Κυβερνοασφάλεια για ΜμΕ

Οδηγός

NCC ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

ncc.cy

Περιεχόμενα

01

Εισαγωγή

Η σημασία της Κυβερνοασφάλειας για ΜμΕ

Η κυβερνοασφάλεια είναι ζωτικής σημασίας για τις μικρές και μεσαίες επιχειρήσεις (ΜμΕ), καθώς όλο και περισσότερο γίνονται στόχος των κυβερνοεπιθέσεων. Η προστασία της επιχείρησής σας από τις κυβερνοαπειλές μπορεί να αποτρέψει οικονομικές απώλειες, να προστατεύσει τα δεδομένα των πελατών και να διατηρήσει την φήμη της επιχείρησής σας.

Επισκόπηση του Τοπίου Κυβερνοασφάλειας στην Κύπρο

Η Κύπρος, όπως και πολλές άλλες περιοχές, αντιμετωπίζει έναν αυξανόμενο αριθμό κυβερνοαπειλών. Οι ΜμΕ είναι ιδιαίτερα ευάλωτες λόγω περιορισμένων πόρων και έλλειψης ενημέρωσης. Η κατανόηση αυτών των απειλών και η λήψη προληπτικών μέτρων είναι απαραίτητη για την προστασία της επιχείρησής σας.

Βασικές Αρχές Κυβερνοασφάλειας

02

Βασικές Έννοιες της Κυβερνοασφάλειας

Η κυβερνοασφάλεια περιλαμβάνει την προστασία συστημάτων, δικτύων και δεδομένων από ψηφιακές επιθέσεις. Οι κύριες έννοιες περιλαμβάνουν:

• Εμπιστευτικότητα: Διασφάλιση ότι οι πληροφορίες είναι προσβάσιμες μόνο σε εκείνους που έχουν εξουσιοδοτημένη πρόσβαση.

• Ακεραιότητα: Προστασία των δεδομένων από μη εξουσιοδοτημένη αλλοίωση ή καταστροφή.

• Διαθεσιμότητα: Εξασφάλιση ότι τα δεδομένα και οι υπηρεσίες είναι διαθέσιμα στους εξουσιοδοτημένους χρήστες όταν χρειάζονται.

Είδη Κυβερνοαπειλών

Η κυβερνοασφάλεια περιλαμβάνει την προστασία συστημάτων, δικτύων και δεδομένων από ψηφιακές επιθέσεις. Οι κύριες έννοιες περιλαμβάνουν:

- Κακόβουλο Λογισμικό (Malware): Κακόβουλο λογισμικό που σχεδιάστηκε για να προκαλέσει βλάβη, διακοπή ή μη εξουσιοδοτημένη πρόσβαση σε υπολογιστικά συστήματα.
- Ransomware: Ένα είδος κακόβουλου λογισμικού που κρυπτογραφεί τα αρχεία του θύματος και απαιτεί λύτρα για το κλειδί αποκρυπτογράφησης.
- Phishing: Προσπάθειες για την απόκτηση ευαίσθητων πληροφοριών με την προσποίηση αξιόπιστης οντότητας.

03

Μέτρα Κυβερνοασφάλειας για ΜμΕ

Ασφάλεια Δικτύου

Τείχη Προστασίας (Firewalls)

Ένα τείχος προστασίας είναι μια συσκευή ασφάλειας δικτύου που παρακολουθεί και ελέγχει την εισερχόμενη και εξερχόμενη κίνηση δικτύου βάσει προκαθορισμένων κανόνων ασφαλείας. Λειτουργεί ως φράγμα μεταξύ του εσωτερικού σας δικτύου και εξωτερικών πηγών, φιλτράροντας την κίνηση για να αποτρέψει μη εξουσιοδοτημένη πρόσβαση.

Προστασία Δεδομένων

Κρυπτογράφηση Δεδομένων

Η κρυπτογράφηση ευαίσθητων δεδομένων είναι απαραίτητη για την προστασία τους από μη εξουσιοδοτημένη πρόσβαση.

Βήματα Δράσης:

• Χρησιμοποιήστε εργαλεία κρυπτογράφησης για την κρυπτογράφηση δεδομένων σε αδράνεια και κατά τη μεταφορά.
• Ενημερώνετε τακτικά τα κλειδιά κρυπτογράφησης.
• Εκπαιδεύστε τους υπαλλήλους για τη σημασία της κρυπτογράφησης δεδομένων.

Προστασία Δεδομένων

Ασφαλή Αντίγραφα Ασφαλείας

Η τακτική δημιουργία αντιγράφων ασφαλείας των δεδομένων και η ασφαλής αποθήκευση αυτών των αντιγράφων είναι κρίσιμη για την πρόληψη απώλειας δεδομένων.

Βήματα Δράσης:

- Εφαρμόστε μια αυτοματοποιημένη λύση δημιουργίας αντιγράφων ασφαλείας.
- Αποθηκεύστε τα αντίγραφα ασφαλείας σε μια ασφαλή, απομακρυσμένη τοποθεσία.
- Δοκιμάζετε τακτικά τα αντίγραφα ασφαλείας για να διασφαλίσετε ότι τα δεδομένα μπορούν να αποκατασταθούν.

Έλεγχος Πρόσβασης

Πολιτικές Κωδικών Πρόσβασης

Οι ισχυροί κωδικοί πρόσβασης είναι απαραίτητοι για την προστασία λογαριασμών και συστημάτων.

Βήματα Δράσης:
• Επιβάλετε τη χρήση σύνθετων κωδικών πρόσβασης (τουλάχιστον 12 χαρακτήρες, περιλαμβάνοντας γράμματα, αριθμούς και ειδικούς χαρακτήρες).
• Εφαρμόστε τακτικές αλλαγές κωδικών πρόσβασης.
• Εκπαιδεύστε τους υπαλλήλους για τη σημασία της χρήσης μοναδικών κωδικών πρόσβασης για διαφορετικούς λογαριασμούς.

Έλεγχος Πρόσβασης

Πολυπαραγοντική Πιστοποίηση (MFA)

Προσθέστε ένα επιπλέον επίπεδο ασφάλειας απαιτώντας πολλαπλές μορφές επαλήθευσης.

Βήματα Δράσης:
- Εφαρμόστε την πολυπαραγοντική πιστοποίηση (MFA) για όλα τα κρίσιμα συστήματα.
- Χρησιμοποιήστε MFA για απομακρυσμένη πρόσβαση και ευαίσθητες εφαρμογές.
- Αναθεωρείτε και ενημερώνετε τακτικά τις ρυθμίσεις της MFA.

Αντιμετώπιση Περιστατικών

Η ύπαρξη ενός σχεδίου για την αντιμετώπιση κυβερνοπεριστατικών μπορεί να ελαχιστοποιήσει τις ζημιές.

Βήματα Δράσης:

- Αναγνώριση και περιορισμός του περιστατικού.
- Ενημέρωση των σχετικών εμπλεκομένων μερών.
- Εξάλειψη της αιτίας του περιστατικού και ανάκτηση των επηρεασμένων συστημάτων.
- Διενέργεια ανασκόπησης μετά το περιστατικό για να εντοπιστούν τα διδάγματα που αποκομίστηκαν.

Σχεδιασμός Αντιμετώπισης Περιστατικών

Αναπτύξτε ένα ολοκληρωμένο σχέδιο αντιμετώπισης περιστατικών για να διασφαλίσετε την ετοιμότητα.

Βήματα Δράσης:
• Ορίστε ρόλους και ευθύνες για την αντιμετώπιση περιστατικών.
• Αναπτύξτε διαδικασίες για την ανίχνευση, την ανταπόκριση και την ανάκαμψη από περιστατικά.
• Δοκιμάζετε και ενημερώνετε τακτικά το σχέδιο αντιμετώπισης περιστατικών.

Επισκόπηση Σχετικών Κανονισμών (π.χ., GDPR)
Κατανοήστε και συμμορφωθείτε με τις νομικές απαιτήσεις που σχετίζονται με την προστασία δεδομένων και την ιδιωτικότητα.

Βέλτιστες Πρακτικές για ΜμΕ

04

Εκπαίδευση Εργαζομένων

1. Προγράμματα Ευαισθητοποίησης για την Κυβερνοασφάλεια

Εκπαιδεύστε τους εργαζομένους σχετικά με τους κινδύνους και τις βέλτιστες πρακτικές της κυβερνοασφάλειας.

Βήματα Δράσης:

- Διεξάγετε τακτικές εκπαιδεύσεις ευαισθητοποίησης για την κυβερνοασφάλεια.
- Παρέχετε πόρους και υλικά για τις κοινές απειλές.
- Ενθαρρύνετε μια κουλτούρα ευαισθητοποίησης για την ασφάλεια.

Εκπαίδευση Εργαζομένων

2. Προσομοιώσεις Phishing

Δοκιμάστε και βελτιώστε την ικανότητα των εργαζομένων να αναγνωρίζουν τις απόπειρες phishing.

Βήματα Δράσης:

- Διεξάγετε τακτικές προσομοιώσεις phishing.
- Παρέχετε ανατροφοδότηση και πρόσθετη εκπαίδευση βάσει των αποτελεσμάτων των προσομοιώσεων.
- Επιβραβεύστε τους εργαζομένους που επιδεικνύουν ισχυρή ευαισθητοποίηση για την ασφάλεια.

Τακτικές Ενημερώσεις και Διαχείριση Ενημερώσεων

Σημασία της Διατήρησης Ενημερωμένων Λογισμικών και Συστημάτων

Τα λογισμικά και τα συστήματα για την προστασία από ευπάθειες πρέπει να ενημερώνωνται τακτικά.

Βήματα Δράσης:
• Ενεργοποιήστε αυτόματες ενημερώσεις για λειτουργικά συστήματα και εφαρμογές.
• Αναθεωρείτε και εφαρμόζετε τακτικά ενημερώσεις ασφαλείας.
• Διατηρείτε ένα απόθεμα λογισμικών και υλικού για την παρακολούθηση των ενημερώσεων

Ασφαλείς Πρακτικές Εργασίας από Απόσταση

1. VPNs

Χρησιμοποιήστε εικονικά ιδιωτικά δίκτυα (VPNs) για την ασφάλεια των απομακρυσμένων συνδέσεων.

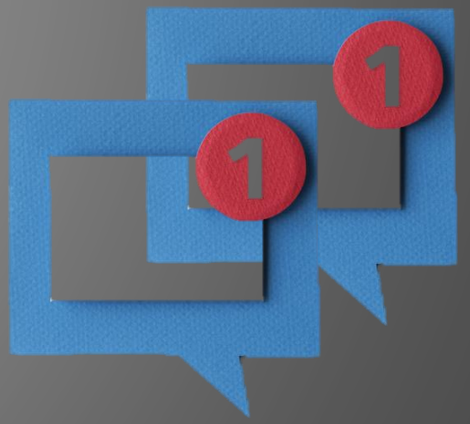
Βήματα Δράσης:
• Εφαρμόστε μια λύση VPN για τους απομακρυσμένους εργαζομένους.
• Απαιτήστε από τους εργαζομένους να χρησιμοποιούν το VPN για την πρόσβαση στους πόρους της εταιρείας.
• Ενημερώνετε και παρακολουθείτε τακτικά τη λύση VPN.

Ασφαλείς Πρακτικές Εργασίας από Απόσταση

2. Ασφαλή Εργαλεία Επικοινωνίας

Εφαρμόστε ασφαλή εργαλεία για απομακρυσμένη επικοινωνία και συνεργασία.

Βήματα Δράσης:
• Χρησιμοποιήστε κρυπτογραφημένα εργαλεία επικοινωνίας (π.χ., ασφαλή email, εφαρμογές μηνυμάτων).
• Εκπαιδεύστε τους εργαζομένους στη χρήση των ασφαλών εργαλείων επικοινωνίας.
• Αναθεωρείτε και ενημερώνετε τακτικά τις πολιτικές ασφαλείας επικοινωνιών.



Διαχείριση Κινδύνων από Προμηθευτές και Τρίτους

1. Αξιολόγηση Ασφάλειας Τρίτων

Αξιολογήστε τις πρακτικές κυβερνοασφάλειας των προμηθευτών και συνεργατών.

Βήματα Δράσης:
• Διεξάγετε αξιολογήσεις ασφαλείας των τρίτων προμηθευτών.
• Συμπεριλάβετε απαιτήσεις κυβερνοασφάλειας στα συμβόλαια με τους προμηθευτές.
• Αναθεωρείτε και ενημερώνετε τακτικά τις πρακτικές ασφαλείας των προμηθευτών.

Διαχείριση Κινδύνων από Προμηθευτές και Τρίτους

2. Συμβόλαια και Συμφωνίες Επιπέδου Υπηρεσιών (SLAs)

Συμπεριλάβετε απαιτήσεις κυβερνοασφάλειας στα συμβόλαια και τις συμφωνίες επιπέδου υπηρεσιών (SLAs).

Βήματα Δράσης:
- Ορίστε τις προσδοκίες και τις ευθύνες ασφάλειας στα συμβόλαια.
- Παρακολουθείτε τη συμμόρφωση με τις συμβατικές απαιτήσεις ασφάλειας.
- Αναθεωρείτε και ενημερώνετε τακτικά τα συμβόλαια και τις SLAs.

05

Πόροι και Εργαλεία

Πόροι Κυβερνοασφάλειας για Βασική Προστασία

- Λογισμικό Antivirus
- Τείχη Προστασίας (Firewalls)
- Εργαλεία Κρυπτογράφησης
- Λύσεις Αντιγράφων Ασφαλείας

Κυβερνητικοί Πόροι

- Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος Κύπρου: Παρέχει υποστήριξη και πόρους για περιστατικά ηλεκτρονικού εγκλήματος.
- Ομάδα Αντιμετώπισης Εκτάκτων Αναγκών Πληροφορικής Κύπρου (CY-CERT): Προσφέρει καθοδήγηση και υπηρεσίες αντιμετώπισης περιστατικών.

Μελέτες Περίπτωσης και Παραδείγματα

06

Πραγματικά Παραδείγματα Κυβερνοπεριστατικών που Επηρέασαν ΜμΕ στην Κύπρο

Παράδειγμα 1: Μια τοπική ΜμΕ έπεσε θύμα επίθεσης ransomware, με αποτέλεσμα την κρυπτογράφηση κρίσιμων επιχειρηματικών δεδομένων. Η εταιρεία αναγκάστηκε να πληρώσει σημαντικά λύτρα για να ανακτήσει την πρόσβαση στα δεδομένα της. Αυτό το περιστατικό θα μπορούσε να είχε αποφευχθεί με τακτικά αντίγραφα ασφαλείας δεδομένων και εκπαίδευση των εργαζομένων στην αναγνώριση phishing emails.

Παράδειγμα 2: Μια άλλη ΜμΕ υπέστη παραβίαση δεδομένων λόγω αδύναμων πρακτικών κωδικών πρόσβασης. Οι κυβερνοεγκληματίες απέκτησαν πρόσβαση στο δίκτυο της εταιρείας χρησιμοποιώντας έναν συμβιβασμένο λογαριασμό εργαζομένου με αδύναμο κωδικό πρόσβασης. Η εφαρμογή ισχυρών πολιτικών κωδικών πρόσβασης και πολυπαραγοντικής πιστοποίησης θα μπορούσε να είχε αποτρέψει αυτή την παραβίαση.

Διδάγματα και Συμβουλές Πρόληψης

• Τακτικά Αντίγραφα Ασφαλείας Δεδομένων (Backups): Διασφαλίστε ότι τα δεδομένα δημιουργούνται αντίγραφα ασφαλείας τακτικά και αποθηκεύονται με ασφάλεια.

• Εκπαίδευση Εργαζομένων: Διεξάγετε τακτικές εκπαιδευτικές συνεδρίες για την αναγνώριση κυβερνοαπειλών και την τήρηση των βέλτιστων πρακτικών.

• Ισχυρές Πολιτικές Κωδικών Πρόσβασης: Επιβάλετε τη χρήση ισχυρών, μοναδικών κωδικών πρόσβασης και εφαρμόστε πολυπαραγοντική πιστοποίηση.

• Σχεδιασμός Αντιμετώπισης Περιστατικών: Αναπτύξτε και δοκιμάζετε τακτικά ένα σχέδιο αντιμετώπισης περιστατικών για να διασφαλίσετε την ετοιμότητα.

07

Κυβερνο-Υγιεινή

Πλαίσιο Κυβερνο-Υγιεινής

• Πολιτική Ασφάλειας

Η ανώτερη διοίκηση του οργανισμού έχει δημιουργήσει, εγκρίνει και επικοινωνήσει την πολιτική κυβερνοασφάλειας εσωτερικά και εξωτερικά. Η πολιτική κυβερνοασφάλειας πρέπει να αναθεωρείται τουλάχιστον μία φορά το χρόνο και να ενημερώνεται όπως απαιτείται.

• Ευαισθητοποίηση και Εκπαίδευση

Το προσωπικό που απασχολείται από τον οργανισμό και οι χρήστες που έχουν πρόσβαση στις πληροφορίες του (ανεξάρτητα από τη σχέση απασχόλησης) πρέπει να είναι ενήμεροι για την ασφάλεια των πληροφοριών και, ιδιαίτερα, για το πώς συμβάλλουν σε αυτήν μέσω του ρόλου τους. Κατάλληλες δραστηριότητες ευαισθητοποίησης για την κυβερνοασφάλεια πρέπει να διεξάγονται τακτικά και τουλάχιστον μία φορά το χρόνο.

Πλαίσιο Κυβερνο-Υγιεινής

• Ενημέρωση Λογισμικού
Τα συστήματα πληροφορικής και επικοινωνιών του οργανισμού πρέπει να έχουν εγκατεστημένες τις τελευταίες ενημερώσεις ασφαλείας που παρέχονται μόνο από αξιόπιστες πηγές (π.χ., τον κατασκευαστή).

• Προστασία από Κακόβουλο Λογισμικό
Προγράμματα και λειτουργίες προστασίας από κακόβουλο λογισμικό είναι εγκατεστημένα σε όλα τα συστήματα πληροφορικής και επικοινωνιών του οργανισμού. Οι ενημερώσεις γίνονται τακτικά.

Πλαίσιο Κυβερνο-Υγιεινής

• Ασφάλεια Δικτύου

Ο οργανισμός έχει εγκαταστήσει και διαμορφώσει τείχη προστασίας (firewalls) σε κατάλληλα σημεία στο δίκτυό του, προκειμένου να προστατεύει αποτελεσματικά τα συστήματα και τις πληροφορίες του από σχετικές απειλές.

• Αντίγραφα Ασφαλείας

Ο οργανισμός αναγνωρίζει τις κρίσιμες πληροφορίες του και δημιουργεί αντίγραφα ασφαλείας των κρίσιμων πληροφοριών τακτικά, σύμφωνα με την αντίστοιχη πολιτική αντιγράφων ασφαλείας.

Πλαίσιο Κυβερνο-Υγιεινής

• Περιστατικά Ασφάλειας
Ο οργανισμός έχει δημιουργήσει μια δομή και διαδικασία για την ανταπόκριση σε περιστατικά ασφάλειας. Το προσωπικό που εμπλέκεται στις αντίστοιχες διαδικασίες είναι κατάλληλα εκπαιδευμένο.

• Μέτρα Φυσικής Ασφάλειας
Ο οργανισμός έχει υιοθετήσει μέτρα φυσικής ασφάλειας για την προστασία των συστημάτων και των εγκαταστάσεων από φυσικές και περιβαλλοντικές απειλές.

• Προστασία Δεδομένων
Ο οργανισμός πρέπει να σχεδιάσει, να υλοποιήσει, να υιοθετήσει και να δημοσιεύσει μια Πολιτική Προστασίας Προσωπικών Δεδομένων βασισμένη στον γενικό κανονισμό GDPR.

Πλαίσιο Κυβερνο-Υγιεινής

• Ανάλυση Επιχειρησιακού Αντικτύπου
Ο οργανισμός έχει σχεδιάσει και υλοποιήσει μια κατάλληλη μεθοδολογία για την ανάλυση επιχειρησιακού αντικτύπου. Τα αποτελέσματα και οι βασικοί δείκτες που προκύπτουν από την εφαρμογή της μεθοδολογίας καταγράφονται, διατηρούνται και τροφοδοτούν τον σχεδιασμό σχετικών μέτρων και υλοποιήσεων.

• Έλεγχος Πρόσβασης
Ο οργανισμός πρέπει να αναγνωρίζει τα σημεία όπου βρίσκονται σημαντικές πληροφορίες. Για τις πληροφορίες αυτές και βάσει του τύπου, της χρήσης και της κρισιμότητας, ο οργανισμός έχει δημιουργήσει μια δομή σε κατάλληλο χώρο αποθήκευσης, η οποία του επιτρέπει να παραχωρεί δικαιώματα πρόσβασης σε εξουσιοδοτημένους και πιστοποιημένους χρήστες, ακολουθώντας την αρχή της ανάγκης γνώσης (need-to-know).

08

Συμπέρασμα

Ανακεφαλαίωση της Σημασίας της Κυβερνοασφάλειας

Η κυβερνοασφάλεια είναι κρίσιμη για την προστασία της επιχείρησής σας από οικονομικές απώλειες, παραβιάσεις δεδομένων και ζημιά στη φήμη. Με την εφαρμογή των μέτρων που περιγράφονται σε αυτόν τον οδηγό, οι ΜμΕ στην Κύπρο μπορούν να ενισχύσουν σημαντικά την κυβερνοασφάλειά τους.

Ενθάρρυνση για την Εφαρμογή του Πλαισίου Κυβερνο-Υγιεινής

Λάβετε προληπτικά μέτρα για να προστατεύσετε την επιχείρησή σας ακολουθώντας τις συστάσεις αυτού του οδηγού. Αναθεωρείτε και ενημερώνετε τακτικά τις πρακτικές κυβερνοασφάλειας σας για να παραμένετε μπροστά από τις αναδυόμενες απειλές. Θυμηθείτε, η κυβερνοασφάλεια είναι μια διαρκής διαδικασία που απαιτεί επαγρύπνηση και συνεχή βελτίωση.

Εθνική Χορηγία για την Ενίσχυση της Κυβερνοασφάλειας στις ΜμΕ από το NCC-CY

Ελάχιστη χρηματοδότηση ανά έργο
20.000 Ευρώ

Μέγιστη χρηματοδότηση ανά έργο
60.000 Ευρώ

Ποσοστό χρηματοδότησης
60%

Επισκεφθείτε την ιστοσελίδα του NCC-CY για περισσότερες πληροφορίες σχετικά με την Εθνική Χορηγία και για να εξερευνήσετε μελλοντικές εκδηλώσεις.

Αναφορές:

1.Advanced Persistent Threats (APTs)

1. FireEye. (2019). "APT28: A Window into Russia's Cyber Espionage Operations?" [Online]. Available: https://www.fireeye.com/current-threats/apt-groups.html
2. CrowdStrike. (2021). "CrowdStrike Global Threat Report." [Online]. Available: https://www.crowdstrike.com/resources/reports/global-threat-report/

2.Cyber Espionage

1. Symantec. (2016). "Operation Shady RAT." [Online]. Available: https://www.symantec.com/connect/blogs/operation-shady-rat-revealed
2. Mandiant. (2013). "APT1: Exposing One of China's Cyber Espionage Units." [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

3.Disruptive and Destructive Attacks

1. Zetter, K. (2014). "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon." Crown.
2. Wired. (2018). "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Αναφορές:

1.Supply Chain Attacks

1. SolarWinds. (2021). "What You Need to Know About the SUNBURST / SolarWinds Orion Supply Chain Attack." [Online]. Available: https://www.solarwinds.com/securityadvisory
2. Cisco Talos. (2017). "CCleaner Supply Chain Attack." [Online]. Available: https://blog.talosintelligence.com/2017/09/avast-distributes-malware.html

2.Critical Infrastructure Attacks

1. Dragos. (2017). "CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations." [Online]. Available: https://www.dragos.com/resource/crashoverride/
2. Schneider Electric. (2018). "Triton/Trisis Malware: A New Dimension of Threats." [Online]. Available: https://www.schneider-electric.com/en/download/document/998-20493509_GMA-US/

3.Data Breaches

1. Equifax. (2019). "Equifax Cybersecurity Incident & Important Consumer Information." [Online]. Available: https://www.equifaxsecurity2017.com/
2. Yahoo. (2016). "An Important Message About Yahoo User Security." [Online]. Available: https://help.yahoo.com/kb/SLN27925.html

Αναφορές:

1.Phishing and Social Engineering

1. Verizon. (2021). "2021 Data Breach Investigations Report." [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/
2. KnowBe4. (2021). "Phishing and Social Engineering: Understanding the Risks." [Online]. Available: https://www.knowbe4.com/whitepaper-phishing-and-social-engineering

2.Influence and Disinformation Campaigns

1. U.S. Senate Select Committee on Intelligence. (2019). "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election." [Online]. Available: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf
2. FireEye. (2020). "Ghostwriter Influence Campaign: An Overview." [Online]. Available: https://www.fireeye.com/blog/threat-research/2020/08/ghostwriter-influence-campaign.html

3.Ransomware

1. Europol. (2017). "WannaCry Ransomware Attack." [Online]. Available: https://www.europol.europa.eu/newsroom/news/global-impact-of-wannacry-ransomware-attack
2. U.S. Department of Justice. (2021). "JBS Pays $11 Million in Ransom After Cyberattack." [Online]. Available: https://www.justice.gov/opa/pr/jbs-pays-11-million-ransom-after-cyberattack