The Insider Threat

A lot of focus is put upon external threats but how can you effectively counter a potential cyber-criminal when they're already inside your organisation?

That's right, the focus of this post will be the much feared 'insider threat': when someone already inside your organisation steals, leaks, destroys or otherwise uses your data or systems in a way they shouldn't.

The threat could be a disgruntled employee or soon to be ex-employee, it could be a contractor working on your systems, or even your close business associates.

This doesn't mean that you should be regarding everyone with undue suspicion and giving side-ways glances to people across the canteen but there are steps you can take to defend against such a threat.

"So much more damaging…"

Mark James, ESET IT Security Specialist, explains that an insider threat can be even more damaging than an external breach.

"Threats of any kind are a very serious risk for any business, if you don't spend as much as you should do on protection or don't have the latest technologies then getting compromised from the outside is a very real threat.

"To be honest a lot has to happen for that to be successful, and even if it is successful there's no guarantee that it's going to amount to anything.

"But attacks that come from the inside can be so much more damaging: gaining control of the right login credentials can reap all the rewards you need in one single simple login process.

"If you think you're safe because you are protected with encryption and the compromised user has admin access then chances are they are already authenticated to view that data.

"They may even have full administrative privileges which would enable the attacker to have complete control of your whole network; there really is no worse scenario."

Education

As per usual education is key in combatting this and practically any cyber threat that exists today. Back that up with robust anti-malware software, top level encryption, a well configured firewall and you're in the best place you can be.

"In theory insider or outside attacks are potentially as bad as each other and should at the very least be treated the same in terms of protecting against.

"Education not just for the staff and users but in current attack processes is a must: spotting phishing emails may seem like a simple mundane task but emails still remain the number one method for spreading malware.

“Segregating networks with very careful consideration to privileged login accounts could be your saving grace and ensuring all endpoints and servers have regularly updating internet security software is essential.

“Keeping your systems patched and up-to-date is a must with Intrusion detection systems in operation at all times.

“Make sure you have a clear line of command for reporting anything suspicious, make sure that everything is reported no matter how small and make sure your system logs are monitored for any unusual activity or log deletion.

“One of the better forms of protection is two-factor authentication (2FA): if your privileged user accounts need 2FA to validate their logins then that may be the difference in a potential financial and or PR disaster.”