Unsplash © Ricardo Arce

7 stages of the cyber attack lifecycle

Cyber attacks on business infrastructure are growing in complexity, frequency and creativity. Cyber security teams are tasked with the unenviable duty of adapting to an array of constantly-evolving threats, detecting intrusions, suspicious activity and anomalies before any damage can be done.

Any potential cyber attack, depending on its severity, comes with high repercussions if a threat is not contained swiftly and appropriately. Not only does the average breach cost a business upwards of *$4.35M (up 2.6% from 2021)*, but high-profile incidents have resulted in tremendous reputational damage, which in many cases is hard or impossible to recover from. For starters, there was the recent *Royal Mail ransomware attack* in January, and in May 2021, *the Colonial Pipeline* suffered a cyber attack which disrupted fuel deliveries for several days, and this is only scratching the surface.

As cyber attacks become almost daily occurrences, every company – regardless of size and industry – must focus on how they can secure their infrastructure from hackers. There is growing reason to believe that any business will, at some point, fall victim to a cyber attack. The FSB (Federation of Small Businesses) reported that small businesses suffered close to *10,000 cyber attacks every day* in 2019, costing an average individual £1,300. What's more, many businesses have come to realise that they have suffered a breach without even realising it. According to *IBM*, it takes a company 197 days to discover a breach, and up to 69 days to contain it.

Therefore, if attacks are not anticipated or addressed in a proactive manner, the financial and non-financial damage can be particularly wounding. Whether your company employs a range of skilled cyber professionals in-house or you outsource to specialist *threat detection and response* teams that provide constant monitoring of your estate, it's crucial to understand what a potential attack might look like.

Knowing what the stages of a typical cyber attack lifecycle are can help organisations contain threats and prevent hackers from accessing networks or systems. Below you will find a seven-stage breakdown of a 'typical' cyber attack lifecycle to help you identify what takes place.

1. Reconnaissance

The preliminary stage of any cyber attack sees the threat actor gathering intelligence and research on their target(s). This will involve reconnaissance and intelligence gathering on networks, a company's assets (e.g. its website and social media platforms like LinkedIn), its current data security posture, and any open-source information about the target such as its premises, IP address, software, DNS information, and employees.

Hackers will typically identify one vulnerable target and pursue a method to gain entry via an endpoint. *Phishing emails are common* ways to engage with unsuspecting employees, where malware can be distributed. Attackers could also identify clients and suppliers to engage in 'social engineering' tactics, such as making fake sales calls.

2. Weaponisation

The next stage involves weaponising the information obtained via reconnaissance and deciding on the appropriate delivery method.

Hackers will consider the networks, software and systems that the target may be running and decide on the most effective code to use to break any defensive barriers down. They will also collect the tools they need to exploit any vulnerabilities they may find when they gain access to the target system or network.

One of the most common ways to compromise a network is by attacking unpatched security software on connected devices. Machines with outdated security software can become easy targets, with attackers weaving their way in via known vulnerabilities that have not been patched via the latest updates.

3. Delivery

At this stage, the attacker will have chosen the target, having identified their

name and role within a business. The hacker's chosen weapon – be it a phishing email, ransomware, malware, fake landing pages or any other type of attack – will be used against this specified target.

In many cases, the user is unsuspecting of a potentially malicious and dangerous link, file, or email. The attacker will then wait for initial access to be granted.

4. Exploitation

The next phase sees the hacker delivering the most vital stage of their attack. A successful breach will see a target grant the attacker primary access to the organisation, via the hacker's chosen delivery method.

The attacker explores the infrastructure and gains a better idea of how it operates, how traffic flows on a network, the connected systems and user accounts, and tries to exploit any additional applications or connected software.

5. Installation

The installation phase is when the attacker ensures continued access to the network. The attacker will have established a secure connection to networks and systems via a persistent backdoor, disabling any firewalls and creating accounts with administrator access, as well as locking any other users out.

Any malicious software will begin to work on the compromised system or network, and once successfully installed, will establish a connection to the hacker's home device. The hacker may also trigger any remote desktop access on other servers and devices connected to a network, to ensure they remain undetected for as long as possible.

6. Command and control

Once unrestricted access has been granted, all the required tools are in place to trigger the command and control phase. Now the attacker can effectively control the network, applications and systems, obtain any user information, and even perform actions on behalf of unsuspecting users. They are at liberty to extract any personal or sensitive information stored on the network.

7. Actions on objectives

The final stage could involve stealing sensitive data, disrupting operations, demanding ransom payments, or further exploiting connected systems and *invading data systems*.

Not all hackers' goals are the same, nor are they *exclusively financially*

motivated, but this type of cybercrime is the most frequent. Some hackers purely target organisations for political or socio-economic reasons, with hackers aiming to cause chaos or send a specific message to a company and its customers.

How to break the cyber attack lifecycle

Despite the high level of risk and potentially devastating damage that a cyber attack can inflict on a company, there are *ways that you can prevent attackers* from carrying out any nefarious activity.

At first glance, it's vital to ensure that you – and your teams – are all clued up on the most recommended cyber resilience measures and security steps. At a basic level, these include:

- Strong, unique passwords for every system or application.
- Enablement of two-factor authentication (TFA), otherwise known as multi-factor authentication (MFA) across all devices.
- Regularly patching and updating the software of all core systems and apps.
- Securing any networks and providing restricted VPN access to remote workers.
- Investing in robust and cohesive antivirus software with built-in firewall and internet security protection.

While the above measures will provide your organisation and team with a sturdier first line of defence, the real strength comes from increased awareness, regular upskilling of staff, and a suitable strategy. Establishing and maintaining a cyber security risk management plan, with clearly defined policies, and commitments from current and future staff, all comprise pillars of sufficient resilience.

Article by DAKOTA MURPHEY