1

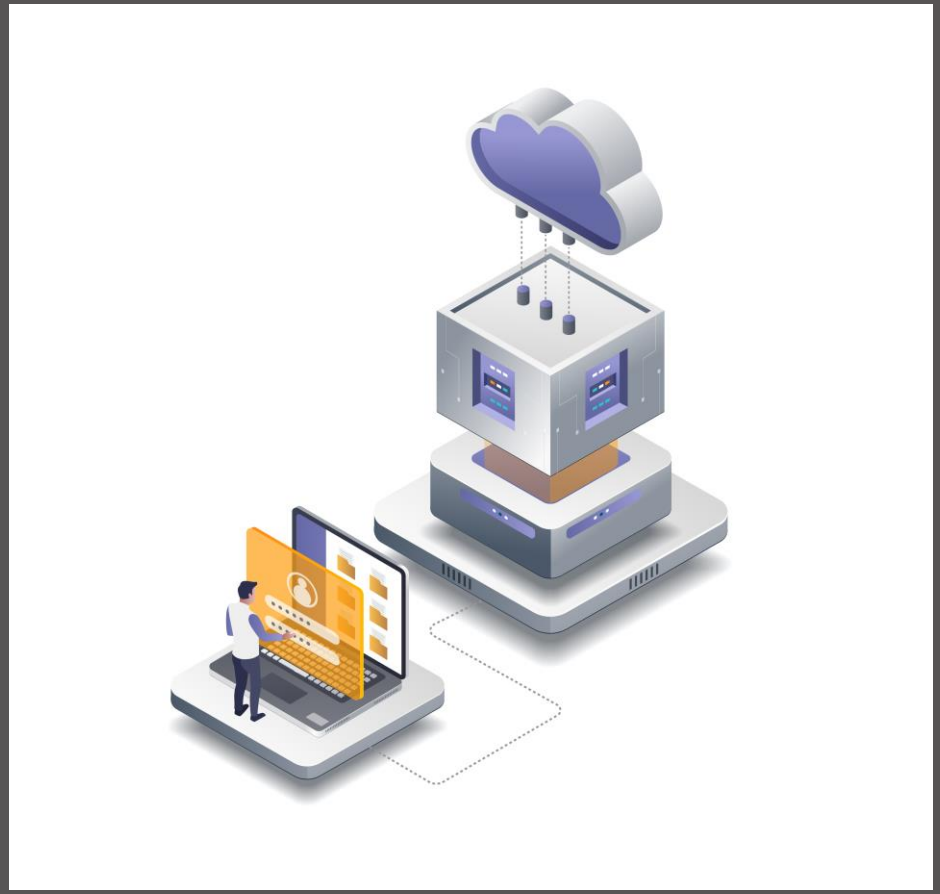
Ο Κρίσιμος Ρόλος της Κυβερνοασφάλειας στις Κυβερνητικές Λειτουργίες

Ο Κρίσιμος Ρόλος της Κυβερνοασφάλειας στις Κυβερνητικές Λειτουργίες

Η Κυβερνοασφάλεια εντός των Κυβερνητικών Οργανισμών είναι Απαραίτητη για την Προστασία των Ακολούθων:

2. Ευαίσθητες Πληροφορίες: Οι κυβερνητικοί οργανισμοί διαχειρίζονται έναν μεγάλο αριθμό ευαίσθητων και εμπιστευτικών πληροφοριών, συμπεριλαμβανομένων προσωπικών δεδομένων των πολιτών, διαβαθμισμένων πληροφοριών και οικονομικών αρχείων.

3. Διασφάλιση της Εθνικής Ασφάλειας: Οι κυβερνοαπειλές ενέχουν σημαντικούς κινδύνους για την εθνική ασφάλεια. Κράτη, τρομοκρατικές ομάδες και άλλοι κακόβουλοι παράγοντες ενδέχεται να στοχεύσουν κυβερνητικά συστήματα για να κλέψουν ευαίσθητες πληροφορίες.

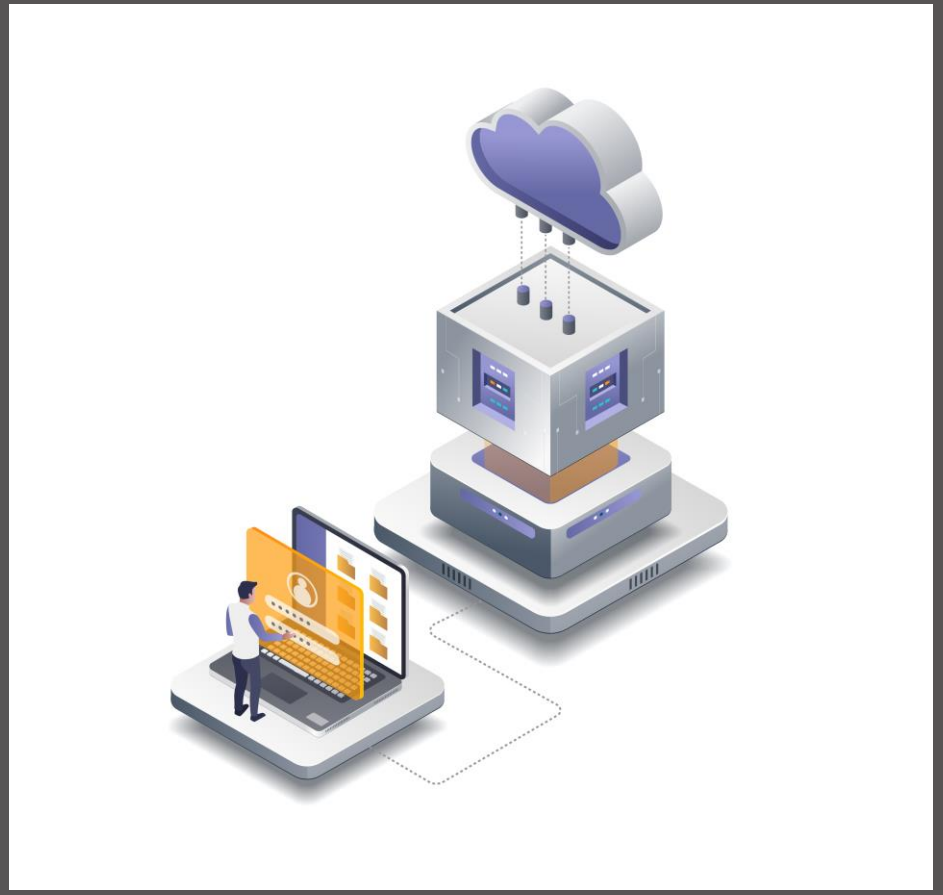


Ο Κρίσιμος Ρόλος της Κυβερνοασφάλειας στις Κυβερνητικές Λειτουργίες

Η Κυβερνοασφάλεια εντός των Κυβερνητικών Οργανισμών είναι Απαραίτητη για την Προστασία των Ακολούθων:

4. Διατήρηση της Δημόσιας Εμπιστοσύνης: Οι πολίτες αναμένουν από την κυβέρνησή τους να προστατεύει τα προσωπικά τους δεδομένα και να διασφαλίζει την αξιοπιστία των δημόσιων υπηρεσιών.

5. Διασφάλιση της Επιχειρησιακής Συνέχειας: Οι κυβερνοεπιθέσεις στα πληροφοριακά και επικοινωνιακά συστήματα της κυβέρνησης μπορούν να διακόψουν τις βασικές υπηρεσίες, προκαλώντας διακοπές, απώλεια δεδομένων και παράλυση.



Ο Κρίσιμος Ρόλος της Κυβερνοασφάλειας στις Κυβερνητικές Λειτουργίες

5. Συμμόρφωση με Νομικές Απαιτήσεις: Οι κυβερνήσεις πρέπει να συμμορφώνονται με τους νόμους και τους κανονισμούς για την προστασία των πληροφοριών και την κυβερνοασφάλεια, για να αποφύγουν νομικές κυρώσεις και να υποστηρίξουν το κράτος δικαίου.

6. Άμυνα κατά της Κυβερνοκατασκοπείας: Οι κυβερνήσεις αντιμετωπίζουν απειλές κυβερνοκατασκοπείας που στοχεύουν στην κλοπή πληροφοριών και πνευματικής ιδιοκτησίας. Τα ισχυρά μέτρα κυβερνοασφάλειας είναι κρίσιμα για την προστασία ευαίσθητων πληροφοριών και τη διατήρηση στρατηγικού πλεονεκτήματος.

Ο Κρίσιμος Ρόλος της Κυβερνοασφάλειας στις Κυβερνητικές Λειτουργίες

7. Προστασία των Διασυνδεδεμένων Κρίσιμων Υποδομών: Διασυνδεδεμένες με τομείς όπως η υγεία, η ενέργεια και τα χρηματοοικονομικά, οι παραβιάσεις κυβερνοασφάλειας στους κρατικούς φορείς μπορούν να επηρεάσουν τις κρίσιμες υποδομές, αναδεικνύοντας την ανάγκη για ισχυρά μέτρα κυβερνοασφάλειας.

2

Κυβερνητικοί Θεσμοί Αντιμέτωποι με Απειλές Κυβερνοασφάλειας

Κυβερνητικοί Θεσμοί Αντιμέτωποι με Απειλές Κυβερνοασφάλειας

Οι απειλές κυβερνοασφάλειας για τις κυβερνήσεις μπορούν να επηρεάσουν σοβαρά την εθνική ασφάλεια, την δημόσια εμπιστοσύνη και την επιχειρησιακή λειτουργικότητα. Οι κύριοι κίνδυνοι περιλαμβάνουν διάφορους και σημαντικούς κυβερνοκινδύνους:

Επιθέσεις από Κράτη: *Ξένες κυβερνήσεις μπορεί να χρησιμοποιήσουν την κυβερνοκατασκοπεία ή τον κυβερνοπόλεμο για να κλέψουν διαβαθμισμένες πληροφορίες, να διαταράξουν υποδομές ή να υπονομεύσουν την εμπιστοσύνη, συχνά μέσω εξελιγμένων και καλά χρηματοδοτούμενων επιθέσεων.*

Κυβερνητικοί Θεσμοί Αντιμέτωποι με Απειλές Κυβερνοασφάλειας

- *Παραβιάσεις Δεδομένων: Η μη εξουσιοδοτημένη πρόσβαση σε κυβερνητικές βάσεις δεδομένων μπορεί να αποκαλύψει προσωπικές πληροφορίες, διαβαθμισμένα έγγραφα και εμπιστευτικά δεδομένα, οδηγώντας σε κλοπή ταυτότητας, εκβιασμό και άλλες κακόβουλες δραστηριότητες.*

- *Ransomware: Οι κυβερνοεγκληματίες μπορούν να διεισδύσουν σε κυβερνητικά συστήματα, να κρυπτογραφήσουν κρίσιμα δεδομένα και να απαιτήσουν λύτρα, παραλύοντας τις λειτουργίες και προκαλώντας σημαντικές οικονομικές απώλειες.*

Κυβερνητικοί Θεσμοί Αντιμέτωποι με Απειλές Κυβερνοασφάλειας

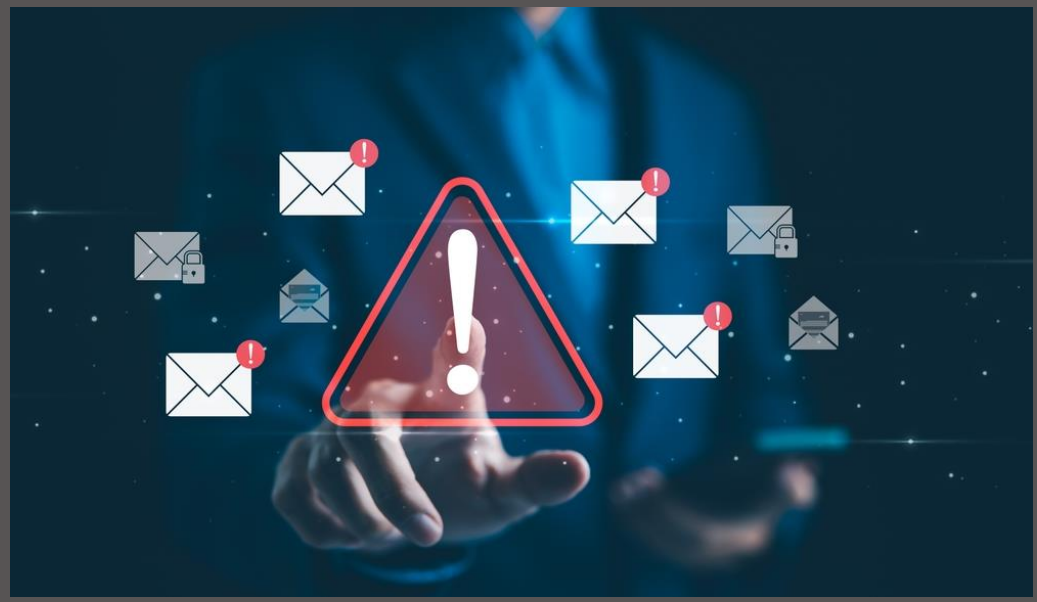
- *Phishing και Κοινωνική Μηχανική: Τα phishing emails και οι τακτικές κοινωνικής μηχανικής στοχεύουν κυβερνητικούς υπαλλήλους για να κλέψουν διαπιστευτήρια σύνδεσης και ευαίσθητες πληροφορίες, γεγονός που μπορεί να οδηγήσει σε μεγαλύτερες παραβιάσεις ασφαλείας.*

- *Εσωτερικές Απειλές: Δυσαρεστημένοι υπάλληλοι ή εργολάβοι μπορούν να διαρρεύσουν δεδομένα ή να σαμποτάρουν συστήματα σκόπιμα, καθιστώντας τις εσωτερικές απειλές δύσκολο να εντοπιστούν και να μετριαστούν.*

Κυβερνητικοί Θεσμοί Αντιμέτωποι με Απειλές Κυβερνοασφάλειας

- *Επιθέσεις Άρνησης Υπηρεσιών (DoS): Οι επιτιθέμενοι μπορούν να κατακλύσουν κυβερνητικούς ιστότοπους με κίνηση, καθιστώντας τους μη προσβάσιμους και διαταράσσοντας τις βασικές υπηρεσίες και την επικοινωνία με το κοινό.*

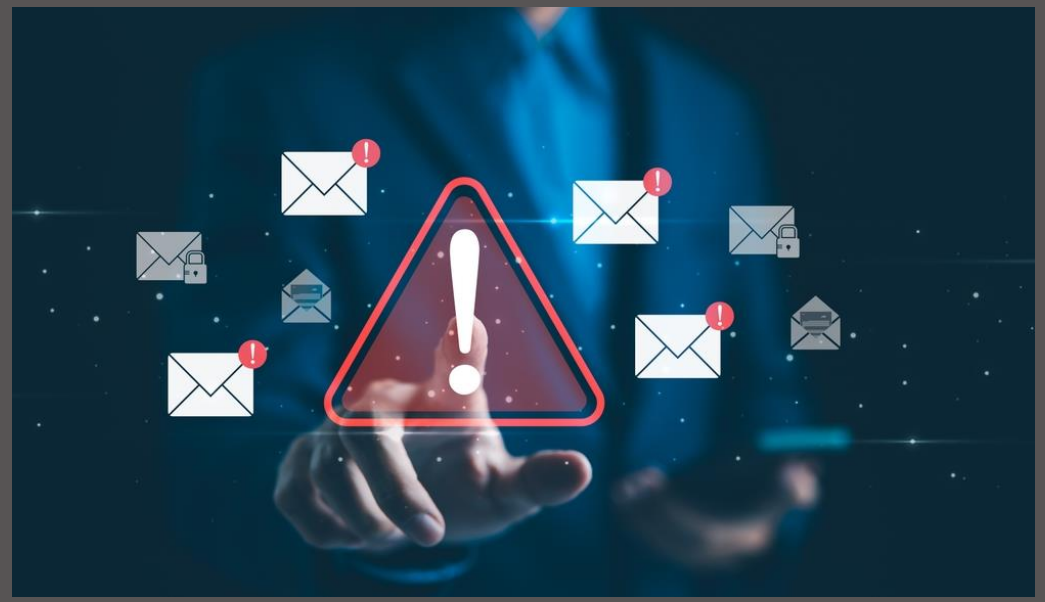
- *Επιθέσεις στην Εφοδιαστική Αλυσίδα: Η παραβίαση των συστημάτων τρίτων προμηθευτών μπορεί να δώσει στους επιτιθέμενους μια πίσω πόρτα στα κυβερνητικά δίκτυα, καθώς οι υπηρεσίες συχνά βασίζονται σε αυτούς τους προμηθευτές για λογισμικό, υλισμικό και υπηρεσίες.*



Κυβερνητικοί Θεσμοί Αντιμέτωποι με Απειλές Κυβερνοασφάλειας

- *Κακόβουλο Λογισμικό και Ιοί: Το κακόβουλο λογισμικό μπορεί να διεισδύσει σε κυβερνητικά συστήματα, προκαλώντας αλλοίωση δεδομένων, μη εξουσιοδοτημένη πρόσβαση και δυσλειτουργίες, συχνά εξαπλωνόμενο μέσω συνημμένων email, λήψεων ή μολυσμένων ιστοσελίδων.*

- *Ευπάθειες Κρίσιμων Υποδομών: Οι κυβερνοεπιθέσεις σε διασυνδεδεμένα κυβερνητικά συστήματα και τομείς κρίσιμων υποδομών όπως η ενέργεια, οι μεταφορές και η υγεία μπορούν να έχουν εκτεταμένες και καταστροφικές επιπτώσεις.*



Κυβερνητικοί Θεσμοί Αντιμέτωποι με Απειλές Κυβερνοασφάλειας

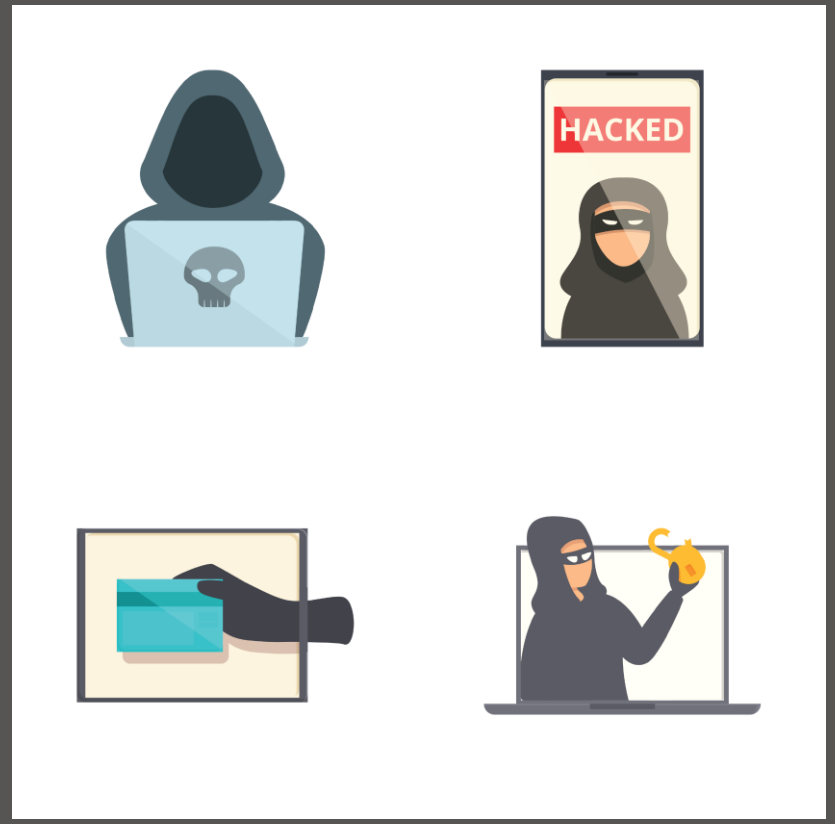
- *Zero-Day Exploits: Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν ευπάθειες μηδενικής ημέρας σε λογισμικό ή υλισμικό, οι οποίες είναι ιδιαίτερα επικίνδυνες λόγω της έλλειψης άμεσων αμυντικών μηχανισμών.*

- *Προηγμένες Επίμονες Απειλές (APTs): Οι APTs, που συχνά διεξάγονται από κράτη, είναι παρατεταμένες και στοχευμένες κυβερνοεπιθέσεις που στοχεύουν στην κλοπή πληροφοριών ή στην παραβίαση συστημάτων. Είναι ιδιαίτερα εξελιγμένες και δύσκολες στην ανίχνευση.*

Κυβερνητικοί Θεσμοί Αντιμέτωποι με Απειλές Κυβερνοασφάλειας

- *IoT και Έξυπνες Συσκευές: Η αυξανόμενη χρήση συσκευών IoT στις κυβερνητικές λειτουργίες δημιουργεί νέες ευπάθειες, καθώς αυτές οι συσκευές συχνά στερούνται ισχυρών μέτρων ασφαλείας, καθιστώντας τις ελκυστικούς στόχους για επιτιθέμενους.*

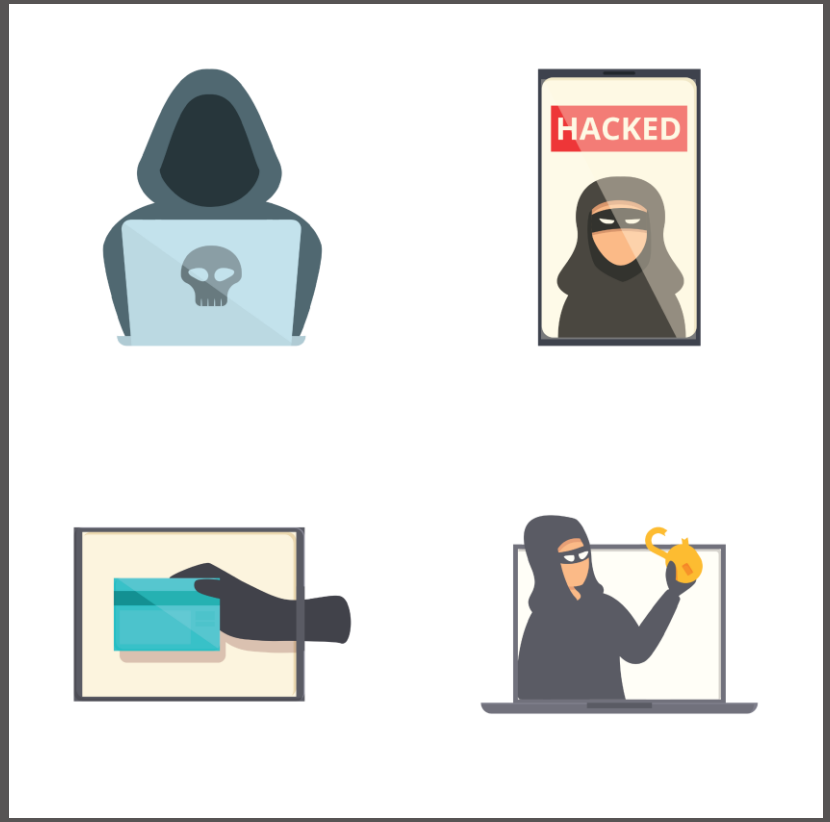
- *Έλλειψη Ευαισθητοποίησης για την Κυβερνοασφάλεια: Η ανεπαρκής εκπαίδευση και ευαισθητοποίηση για την κυβερνοασφάλεια μεταξύ των κυβερνητικών υπαλλήλων αυξάνει τον κίνδυνο επιτυχημένων επιθέσεων, καθώς το ανθρώπινο λάθος είναι ένας σημαντικός παράγοντας σε πολλές παραβιάσεις ασφαλείας.*



Κυβερνητικοί Θεσμοί Αντιμέτωποι με Απειλές Κυβερνοασφάλειας

- *Κίνδυνοι Ασφάλειας στο Cloud: Καθώς οι κυβερνητικοί φορείς υιοθετούν όλο και περισσότερο υπηρεσίες cloud, πρέπει να διαχειρίζονται νέες προκλήσεις ασφαλείας που σχετίζονται με την ιδιωτικότητα των δεδομένων, τον έλεγχο πρόσβασης και τη συμμόρφωση με τους κανονισμούς.*

- *Συστήματα Παλαίωσης: Πολλοί κυβερνητικοί φορείς βασίζονται σε παλαιωμένη τεχνολογία και συστήματα παλαίωσης που μπορεί να στερούνται σύγχρονων χαρακτηριστικών ασφαλείας. Αυτά τα συστήματα μπορεί να είναι πιο ευάλωτα σε επιθέσεις και πιο δύσκολα στην ασφάλιση.*



Κυβερνητικοί Θεσμοί Αντιμέτωποι με Απειλές Κυβερνοασφάλειας

Η αντιμετώπιση των κινδύνων κυβερνοασφάλειας απαιτεί μια ολοκληρωμένη προσέγγιση, συμπεριλαμβανομένων ισχυρών πολιτικών ασφαλείας, τακτικής εκπαίδευσης των εργαζομένων, επενδύσεων σε σύγχρονες τεχνολογίες ασφαλείας και συνεργασίας με άλλους φορείς και ιδιωτικούς εταίρους.

Αποτελεσματικά σχέδια αντιμετώπισης και ανάκαμψης περιστατικών είναι επίσης απαραίτητα για την ελαχιστοποίηση των επιπτώσεων από τυχόν παραβιάσεις ασφαλείας που μπορεί να συμβούν.

3

Μελέτες Περίπτωσης Κυβερνοασφάλειας σε Κυβερνητικούς Θεσμούς

Ιούλιος 2024:

- **Η στρατιωτική υπηρεσία της Νότιας Κορέας ερευνά τη διαρροή ιδιαίτερα ευαίσθητων πληροφοριών σχετικά με τις κατασκοπευτικές δραστηριότητες της Σεούλ και εξέδωσε ένταλμα σύλληψης για έναν ύποπτο. Οι πληροφορίες περιλάμβαναν προσωπικά δεδομένα για ανεπίσημους πράκτορες της Σεούλ που διεξάγουν μυστική κατασκοπεία στο εξωτερικό. Οι πληροφορίες μεταφέρθηκαν στον προσωπικό φορητό υπολογιστή του υπόπτου πριν διαρρεύσουν. Οι νομοθέτες δήλωσαν ότι η διαρροή ανακαλύφθηκε για πρώτη φορά τον Ιούνιο και δεν ήταν αποτέλεσμα hacking.**
- **Μια ελαττωματική ενημέρωση λογισμικού για τα Microsoft Windows που εκδόθηκε από την εταιρεία κυβερνοασφάλειας CrowdStrike προκάλεσε παγκόσμια διακοπή λειτουργίας IT που διέκοψε τις λειτουργίες αεροπορικών εταιρειών και νοσοκομείων. Επηρέασε περίπου 8,5 εκατομμύρια μηχανήματα και κόστισε στις εταιρείες του Fortune 500 περίπου 5,4 δισεκατομμύρια δολάρια, σύμφωνα με αναφορές.**

Ιούλιος 2024:

Η Γερμανία κατηγόρησε την Κίνα για την οργάνωση μιας "σοβαρής" κυβερνοεπίθεσης κατά του Ομοσπονδιακού Γραφείου Χαρτογραφίας και Γεωδαισίας (BKG), το οποίο διεξάγει ακριβή χαρτογράφηση της χώρας, το 2021. Τα ευρήματα προέκυψαν στο τέλος μιας τριετούς έρευνας για το περιστατικό και καθώς η Γερμανία σχεδιάζει ένα έργο αντικατάστασης των κινεζικών τηλεπικοινωνιακών υποδομών στη Γερμανία λόγω ανησυχιών για την ασφάλεια.

Ιούλιος 2024:

Η Αυστραλία, οι Ηνωμένες Πολιτείες, ο Καναδάς, το Ηνωμένο Βασίλειο, η Γερμανία, η Ιαπωνία, η Νότια Κορέα και η Νέα Ζηλανδία εξέδωσαν προειδοποίηση για κακόβουλη κυβερνοδραστηριότητα που υποστηρίζεται από το κινεζικό κράτος στα δίκτυά τους. Ήταν η πρώτη φορά που η Νότια Κορέα και η Ιαπωνία ενώθηκαν με την Αυστραλία για να αποδώσουν κακόβουλες κυβερνοενέργειες στην Κίνα, και η πρώτη φορά που η Αυστραλία ηγήθηκε μιας προσπάθειας αποδοχής κυβερνοεπίθεσης εναντίον της Κίνας.

Ιούνιος 2024:

Ο διαστημικός οργανισμός της Ιαπωνίας έχει υποστεί μια σειρά από κυβερνοεπιθέσεις από πέρυσι, σύμφωνα με την ιαπωνική κυβέρνηση. Ο Ιάπωνας Γραμματέας του Υπουργικού Συμβουλίου ισχυρίστηκε ότι τα στοχευμένα δίκτυα δεν περιείχαν ευαίσθητες πληροφορίες για πυραύλους ή δορυφόρους και ότι οι επιτιθέμενοι ήταν "από το εξωτερικό."

Ιούνιος 2024:

Οι χάκερς ανέπτυξαν ransomware στο εθνικό κέντρο δεδομένων της Ινδονησίας, το οποίο διέκοψε για λίγο διάφορες υπηρεσίες μετανάστευσης, συμπεριλαμβανομένων των υπηρεσιών διαχείρισης εγγράφων μετανάστευσης στα αεροδρόμια, και διέγραψαν πληροφορίες που δεν είχαν δημιουργηθεί αντίγραφα ασφαλείας. Η επίθεση προκάλεσε την παραίτηση του Γενικού Διευθυντή Εφαρμογών Πληροφορικής του Υπουργείου Επικοινωνιών και Πληροφορικής της Ινδονησίας και οδήγησε σε εθνικό έλεγχο των εθνικών κέντρων δεδομένων της Ινδονησίας.

4

Μελέτες Περίπτωσης Κυβερνοασφάλειας σε Κυβερνητικούς Θεσμούς - Στόχοι

Μελέτες Περίπτωσης Κυβερνοασφάλειας σε Κυβερνητικούς Θεσμούς - Στόχοι

Τυπικές Στοχευμένες Ευπάθειες των Κυβερνητικών Οργανισμών:

Κρίσιμες Υποδομές:
Οι επιτιθέμενοι αναζητούν μακροχρόνια πρόσβαση για να συλλέξουν πληροφορίες και να αναπτύξουν μέσα για να απενεργοποιήσουν κρίσιμες υποδομές και βιομηχανίες. Οι υπηρεσίες κοινής ωφέλειας, όπως οι εταιρείες ηλεκτρικής ενέργειας και τηλεπικοινωνιών, διαθέτουν επίσης μεγάλες ποσότητες προσωπικά αναγνωρίσιμων πληροφοριών (PII).

Πνευματική Ιδιοκτησία:
Οι επιτιθέμενοι επιδιώκουν να κλέψουν πνευματική ιδιοκτησία που είναι δαπανηρή στην ανάπτυξη σε τομείς όπως η υψηλή τεχνολογία, η ιατρική, η άμυνα και η γεωργία.

Τυπικές Στοχευμένες Ευπάθειες Κυβερνητικών Υπηρεσιών:

Ερευνητικά Δεδομένα:
Αναζητούν την απόκτηση τέτοιων δεδομένων για να επιταχύνουν τη δική τους ανάπτυξη λύσεων σε διάφορους τομείς, συμπεριλαμβανομένων των στρατιωτικών και βιοεπιστημών. Αυτό μπορεί να έχει κίνητρο κατασκοπείας ή κέρδους.

Προσωπικά Δεδομένα:
Χάκερ που υποστηρίζονται από το κράτος επιδιώκουν να εκμεταλλευτούν προσωπικά δεδομένα βασικών υψηλόβαθμων αξιωματούχων και υπεύθυνων λήψης αποφάσεων. Αυτές οι Προσωπικά Αναγνωρίσιμες Πληροφορίες (PII) θα μπορούσαν να χρησιμοποιηθούν ως μοχλός για την προώθηση της δικής τους ατζέντας.

5

Βέλτιστες Πρακτικές Κυβερνοασφάλειας για Κυβερνήσεις

Η Κοινωνική Μηχανική περιλαμβάνει την χειραγώγηση ανθρώπων για να εκτελέσουν συγκεκριμένες ενέργειες ή να αποκαλύψουν πληροφορίες που είναι χρήσιμες σε έναν επιτιθέμενο. Μία από τις πιο κοινές μορφές κοινωνικής μηχανικής είναι μέσω των phishing emails.

Ευθυγραμμίστε τα δικαιώματα πρόσβασης με τις ευθύνες.
Διασφαλίστε ότι το προσωπικό σας έχει το χαμηλότερο επίπεδο δικαιωμάτων που απαιτείται για να εκτελέσει τη δουλειά του. Αυτό μπορεί να μειώσει τον αντίκτυπο των επιτυχημένων επιθέσεων phishing.

Δημιουργήστε σχέδιο ανταπόκρισης σε επιθέσεις κοινωνικής μηχανικής.
Αλλάξτε τους κωδικούς πρόσβασης και σαρώστε για κακόβουλο λογισμικό μόλις υποψιαστείτε ότι μια επίθεση phishing μπορεί να ήταν επιτυχημένη.

Η Κοινωνική Μηχανική περιλαμβάνει τη χειραγώγηση ανθρώπων για να εκτελέσουν συγκεκριμένες ενέργειες ή να αποκαλύψουν πληροφορίες που είναι χρήσιμες σε έναν επιτιθέμενο. Μία από τις πιο κοινές μορφές κοινωνικής μηχανικής είναι μέσω των phishing emails.

Ελέγξτε για προφανή σημάδια phishing και προετοιμαστείτε για τα μη προφανή.
Ως γενικός κανόνας: Εάν δεν το περιμένατε – μην κάνετε κλικ σε αυτό! εκτός αν έχετε επιβεβαιώσει την εγκυρότητα του χρησιμοποιώντας εναλλακτικά μέσα από αυτά που παρέχονται στο email.

Προσέχετε την παρουσία σας στα κοινωνικά μέσα δικτύωσης.
Ποτέ μην χρησιμοποιείτε τους επιχειρηματικούς σας λογαριασμούς για να εγγραφείτε σε Κοινωνικά Δίκτυα ή για να δημιουργήσετε λογαριασμούς σε λύσεις για Καταναλωτές (δωρεάν). Πάντα να είστε προσεκτικοί με ό,τι κάνετε στο διαδίκτυο. Ό,τι δημοσιεύετε μπορεί και θα χρησιμοποιηθεί εναντίον σας (από επιτιθέμενους).

Η ανθρώπινη φύση επηρεάζει τα συναισθήματά μας και πώς αυτά μπορούν να μας κυριαρχήσουν. Από τη φύση τους, τα συναισθήματα και οι αισθήσεις μας ενεργοποιούνται πριν από τη λογική μας σκέψη. Οι κοινωνικοί μηχανικοί εκμεταλλεύονται αυτά τα ερεθίσματα.

Περιέργεια
Οι τρόποι κοινωνικής μηχανικής συχνά εκμεταλλεύονται την ανθρώπινη περιέργεια για να πετύχουν τον στόχο τους. (π.χ. Ρίχνοντας ένα μολυσμένο USB σε έναν διάδρομο)

Επείγουσα Ανάγκη
Χρησιμοποιούν επίσης μικρές προθεσμίες για να σας αποσπάσουν από την υπόλοιπη ιστορία (π.χ. Απαντήστε ΑΜΕΣΑ ή ο λογαριασμός σας θα διαγραφεί)

Βέλτιστες Πρακτικές Κυβερνοασφάλειας για Κυβερνήσεις

Η ανθρώπινη φύση επηρεάζει τα συναισθήματά μας και πώς μπορούν να μας κυριαρχήσουν. Από τη φύση τους, τα συναισθήματα και οι αισθήσεις μας ενεργοποιούνται πριν από τη λογική μας σκέψη. Οι τρόποι κοινωνικής μηχανικής εκμεταλλεύονται αυτά τα ερεθίσματα.

Εξουσία
Ή προσποιούνται ότι είναι ανώτεροι υπάλληλοι, αξιόπιστοι συνάδελφοι ή αξιόπιστες εταιρείες και σας ζητούν να κάνετε κάτι για αυτούς.

Μιμητισμός
Μερικές φορές, οι επιτιθέμενοι φτάνουν στο σημείο να μαθαίνουν τις καθημερινές σας συνήθειες, ενδιαφέροντα και επιχειρηματικούς κύκλους (που εισάγονται π.χ. από τα κοινωνικά σας μέσα) για να σχεδιάσουν πολύ στοχευμένες επιθέσεις που φαίνονται απόλυτα νόμιμες.

6

Επαφές Ενδιαφέροντος σε Περίπτωση Κυβερνοεπεισοδίου

NCC ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ Αρχή Ψηφιακής Ασφάλειας

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

ncc.cy

Επαφές Ενδιαφέροντος σε Περίπτωση Κυβερνοεπεισοδίου

Οι κυβερνητικές υπηρεσίες, σε περίπτωση περιστατικού, πρέπει να ενημερώσουν τις αρμόδιες αρχές. Η λίστα επαφών των αρμόδιων αρχών περιλαμβάνει:

- **Data Protection Commissioner**
  Tel: +357 22818456 Email: commissioner@dataprotection.gov.cy
- **CY Police Electronic Crime Division**
  Tel: +357 22808200 Email: cybercrime@police.gov.cy
- **Cyprus CSIRT**
  Tel: +357 22693094 Email: info@csirt.cy
- **Cyprus Digital Security Authority**
  Tel: +357 22693000 Email: contact@dsa.ee.cy

Σας Ευχαριστούμε

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