Red Teaming

“If you know the enemy and you know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle” (the Art of War, S. Tzu).

If you’re reading this blog it’s safe to assume that you recognise the threat posed to organisations of every kind by cyber-crime. Bearing aware of the danger and being equipped to protect your organisation from that danger are two different things, however. This is evinced by the latest edition (2019) of the UK government’s Cyber Security Breaches Survey, which reveals that just 31% of organisations in the UK have carried out a cyber-risk assessment in the past 12 months, and only 57% of even larger companies have cyber-security incident responses in place. It’s not difficult to find further examples of the general unpreparedness of organisations to deal with cybercrime in general and with the ever-changing nature of that threat in particular.

The issue of insider threats, for example, is one which most organisations are still struggling to come to terms with, with 82% stating that they can’t guarantee they can detect insider threats from personal devices and 50% saying the same for insider threats from the cloud, with 81% struggling to assess the impact of insider threats in general. Organisations like Microsoft and the UK government closely monitor not only the scale and impact of the cyber-crime risk but also the tactics which the perpetrators are most likely to utilise. According to the Microsoft Digital Defense Report, for example, there has been a shift in recent times toward credential harvesting and ransomware, as well as an increasing focus on the Internet of Things (IoT), with the latter seeing a 35% rise in the total attack volume during the first half of 2020. Another shift noted in the report is one away from malware attacks and toward phishing attacks, which have risen by 70% as a method, with the emails used often imitating brands like Amazon, Apple and Zoom. A similar shift was picked up in the UK government report, with phishing attacks rising from 72% to 86%, while viruses and malware dropped from 33% to 16% and ransomware from 17% to 8%.

What the figures above demonstrate is that the cyber-crime threat facing organisations is constantly shifting and evolving. For that reason more than any other, the use of Red Team / Blue Team exercises to evaluate the effectiveness of the defences in place at an organisation is one of the few methods which genuinely reflects the nature of the real world threat being faced. A useful image to employ when evaluating the effectiveness of Red Teaming is that of a military exercise in which one team of soldiers attacks another in a genuine recreation of the tactics, weapons and methods which any presumed enemy would be expected to employ. In the case of cyber security the Red Team will be made up of cyber security professionals with the skill and know-how to employ the tools and techniques of real world cyber-criminals in order to undertake a multi-faceted simulation designed to test every aspect of an organisations cyber defences.

During Red Teaming itself (also sometimes known as Adversary Simulation) the cyber security professionals will attempt to breach the cyber defences of an organisation via the widest possible range of attack surfaces. In doing so they will endeavour to identify and flag up gaps in prevention, detection and response, making use of exactly the kind of tools which real world attackers will utilise. As explained above, the nature of these tools is constantly

changing and an effective Red Team will be one which is aware of these shifts and is able to test defences against the techniques which attackers will be using tomorrow, not those which posed a threat yesterday. These techniques might include phishing emails, social engineering and attempts to gain access to server rooms. Amongst the aspects of an organisations IT infrastructure being tested via attack by the Red Team are likely to be:

- Hardware and software systems such as routers, switches, appliances, IoT devices, networks and applications
- People, often the weakest link in any organisations cyber defences, including members of staff, independent contractors and business partners

By monitoring this process closely the organisation will be able to gather first hand data on how to detect and defend an attack, where the areas of vulnerability lie and what form response and repair might take. Much of this work will be carried out by the Blue Team, which is made up of security professionals tasked with defending against any Red Team attack. The Blue Team, like the Red Team, needs to be aware of the tactics and techniques which real world attackers are likely to employ, and is there to develop and enhance the cyber-security infrastructure of the organisation using techniques such as security audits, DDoS testing, risk intelligence data analysis, reverse engineering and log and memory analysis. The chief advantage of Red Teaming over other tactics such as penetration testing is that it mimics as precisely as possible the actual reality of a cyber-attack and places the Blue Team in the position of having to deal with that attack. In this way it highlights the importance of detection and containment over and above the more static measure of prevention, and reflects the reality that no IT infrastructure can ever be declared fully secure and that what matters, therefore, is the ability to respond to breaches. To this end, a Red Team attack and Blue Team response will be able to pinpoint vital metrics such as the time between first point of compromise and the ability of an attacker to move across other systems in the network. The Purple Team, which is less a separate entity and more a combination of the other teams and the information they have gathered, describes the process via which the threats utilised and weaknesses identified by the Red Team are combined with the defence strategies and controls employed by the Blue Team in order to create an overarching picture which can inform cyber-security planning in the future.