How suppliers of everyday devices make you vulnerable to cyber attack – and what to do about it

July 4 2018, by Richard Matthews And Nick Falkner

Credit: cottonbro studio from Pexels

If you run a business, you're probably concerned about IT security. Maybe you invest in antivirus software, firewalls and regular system

updates.

Unfortunately, these measures might not protect you from malicious attacks that enter your systems through everyday devices.

On the evening of Friday the 24th of October 2008 Richard C. Schaeffer Jr, the NSA's top computer systems protection officer was in a briefing with US President George W. Bush when an aide passed him a note. The note was brief and to the point. They had been hacked.

How did it happen? The culprit was a simple USB.

USB supply chain attacks

The attack was unexpected because classified military systems are not connected to outside networks. The source was isolated to a worm loaded onto a USB key that had been carefully set up and left in large numbers to be purchased from a local internet kiosk.

This is an example of a supply chain attack, which focuses on the least secure elements in an organisation's supply chain.

The US military immediately moved to ban USB drives in the field. Some years later, the US would use the same tactic to breach and disrupt Iran's nuclear weapons program in an attack that has now been dubbed Stuxnet.

The lesson is clear: if you are plugging USB drives into your systems, you need to be very sure where they came from and what's on them.

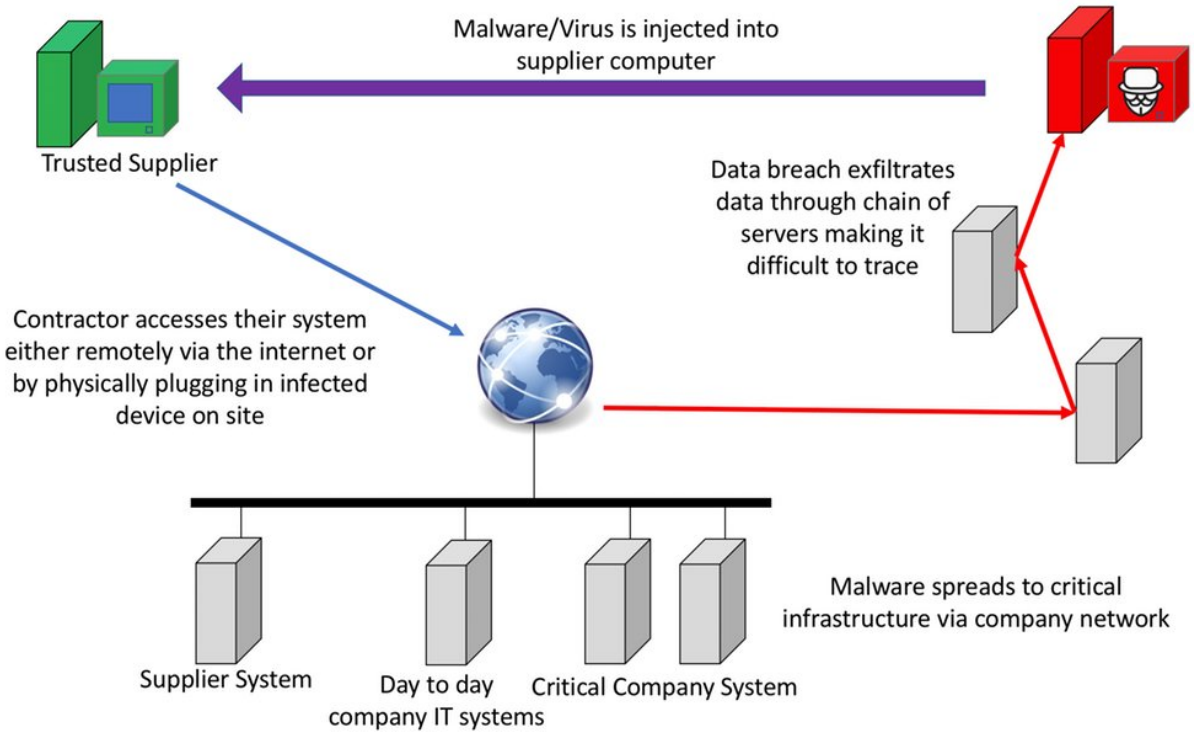
If a supplier can get a secret payload onto a USB stick, then there is no safe period in which a USB is a good choice. For example, you can currently buy a USB stick that is secretly a small computer, and it will,

on insertion, open up a window on your machine and play the Death Star march.

This is just one kind of supply chain attack. What are the other kinds?

Network supply chain attacks

Computer users have an increasing tendency to store all their information on a network, concentrating their assets in one place. In this scenario, if one computer is compromised then the entire system is open to an attacker.



The basic model of a network supply chain attack shows how vulnerable interconnected systems are within an organisation. Author Supplied

Consider a conference phone used in your organisation. Suppose this network-enabled phone had a built in fault that would allow attackers to listen in on any conversations in the vicinity. This was the reality in 2012 when more than 16 versions of Cisco's popular IP phone were affected. Cisco released a patch for their phones, which could be installed by most companies' IT security departments.

In 2017, a similar issue arose when a brand of hospital grade dishwasher was affected by a built-in insecure web server. In the case of a hospital, there is a great deal of private data and specialist equipment that could be compromised by such a vulnerability. While a patch was eventually released, it required a specialised service technician to upload it.

Supply chain attacks have recently been implicated in the disastrous failure rate of the North Korean missile program. David Kennedy, in a video for The Insider, discusses how the US has previously disrupted nuclear programs using cyber. If they still possess this capability, it's possible they would wish to keep it covert. Should this be the case, it's conceivable one of the numerous North Korean failures could have been a test of such a cyber weapon.

Five ways companies can protect themselves

To protect yourself against all of this you need to set up basic cyber hygiene processes that can help keep your business free from infection.

1. Purchase and install good anti-virus software and run it in protective mode, where it scans everything on your machine. Yes, even Macs get viruses
2. monitor who is on your network, avoid using untrusted devices such as USBs and have your administrators block autorun as a system-wide policy
3. segregate your networks. Have critical plant infrastructure? Don't

have it on the same network as your day to day, public-facing or guest access networks
4. update regularly. Don't worry about the latest and greatest issues, patch the known vulnerabilities in your systems – especially that one from 1980
5. pay for your software and labour. If you're not paying for the product, then someone is paying for you *as* the product.

Cyber awareness is crucial

Finally, you can maximise cyber resilience by training everyone in your organisation to learn new skills. But it's vital to test whether your training is working. Use actual exercises – in conjunction with security professionals – to examine your organisation, practice those skills, and work out where you need to make improvements.

The price of any connection to the internet is that it's vulnerable to attack. But as we've shown, not even standalone systems are safe. Deliberate practice and thoughtful approaches to security can increase the protection of your business or workplace.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation