PARA FLARE

COMPREHENSIVE CYBER DEFENCE

Combines self defence, passive defence and active defence.

KNOWING THE DIFFERENCE WILL SAVE YOUR BUSINESS A LOT OF PAIN

Any comprehensive approach to cyber security must include the implementation of measures that address self defence, passive defence and active defence.

None of these three defensive measures is a "silver bullet", despite the claims of many vendors. Each must be addressed.

Self defence

Self defence, or in reality self protection, is everyone's responsibility and relates to culture and awareness. This is the defensive measure where we educate our workforce to not click on the link in the phishing email, or plug a random USB stick into our system. Self defence considers our vulnerability to socially engineered cyber attacks, where information freely available to the internet is used by a professional threat actor to attack us.

The ultimate aim of self defence is to encourage people to perform the individual actions that contribute to the protection of themselves, their families, their friends and their organisation in cyberspace.

Passive defence

Passive defence is the defensive measure that is the fundamental basis for cyber security. It relates to network hygiene, and is the responsibility of CIOs and system administrators. Passive defence includes firewalls and anti-virus. In the physical world, they're like your locked doors and alarm systems – the foundations of good security.

Passive defence is the measure where those responsible for the organisation's information technology (IT) and operating technology (OT) think about the defence of those systems. It considers compliance with the ASD 'Essential Eight', including patching of systems, whitelisting applications, encryption of data, and limiting the number of people with privileged or administrator rights.

Active defence

Active defence is a critical augmentation of passive defensive measures. It is a specialised function that involves highly skilled and specialised 'hunt teams' operating inside the organisation's IT and OT infrastructure, to actively detect, contain and resolve breaches of passive defensive measures.

Active defence is a level of cyber protection that many businesses and organisations may be unaware they need; believe they already have; or be reluctant to invest in. With reports of new malware being available to threat actors every 7-12 seconds, it is not sufficient to rely only on passive defensive measures for an organisation's cyber security. In this environment, it is not a question of if passive defence will fail – it is when.

That is why active defence, along with self defence and passive defence, is a critical element of any comprehensive approach to cyber security.

NEED MORE INFORMATION?

Email us at
info@paraflare.com

or call
1300 292 946