precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 27 November 2023

In today's issue of our newsletter, we will be looking at the Increasing number of Cyberattacks in Trinidad. We will also be looking at the impact these attacks have and what can be done to mitigate the risk of these attacks occurring.

Dr. Ronald Walcott
Managing Director

INTRODUCTION

As the digital surface is ever expanding, there has been increasing connectedness of our global landscape. In Trinidad and Tobago, this has brought about changes and advancements which transform the way we communicate, conduct business and navigate our lives. However, along with this transformation increases the attack surface for cyber-attacks and threats. As the nation embraces the benefits of technological progress, it grapples with the darker side of connectivity—cyberattacks that pose substantial risks to individuals, businesses, and critical infrastructure. Trinidad has been a target for hacking groups in recent times.

There have been several instances of large organizations falling victim to cyber-attacks in recent times. These organizations were targeted by various hacker groups. These groups are responsible for exfiltrating, encrypting, locking information and resources such as endpoints, servers, customer lines, ID scans, gitlab projects and database dumps. Sometimes, these organizations do not publicly comment on the claims of compromise made, since there is no provisioning in the Data Protection Act which mandates that they must notify the victims of the data breach. These hacker groups demand that companies pay them a ransom and threaten to release the contents of the data/information that they got their hands on, if the ransom was not paid. In instances where information is released on the dark web, we can assume that the ransom was not paid since a lot of PII (Personal Identifiable Information) was released on the dark web. This usually has serious backlash on companies if victims find that their sensitive information was released.

We can see that even large organizations can fall victim to cyber-attacks. Some of the types of attacks and sectors they occur in, are as follows:

1. **Ransomware Attacks on Businesses:** Cybercriminals may target businesses in Trinidad with ransomware, encrypting critical data and demanding a ransom for its release. Such attacks can disrupt operations and lead to significant financial losses.
2. **Ransomware Attacks on Businesses:** Cybercriminals may target businesses in Trinidad with ransomware, encrypting critical data and demanding a ransom for its release. Such attacks can disrupt operations and lead to significant financial losses.

CONTINUED ON PAGE 2

In this Issue:

IMPACT OF THESE ATTACKS

The impact of cyberattacks can be multifaceted, affecting individuals, businesses, and the overall economic and societal landscape. Here are some common impacts associated with various types of cyberattacks:

Financial Losses:
Businesses may suffer significant financial losses due to disruptions in operations, the cost of remediation, and potential legal consequences. Ransomware attacks, in particular, often demand payments in cryptocurrency, adding another layer of complexity to financial recovery.

Data Breaches and Privacy Violations:
The compromise of sensitive information through data breaches can lead to severe privacy violations. Individuals may experience identity theft, financial fraud, or other forms of exploitation.

Operational Disruption:
Cyberattacks can disrupt day-to-day operations, affecting productivity and service delivery. In critical infrastructure sectors, such as energy or healthcare, the consequences of disruptions can be especially severe and may impact public safety.

Reputation Damage:
Businesses and organizations may suffer reputational damage in the aftermath of a cyberattack. Loss of trust from customers, clients, and partners can have long-term consequences on brand reputation.

MITIGATE THE RISK OF THESE ATTACKS OCCURRING

Mitigating the risk of cyberattacks involves a combination of proactive measures, cybersecurity best practices, and ongoing vigilance. Here are key strategies that individuals, businesses, and organizations can adopt to enhance their cybersecurity posture:

1. **Educate and Train Employees:** Conduct regular cybersecurity awareness training for employees to recognize and avoid phishing attacks, use strong passwords, and follow best practices for online security.
2. **Implement Strong Access Controls:** Enforce the principle of least privilege, ensuring that individuals have the minimum level of access required for their roles. Regularly review and update access permissions.
3. **Keep Software and Systems U dated:** Regularly update operating systems, software, and applications to patch vulnerabilities. Enable automatic updates whenever possible to ensure timely protection against known security threats.
4. **Use Antivirus and Anti-Malware Solutions:** Deploy reputable antivirus and anti-malware solutions to detect and mitigate threats. Keep these security tools updated to defend against evolving cyber threats.

Frequently Asked Questions:

WHAT CAN BE DONE TO REDUCE THE IMPACT IF AN ATTACK IS SUCCESSFUL?

1. **Back Up Data Regularly:** Conduct regular backups of critical data and ensure that backup systems are secure. In the event of a ransomware attack or data loss, having up-to-date backups can facilitate quick recovery.
2. **Establish an Incident Response Plan:** Develop and regularly test an incident response plan that outlines the steps to be taken in the event of a cyber incident. This includes communication protocols, roles and responsibilities, and procedures for containing and mitigating the impact of an attack.

WHAT KIND OF TECHNOLOGY CAN BE EMPLOYED TO HELP MITIGATE THE RISK OF AN ATTACK?

1. **Monitor Network Traffic using AI:** Implement robust network monitoring to detect unusual or suspicious activities. Intrusion detection systems and security information and event management (SIEM) solutions can help identify potential threats in real-time.
2. **Secure Endpoint Devices:** Ensure that all devices connected to the network, including computers, mobile devices, and IoT devices, are secure. Use endpoint protection solutions to detect and prevent malware infections.
3. **Firewalls:** These devices are configured to enforce rules on a network that protect you against suspicious activity.

WHAT IS THE AVERAGE COST TO RECOVER AFTER A CYBER-ATTACK?

There is no one set cost. The cost varies depending on multitude of variables such as the amount of endpoint devices affected, the amount of information stolen or locked, the criticality of the attack in regard to the functionality of basic everyday functions, etc. and most of all, how valuable is the data and resources to you, the company. For example, attacks can cost companies a couple hundred thousand to hundreds of millions of dollars (USD) because the data and resources are worth that much to them to regain.

Headline News

Hackers claim ransomware attack on TSTT

Reports of the breach were made three days ago. Lyndersay wrote of it on his site, technewstt.com.

In that article, Lyndersay said, "According to FalconFeeds.IO, a cyber security firm that offers a Twitter feed reporting on breaches, tstt.co.tt and bmobile.co.tt were compromised, with a reported 6GB of customer lines, ID scans, gitlab projects and database dumps as part of the haul."

A check of FalconFeeds.io twitter account on October 27 said, "Ransomexx #ransomware group has added Telecommunications Services of Trinidad and Tobago (http://tstt.co.tt) to their victim list. They claim to have access to 6GB of organisations (sic) data."

There has been no official word from the Telecommunications Services of Trinidad and Tobago (TSTT) on the matter and calls to its CEO Lisa Agard went unanswered. Calls to Minister of Public Utilities Marvin Gonzales also went unanswered.

In a phone interview on Sunday, Lyndersay said, "It is an issue of customer privacy and the customer's right to know."

With ransomware, if the ransom is not paid the data is released, he said.

This has happened before in TT and Jamaica, he added.

"Before they release the data, it is customary that a ransomware organisation will produce proof with a selection of the data they exfiltrated (withdraw surreptitiously) which they post to the dark web to say, 'Yes we have your data. Now pay us.'

"In that cache of exfiltrated data that was posted as proof is a 300mb file that has got the personal identifiable information of 800,000 TSTT customers," Lyndersay said.

This meant phone numbers, addresses, IDs etc.

Last year, there were reports of a malware incursion into its software. In later reports the company said it never paid a ransom and got international cyber security experts to help with the matter.

Lyndersay said that there was no legal requirement under TT's laws for a company or government agency to disclose that they were hacked and data stolen.

Dlapiperdataprotection.com, a website which monitors data protection laws around the world, says that there was no provision in the Data Protection Act of notifying data subjects of the Information Commissioner of a security breach.

"That is the law in Barbados and I believe, I can't say for sure about Jamaica but I also believe it has been made law in Jamaica but it is not a law in TT. There is no legal requirement to disclose."

Lyndersay said he believes this is in draft bills but it has not been passed into law. He believes it should be law because if people's personal information have been stolen, they should at least know it has happened.

He said his biggest concern was that he began posting about it 24 hours ago and thinks that a lot of people do not understand what has happened.

The real-world implications for this kind of issue are if the data is available and people could make use of it, then, it needed to be considered exactly what kind of use they would make of it.

Lyndersay said people needed to be aware that they have a right to privacy and, when not enshrined in law, should be interested that it becomes so.

Upcoming Events

FRAUD, SECURITY AND RISK MANAGEMENT SUMMIT
February 13th, 2024
New York

CYBERSECURITY SUMMIT
June 20th, 2024
North America Midwest

HEALTHCARE CYBERSECURITY SUMMIT
July 18th, 2024
New York