Embrace digital technology and move your business online to survive and thrive!

#GoDigitalWC Articles

Get tips and learn how to take your business online, click here

#GoDigitalWC Webinars

Hear from experts and thought leaders on digitizing your business, click here

#GoDigitalWC Tech Volunteers Initiative

Find out more about our FREE digital advisory support offer, click here

Article 15: Understanding Cyber Security

Introduction

Cyber security is the coordinated efforts of a body of technologies and processes aimed at protecting hardware, software and data from unauthorized access, modification, damage and deletion. It is the digital data that is stored, transmitted and in use on servers, networks or computers/devices that ultimately requires protection. This can no longer be regarded as just an IT issue, and is increasingly being recognized to be a much broader business issue. Cyber security is relevant and necessary at all levels, to protect personal information in a private capacity and, largely at a Government level, to protect against cyber terrorism and the access of sensitive national information.

There is significant interest in the marketplace about business' abilities to appropriately deal with cyberattacks and breaches. Businesses within certain sectors of the economy, such as the financial sector, generally have sophisticated teams dedicated to building threat intelligence agendas and infrastructures. In such businesses, the strength of their cyber security capabilities provides a competitive advantage within the market.

Quantifying cybersecurity breaches in South Africa

- Malware attacks in SA increased by 22% in the first quarter of 2019 compared to the first quarter of 2018, translating to around 13 842 attempted cyberattacks per day.

- A data breach in South Africa costs an average of R36.5 million, and the long tail costs of a data breach can be felt for years after the incident. South Africa ranked 7 out of 16 countries polled for the highest cost of a cyber breach.

- In terms of the cost per record breached, South Africa ranks much higher at 11 on a scale of 16 polled countries, costing US$155 per record – the same as the UK and not that far behind the USA ($242 per record), which is alarming when you consider the size of the USA's economy compared to ours.

- In 2019, the average time to identity a breach in South Africa was 175 days and 56 days to contain it.
- Large businesses are not the only targets and hackers are indiscriminate: 43% of cyber-attacks target small businesses.

Why cybersecurity is so important

The sheer volume of threats is increasing rapidly. According to the report by McAfee, cybercrime stood at over $400 billion in 2019, while it was $250 billion two years ago. As demonstrated in the figures above, cyberattacks can be extremely expensive for businesses to endure. In addition to financial damage suffered by the business, a data breach can also inflict reputational damage. Cybercriminals are using increasingly sophisticated ways to initiate cyberattacks which are becoming progressively destructive. New regulations such as the Protection of Personal Information Act (POPIA), force business and governments to take better care of the personal information they hold.

The potential targets for cyberattacks

Any and all devices connected over the Internet or devices shared between users are potential targets for attackers. Cybercriminals attack an individual user's privacy, steal passwords, empty bank accounts or shop at the expense of the victim. The many connected devices used by individuals — including devices such as routers, tablets, CCTV cameras or PCs — if not appropriately secured, can be hijacked or attacked by cyber criminals.

Attackers try to steal business and personal secrets through infecting connected devices with viruses retrieving personal or business data and using this information to sabotage a business or access banking accounts or other information. In the case of attacking a state's infrastructure, power grids (such as in Ukraine in 2015) and even the entire Internet of another country (as was the case in Estonia in 2007) have been crippled.

Types of Viruses

Cybercrime and cyber attackers are always changing their approach as systems change. There are a variety of approaches used by cybercriminals to infect and access your personal and business devices. Shown below are some of the more common types of cyberthreats:

Malware

Malware, or malicious software, is a blanket term for any kind of computer software with malicious intent. Most online threats are some form of malware.

Hacking

Hacking refers to activities that seek to compromise digital devices, such as computers, smartphones, tablets, and even entire networks. Hackers are motivated by personal gain, to make a statement, or just because they can.

Adware

Adware is a form of malware that hides on your device and serves you advertisements. Some adware also monitors your behavior online so it can target you with specific advertisements.

Ransomware

Ransomware is an emerging form of malware that locks the user out of their files or their device, then demands an anonymous online payment to restore access.

Spyware

Spyware is a form of malware that hides on your device, monitors your activity, and steals sensitive information like bank details and passwords. These are sent out by your device to the creator of the spyware.

Phishing

Phishing is a method of tricking you into sharing passwords, credit card numbers, and other sensitive information by posing as a trusted institution in an email or phone call

Trojans

Trojans are programs that claim to perform one function but actually do another, typically malicious. Trojans can take the form of attachments, downloads, and fake videos/programs.

Spam

Spam is any kind of unwanted, unsolicited digital communication that gets sent out in bulk. This is more than a nuisance and remains a serious threat

Basic principles to protect yourself and your business

1) Antivirus software

Antivirus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more. It is important that all computers and mobile devices have some sort of antivirus software installed and this is updated regularly. Without this basic level of protection, your computer may be infected within minutes of accessing the internet.

Antivirus software providers release regular updates to ensure that they can detect and protect you from any possible attacks. Businesses and individuals must ensure that antivirus software is constantly updated as cyber criminals continuously look for new ways of breaching these anti-viruses and accessing your information. There are some credible free antivirus packages, as well as paid / subscription services.

2) External devices

Attackers can use USB and external hard-drives to infect computers with malware that can detect when the USB/external drive is plugged into a computer. The malware then downloads a malicious code onto the drive. When the USB/external drive is plugged into another computer, the malware infects that computer as well.

Here are a few tips to protect your data:

- Do not plug an unknown USB/external drive into your computer.
- If you have been given a USB drive for free or in an unsealed package, do not use it.
- Keep your business and personal USB drives separate.
- Maintain and ensure all security software is up to date.

3) Public WiFi

Along with the convenience of public WiFi hotspots be aware that they can also provide an easy way for identity thieves and cybercriminals to monitor what you're doing online and to steal your passwords, your personal information, or both. Never assume that a public WiFi network is safe or secure.

Follow these simple steps to protect yourself when using public WiFi:

- It is preferable not to access it but if you must, enable your Firewall.
- Turn off your file sharing.
- Ensure that there is an HTTPS in the browser bar when sending personal information over the internet.
- Turn off the automatic connection feature on your personal device.
- Ensure the antivirus software is updated.
- Do not share personal information on a public WiFi network.
- Use a Virtual Private Network (VPN) if you have one.

Password Protection

A **strong password** provides protection from fraud and identity theft. Breaking passwords could cause personal and financial complications to a business and individual. Guessing passwords is one of the most common ways hackers break into computers. It is critical that individuals use strong secure passwords on their personal and business devices, as well as on registered websites and apps i.e banking, email accounts etc.

Here are some suggestions to create a strong password:

- Choose complex passwords by combining uppercase, lower case, numbers and special characters.
- Using a phrase or a statement with spaces between words increases the complexity of the password. This is also known as a passphrase.
- Do not use personal information such as family names, birthdays, sports teams, pet names etc.
- Update and change your password regularly.
- Do not share your password with anybody ever, even people from the bank or your company IT person.
- Do not write or type your password in any journal, calendar, spreadsheet etc.
- Use an online random password phrase generator to generate a password / passphrase
- Change your passwords and passphrases regularly. If your system can enforce periodic password changes then implement this.

The Golden Rule of cybersecurity

The Golden Rule of cybersecurity is to be ever-vigilant. Criminals are forever looking for new ways to separate you from your assets— money, data, identity and other. At each turn, pause to consider what information you are providing, who is asking for it, and how it is being sought.

Additional resources

As more people and businesses embrace and adopt digital technologies accelerated by the Fourth Industrial Revolution and most recently the COVID-19 pandemic, it is essential that cybersecurity risks are understood and mitigated. In support of this, please listen to the webinar on cybersecurity (https://www.westerncape.gov.za/site-page/godigital-webinars), brought to you by the Department of Economic Development and Tourism, Digital Economy team.

Many other resources are available to research and read online, alternatively contact a cybersecurity specialist or company to help you determine any potential security gaps in your business and how best to alleviate and prevent them.

References

https://enterprise.verizon.com/resources/reports/dbir/

https://businesstech.co.za/news/it-services/257855/the-average-cost-of-a-data-breach-in-south-africa-hits-r36-5-million/

https://www.malwarebytes.com/cybersecurity/

Disclaimer: There are many website and Internet resources available and this article is by no means exhaustive. The information, company and brand names of many products and services are mentioned, without their express permission, and other companies and brands are available. The intent of providing this information is to inform the public and business communities, thereby driving digital adoption. Their understanding is greatly appreciated.