BIZCOMMUNITY

Prevention through awareness

By Simon Campbell-Young

12 May 2014

Scarcely a day goes by without a report of a breach, or a new threat raising its ugly head. Cyber criminals are increasingly cunning and devious, writing malware to bypass almost every security control.

Particularly with so much business being conducted over the Internet, online shopping, social media and so on, customers need to be able to trust that their information is 100% safe. If they can't, their business might be gone for good. Businesses need to keep abreast of what is happening in the security sphere in order to better protect their customers.

Information compromised

Firstly, over the last two years, several high profile brands were compromised by attackers, resulting in millions and millions of user names and passwords being exposed. RSA, Verizon, Google, Yahoo - and most recently Adobe are examples. Hundreds of thousands of users were forced to update their passwords following the breaches, and even more had their private data compromised.

Beyond the obvious costs to these businesses in terms of mitigation and clean-up following the breach, was the cost of loss of trust by their customers. It is almost impossible to put a price tag on this loss of trust. How many customers were lost for good? How many potential customers were put off using these products and services? Loss of reputation can be a death blow for a business.

Many of these companies upped their security controls through means such as two-factor authentication, which, while not a silver bullet, is an added layer of security that is an improvement. It is likely that there will be many further data breaches in the future.

Vulnerability

All businesses are vulnerable. All that is needed is a tiny chink in a company's security armour, and a cyber-criminal will surely try to exploit it. Should your business suffer a breach, you could end up losing customers. Permanently.

Another concern for organisations, is the increase in malware, both in terms of volume and sophistication. Malware is used to compromise a device or system, be it a mobile phone, laptop, pc, network etc. In fact, the past year has seen some new and bizarre pieces of hardware being added to the malware authors' lists, including pacemakers, cars and light bulbs.

Most malware is designed to steal information, be it passwords, usernames, account information, or financial data. Also

concerning, is the increase in mobile malware, which has leaped a hundred fold in the last few years, making all sensitive data stored on a mobile device vulnerable to attack. All businesses should be aware of the latest threats doing the rounds, and update and patch accordingly. For consumers, a good AV product, both for mobiles and for PCs is essential.

Hacktivism

The rise in hacktivism is also causing headaches for businesses. The last year has seen several high profile attacks of companies' Twitter accounts, whereby the attackers have compromised the account, to post pictures or change tweets. Should cyber criminals spread misinformation or defamatory statements via a 'valid' Twitter account, the repercussions to the business could be severe. Not to mention there might be a perception that if a business can't even protect their social media accounts, their other security measures could be woefully inadequate. Social media accounts, be they Twitter or Facebook are often the face of the business these days. Companies must ensure that these are safe and protected.

Distributed denial of service (DDoS) attacks have also risen dramatically over the past few years. DDoS attacks are essentially an attempt by attackers to make a Web site or network resource unavailable to its intended users. Generally, threat actors attempt to temporarily or indefinitely disrupt services of a host that connects to the Web.

Although perpetrators of these attacks generally go after high-profile targets, such as financial institutions, no Web sites are really safe. Hacktivists are using these attacks more and more as a means of protest against perceived injustices, while advanced persistent threat attackers will often use a DDoS attack as a means of obfuscating their true target or purpose. Either way, businesses must be on the lookout for DDoS attacks, and have some protection or means of mitigation in place. Customers who are constantly denied access to a site or service because a DDoS attack is rendering them unavailable, will eventually go elsewhere.

Companies who are unaware of how the threat landscape could affect their business will be negatively impacted at some point. The first step in protecting your business, and with it your customers, is being aware, and understanding what is out there. Keeping a secure online presence is vital. Protect your company, and your users' information, or soon you will have no customers to protect at all.

ABOUT SIMON CAMPBELL-YOUNG

Having started his career as a startup partner for FSA Distribution in 1990, Simon Campbell-Young went on to start his own company called Memtek Distribution in 1995. This was sold to a public company called Siltek Holdings between 1998 to 2000. Shortly thereafter, he took his experience in the technology sector, garnered over more than 23 years, to form specialist distribution company Phoenix Distribution in 2000.

- Adding threat intelligence to the security mix - 26 Nov 2018
- Digital forensics is crucial to the security chain - 6 Nov 2018
- App permissions can be used to exploit your data - 26 Oct 2018
- 57 million riders, drivers affected by Uber breach - 13 Dec 2017
- Prevention through awareness - 12 May 2014

View my profile and articles...