precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 14 October 2022

Today, we are going to focus on, our level of preparedness for cyberattacks in the Caribbean.

Dr. Ronald Walcott
Managing Director

In the Caribbean, we have been gradually growing and improving the amount of cybersecurity measures and infrastructure needed to protect individuals, businesses, and the government from malicious cyberattacks. Some countries have been taking greater measures than others. Countries such as Trinidad and Tobago, have taken the initiative and seen the importance of having good cybersecurity in place, before attacks occur. There are some companies that offer services to help businesses bolster their defenses in the event of a cyber-attack. These companies do different tests (penetration testing, vulnerability testing, etc) to find out the weak points in the current security implemented. They also install the best software that suits the needs of the business and help respond to attacks in the event that there is a breach. However, even with these measures and strategies in place, it does not completely stop cyberattacks from happening.

In an article released, 21st October 2022 by the Guardian Newspaper, it stated that Massy Stores is investigating claims that over 700,000 files containing customer personal information and employee information obtained in an attack earlier this year. On April 28th ,2022, Massy stores confirmed that it was the target of a cyberattack. The hackers dumped the data they found on the dark web. At the time of the breach in April, Massy denied the leak of sensitive information. However, it is undeniable that the data that has been dumped is Massy's data as experts says that it shows documents that bear the company's markings.

DO WE HAVE INFRASTRUCTURE, TECHNOLOGY AND SKILLS LOCALLY (WITHIN THE CARIBBEAN) IN PLACE TO COMBAT CYBERCRIMES AND ATTACKS?

The first Security Operations Centre (SOC) in the Caribbean region is being established in Trinidad by none other than Precision Cybertechnologies and Digital Solutions Ltd. This SOC will help monitor and respond to any irregular cyber activities that may occur on their client's networks. A team of highly skilled Analysts would be monitoring and responding to any threats/attacks that may occur. Of course, companies are encouraged to practice good cybersecurity policies and procedures as well to even further mitigate potential attacks.

Alongside Precision, Digicel has also begun offering cybersecurity ser-

In this Issue:

Headline News:

UK Firm Fined for Poor Security Prior to Ransomware Attack

Britain's data watchdog levied a 4.4 million-pound fine against a facilities management outsourcing and construction firm for a ransomware attack that exposed employee data.

Hackers penetrated Interserve Group Limited in late March 2020, breaching the confidentiality of four human resources databases containing personal data of 113,000 employees. The fine, which is approximately US$5 million, should "cause directors and chairmen to sit up and start asking questions of chief executives about cyber preparedness," U.K. Information Commissioner John Edwards told The Guardian.

Among the exposed data were contact details and identifying information including birthdate as well as sensitive data such as marital status, dependents and salary amounts.

The U.K. Information Commissioner's Office says the company failed to put appropriate security measures in place to prevent the intrusion, including by running unsupported versions of the Windows server operating system and using an outdated version of McAfee antivirus software.

Attackers got into company systems via a phishing email with a malicious .zip file attached. The company did not enable host-based firewalls at the time of the incident nor did it prevent macros from executing on the computer of the employee who opened the phishing email, the ICO says. The company also had 280 users with domain administration permissions, a number the ICO says was excessive. Hackers compromised 12 of those accounts.

A cybersecurity tool did detect the initial infection, but it wrongly reported the malware as having been successfully removed. The company didn't verify the tool's actions, and the attacker retained access.

The office cites the General Data Protection Regulation as the legal basis for the fine - a European Commission regulation that the United Kingdom incorporated as domestic law in 2018 ahead of its withdrawal from the European Union. Adherence to the GDPR is a cornerstone of a June 2021 agreement that allows commercial data flows to continue crossing the English Channel.

Members of the U.K. Conservative Party, which currently controls Parliament, have put continued adherence to the GDPR in doubt. Secretary of State for Digital, Culture, Media and Sport Michelle Donelan during the annual party conference earlier this month announced an effort to replace the GDPR with a "truly bespoke British system of data protection."

The ICO says the company didn't just violate continental standards but also its internal policies for systems management, which required it to keep servers up to date on patches and to have malware protection.

At the time of the attack, Interserve was processing personal data on 18 servers whose operating system was Windows Server 2003 R2, for which Microsoft withdrew mainstream support in 2010. Another 22 servers ran on Windows Server 2008 R2, for which Microsoft terminated mainstream support in 2015. At the time of the attack, the company also widely deployed network file sharing protocol Server Message Block version 1. Microsoft deprecated SMBv1 in 2013.

Whether Interserve pays the fine is an open question. The company is the successor of Interserve Plc, a company that went into the U.K. version of bankruptcy in March 2019. Its construction business has spun off into a company that assumed a previous Interserve corporate identity of Tilbury Douglas while its outsourcing components have been acquired by other companies.

Source: https://www.databreachtoday.com/

Cyberattack preparedness in the Caribbean... cont'd

vices within the Caribbean. Digicel is also establishing a SOC within the Caribbean, however it is not known exactly where the SOC is located. By such a large networking firm branching off its resources into this sphere, we can clearly tell that the frequency of cyber-attacks has been increasing and how important it is for us all to protect our information from cyber criminals.

These companies are also partnered with other companies in other countries within the Caribbean and LATAM regions to provide cybersecurity for businesses

HOW DOES HAVING THE CYBER SECURITY MEASURES/RESOURCES IN PLACE LOCALLY BENEFIT US INDIVIDUALS AND BUSINESSES?

It is becoming even more necessary to have better and more security measures in place for your information. Hackers are becoming more and more innovative with their scripts and methods to access people's sensitive information. Knowing this, it is safe to say that having good cybersecurity measures and resources available is extremely important and beneficial to both individuals and businesses.

Here are some ways in which both individuals and businesses benefit from this:

- Software blocks previously known malware and methods of attacks as well as new attacks and malware. SIEMs act as a real-time monitoring tool and is operated by AI and machine learning. Eg. Splunk, Elastic Stack, QRadar
- Saves people and businesses from facing dire consequences in the future such as having their data leaked or held hostage and having their services (cloud, credit card, etc) become unavailable for a period of time. All these things are very frustrating and can take a long time to recover from.
- Significantly reduce the risk of having your sensitive information leaked. (Banking, address, phone number, credit card number, etc.)

Frequently Asked Questions:

HOW OFTEN DO CYBERATTACKS OCCUR WITHIN THE CARIBBEAN REGION?

Cyberattacks are becoming more and more frequent within the Caribbean region as time goes on. Cybercriminals are always looking to expand their scope and target businesses and people that may be less secure.

WHAT ARE SOME RAMIFICATIONS OF BEING TARGETED BY CYBERCRIMINALS?

If cybercriminals are able to break through your security (passwords, firewall, antivirus, etc.) they can get access to and use information that can cripple people's and businesses lives. Some of this information may include banking information (credit card info, bank account number, etc.), personal information (name, age, address, etc.) and also employee account information (usernames, passwords, etc.). This information is supposed to be confidential and protected, therefore if this information is leaked while under the watch of one party, they can be held accountable by law in some instances.

Upcoming Events

AMCHAM/ HSSE CONFERENCE 26TH ANNUAL HEALTH, SAFETY, SECURITY AND ENVIRONMENT (HSSE) CONFERENCE & EXHIBITION. RE-IMAGINING HSSE

1st and 2nd November, 2022 Location: Hyatt Regency

TT CHAMBER OF INDUSTRY AND COMMERCE CRIME & JUSTICE COMMITTEE IN CONJUNCTION WITH PCDS WILL HOST A BREAKFAST TABLE DISCUSSION ON SECURING YOUR DIGITAL PRESENCE. –

4th November 2022 at the TT Chamber headquarters, Columbus Circle Westmoorings.

868-610-7237

sales@precision-cyber.com

www.precision-cyber.com

1st Floor, Brair Place, 10-12 Sweet Road
St. Clair, Port of Spain, Trinidad