ΚΥΠΡΙΑΚΟ
ΕΜΠΟΡΙΚΟ ΚΑΙ
ΒΙΟΜΗΧΑΝΙΚΟ
ΕΠΙΜΕΛΗΤΗΡΙΟ

01/11/21

Προς: Όλα τα Μέλη

Απο: Τμήμα Υπηρεσιών, Εμπορίου & Ψηφιοποίησης

Θέμα: Αντιμετωπίζοντας επιθέσεις Ransomware

Αγαπητά μέλη,

Σας αποστέλλεται πιο κάτω ενημέρωση από την Πρεσβεία των Ηνωμένων Πολιτειών Αμερικής στην Κύπρο, αναφορικά με τρόπους αντιμετώπισης κυβερνοεπιθέσεων ransomware.

Η συγκεκριμένη μέθοδος κυβερνοεπίθεσης χρησιμοποιείται από τους hackers για εκβιασμούς, αφού το συγκεκριμένο κακόβουλο λογισμικό κλειδώνει την οθόνη ή κρυπτογραφεί τα δεδομένα που είναι αποθηκευμένα. Η επίθεση ολοκληρώνεται με απαίτηση για καταβολής λύτρων με αναλυτικές λεπτομέρειες πληρωμής, αφήνοντας τα δεδομένα κλειδωμένα μέχρι το θύμα να προχωρήσει σε πληρωμή.

Με εκτίμηση,

Πόλυς Περατικός
Ανώτερος Λειτουργός

ΚΥΠΡΙΑΚΟ
ΕΜΠΟΡΙΚΟ ΚΑΙ
ΒΙΟΜΗΧΑΝΙΚΟ
ΕΠΙΜΕΛΗΤΗΡΙΟ

Info on cybersecurity (ransomware)

In case you are not able to open the document I sent earlier, here's the info in text below. Thanks. Ephie

Dealing with Ransomware

What is Ransomware?

Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. 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 US $1 million. Ransomware incidents have become more destructive and impactful in nature and scope.
https://www.cisa.gov/stopransomware/ransomware-101

Looking to learn more about this growing cyber threat?

- The Ransomware Guide from the Cybersecurity and Infrastructure Security (CISA) and the MS-ISAC (Multi-State Information Sharing & Analysis Center) is a great place to start. Released in September 2020, this joint Ransomware Guide includes industry best practices and a response checklist that can serve as a ransomware-specific addendum to organization cyber incident response plans.
- The U.S. Secret Service provides a guide that describes what actions organizations should take to cultivate an understanding of the technological and regulatory limitations, responsibilities, and resources available to them, and how to apply the acquired knowledge to their operations.
- NIST's CSF Ransomware Profile can be applied to organizations using or looking to use the NIST Cybersecurity Framework.

How Do I Avoid Being Hit by Ransomware?

There are several no-cost resources to help you take a proactive approach to protecting your organization against ransomware. You can find Ransomware prevention best practices, tips, services, and other related information here: https://www.cisa.gov/stopransomware/how-can-i-protect-against-ransomware

I Have Been Hit by Ransomware – What Can I do?

- **RANSOMWARE RESPONSE CHECKLIST**

The Cybersecurity and Infrastructure Security Agency (CISA) strongly recommends responding to ransomware by using the following checklist provided in a Joint CISA and Multi-State Information Sharing and Analysis Center (MS-ISAC) Ransomware Guide. This information will take you through the response process from detection to containment and eradication. Be sure to move through the first three steps in sequence.