RESOLVE DEFENCE

Business Security

Cyber attacks are now very real in New Zealand. Being “that little country at the bottom of the world in the middle of the ocean” is no longer isolating us from these attacks.

Protecting your business investment

It is now becoming prudent to have a regular check-up of your IT system, like a car’s warrant of fitness.

Why does the attacker care about my network, I have nothing interesting in there?

Cybercriminals while attempting to exploit you by “tricking” one of your users to “open a door” for them, they also subscribe to all the IT systems bulletin boards that publish new vulnerability alerts. Using intelligent automated tools to all the work they scan for these systems and attempt to breach your systems utilising these published alerts.

It is critical that all area of your IT systems are kept patched, and are using current supported version of your applications and IT supporting services.

Attackers also look for networks to host their Malware or to use your network to then attack other networks, especially those of your clients that a trusted with the information sent between you. They may also take over parts of your network to create new attacks originating from your internet address, and being local NZ origin, is more trusted than the likes of China and Russia. With all computer systems there are so many options available to a configure your system that with intrinsic growth and changes over time, these configurations can end up quite different from the original planned system design. As systems are updated for new software releases or implementation of new IT services the configuration of your network must change to support the new technologies.

This business security assessment interrogates your business IT systems with a variety of “safe” scanning tools to identify what is operational on the network and if it is “up to date”. These checks are against all devices identified as connected to your network, plugged in or via WIFI.

The program ensures that the commonly targeted exploitation areas of your network are identified, scanned, and weaknesses / vulnerabilities are identified and reported. This report provides a list of actionable changes aimed to reduce your systems vulnerability, protecting your network, business and client’s data, and your investment. Cybercriminals have budgets too and making it just that bit harder for a cybercriminal to get foot in your network the more likely they will look elsewhere.

Contact a Resolve Account Manager to discuss starting this program in your business.