How cybercrime has changed over the past five years (it hasn't got any better)

September 3 2015, by David Glance

Giving away the keys to cybercriminals. Credit: Intel Free Press/flickr

Intel has used the 5th anniversary of their purchase of security company McAfee to release a review of how the cybersecurity landscape has changed in that time.

There are a number of surprising observations from the report and a few that were expected. Of little surprise has been the continued lack of importance a large number of companies, and individuals, have placed on implementing basic security practices like applying updates to software and implementing policies around passwords. The reasons for this may be that people are "playing the odds" by believing that the risks are relatively small of cybercrime happening to them. It may also be that they simply don't want to put in the effort or pay for the computer support or advice.

Cybercrime as an industry

More surprising, to McAfee at least, has been the rapid development of cybercrime into a fully fledged industry with "suppliers, markets, service providers ("cybercrime as a service"), financing, trading systems, and a proliferation of business models". The growth of this industry has been fuelled by the use of cryptocurrencies like Bitcoin and the protective cloak for criminals provided by technologies like Tor).

The sophistication of the cybercrime industry has led to changes in the focus of criminals away from simply stealing credit cards to the perhaps more lucrative, large scale implementation of "ransomware". This has ranged from encrypting the contents of a user's computer and then demanding payment to unlock it, to the recent exploit of users caught up in the publishing of personal sexual information from the Ashley Madison dating site.

Mobile phones have remained "relatively" cybercrime free

What hasn't come to pass (yet) is the pervasive hacking of mobile phones. Part of the reason for this has been Apple's, and increasingly

Google's, approach of controlling the software that is allowed to be installed on the devices. The other reason is perhaps the fact that these devices are backed up more frequently and automatically, making recovery a much easier option. There is also potentially less of interest to cybercriminals on a mobile phone device as most of the actual important, and valuable, personal content is stored in the Cloud.

The recent exception to the relative safety of mobile devices was the report that up to 225,000 Apple accounts had been compromised from Apple phones. The compromise in this case only affected mobile phones that had been "jailbroken", a process that allows the user of the phone to circumvent Apple's restrictions on what apps can run on the phones. Of course, what this has demonstrated is that the restrictions on what software can run on Apple and Android phones is actually a major security feature and so avoiding that increases the risk of being compromised significantly.

The threat to the Internet of Things

Along with mobile phones, smart devices that make up the Internet of Things have also been relatively free of large scale hacks. Researchers have demonstrated that it is possible to hack things like cars, including being able to apply the brakes of a car by sending the control system of the vehicle an SMS. In the case of this type of vulnerabilities, car manufacturers have moved to plug security holes quickly. The fact that criminals haven't turned their attention to smart devices however is probably because of the lack of means of commercialising these types of compromises.

People are still the problem

Organisations like McAfee are fighting a largely losing battle as long as companies continue not to take security seriously. In fact, US companies are spending and doing less where security is concerned than in previous years. This has led organisations like the OECD to recommend national strategies around the development of cybersecurity insurance. A benefit of having this type of insurance would be the requirements that insurance companies would place on implementing a basic level of security best practice.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: How cybercrime has changed over the past five years (it hasn't got any better) (2015, September 3) retrieved 2 May 2024 from https://phys.org/news/2015-09-cybercrime-years-hasnt.html