Expert IT Solutions Newsletter

Issue 10 September 2015

Welcome to the fifth newsletter for the year. This time we look at Multi Factor Authentication (MFA) and Surface Pro 3. A quick warning first regarding Crypto locker attacks is also timely.

Crypto Locker

Because of the rise of CryptoLocker attacks right now in Australia we need to remind you about the risks of emails with attachments. These can appear to come from Telstra, Australia Post or any other "official" source. Once you click on the attachment, all documents (Word, Excel, Pictures, PDF etc.) on your local machine are encrypted, along **with any documents on the server** that you have access to. A message is then displayed on your PC, requiring payment (in some form of electronic, hard to trace, currency) for the decryption keys. Once this have happened there are only two options – pay to (perhaps) get the required keys. Or restore all encrypted documents from last nights (or last weeks?) backup.

Please make sure all staff are careful about clicking on email attachments from unknown senders. Yes, your antivirus system should catch it but the malware keeps changing to make it harder to identify.

Multi Factor Authentication (MFA)

Hardly a week goes by nowadays without some news, even in mainstream media, of a data breach in some large organisation. Particularly large data breaches that come to mind are OPM, Target US and Home Depot, Ashley Madison, Anthem and Sony. If that list seems focused on the US that's simply because Australia doesn't have legislation for mandatory disclosure (yet). Here's an article that lists a few of the 104 voluntary data breaches recorded in 2014 in Australia.

There's a pattern to the breaches mentioned. Some of them are simply stealing credit cards (in the 100's of millions of them) for monetary gain but others are chasing personally identifiable information. If I'm a hacker, once I have enough information about you I can use that to impersonate you to gain access to other systems. Another pattern in these breaches are that they often started with the theft of an identity / account of a particular person which was then used to gain deeper access to the system.

"So what" you're probably thinking. Those are high profile, global corporations and organisations, easy targets for hackers. We're a small business, no-one is going to bother hacking us.

Well, think again. The picture of the hacker as a teenager in his parent's garage, hacking into systems just to show that he can and for the glory and recognition of his peers is long gone. Hackers today are part of a many 100's Billion dollar industry, run by organised crime (Russia, Eastern Europe and parts of Asia are particularly strong players here). They don't care about your size, just whether there's a way to use your business for financial gain.

In today's multi connected, cloud service world, the internal network of your business and your firewall is no longer the only defence from the "big bad world" of the internet. The other part is yours and your employee's identity. In fact, identity is becoming the hottest target for the bad guys.

So what can you do? Let's start with personal / consumer services (such as the ones that your staff are using on your network every day). Gmail (and other Google services), Microsoft accounts (Outlook, Hotmail etc.), Dropbox and Facebook all offer the option for adding **Two Factor Authentication (2FA)**. Also called **Multi Factor Authentication (MFA)**, when you have choices for the second factor, the basic idea is that instead of just relying on a username and password to prove who you are, you also need a second factor of authentication: something you **have**, not just something you **know**. That something is generally your smartphone, although it can be a smart card, your device (modern tablets can come with something called a Trusted Platform Module (TPM) chip). So when you login to one of the services above, your smartphone will ring or a text message will arrive that you need to do something with to prove that you are indeed who you say you are. I hope the point is now becoming clear: if I steal your username and password and I'm attempting to login as you, I can't do the last step because you still have your phone. (And if your phone has been stolen, it would be a good idea to reset your passwords as a first step). Of course this isn't going to happen every time you login, these systems have the "smarts" to know that if you logged in an hour ago from the same device in the same location, it's not going to trigger MFA. But if you (or someone who has your username and password) are on a different device, in a different location or hasn't logged on for a week, then MFA will be triggered.

What about your network login, the one you use every day to access your server? We can do the same using AuthAnvil for a Small Business Server or ordinary Windows servers. And if you're considering cloud services such as Office 365 or Azure, MFA comes built in.

If you're interested in improving the security of your business identities using 2FA / MFA please contact us for more information.

Surface Pro 3

Recently, at special event on the 9th of September, Apple announced the iPad Pro. Clearly taking its design cues from Microsoft's very popular Surface Pro 3, the pundits are hailing this as "the next big thing" from Apple.

The idea is that basic tablets are excellent for consuming content (websites, films, music, and reading) but not so good for being productive. Having a 2 in 1 device that can be a tablet for consumption, and with a detachable keyboard (unlike a laptop) clipped on turned into a device that you can be productive on seems like its hit the sweet spot for many people.

I know I love my Surface Pro 3. I love the lightness, the performance (it's an i7 with 8 GB of RAM and a 256 GB SSD for storage), and the fact that it runs all my normal Windows applications. And then add the pen, being able to ink my notes (and sketches) into OneNote or use Photoshop with a "brush" that gives me more ink if I press harder and it's easily the best personal computing device I've ever owned. Unfortunately Expert IT Solutions aren't part of the exclusive list of resellers that are allowed to resell Surface Pro 3.

Note that even though the iPad Pro can have a keyboard attached and an optional pencil, there's no USB port, or HDMI output, or mouse support. On the plus side it does come with inbuilt 3G connectivity, still sorely lacking in Surface Pro 3 (but available in the smaller cousin Surface 3).

Need more proof that a 2 in 1 is the "best" device (depending on use case) for most professionals? Lenovo's Miix 700 was also recently announced and it also clearly takes its cues from Surface Pro 3. Dell is also rumoured to have a copy in the works. And Surface Pro 4 is being announced in October.

If imitation is the sincerest form of flattery I think Surface Pro 3 should be VERY flattered ☺.

If you'd like a demo of the Surface Pro 3 in action (now running Windows 10) and my personal experiences (both good and bad), along with looking at the applicability for your particular business scenario please don't hesitate to contact us.

If you have any questions or suggestions for topics you'd like covered in this newsletter, please email us.

In the next newsletter we will look at a security checklist for improving overall IT resiliency in your business as well as well as Surface Pro 4.

If you no longer wish to receive this newsletter please email unsubscribe@expertitsolutions.com.au. If you have colleagues, friends or relatives that could benefit from this newsletter, please ask them to email subscribe@expertitsolutions.com.au.