The Day the world went Dark – How would you approach a DDoS attack in your business

By Andrew Potgieter, Security Solutions Director at Westcon-Comstor Southern Africa

On Friday 21 October the "Day the world went Dark", a major US-based DNS hosting company DYN Inc. experienced what is arguably the largest distributed denial of service (DDoS) attack in history on its servers. At 4:22 PM EST the company was reported as saying "Looks like this is probably going to get worse before it gets any better" as they were hit with a third wave of attacks. The attacks on tens of millions of IP addresses at same time sparked a global crisis of what one could only describe as nuclear proportions.

The most crippling aspect of the attack, conducted by the group New World Hackers, was really how unprepared those companies at the end of the attack were for the situation, which quickly escalated to a crisis for many of those "born-in-the-cloud" businesses 100% reliant on their websites for their livelihood. Some of the best-known sites affected included: Twitter, Spotify, PayPal, Amazon, Netflix, Tumblr, Etsy, DropBox, Pinterest, Basecamp and AirBnB, with dozens more, too.

Behind the scenes of 21 October attack
But what sparked this almost situation room and warlike response to the attacks and how did this attack take shape?

DDoS attacks work by a collective targeting of a website or host with so much traffic that the service can no longer cope and becomes unavailable, hence the term Distributed Denial of Service. In this instance the DDoS targeted the Domain Name Servers (DNS) of DYN Inc., the service provider. DNS is, in short, the Internet's 'phone book' and when you type in a website address this needs to be translated to the physical address of the server(s) hosting it. If the DNS provider who holds these address translation tables for your website is down, in this case DYN, your site is down.

How did they get in?

According to ComputerWorld a Chinese electronics component manufacturer has admitted that some of its products inadvertently played a role in the cyber attack on Friday. The company sells DVRs and Internet-connected cameras, some of the devices that enable the Internet of Things (IoT). These devices come with weak default passwords which, if not changed, enable malware infections of the devices. These infections enable attackers to create one large connected network or botnet by taking over control of the devices.

An IoT botnet
But they are not alone, with the number of IoT devices growing and the lackadaisical approach by end users to change the passwords on these devices it was very easy for the New World Hackers to use the IoT malware Mirai (available on the dark web) to take hold of their websites and literally bring the Internet to its knees.

By enslaving IoT devices, which could be your CCTV camera in your home or the office, your kettle, fridge, web camera, home automation system, or anything else connected to the Internet, Mirai's massive connected network bombarded the websites in question. It is estimated that there are over 500,000 (known) Mirai infected devices in the market as we speak.

Why is this terrifying?

Let's argue for a minute that this attack hasn't woken up people to the threat of weak default

passwords and consider that with an anticipated 25 billion (this figure varies depending on source) connected IoT devices in the world by 2020, the global consequence of an attack of this nature could be viewed as of 'nuclear proportions'.

The message from the hactivists in this particular DDoS attack doesn't seem to be one of malice, instead they are urging the company to put better security and servers in place with redundancy, or they will bring the Internet down.

So what can you do?

Update all your passwords and, in particular, those devices you have installed on the periphery, such as CCTV cameras, home automation systems, smart TV's etc. While the US might be more IoT savvy than South Africa at this stage, the evidence of this attack is that it was conducted globally and from multiple geographies, with new waves coming from new areas throughout the attack, so your CCTV cameras in SA might well have been used to ping traffic in this particular event.

Is your business ready for DDoS?
One thing is clear, even with all the foreseeable security you can purchase put in place, companies must adopt a risk-ready approach. While a DDoS attack may constitute a risk for some it may well be a crisis for another.

Three things you need to ask of your business today are:
· Firstly, what is the potential severity of a DDoS attack on your business based on how important being online is to your business?.
· Secondly identify ways to mitigate the risk and that means talking to your service providers and security vendors to ensure you have a plan to manage it.
· And lastly develop a crisis preparedness programme – fixing the problem isn't enough if it has had a negative impact on your clients – you will need to communicate with them so have those answers ready.

Once you have answers to these questions you need to take a closer look at the overall IT security of your business. Securing at the perimeter is no longer enough – security needs to be the glue that holds everything together. It must be everywhere, from the device to the server, to the cloud and through all endpoints, right back through to all of your service providers.

Naturally some of these attacks are going to be inevitable so its critical to establish a plan on how to deal with these unfortunate eventualities, which again begs of your business to develop crisis communication strategies for IT security breaches today. If Friday has alerted us to anything, it is that you need to be asking of yourself "what if it happens to me?"

As a consumer perhaps its time to reflect on how one will survive when the IoT is so pervasive that we can't function in society without access to the Internet, as our banks, petrol stations, electricity and everyday appliances are all connected. Perhaps then governments will have Internet-based situation rooms and these attacks will start being considered with the same severity as a nuclear strike.