CIONET

DISCUSSION SUMMARY

FIGHTING CYBERCRIME: WHO IS THE ADVERSARY?

This article was written by Roger Camrass, director of CIONET UK and a visiting professor of the University of Surrey, and is based on the conversations during a dinner in October, 2019, on Fighting Cybercrime – who is the adversary, sponsored by Phoenix Datacom and FireEye.

Cyber adversaries have different motivation

Corporations are increasingly aware of two types of actor in the war against cybercrime. The first is the state actor such as China, Iran, North Korea and Russia who have been targeting western governments and private companies. The second is the cybercriminal who can operate anywhere in the World.

State actors are sponsored by their governments to pursue political strategies. For example, North Korea is financially motivated, using cybercrime to generate its primary source of foreign income. China has stolen trillions of dollars of intellectual property to help kick-start its own industrial revolution. Russia is keen to disrupt political processes amongst its neighbours such as the Ukraine. Iran pursues aggressive acts of military aggression against its enemies such as Saudi Arabia and Israel.

According to FireEye, companies should be aware of both types of actor, but pay greater attention to cybercriminals who operate with high degrees of agility and speed compared to state actors who tend to be more regulated.

How does cybercrime evolve?

Cybercriminals are motivated to 'go where the money is'. In the early days they focused on credit cards and retail transactions that were a relatively soft target. Activity soon progressed into the mainstream of financial services such as bank account fraud, ATM theft and supply chain disruption. More recently, criminals have engaged in ransomware as exemplified by the attack on large corporates such as Maersk and government organisations such as the NHS. Such attacks have now filtered down to small companies and individuals on a global scale.

The 'attack lifecycle' is also evolving. Cybercriminals conduct reconnaissance on their targets, looking to achieve initial compromises that often go undetected (the average dwell time to detection is still over 70 days in Europe). Email is an effective form of first attack, targeting low level staff who are likely to click on unauthorised links. Once established within a corporate network, the cybercriminal can progress rapidly to more aggressive tactics such as the breach of critical commercial data, as seen in the recent BA malicious attack on its website where 380,000 customer records were removed.

Assessing cyber risks

Context is important in assessing cyber risk. For example, the Russian attack on Maersk was motivated by a family connection in the Ukraine. Iran has directed much of its energy towards Aramco as a principle Saudi state asset. Organisations need to evaluate where attacks would make most sense to both state actors (focusing on disruption) and cybercriminals (focusing on financial gain).

The need to invest ahead of cyber attacks is often difficult to justify to main boards. Even today few companies recognise cyber on their corporate risk registers, and cyber insurance is often understated compared to potential commercial damage to brand as well as operations. The BA data breach incurred a penalty of £180M. The ransomware attack on Reckitt Benckiser's manufacturing operations cost the company over £100M in lost production.

One approach to quantifying risk is to develop 'worst case' scenarios each of which represent specific losses to the business. In the private sector these can be connected to loss of trust in the brand, disruption of operations and theft of intellectual property. Within the public sector, risk may relate to social and economic breakdown, as well as potential life and death situations as illustrated by the NHS WannaCry attack this year.

Mitigating cyber attacks

Although technology can be a critical defence tool, psychology and emotions are of equal importance. Humans are often the weakest link in any defence strategy and require intensive training and encouragement to avoid criminal penetration, especially in cases of 'phishing' via emails. Many of the organisations around the table conduct regular tests to identify which members of staff might open an unauthorised email. The view was to equip staff as an army of cyber warriors. In addition, most employ external agencies to conduct penetration tests on a periodic basis. Ethical hacking enables management to assess possible areas of vulnerability and take appropriate actions.

There was an animated debate about the value of penetration testing versus red teaming, where the latter can be focused on contextual risks relating to a specific attack landscape. There was agreement that automated testing alone was not enough to avoid cyber-attacks. Human intervention and training have proven to be the most effective means of managing cyber risk.

What to consider as next steps

The inventiveness of cybercriminals combined with the aggressive motivations of state actors implies that increasing attention is required to minimise potential risks.

Here are some actions that CIOs and CISOs may consider to be relevant to their organisations:

- Gain a better understanding of the context under which attacks could take place – assess the motivation of potential cyber actors, both state and private
- Develop scenarios that illustrate the potential damage caused by such attacks and assess the financial impact – set against cyber insurance policies
- Conduct regular penetration testing and red teaming to identify and resolve areas of cyber vulnerability
- Engage the Board in cyber matters well ahead of any potential attack – learning from the experiences of previous incidents such as BA, NHS and Maersk

The price of getting this wrong is evident in the recent fines and profit losses imposed on organisations across Europe and the USA. Top management should become better informed about such penalties and risks.

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