precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 9 April 2022

Shaping the Future of Cybersecurity

Dr. Ronald Walcott
Managing Director

One of the most remarkable achievements coming out of the pandemic was the ability of organizations to remain productive with the acceleration of the global adoption of digital transformation. Commendably, technology departments figured out ways to allow executives to grant unprecedented flexibility to their employees during the pandemic. With the acceleration of digital transformation and increased online presence, businesses are now more vulnerable to cybercrime attacks. Cybersafety continues to be overlooked by many organizations in both the private and public sectors. Organizations must take a more careful review of their cybersecurity needs to support their digital presence. Cybersecurity attacks can have a disastrous impact on an organization, resulting in revenue losses, denial of service (DOS), reputational impact, and legal issues, among many other challenges. There are undoubtedly many benefits from the shift in workplace protocols, but when any technology is adopted as rapidly as we took to remote work, vulnerabilities and criminal elements looking to exploit them soon follow.

What we are seeing now in recent times is that Cybercriminals are recognizing that many organizations' networks lack the security to safeguard against the cracks exposed by new remote workplace practices in three key areas. We draw your attention to the recent attacks on Costa Rica declared a national emergency after a massive hack across multiple ministries, including the digital systems of Costa Rica's treasury ministry, "Ministerio de Hacienda", hit by the Conti Ransomware, a Russian-based Cyber organization.

Precision Cybertechnologies and Digital Solutions is aiming to generate more cybersecurity awareness in Trinidad and Tobago and the region by extension. Their goal is to enable any enterprise to proactively eliminate security gaps, defend against hackers' malicious intentions, and minimize the enterprise risk with 24x7 monitoring and high-quality incident response and mediation. Since its inception, Precision has conducted multiple assessments and provided innovative and cost-effective cybersecurity and digital solutions and services to small, medium, and large enterprises.

In this Issue:

Over the last year, Precision has developed key partnerships and alliances with internationally recognized organizations that support every cybersecurity and digital solution offered.

Join PCDS on Monday, June 13th, as they bring a host of international speakers for their webinar "Shaping the Future of Cybersecurity" to discuss how organizations can become more diligent about stopping cybercrime while maintaining flexibility and digital transformation strategies. According to Managing Director Dr Ronald Walcott," remote work isn't going anywhere, neither are cybercriminals. Although workers may be headed back to their office jobs, many of them will, no doubt, have flexible hours when needed. What this has alluded to is an era where cybercrime has moved into a new phase, and the best way for organizations to stay vigilant is to prioritize security as they've never done before." **Registration is available at www.precision-cyber.com or you can email info@precision-cyber.com for further details.**

As we prepare for our webinar, we'd like to give a refresher to help you follow along during our webinar.

LET'S TALK RANSOMWARE

What is it?

Ransomware is a type of malware than encrypts user data and prevents access until a ransom payment is made. There are many techniques used to gain access and spread this malware such as phishing and social engineering.

While an easy fix might be to pay, there is no guarantee that they will follow through after payment. It's always good to keep in mind that you're dealing with cybercriminals.

Types of Ransomware

There are various types of ransomware, the most common of those can be seen below.

Crypto ransomware

Crypto ransomware prevents access to files or data through encryption with a different randomly generated symmetric key for each file. The symmetric key is then encrypted with a public asymmetric key; attackers then demand the ransom payment for access to the asymmetric key.

Doxware

Doxware is a form of crypto ransomware where victims are threatened with not only losing access to their files, but also having their private files and data made public through "doxing".

Locker ransomware

Locker ransomware locks the computer or device by preventing users from logging in; an infected machine can display an official looking message warning the user. This type of malware does not actually encrypt files on the device.

Here are a few tips to help prevent and mitigate the loss of ransomware

- Harden Endpoints
- Offline backups
- Restricted access to management infrastructure
- Develop and test with an incident response plan
- Utilize an identity and access management program

Upcoming Events

SHAPING THE FUTURE OF CYBERSECURITY
June 13, 2022 (PCDS)
www.precision-cyber.com

FRAUD SUMMIT
JUNE 16, 2022

NORTHEAST US CYBERSECURITY SUMMIT
June 21, 2022

Frequently Asked Questions:

WHAT ARE THE IMPACTS OF RANSOMWARE?

Ransomware can be devastating to an individual or an organization. Some victims pay to recover their files, but there is no guarantee that they will recover their files if they do. Recovery can be a difficult process that may require the services of a reputable data recovery specialist.

Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. The monetary value of ransom demands has increased, with some demands exceeding $1 million. Ransomware incidents have become more destructive and impactful in nature and scope. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small.

WHAT ARE SOME MITIGATIONS AGAINST RANSOMWARE?

CISA recommends the following precautions to protect users against the threat of ransomware:

- Update software and operating systems with the latest patches. Outdated applications and operating systems are the target of most attacks.
- Never click on links or open attachments in unsolicited emails.
- Back up data on a regular basis. Keep it on a separate device and store it offline.
- Follow safe practices when using devices that connect to the Internet

Headline News:

U.S. Sets Up Multiagency Initiatives to Curb Ransomware

The U.S. is setting up a Joint Ransomware Task Force, headed by the Cybersecurity and Infrastructure Security Agency and the FBI, as well as two international initiatives, chaired by the Department of Justice, to tackle illegal cryptocurrency activities related to ransomware.

The announcement was made at the Institute for Security and Technology event celebrating the one-year anniversary of the Ransomware Task Force. The task force comprises industry, government and civil society members to counter the ransomware threat. It was set up by the Department of Justice in March 2021.

RANSOMWARE INITIATIVE

The Joint Ransomware Task Force was set up under the guidance of the Cyber Incident Reporting for Critical Infrastructure Act of 2022, an omnibus spending bill passed last month. The bill required CISA to launch a program that would coordinate federal efforts to warn organizations of vulnerabilities that ransomware actors could likely exploit.

CISA Director Jen Easterly, at the Friday event, said: "Given what's in that legislation and what the Task Force is envisioned to do - there's a lot of disruption of ransomware actors infrastructure, finances - I thought it was really important that the FBI co-chairs."

The group, she said, will hold its first official meeting in the next few months. "It's very likely that industry is going to see a cyberattack on the homeland before we see it... We have to be in the same room. We have to trust each other."

SOURCE: https://www.databreachtoday.com

868-610-7237 | salesinfo@precision-cyber.com | www.precision-cyber.com | 1st Floor, Brair Place, 10-12 Sweet Road St. Clair, Port of Spain, Trinidad