Kevane Grant Thornton

Advisory

Organizations

Cybersecurity

Increase preparedness for Cybersecurity attacks

March 10, 2022

In the recent events between Ukraine and Russia, the government and private organizations observed an increase in cybersecurity attacks that has been mostly used to target organizations in Ukraine and that may spread to other countries.

Some of the new attacks detected during the recent events include:

- WhisperGate, a malware intended to render targeted devices inoperable.
- HermeticWiper, a malware being used to target Windows devices, manipulating the master boot record, which results in subsequent boot failure.

Destructive malware can present a direct threat to an organization's daily operations, impacting the availability of critical assets and data. These and other malwares represent a threat to business operations that may impact the availability of important assets and sensitive information. Organizations should increase awareness and assess their capabilities including planning, preparation, detection, and response for these types of events.

There are specific actions that organizations may do to reinforce logical security controls and strengthen the security of your infrastructure. You may want to prioritize in the following controls:

- security awareness – communicate with your employees and consultants to be aware of any e-mail attacks such as phishing, business email compromise (BEC) and ransomware. they are organization's first line of defense.
- identity access – strengthen password policies and ensure Multi-factor Authentication (MFA) is used for all cloud and remote access services.
- vulnerability management – ensure all assets are being scanned for vulnerabilities and patches are being applied. Critical vulnerabilities must be remediated immediately.
- malware updates – ensure all organization devices are up-to-date and with the latest virus definition.

In addition, it is also important, that organizations create or update their Cybersecurity Program. A good program must include, at least, the following components:

- a management oversight of cybersecurity activities.
- adopt cybersecurity framework (i.e., NIST, CIS Controls, COBIT that is followed to design, implement, and monitor cybersecurity controls).
- designate a management level individual responsible for the cybersecurity program.
- establish a cybersecurity team (whether internal or outsourced) with the appropriate skills and appropriate reporting structure for designing, implementing, and monitoring cybersecurity controls.

- periodic assessment of the information technology (IT) environment for cybersecurity threats and vulnerabilities including, but not limited to, performing vulnerability and penetration testing.

It is also particularly important that upper management is in constant communication with the Cybersecurity team and that software vendors ensure active monitoring in order to make sure security controls are established and working as intended. In addition, the Incident Response Plan should be reviewed to ensure that new possible attack scenarios are identified, and response scenarios documented with possible response activities are discussed and approved.

The following is a list of resources that can help you increase your Cybersecurity controls and awareness:

- CyberSecurity & Infrastructure Security Agency (Homepage | CISA)
- National Institute of Standards and Technology (NIST) – Cybersecurity
- Center for Internet Security (CIS) – CIS Critical Security Controls v8
- National Institute of Standards and Technology (NIST) – Computer Security Incident Handling Guide

Resource:

Destructive Malware Targeting Organizations in Ukraine | CISA

We are committed to keep you updated of all developments that may affect the way you do business in Puerto Rico. Please contact us for assistance in relation to this or any other matter, we will be glad to assist you.

Marta Rodríguez
Partner Head of Advisory
E marta.rodriguez@pr.gt.com

Roberto Luciano
Audit and Advisory Partner
E roberto.luciano@pr.gt.com

Jorge Paredes
Advisory Manager
E jorge.paredes@pr.gt.com

Kevane Grant Thornton

grantthornton.pr