TLP: WHITE

Σημασία των πολιτικών και διαδικασιών κυβερνοασφάλειας

NCC ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ Αρχή Ψηφιακής Ασφάλειας

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

ncc.cy

Περιεχόμενο

TLP: WHITE

01 Εισαγωγή

02 Πολιτικές κυβερνοασφάλειας

03 Διαδικασίες κυβερνοασφάλειας

04 Πολιτικές διαχείρισης κινδύνων

05 Εφαρμογή και συμμόρφωση

06 Πόροι και εργαλεία

07 Συμπέρασμα

1 Εισαγωγή

- Οι πολιτικές και οι διαδικασίες κυβερνοασφάλειας είναι κρίσιμες για τη δημιουργία ενός ασφαλούς οργανωτικού περιβάλλοντος και την προστασία των ευαίσθητων δεδομένων.
- Διασφαλίζουν τη συμμόρφωση με νομικές απαιτήσεις και βοηθούν στη μείωση των κινδύνων που σχετίζονται με τις κυβερνοαπειλές.
- Οι οργανισμοί αντιμετωπίζουν απειλές όπως το phishing, το κακόβουλο λογισμικό, το ransomware και τις εσωτερικές απειλές.
- Οι ισχυρές πολιτικές κυβερνοασφάλειας βοηθούν στην προστασία από αυτές τις απειλές, εξασφαλίζοντας τη συνέχεια των επιχειρηματικών λειτουργιών.

2 Πολιτικές κυβερνοασφάλειας

Πολιτική Αποδεκτής Χρήσης

TLP: WHITE

Ορίζει την αποδεκτή χρήση των οργανωτικών πόρων και συστημάτων πληροφορική

Στοιχεία πολιτικής:

- Οι χρήστες πρέπει να χρησιμοποιούν τους πόρους πληροφορικής μόνο για εξουσιοδοτημένους σκοπούς.
- Απαγορευμένες δραστηριότητες περιλαμβάνουν την πρόσβαση σε ακατάλληλο περιεχόμενο, παράνομες δραστηριότητες και μη εξουσιοδοτημένη κοινοποίηση ευαίσθητων πληροφοριών.
- Συνέπειες για παραβιάσεις της πολιτικής.

NCC ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ
ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ Αρχή Ψηφιακής Ασφάλειας
Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης
ncc.cy

Πολιτική Κωδικών Πρόσβασης

TLP: WHITE

Καθορίζει τις απαιτήσεις για τη δημιουργία και διαχείριση κωδικών πρόσβασης

Στοιχεία πολιτικής:

- Οι κωδικοί πρόσβασης πρέπει να έχουν τουλάχιστον 12 χαρακτήρες και να περιλαμβάνουν συνδυασμό γραμμάτων, αριθμών και ειδικών χαρακτήρων.
- Οι κωδικοί πρόσβασης πρέπει να αλλάζουν κάθε 90 ημέρες.
- Ενθαρρύνεται η χρήση διαχειριστών κωδικών πρόσβασης.
- Απαγόρευση κοινοποίησης κωδικών πρόσβασης.

Πολιτική Ελέγχου Πρόσβασης

Ορίζει τον τρόπο με τον οποίο παρέχεται και διαχειρίζεται η πρόσβαση σε πληροφορίες και συστήματα.

Στοιχεία πολιτικής:

- Πρόσβαση βάση της αρχής της ελάχιστης προνομίας.
- Εφαρμογή ελέγχου πρόσβασης βάση ρόλων (RBAC).
- Τακτική αναθεώρηση και ανάκληση δικαιωμάτων πρόσβασης για πρώην υπαλλήλους.

Πολιτική Προστασίας Δεδομένων

TLP: WHITE

Περιγράφει τα μέτρα για την προστασία ευαίσθητων δεδομένων.

Στοιχεία πολιτικής:

- Οδηγίες ταξινόμησης και διαχείρισης δεδομένων.
- Απαιτήσεις κρυπτογράφησης για δεδομένα σε κατάσταση αδράνειας και σε μεταφορά.
- Διαδικασίες ασφαλούς διάθεσης δεδομένων.

Πολιτική Απόκρισης σε Περιστατικά

Παρέχει οδηγίες για την ανταπόκριση σε περιστατικά κυβερνοασφάλειας.

Στοιχεία Πολιτκής:

- Διαδικασίες αναγνώρισης και αναφοράς περιστατικών.
- Ρόλοι και ευθύνες της ομάδας απόκρισης σε περιστατικά.
- Βήματα για τον περιορισμό, την εξάλειψη και την αποκατάσταση από περιστατικά.

Πολιτική Απομακρυσμένης Εργασίας

TLP: WHITE

Θέτει τις απαιτήσεις για ασφαλείς πρακτικές απομακρυσμένης εργασίας.

Στοιχεία πολιτικής:

- Χρήση VPN για απομακρυσμένη πρόσβαση.
- Ασφαλής διαμόρφωση των απομακρυσμένων συσκευών.
- Οδηγίες για τη διαχείριση ευαίσθητων πληροφοριών εκτός γραφείου.

NCC ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ Αρχή Ψηφιακής Ασφάλειας

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

ncc.cy

Πολιτική Διαχείρισης Προμηθευτών

TLP: WHITE

Διασφαλίζει ότι οι τρίτοι προμηθευτές συμμορφώνονται με τα πρότυπα κυβερνοασφάλειας.

Στοιχεία πολιτικής:

- Αξιολόγηση κινδύνου προμηθευτών και διεξοδικός έλεγχος.
- Μέτρα ασφαλείας στις συμβάσεις με προμηθευτές.
- Τακτική παρακολούθηση και έλεγχοι των πρακτικών ασφάλειας των προμηθευτών.

NCC ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ
ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ Αρχή Ψηφιακής Ασφάλειας
Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης
ncc.cy

TLP: WHITE

Πολιτική Χρήσης Ηλεκτρονικού Ταχυδρομείου και Επικοινωνίας

Ορίζει την ασφαλή χρήση του ηλεκτρονικού ταχυδρομείου και των εργαλείων επικοινωνίας.

Στοιχεία πολιτικής:

- Χρήση ασφαλών καναλιών επικοινωνίας.
- Απαγόρευση αποστολής ευαίσθητων πληροφοριών μέσω μη κρυπτογραφημένων emails.
- Ευαισθητοποίηση για phishing και διαδικασίες αναφοράς περιστατικών.

3 Διαδικασίες Κυβερνοασφάλειας

NCC ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ Αρχή Ψηφιακής Ασφάλειας

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

ncc.cy

Αξιολόγηση και Διαχείριση Κινδύνων

Συστηματική διαδικασία για την ταυτοποίηση, αξιολόγηση και μείωση των κινδύνων.

Βήματα Διαδικασίας:

- Διεξαγωγή τακτικών αξιολογήσεων κινδύνων για την ταυτοποίηση πιθανών απειλών.
- Αξιολόγηση της πιθανότητας και της επίδρασης των εντοπισμένων κινδύνων.
- Ανάπτυξη και εφαρμογή στρατηγικών μείωσης κινδύνων.
- Παρακολούθηση και επανεξέταση των κινδύνων περιοδικά.

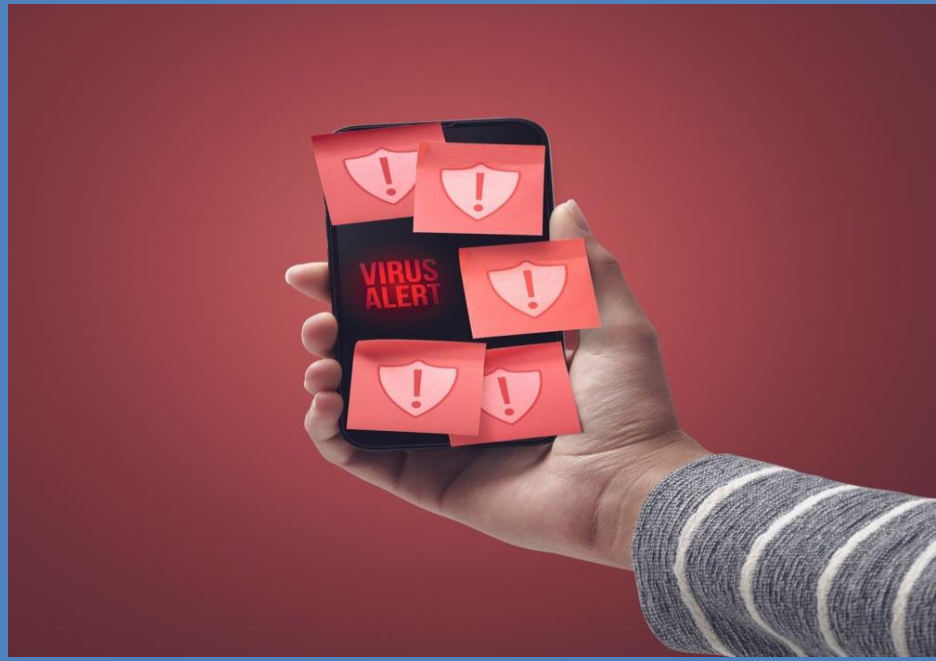
TLP: WHITE

Εκπαίδευση και Ευαισθητοποίηση Εργαζομένων

Προγράμματα εκπαίδευσης για την ενημέρωση των εργαζομένων σχετικά με τις πρακτικές κυβερνοασφάλειας.

Βήματα Διαδικασίας:

- Διεξαγωγή τακτικών συνεδριών εκπαίδευσης σχετικά με την κυβερνοασφάλεια.
- Εφαρμογή προσομοιώσεων phishing και ασκήσεων.
- Παροχή πόρων και υλικών σχετικά με τις βέλτιστες πρακτικές και τις νέες απειλές.



NCC ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ
ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ Αρχή Ψηφιακής Ασφάλειας
Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης
ncc.cy

Διαδικασίες Αντιμετώπισης Περιστατικών

Βήματα για την αντιμετώπιση ενός περιστατικού κυβερνοασφάλειας.

Βήματα Διαδικασίας:

- Άμεση αναφορά του περιστατικού στην ομάδα ανταπόκρισης.
- Απομόνωση των επηρεαζόμενων συστημάτων για την αποφυγή περαιτέρω ζημιών.
- Διενέργεια προκαταρκτικής αξιολόγησης για την κατανόηση της έκτασης και της επίδρασης.
- Εξάλειψη της απειλής και αποκατάσταση των επηρεαζόμενων συστημάτων.
- Τεκμηρίωση του περιστατικού και διεξαγωγή ανασκόπησης μετά το περιστατικό.

Διαδικασίες Δημιουργίας Αντιγράφων Ασφαλείας και Ανάκτησης Δεδομένων

TLP: WHITE

Εξασφάλιση της διαθεσιμότητας και ακεραιότητας των δεδομένων μέσω τακτικών αντιγράφων ασφαλείας.

Βήματα Διαδικασίας:

- Εφαρμόστε αυτοματοποιημένες λύσεις δημιουργίας αντιγράφων ασφαλείας για κρίσιμα δεδομένα.
- Αποθηκεύστε τα αντίγραφα ασφαλείας σε ασφαλείς τοποθεσίες εκτός του οργανισμού.
- Δοκιμάστε τακτικά τις διαδικασίες δημιουργίας αντιγράφων ασφαλείας και ανάκτησης δεδομένων.
- Τεκμηριώστε τα προγράμματα και τις διαδικασίες δημιουργίας αντιγράφων ασφαλείας.

NCC ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ
ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ Αρχή Ψηφιακής Ασφάλειας
Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης
ncc.cy

Διαχείριση Ενημερώσεων Λογισμικού και Επιδιορθώσεων

Διατήρηση της ασφάλειας του συστήματος μέσω τακτικών ενημερώσεων.

Βήματα διαδικασίας:

- Ενεργοποιήστε τις αυτόματες ενημερώσεις για λειτουργικά συστήματα και εφαρμογές.
- Εξετάζετε και εφαρμόζετε τακτικά τις επιδιορθώσεις ασφάλειας.
- Διατηρήστε μια απογραφή του λογισμικού για την παρακολούθηση των ενημερώσεων και των τρωτών σημείων.

Διαδικασίες Ασφαλείας Δικτύου

Προστασία της δικτυακής υποδομής
από μη εξουσιοδοτημένη πρόσβαση.

Βήματα Διαδικασίας:

- Διαμορφώστε και διατηρήστε τα firewalls για τον έλεγχο της κυκλοφορίας του δικτύου.
- Εφαρμόστε τον διαχωρισμό του δικτύου για να περιορίσετε την πρόσβαση σε ευαίσθητες περιοχές.
- Παρακολουθήστε τη δραστηριότητα του δικτύου για ύποπτη συμπεριφορά.
- Διεξάγετε τακτικές αξιολογήσεις ευπάθειας και δοκιμές διείσδυσης.

4 Πολιτικές Διαχείρισης Κινδύνου

NCC ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ
ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ Αρχή Ψηφιακής Ασφάλειας
Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης
ncc.cy

Πολιτικές Διαχείρισης Κινδύνου

1. Αναγνώριση Κινδύνου

Διαδικασία για την αναγνώριση πιθανών κινδύνων κυβερνοασφάλειας.

- Τακτική αναθεώρηση και ενημέρωση του καταλόγου κινδύνων.
- Συμμετοχή των ενδιαφερομένων μερών σε δραστηριότητες αναγνώρισης κινδύνων.
- Χρήση πληροφοριών απειλών για να παραμείνετε ενημερωμένοι για νέες απειλές.

2. Αξιολόγηση Κινδύνων

Αξιολόγηση της πιθανότητας και του αντίκτυπου των αναγνωρισμένων κινδύνων.

- Διεξάγετε ποιοτικές και ποσοτικές αξιολογήσεις κινδύνων.
- Δώστε προτεραιότητα στους κινδύνους βάσει του πιθανού αντίκτυπου τους.
- Τεκμηριώστε τα ευρήματα των αξιολογήσεων και ενημερώστε τα μητρώα κινδύνων.

Πολιτικές Διαχείρισης Κινδύνου

3. Μετριασμός Κινδύνων

Εφαρμογή στρατηγικών για τη μείωση της έκθεσης σε κινδύνους.

- Αναπτύξτε και εφαρμόστε σχέδια μετριασμού κινδύνων.
- Αναθέστε την ιδιοκτησία και την ευθύνη για τους κινδύνους.
- Παρακολουθήστε την αποτελεσματικότητα των στρατηγικών μετριασμού και προσαρμόστε τις εάν χρειάζεται.

4. Παρακολούθηση και Αναφορά Κινδύνων

Συνεχής παρακολούθηση και αναφορά της κατάστασης των κινδύνων.

- Καθιερώστε βασικούς δείκτες κινδύνου (KRIs) για την παρακολούθηση των επιπέδων κινδύνου.
- Αναθεωρείτε και ενημερώνετε τακτικά τις αναφορές διαχείρισης κινδύνων.
- Επικοινωνήστε την κατάσταση των κινδύνων με τη διοίκηση και τα ενδιαφερόμενα μέρη.

5 Εφαρμογή και Συμμόρφωση

NCC ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ
ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας
Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης
ncc.cy

Βήματα Εφαρμογής Πολιτικών και Διαδικασιών Κυβερνοασφάλειας

TLP: WHITE

Οδηγίες για την εφαρμογή μέτρων κυβερνοασφάλειας.

Βήματα Εφαρμογής:

- Εξασφαλίστε την υποστήριξη της διοίκησης και κατανείμετε πόρους.
- Αναπτύξτε ένα λεπτομερές σχέδιο υλοποίησης με χρονοδιαγράμματα και αρμοδιότητες.
- Επικοινωνήστε τις πολιτικές και τις διαδικασίες σε όλους τους υπαλλήλους.
- Παρέχετε εκπαίδευση και υποστήριξη για να διασφαλίσετε την κατανόηση και τη συμμόρφωση.

NCC ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ Αρχή Ψηφιακής Ασφάλειας

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

ncc.cy

Διασφάλιση Συμμόρφωσης και Τακτικές Αναθεωρήσεις

Διατήρηση της συμμόρφωσης με τις πολιτικές και τις διαδικασίες.

Βήματα Συμμόρφωσης:

- Διεξαγωγή τακτικών ελέγχων και αξιολογήσεων για τη διασφάλιση της συμμόρφωσης.
- Χρήση αυτοματοποιημένων εργαλείων για την παρακολούθηση της συμμόρφωσης με τις πολιτικές.
- Αντιμετωπίστε τα ζητήματα μη συμμόρφωσης άμεσα και αποτελεσματικά.

Συνεχής Βελτίωση

Τακτική ενημέρωση και βελτίωση των μέτρων κυβερνοασφάλειας.

Βήματα Βελτίωσης:

- Μείνετε ενημερωμένοι σχετικά με νέες απειλές και βέλτιστες πρακτικές.
- Ζητήστε ανατροφοδότηση από υπαλλήλους και ενδιαφερόμενα μέρη.
- Αναθεωρείτε και ενημερώνετε τακτικά τις πολιτικές και τις διαδικασίες.

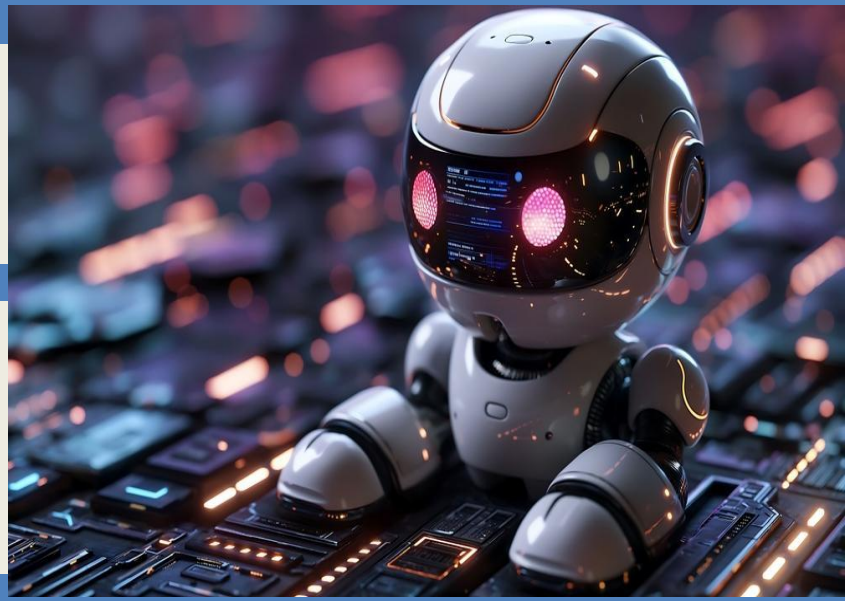
6 Πόροι και εργαλεία

NCC ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ
ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ Αρχή Ψηφιακής Ασφάλειας
Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης
ncc.cy

Συνιστώμενα Εργαλεία και Λύσεις όπως και Κυβερνητικοί και Βιομηχανικοί Πόροι

TLP: WHITE

Λίστα εργαλείων για την υποστήριξη των προσπαθειών κυβερνοασφάλειας.	• Λογισμικό Αντιιών • Firewalls • Εργαλεία Κρυπτογράφησης • Λύσεις Αντιγράφων Ασφαλείας
Σύνδεσμοι προς χρήσιμους πόρους και κατευθυντήριες γραμμές.	• Κυπριακή Αστυνομία - Τμήμα Κυβερνοεγκλήματος • Κυπριακή Ομάδα Αντιμετώπισης Περιστατικών Κυβερνοασφάλειας (CY-CERT) • Ευρωπαϊκός Οργανισμός για την Κυβερνοασφάλεια (ENISA)



7 Συμπέρασμα

- Η εφαρμογή ισχυρών πολιτικών κυβερνοασφάλειας είναι ζωτικής σημασίας για την προστασία των οργανισμών από τις κυβερνοαπειλές και την εξασφάλιση της προστασίας των κρίσιμων περιουσιακών στοιχείων.
- Η συμμόρφωση με τις κατευθυντήριες γραμμές αυτού του εγγράφου ενισχύει τη στάση κυβερνοασφάλειας και διατηρεί ένα ασφαλές περιβάλλον μέσω συνεχούς βελτίωσης και τακτικών αναθεωρήσεων.
- Ο οδηγός παρέχει ένα ολοκληρωμένο πλαίσιο για τη δημιουργία και διατήρηση αποτελεσματικών πολιτικών και διαδικασιών κυβερνοασφάλειας.
- Αυτές οι κατευθυντήριες γραμμές βοηθούν τους οργανισμούς να μειώσουν τους κινδύνους, να προστατεύσουν ευαίσθητες πληροφορίες και να βελτιώσουν τη συνολική τους κυβερνοασφάλεια.

Ευχαριστούμε

NCC
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΚΥΠΡΟΥ

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ
Αρχή Ψηφιακής Ασφάλειας

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

ncc.cy

References

- Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*, *57*, 14-30. https://doi.org/10.1016/j.cose.2015.11.001 (Introduction)

- Alhogail, A. (2020). Developing a cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003. https://doi.org/10.1016/j.cose.2020.102003 (Cybersecurity Policies)

- Disterer, G. (2019). ISO/IEC 27000, 27001, and 27002 for information security management. *Journal of Information Security and Applications*, *46*, 27-37. https://doi.org/10.1016/j.jisa.2019.02.002 (Cybersecurity Procedures)

References

- Shedden, P., Ruighaver, A. B., & Ahmad, A. (2016). Risk management standards – The perception of ease of use. *Computers & Security*, *57*, 90-110. https://doi.org/10.1016/j.cose.2015.12.001 (Risk Management Policies)

- Tounsi, W., & Rais, H. (2020). A cybersecurity culture framework for assessing organization preparedness. *Journal of Information Security and Applications*, *53*, 102526. https://doi.org/10.1016/j.jisa.2020.102526 (Implementation and Compliance)

- Sari, A., & Azad, M. A. (2019). An integrated cybersecurity risk management approach for a cyber-physical system. *Journal of Information Security and Applications*, *46*, 193-208. https://doi.org/10.1016/j.jisa.2019.02.007 (Conclusion)