Regulatory Authority of Curaçao

ADVISORY ON RANSOMWARE PREPAREDNESS

JULY 28, 2025

TLP: GREEN

INTRODUCTION

In light of recent developments indicating an increased cyber threat landscape targeting organizations across our island, the Regulatory Authority of Curaçao / CARICERT is issuing this formal advisory on ransomware preparedness. This advisory aims to promote enhanced cyber hygiene practices and bolster resilience against malicious cyber actors. The threat of ransomware is both real and imminent, and as such, all organizations must adopt a proactive approach to safeguard their digital infrastructure.

SITUATION OVERVIEW

The limited availability of IT vendors and services on the island has led to a high degree of uniformity in IT environments across various sectors. Consequently, it is reasonable to assume that many organizations share similar configurations of hardware and software. This uniformity, combined with possible shortcomings in system hardening and patch management, increases the collective vulnerability of our digital ecosystem.

THREAT ASSESSMENT

Malicious actors continue to exploit vulnerable IT environments to extort organizations. They may target specific users, groups, or vulnerable applications to achieve their objectives. IT environments that are connected to the Internet and lack the necessary security measures are particularly vulnerable. Currently, various ransomware groups are actively scanning and targeting domains and IP addresses in Curaçao.

RISKS

As previously noted, vulnerable IT systems connected to the Internet, are inherently susceptible to cyberattacks. When cyber security best practices are not followed, and systems remain unpatched or misconfigured, the attack surface significantly increases.

There is a high realistic risk that your sensitive data may be encrypted and rendered inaccessible. This specific form of cyber extortion is known as Ransomware. The purpose of such attacks is to exert pressure on the targeted organization by disrupting operations (e.g. Denial of Service), threatening to publicly disclose stolen sensitive information, and ultimately extorting individuals whose personal information is among the exfiltrated content. Typically, the attackers demand payment in cryptocurrency. The consequences for the affected organization include severe operational disruption, substantial financial losses, and long-term reputational damage.

RECOMMENDED ACTIONS

We strongly urge all organizations to adopt the following comprehensive measures without delay:

COMPREHENSIVE MEASURE 1

ACCESS MANAGEMENT

- Review all (user) accounts on domain controller, servers, firewall, switches, laptops and cloud accounts.
- Remove unused and inactive/dormant accounts.
- Apply the principle of least privilege for the admin accounts.
- Proactively monitor and review high privilege accounts.

COMPREHENSIVE MEASURE 2

SYSTEM AND NETWORK SECURITY

- Harden all layers of your infrastructure.
- Use the latest versions of all software: applications, security tools, management tools, monitoring tools, virtualization tools, security devices and back-up tools.
- Keep all systems and (security) tools regularly updated and patched.
- Divide your network in segments with rules regulating the traffic between these segments and devices.
- Use secured DNS (filter) services (e.g. Cloudflare, Google, Quad9 and OpenDNS).

COMPREHENSIVE MEASURE 3

AUTHENTICATION AND BACKUP

- Implement strong passwords in combination with 2FA and conditional access.
- Establish a comprehensive and adequate back-up strategy and hardware to be able to restore operations soon and minimize downtime.
- Define clear and proper Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) based on your business continuity needs.
- Make sure you have offnet (airgapped/cut-off or your internal network) and offsite backup files of data and system configuration.
- Ensure critical data backups are protected from modification or deletion (use immutable back-up feature or data-diodes).

COMPREHENSIVE MEASURE 4

DATA PROTECTION

- Utilize data leakage and Personal Identifiable Information (PII) detection tools.
- Sensitive data and classified information must be protected by encryption to minimize the impact of potential data breaches.
- Review contracts with (cloud) service providers to ensure robust back-up and recovery agreements.
- Store physical (hard)copies of critical documents (contracts, insurance policies, banking details, licenses, contact lists etc.) securely in a physical safe.
- Organizations using Microsoft cloud services and other datacenters for back-up should also revisit all recommendations as these cloud solutions are not fully hardened and secured by default.

COMPREHENSIVE MEASURE 5

MONITORING AND DETECTION

- Regularly review scheduled tasks on servers for unfamiliar or suspicious activity.
- Deploy tools to monitor or detect (mass) changes across your IT environment.
- Conduct regular logfile analysis, preferably using automated tools enhanced with AI and SIEM capabilities.
- Use detection and response tools like MDR, XDR and EDR.
- Subscribe to a dark web monitoring service to monitor your domain name.

COMPREHENSIVE MEASURE 6

EMAIL AND ENDPOINT PROTECTION

- Educate your employees about cybersecurity hygiene and the risks of interacting with emails or attachments from unknown sources.
- Train your staff to recognize phishing emails and report suspicious communications.
- Implement the needed countermeasures for your email environment: SPF, DKIM and DMARC.
- Consider labeling emails received from outside your organization.
- Use mail content scanner and disable active hyperlinks in incoming emails.
- Avoid uncontrolled use of remote monitoring and management tools (RMM).
- Regularly review VPN usage and remove unnecessary access.
- Never store/save passwords in web browsers.

COMPREHENSIVE MEASURE 7

POLICY AND RESPONSE PLANNING

- Perform regular security audits.
- Proactively review and update your firewall configurations.
- Ensure critical events are logged with adequate retention policies.
- Regularly, test the back-up restore procedure and the recovery plan.
- Maintain, test and review your incident response plan to ensure organizational readiness.

FURTHER READING AND SUPPORT

For additional resources and best practices on ransomware prevention, visit:
www.caricert.cw/ransomware/

For questions or to report incidents, please contact us at:

General inquiries : info@caricert.cw | info@rac.cw
Incident reporting : cert@caricert.cw
Website : caricert.cw | rac.cw

Published by RAC / CARICERT
Regulatory Authority of Curaçao / National Cyber Emergency Response Team