Grant Thornton
An instinct for growth™

Information Security

It's 2018: why are our systems still insecure?

June 2018

3698GT-06-18

We continue to hear sorry tales of companies' systems being hacked: as I write this, the latest big story (https://www.theregister.co.uk/2018/06/13/dixons_carphone_breach/) is Dixons Carphone experiencing a hack involving 5.9 million payment cards and over a million personal data records.

They're a big company – which means they have no excuse: with a pre-tax profit of over £380 million in 2017-18, they could afford to spend more on information security. But what about small businesses who don't have this kind of money to splash on security? Well, judging from what I see in the Channel Islands, there's a lot of IT kit out there just sitting waiting to be hacked.

Before I start, let me point out that every fact I state here is in the public domain. The information is freely and easily available to anyone with a computer and a Web browser. The fact that I can see it means that hackers can see it too, and can use it to find and attack vulnerable systems. I'm going to work in generalities so as not to point to specific systems and their vulnerabilities – but bear in mind that it took me only a couple of hours to get enough research material to write this article, so anyone with bad intentions can go through exactly the same process as me.

The tools are there

Back in the day, an attacker had to put together a toolkit that would scan the Internet for systems that were sitting waiting for connections. These days you need neither knowledge nor tools, because the search engine at https://www.shodan.io/ has done it for you. As I write this it can see 7,023 systems in Jersey and 8,067 in Guernsey – that's a total of about 15,000 systems that anyone on the Internet can see and connect to.

Of course, some of these systems are there for a purpose. There are about 2,000 things that look like Web servers, for example – and of course you'd want a Web server to be visible to people on the Internet. Hang on, though: if we look, most of them aren't actually Web servers. Connect to some of them and you get the login page for the management interface of a broadband router. Most of them have secure passwords – but some don't. Why would you want to expose your router so that everyone on the Internet can see it and – if they can guess the password – even change its settings?

Unconfigured means potentially insecure

And the systems that really are Web servers are often not properly configured: one I just picked at random shows me the Web server test page – which is what you see when you've first installed the Web server software but haven't configured it yet. Helpfully it tells me not only that it's running a particular Web server application but also that it's running on a particular version of Linux: hackers love this, because they can limit their efforts to just the attacks they know might work against that particular system.

I mentioned broadband routers: well, many routers can also be managed via a text-based mechanism called a Command Line Interface, or CLI. PCs and Macs have a built-in program called Telnet, which can connect to these devices. There are 357 to go at, and not all of them have secure passwords set: most systems of this type have an unimaginative password set in the factory ("password" is fairly common, for instance) and for small business and home users in particular, it's common to install the device but not to change the password to something less guessable.

"Here I am!"

Worse still, not far down the list there's a system that tells you the moment you connect (without you even having to type anything) its make and model, what software version it's running and even its serial number. Again, the hacker will be reaching for the vulnerability list for that software revision and they've not even had to guess the password.

There's another network management tool called SNMP, or the Simple Network Management Protocol. It's traditionally been really insecure: early versions don't have any encryption and many systems have some very guessable passwords (they're called "community strings" in SNMP terms, but they're really just passwords) that people often don't change. We can see 114 systems that anyone can connect to with an SNMP application – there's a pile of broadband routers, but we can also see a variety of other stuff – some printers and several firewalls, for example. I even

see an enterprise-grade Cisco network device that's telling the world about itself. With regard to firewalls: these are devices whose sole purpose is to protect the organisation against hackers – yet in several cases these devices are letting anyone in the world connect using SNMP and read the configuration, which will give clues about how to hack them. Could I change any settings on these devices? Maybe, but I'm not about to try.

It goes on. There are 362 devices advertising their storage as Windows shared folders: from what Shodan tells us it looks like many of these are where someone's connected a USB memory stick to their router to make it a shared device (why you'd do that and advertise it to the Internet is a question I can't answer – I certainly wouldn't do it). There's a videoconferencing system. There are 32 systems using the VNC remote control application (so with the right password you could take over the machine). There are 2,500 systems running an ancient (and insecure) version of the security protocols that underpin supposedly "secure" Web servers. The list goes on.

Vulnerability lists on a plate

And it gets scarier. You know I mentioned that hackers like to know about systems so they can narrow down the set of hacks they try? Well, they don't have to even look things up themselves: a simple command to Shodan and it'll give you a list of all the devices it's come across with known vulnerabilities (if you're wondering, the most common dates back to 2010 and there are 378 vulnerable systems in our collection of 15,000 devices).

Why is the situation so bad?

Security vulnerabilities exist for a number of reasons. In the case of the Dixons Carphone hack I mentioned earlier it would be easy to scream "incompetence", but my guess is that it's more subtle than that. I bet they have the tools and expertise to keep their systems secure, and policies and procedures to work to: it's common to find in cases like this that there was some kind of esoteric set of circumstances that weren't caught by the policies, or perhaps that there was an omission in training that caused someone not to follow the right procedure.

In smaller companies, though, it's usually down to lack of time, funds and knowledge. Managing IT systems isn't an easy job, and understanding the security implications around systems is particularly hard. The person installing a new broadband router might not realise, for example, that its SNMP interface is turned on by default – after all, they might not even know what an SNMP interface is. In my experience it's very rare to come across a security breach that was caused deliberately: most of the time it's something that the victim unwittingly did wrong – or, in the case of changing a default setting, something someone didn't do – and most of the time it's through lack of knowledge of how to do it right.

What can I do?

The first thing to bear in mind is that tools like Shodan are there for the good guys to use, not just the bad guys. It's dead easy to use widely available tools to check your own systems for vulnerabilities and to make sure you're not inadvertently opening yourself up to attack. So do so – and if you don't understand how to use them, engage with a third party who does.

Be ruthless to stamp out what's called "shadow IT". This is where technology starts springing up around the organisation because the department using it has decided – rightly or wrongly – that it's quicker/easier/better to do it themselves rather than wait for the IT department to do it for them. Shadow IT exists because it can save people time, but from a security point of view it's an absolute menace.

Check out the National Cyber Security Centre's Cyber Essentials standard (https://www.cyberessentials.ncsc.gov.uk/) and become compliant with it. This is a really great little standard that defines a solid baseline of simple steps you can take to protect against the majority of hacks. It's something that Jersey businesses should be doing already, in fact, because from 1 January 2020 the States of Jersey won't let you interact electronically with them unless you have a CE certificate.

Consider whether you have enough expertise to deal with the security of your systems: if not, consider either employing someone or, more likely, engaging with an external support partner to help you out. If you do use an external support partner, be clear on what each party's responsibilities are regarding security and have regular meetings to ensure that they're doing everything they should.

Finally, get an independent opinion of how good (or bad) your information security is. Even if you've already contracted a service provider to manage your systems for you, an independent assessment will validate how well they are doing their job, and may identify areas for improvement that weren't spotted by the day-to-day service provider.

For more information please contact:

David Cartwright
Senior Consultant, Information Security
T +44 (0) 1534 885813
E david.cartwright@gt-ci.com

Grant Thornton

An instinct for growth™

grantthorntonci.com

© 2017 Grant Thornton Limited. All rights reserved.

'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. Grant Thornton International Ltd (GTIL) and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.