Preparing for Cyber Warfare – Why you need a simulation tool and what to look for

The cyber landscape continues to be a challenging place for public and private organisations alike. Both are often on the back foot when it comes to fending off intelligent, determined and motivated attackers focussed on inflicting cyber warfare and cybercrime attacks on their targets. Such has been the concern of the impact on a global footing, the World Economic Forum's Global Risk Landscape report has previously rated cyber-attacks to be one of the highest risks in terms of impact and likelihood, only closely behind natural disasters and extreme weather events.

In an equally telling way, NATO formally recognises cyberspace as a domain of operations in which it must defend as effectively as it does in the air, on land, in space and at sea. Cyber-attacks and warfare are a real threat and the attackers are numerous, ranging from inexperienced hacktivists and script kiddies through to highly capable cybercriminals and nation state groups.

State sponsored cyber warfare is often targeted at nations and their essential services. Deeply disruptive activities are used to conduct a range of nefarious activities such as; constrain reform, affect democracy, weaken government networks and reduce the capability of critical national infrastructure such as energy, defence, finance, transportation and communication. State backed cyber-attacks are at times also directed at commercial organisations where they are used to disrupt trade and ultimately impact the economies of their enemies and targets.

In some instances, commercial organisations are caught in the cross hairs of nation state cyber aggression. An example that springs to mind is an attack that temporarily crippled the network of one of the world's largest law firms, DLA Piper, whose global network was heavily impacted when it became the collateral damage of a hostile nation conducting cyber-attacks thought to be designed to destabilise the economy of the Ukraine.

There is little doubt that cyber warfare is raging, and it's not just nation on nation. For every attack that is targeted at a nation, there are many more that are deliberately aimed at commercial organisations and for motivations such as investigative journalism, competitive advantage, revenge and financial gain. Some estimates place the annual value of cybercrime to be $1.5tn a year, making it broadly equivalent to the GDP of Russia.

The Challenge – It is difficult to anticipate and eliminate weaknesses

Regardless of whether a cyber incident is the outcome of an individual and surgical precision attack, or the collateral damage of a bulk attack, state owned and private organisations will benefit from the ability to limit the likelihood of an attack, anticipate its impact and then eliminate weaknesses in the cyber infrastructure and team. However, simulating realistic attacks is a real challenge for many organisations, and the bigger the target, the more difficult it is to predict, mimic and replay adversarial attacks.

Today, penetration testing is widely mandated by regulation, industry bodies and supplier contracts. It is undertaken as best practice by responsible organisations who seek to routinely (usually annually or upon significant change) identify exploitable vulnerabilities in their systems. However, penetration testing falls short of helping to recognise attacks as they occur or discover insidious low-level attacks that quietly conduct a range of nefarious activities from hidden locations within a network. This is the job of tools such as Telesoft's Flowprobe 400 and Data Analytics Capability (TDAC) platform, which blends near real-time network monitoring at scale with analytics and threat intelligence.

The creation of incident playbooks, the training of incident teams and rehearsal of response activities are great strategies for minimising the impact of an attack, however these are often untested until the heat of an incident. When they are rehearsed in advance, they are often played out in boardrooms as theoretical exercises and base their starting positions on an estimate of how the technology has been impacted by an attack rather than a known state one.

The Solution – Realistic attack simulation tools

To truly understand an organisation's ability to withstand a cyber-attack, systems proving should include a known state derived from the use of a simulated but realistic attack. This is the role of cyber warfare attack simulation tools that can be easily deployed, used by penetration testers, digital forensic professionals and situational awareness experts across Red, Blue and Purple teams to plan, prepare, execute, identify and prove their organisation's ability to detect malicious activity at each stage of an attack's escalation. This approach can be likened to that used by NATO who bring together experts from multiple nations as a method of preventing, detecting and responding to an adversary. The difference of course, is the ability to create realistic threats with a flexible and powerful tool without the need and expense of large-scale collaborations. It also brings the ability to test, test and test again and, borrowing the words of Dr Bernhards Blumbergs, a former Technical Director of NATO's cyber operations exercise Crossed Swords - Fail, fail again, fail better.

But what are realistic attacks?

They are those that;

- Emulate the behaviours of real-life attackers
- Coordinate multiple concurrent attacks to create confusion
- Include a variety of attacks from password spraying and large-scale DDoS to AI poisoning
- Use the latest threat intelligence and honeypot data to ensure known and emerging threats are included
- Can be delivered at speeds that reflect the capability and resources of an attacker

How well prepared is your organisation and do you have the right people, process and technologies available to reduce the likelihood and impact of an incident.

Want to understand more about this subject ? Get in touch at info@cortida

+44 (0) 207 164 669
info@cortida.com
www.cortida.com
150 Minories, London, EC3N 1LS