The Total Team
www.totalteam.co.nz

7 July 2017

THE NEW SECURITY PERIMETER

The Changing Landscape

By Ian Burgess

Everybody has an opinion on security. This is my opinion based on the trends, issues and responses within the industry.

Traditionally we considered security at our perimeter. A good firewall, or if we were a smaller company this could be the default router supplied by our ISP. Yes we believed in Antivirus and even tried to keep it up to date.

Our usage patterns are changing, we increasingly allow our staff to have access to our systems on the road or at home. Or our systems are within the cloud.

Our data is changing. There is more electronic sharing of information and more information is available via the internet. The speed at which things proliferate is now much quicker. The antivirus company 48 hour or days response to issues is no longer acceptable.

The security border is no longer our firewall. We need a strategy for security that protects the end devices from many possible attack vectors in a timely manner.

Through significant research by my team especially Darrin Cooke, many things became evident. Cisco suffered a security issue that made them realize the changed landscape. Steve Martino, Chief Information Security Officer for Cisco embarked on a journey to secure Cisco. http://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html?stickynav=4

That journey certainly has shaped our thinking of appropriate security.

We realize that the building blocks for security for New Zealand companies need to be affordable and not incurring significant capital expenditure, while being the best and most efficient in the industry.

I will discuss these building blocks below, but having the right building blocks in place without the right oversight is like deploying a state of the art alarm for your premises and not having it monitored or serviced.

Contact The Total Team for further information.
Ian Burgess iburgess@totalteam.co.nz
or the office 0800 88 8326

Endpoint Strategy

By Ian Burgess
There are two building blocks to endpoint security that create a complete solution.

The first is the ability to control access to sites at the DNS level. This means that as "bad" sites are identified, that the devices no longer connect to the known bad sites. Even if your device has a virus, this can prevent it from calling home and can prevent damage being done to your company. This solution works for your corporate or business environment as well as the remote worker.

The second building block is AMP (Advanced Malware Protection). This is much more than an antivirus. Yes, it will recognize known viruses and quarantine or delete without letting it action. But it is the unknown files that really make this product a must have. It will request a file be checked by the core system, and while it waits for a response it will track what the file does and where it goes within the system. If it gets the notification that the file is "bad" it will undo the steps retrieve the file and action the quarantining.

The glue that brings these building blocks together is a cloud based solution that relies on crowd-sources for malware from a closed community and analyzes all samples using proprietary, highly secure techniques that include static and dynamic (sandboxing) analysis. It correlates the results with hundreds of millions of other analyzed malware artifacts to provide a global view of malware attacks, campaigns, and their distribution.

Articles to Come Soon

Email Gateway Solution
It is important to not only protect your own company, but also your business partners or clients as well.
An email gateway strategy that uses the same technology as your endpoint strategy obviously creates a more complete solution.

Firewall Strategy
Even small businesses need to ensure that a Next Generation Firewall protects their perimeter. The knowledge of a firewall that you are going to a specific site is not enough. But what data is flowing and whether they are good or bad flows of data is now what a firewall needs to act upon.

The role of an NSOC

As the security landscape increases, it becomes beyond the ability of most IT staff to administer, control, monitor and report on the diverse security landscape.

Specialists are required to be the Network and Security Operations Center.
They need to be up to date with events.
They need to ensure the tools are used properly within the greater company network. The most affordable way to achieve this is to outsource to a team who has the tools, the ethos and the integrity to act on your behalf

Who is your NSOC?.

Contact The Total Team for further information.
Ian Burgess iburgess@totalteam.co.nz
or the office 0800 88 8326