18 May 2017
The Australian, Australia

Author: Robert Gottliebsen • Section: Business News • Article type : News Item
Audience : 96,602 • Page: 33 • Printed Size: 336.00cm² • Market: National
Country: Australia • Words: 752 • Item ID: 776705404

isentia.mediaportal

Cyber attack: business must be on the alert

ROBERT GOTTLIEBSEN

The massive global computer hacking attack, termed WannaCry, is a much bigger event than simply the crippling of a few hundred thousand enterprises around the world — albeit that the damage created is a huge disaster.

Previously most businesses thought that if they were careful with emails they would be safe. WannaCry spread through the Microsoft system and not via email and researchers are still trying to determine how it works.

And what makes it scarier is that WannaCry was not a sophisticated money-raising event. Relatively little money has been raised. Its like a trial run for something much bigger.

I am not a technology journalist but I believe that it is important my readers are put on alert. And that alert particularly applies to smaller enterprises, where livelihoods can be destroyed overnight without proper backup that is completely separate from the base enterprise system.

All too often in Australia bankers rely on the family home as security for enterprise loans so if the business is destroyed by hackers the home must be sold. I have seen it happen.

WannaCry is also affecting the productivity of millions of businesses as they become much more cautious in their use of the internet.

And the origins of WannaCry also extend its potential impact. The US National Security Agency (a military intelligence organisation which is part of the US Department of Defence) used its knowledge of Microsoft systems to discover a hacking tool codenamed EternalBlue which ended up in the hands of the hackers.

I believe Eternal Blue was used to gather knowledge of looming terrorist attacks and detect money laundering. No one knows to what extent global anti terror and money laundering have been compromised but the failure to extract large sums of money via this attack indicates a different agenda.

In the case of the WannaCry attack, small enterprises were not the main target and it was used primarily against large organisations. Most large organisations have procedures to back up material although sometimes these backups are delayed and in the case of the UK health system they were very vulnerable because they were using an old computer system.

In the day-to-day hacking world the attackers concentrate on small enterprises because they usually do not have the same defences. Close to three-quarter's of global hackings are directed towards smaller enterprises. They are the main targets for ransom.

Last night I was yarning to the former head of Google Asia, Charif Elansari, who is now chief executive of Dropsuite Limited, — a listed company that specialises in data base backups for small enterprises. Clearly he has a bias towards boosting his enterprise but he is also frightened by the speed, depth and impact of this global cyber attack which indicates that not only are attacks going to continue, but they are going to get more disruptive to businesses.

In Australia we are no different from most parts of the world and most enterprises outside the giants do nothing, and hope they don't become a victim of attacks. Elansari says most are in denial that a breach will happen to them.

The first line of defence is to deploy antivirus software and training staff on how to avoid becoming a victim of cyber attacks including those demanding ransoms.

The trouble is that it just takes one employee to click on an infected email link, or one virus to make its way through your antivirus firewall, and the business system will go down and with it your data and customer relations. In any event WannaCry did not spread via emails so backing up data becomes vital.

The backup must be automated and not just at the end of the day. In addition the backup data must be housed totally separately, probably on the cloud. If you have that sort of system it is possible to buy data insurance.

In a world where margins are tight it's another cost. But the internet has delivered us great new possibilities and opened up new businesses by allowing smaller enterprises to attack larger ones.

But it is now clear the dangers so created require protection.

Unfortunately WannaCry comes at a time when political vandals damaged our power systems. The politicians are like the hackers and have caused a similar need for protection.

So in eastern states, as well as investing in computer systems backup and insurance, enterprises need diesel power generation or battery storage to be safe from the danger of blackouts.

Ooops, your files have been encrypted!
Payment will be raised on
Time Left
02:22:26:11
Your files will be lost on
Time Left
06:22:26:11
bitcoin
Send $300 worth of bitcoin to this address:
Check Payment
Decrypt
Contact Us
KISA2

AFP

Monitoring the speed of ransomware attacks in Korea