Supplementary Submission to the Joint Committee of Public Accounts and Audit

Inquiry into Cyber Security Compliance

May 2017

Introduction

Macquarie Telecom Group (MTG) is pleased to provide this supplementary submission to the inquiry. It is written in the context of the impact of the global WannaCry cyber security event, which began on May 12 and 13, and the lessons that can be derived from those events for cyber security practice and compliance.

MTG submits there are very important messages for the Government from the WannaCry incident about the nature and limits of cyber security guidelines and compliance models as they are presently implemented.

It must first be acknowledged that the impact on the Australian community, compared to the profound, frightening and widespread effects in Europe, was limited and there were no reports of Government or its agencies being effected.

There is no doubt Australia benefited from the timing of the event (i.e it was first reported outside of the working week in Australia). This gave Australia business and government agencies time to respond before the majority of end users were online at workstations.

For its part, MTG, through its Macquarie Government and Macquarie Cloud Services business units, took a series of actions that are described below, as well as advising clients of actions they should take, during the weekend. Many others did the same.

It is also possible that Australian business and agencies were in a less vulnerable position to those in other countries because they have a better cyber security stance.

However, both the Minister Assisting the Prime Minister on Cyber Security, Dan Tehan, and the Special Adviser to the Prime Minister, Alastair MacGibbon, have publicly indicated their belief that the timing of the attack was the main reason for the lesser impact in this country.

While there could be reasons that Australia is less vulnerable, MTG agrees that the timing of the attacks had a very important bearing on the outcome in Australia.

With that in mind, MTG submits that the important issues to be examined in order to gain lessons for the future are;

- Would/were compliance with the Top 4/Essential 8 effective means of protecting users from WannaCry?
- What other policies were relevant and how effective were they?
- If these policies should have been effective, what factors could cause non-compliance, and how can they be addressed to protect users more effectively from a future incident?

Background: The Nature of the Incident

The WannaCry incident was unprecedented in impact, scale and reach, but not technologically.

In simple terms, it brought together three known and common types of malware (or malicious software).

- It entered the computers and networked computing environments of organisations via fake emails to end users that carried infected code. This is commonly known as phishing.
- Once inside networks and computers the malicious code spread around networks of computers by targeting and a known vulnerability in certain Microsoft software that allows computers to work together. It used this vulnerability to trick the software to send the malicious code to other computers. Malware that targets a vulnerability is known as an “exploit” and malware that spreads through a network is known as a “worm”.
- Finally, having accessed numerous computer and work stations, it activated another malicious program that locked users out of their data and files by encrypting the data. It demanded they pay a ransom to have the files unlocked. This is called Ransonware.

Phishing, exploits, worms and ransomware have each existed as common, indeed, daily threats for many years. While they have changed and evolved, so too technologies and protocols to combat them are common and evolving.

The combination of these elements is also not unique, although the scale of the attack and the widespread nature of the Microsoft vulnerability allowing a worm to spread ransomware so quickly did set this attack apart from others.

The specific vulnerability in the Microsoft software was unique, but such weaknesses are being found and fixed continuously.

As has been widely reported, Microsoft released a patch for this particular vulnerability in most versions of its software in March.

It had not released patches for some other software versions because it judged those versions too old to be supported. It did so quickly after the attack began.

The "exploit" that took advantage of the vulnerability was released among the criminal and hacker communities on the Internet in April.

Anti-virus software often identifies malware by identifying unique parts of its code, called a signature. Anti-virus software can be updated to look for these signatures and block traffic – such as emails – in which it is found.

The signature for the exploit was identified and released soon after the exploit was released, allowing anti-virus software vendors to add this signature to their list of known threats some weeks ago.

That means modern and up to date anti-virus software employed on computers and Internet firewalls should have been able to see and stop a WannaCry attack.

The Top Four, Essential Eight and Compliance Framework in Theory and Practice

The relevance and efficacy of the Australian Signals Directorate Top 4 and Essential Eight mitigation strategies are strongly validated by the WannaCry experience.

To be compliant with the ASD advice, organisations should have up to date software and programs to educate staff on cyber security risks and best practices.

In this instance, organisations that had the latest versions of Microsoft software and that had applied the latest patches to these products should have had no vulnerability to be exploited. That is, the malicious worm could not have spread.

Any phishing email that was received by users educated in not opening unsolicited and suspicious emails could also have been protected by this good user hygiene practice. That is, individual computers could be protected by vigilant users not opening infected emails.

These are defences and mitigation strategies that users apply inside their IT environments.

However, the Government has an additional policy in place to protect its agencies before the malicious content gets even that far.

The Lead Agency Gateway (LAG) program operates a security screen at the perimeter of Government IT environments. Its role is highly relevant in this incident.

Under this program a small number of providers of Secure Internet Gateway (SIG) services (including Macquarie Government) operate a "stack" of security software and protocols on behalf of the Government at the point where agencies connect to the Internet.

Department and agencies are required to connect to the Internet through one of these Gateways under a policy first announced in 2010 and implemented between 2012 and 2013.

This provided protection in addition to any action taken by the agencies on their own behalf.

Firstly, there are several different anti-virus software products operating on the SIG. Each of these should have been updated with the signature to identify the particular malware.

When the global crisis began on Friday, Macquarie Government was monitoring traffic to its government client agencies, but was not seeing the suspect signature in the logs from the firewall software. While there was no evidence that this meant the anti-virus software was not working, the security team decided to take additional action by blocking all access to the "port" (a type of sub address) to which the exploit was known to be directed.

Macquarie also directly advised all its government and corporate customers of the emerging global crisis and the actions they should take in relation to their internal ICT environments (immediately patch, isolate infected workstations and systems).

From the above it is clear that:

1. Implementation of the Essential Eight would most likely have protected any user from the WannaCry virus, and;
2. Implementation of the Lead Agency Gateway Program provided a shield across all agencies that participated in the program, including any agency that was itself not fully compliant with the Top 4
3. Hundreds of thousands of users worldwide were not implementing these most basic of protocols, and
4. In Australia, it is the view of the most senior Government cyber security experts that we were saved from the worst by circumstance rather than universal good practice.

A key question this raises for Government in relation to its own future risk is;

> If, as can be seen from the above, the advice is good, and if, combined with the perimeter defences of the SIG, the likelihood of infection was extremely low, why is the ASD advice not being universally followed, why are not all agencies being required to comply with the Lead Agency Gateway program, and how can this be fixed quickly?

Can the Essential Eight/Top 4 Ever be Universal?

The ANAO report that prompted this inquiry demonstrates that, even among the most advanced and sophisticated Government agencies, compliance is inconsistent. Research commissioned by MTG from the National Security College[i] last

year found that medium sized public and private enterprises in Australia had patchy and often fragile cyber security governance systems, which further suggests the full adoption of the Top 4/Essential Eight is undoubtedly far short of ubiquitous.

Partly, the reason is awareness of risk. However, examples of cyber breaches have now been so extensively reported that failure to become informed borders on organisational irresponsibility.

It must also be acknowledged that the implementation of the mitigation strategies is not trivial and not inexpensive. The continued widespread use of old software revealed by the WannaCry experience reflects the cost decisions made by many businesses. The capital expense of upgrading software, and the operational disruption, can be a huge disincentive.

This is also the case for smaller Government agencies, here and overseas, and has been reported to have been a factor in the vulnerability of many National Health Service agencies in the UK that was exposed by this incident.

As discussed in MTG's primary submission to this inquiry, the LAG model was created to share the high costs of maintaining a standard universal security perimeter across agencies of all sizes.

The software operated in the Gateway's firewalls is updated and patched continuously by a specialised security team employed by Macquarie Government, whose only job is to manage these responsibilities. We understand the same can be said for other LAG operators.

There are, however, smaller agencies that have not complied with the requirement to join the LAG program. We understand the Australian Bureau of Statistics applied for and was granted an exemption some years ago, for example. Other agencies have not joined a LAG group seemingly without receiving an exemption because there is no process by which they are compelled to comply with the policy.

The WannaCry experience should be the catalyst to end these exemptions as a matter of urgency.

In relation to the compliance of internal IT systems with Top 4/Essential Eight advice about software patching and new releases, MTG submits that the "old ways" may no longer be fit for purpose.

That is the combination of the cost of upgrades and the speed of the changes in the cyber security threat landscape could mean that even the most well intentioned smaller agency is chasing a moving horizon, without having the internal resources and expertise to be able to always keep up.

However, part of the solution to this may also be in existing policy, in this instance the Government's Cloud First policy.

Agencies could be helped to understand that the Government's policy to encourage them to consider cloud computing solutions before investing more heavily in computing resources they manage and own entirely on their own is a means to transition to a more robust security environment, as well as a more efficient model of obtaining computing resources.

Cloud based services, like the LAG program, take advantage of scale to defray costs of upgrades across a wide user base, and recovery of those costs are operational expenses rather than "lumpy" capital expenses.

The providers of these services can be required to keep their computing environments up to date with software and security releases, and a cloud computing business model means they should be able to develop the scale to do this economically.

Recommendations

MTG submits that the committee should consider two recommendations to lift the Federal Government's cyber security stance in the light of the lessons from the WannaCry event.

- Agencies that are subject to the Lead Agency Gateway policy of 2010, but have not migrated their environments behind a combined gateway, should do so without undue delay.
- Government Agencies should accelerate their transition to cloud computing services, but should ensure that security measures are integrated into those new services delivery models from the point of design.

Contact

David Forman
Senior Manager, Industry & Policy
Macquarie Telecom Group
[redacted]

[i] http://nsc.anu.edu.au/news-events/news-20161102