks. Conclusions from the 2019 M-Trends Report include:

- The median dwell time, or time it takes an organisation to detect a breach, is falling dramatically from 416 days in 2011 to 78 days in 2019
- Discovery of compromises is getting better internally, as opposed to being informed by external sources such as law enforcement (from just 4% of total breaches in 2011 to 59% internal detection this year)
- Retargeted attacks (two or more attacks on the same organisation from the same attack group) within a year continue to increase from 56% in 2018 to 64% in 2019

Governance is key to cyber-defence

Despite the obvious dangers of cyber-crime, senior executives have yet to fully appreciate the risks that they are taking on a day-to-day basis. Many of the delegates confirmed that Board engagement is improving but it is not yet at a level where appropriate resources are being committed to offset cyber risk. A further concern is the lack of awareness of Cyber risk amongst the broader body of government staff. Technology-based defence is only part of the answer. A much greater appreciation of how to avoid malware and other criminal weapons is needed to ensure that departments are constantly vigilant to attack – often conducted on an individual basis via phishing.

One aspect that emerged in discussion is the vulnerability of eco-systems and the need to introduce effective cyber-governance between partners. Public bodies such as the NHS are dependent on a multiplicity of third parties. Such relationships need to involve common security goals and objectives – as is the case between Virgin Care and the hospitals that it manages. Contracts between such partners are usually reviewed on an annual basis in contrast to the daily developments in the field of cyber-attacks.

What are the top themes for 2019?

The evening concluded with a summary of top themes for 2019 which include:

- Advances in cyber weaponry such as use of AI and predictive analytics
- Physical security of buildings, national infrastructures, energy resources
- Extended reach of criminal activity, from institutions to individuals
- Collaborative efforts between trading partners to eliminate end-to-end risk

CIONET

About CIONET

CIONET is the leading community of more than 10,000 digital leaders in 20+ countries across Europe, Asia, and the Americas. Through this global presence CIONET orchestrates peer-to-peer interactions focused on the most important business and technology issues of the day. CIONET members join over a thousand international and regional live and virtual events annually, ranging from roundtables, programs for peer-to-peer exchange of expertise, community networking events, to large international gatherings. Its members testify that CIONET is an impartial and value adding platform that helps them use the wisdom of the (IT) crowd, to acquire expertise, advance their professional development, analyse and solve IT issues, and accelerate beneficial outcomes within their organisation.

cionet.com