iT SECURITYPRO

CYBERSECURITY & BUSINESS IT, IN-DEPTH ANALYSIS

03/04/05.2024 • Τεύχος 84 WWW.ITSECURITYPRO.GR Τιμή 5€

NIS2 - ΑΠΑΙΤΗΣΕΙΣ ΓΙΑ ΣΥΜΜΟΡΦΩΣΗ, ΠΡΟΚΛΗΣΕΙΣ ΚΑΙ ΕΥΚΑΙΡΙΕΣ

- ΣΥΝΕΝΤΕΥΞΗ: ΚΩΝΣΤΑΝΤΙΝΑ ΣΥΝΤΙΛΑ
- 14ο INFOCOM SECURITY 2024
- CYBERSECURITY INCIDENTS: Η ΣΗΜΑΣΙΑ ΤΟΥ INCIDENT RESPONSE

Cover Issue

NIS2 - ΑΠΑΙΤΗΣΕΙΣ ΓΙΑ ΣΥΜΜΟΡΦΩΣΗ, ΠΡΟΚΛΗΣΕΙΣ ΚΑΙ ΕΥΚΑΙΡΙΕΣ

Η Οδηγία NIS2 αντιπροσωπεύει ένα σημαντικό βήμα στις προσπάθειες της ΕΕ να ενισχύσει τις αμυντικές της ικανότητες στον κυβερνοχώρο. Με το να διευρύνει το πεδίο εφαρμογής της ρύθμισης, να τυποποιεί την αναφορά και να τονίζει την προληπτική παρακολούθηση της ασφάλειας, το NIS2 στοχεύει στη δημιουργία μιας πιο ανθεκτικής ψηφιακής υποδομής ικανής να αντιμετωπίζει τις απειλές του σύγχρονου κόσμου.


ΠΑΝΑΓΙΩΤΗΣ ΚΑΛΑΝΤΖΗΣ
Cyber Security & Data Privacy Expert

Στις 16 Ιανουαρίου 2023, τέθηκε σε ισχύ η Οδηγία (ΕΕ) 2022/2555 Οδηγία για την Ασφάλεια Δικτύων και Πληροφοριών (Οδηγία NIS2), η οποία στοχεύει στην ενίσχυση της κυβερνοασφάλειας σε ολόκληρη την ΕΕ. Η Οδηγία NIS2 επιβάλλει νέες και βελτιωμένες υποχρεώσεις που σχετίζονται με την κυβερνοασφάλεια σε εταιρείες και άλλους ιδιωτικούς ή δημόσιους φορείς σε ορισμένους τομείς, μεταξύ των οποίων απαραίτητα μέτρα ασφαλείας και υποχρεώσεις αναφοράς σχετικών περιστατικών.

Τα κράτη μέλη της ΕΕ έχουν **προθεσμία έως τις 18 Οκτωβρίου 2024** για να εφαρμόσουν την Οδηγία NIS2 στην τοπική νομοθεσία. Στη Γερμανία, για παράδειγμα, ένα προσχέδιο γερμανικής πράξης για την εφαρμογή της Οδηγίας NIS2 και την ενίσχυση της κυβερνοασφάλειας (Γερμανικός νόμος εφαρμογής NIS2) βρίσκεται στο τραπέζι από την άνοιξη του 2023. Στο παρόν άρθρο, θα επιχειρήσουμε μια κατά το δυνατόν ολοκληρωμένη επισκόπηση των απαιτήσεων της Οδηγίας NIS2 καθώς και την επίπτωσή τους σε οργανισμούς εντός του πεδίου εφαρμογής της Οδηγίας.

Η ΟΔΗΓΙΑ NIS2 ΩΣ ΜΕΡΟΣ ΤΗΣ ΝΟΜΟΘΕΣΙΑΣ ΤΗΣ ΕΕ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Το πολύπλοκο κανονιστικό περιβάλλον ΕΕ για τον ψηφιακό τομέα περιλαμβάνει ολοένα και περισσότερο την κυβερνοασφάλεια. Το **2019**, ο **Κανονισμός Κυβερνοασφάλειας της ΕΕ** (Κανονισμός (ΕΕ) 2019/881) καθιέρωσε μόνιμη εντολή για τον **Ευρωπαϊκό Οργανισμό Κυβερνοασφάλειας (ENISA)**, συνοδευόμενος από την εισαγωγή ενός ενιαίου ευρωπαϊκού πλαισίου πιστοποίησης για προϊόντα, υπηρεσίες και διαδικασίες Πληροφορικής και Επικοινωνιών. Η Οδηγία NIS2 αποτελεί βασικό στοιχείο του μελλοντικού ρυθμιστικού τοπίου της ΕΕ στον τομέα των ψηφιακών υποδομών. Αυτό το τοπίο περιλαμβάνει επίσης έναν αριθμό νέων νόμων για την κυβερνοασφάλεια, συμπεριλαμβανομένης της **Οδηγίας για την Ανθεκτικότητα των Κρίσιμων Οντοτήτων (Οδηγία (ΕΕ) 2022/2557), του Κανονισμού για την Ψηφιακή Λειτουργική Ανθεκτικότητα (Οδηγία (ΕΕ) 2022/2554 – DORA)** που επικεντρώνεται στις χρηματοπιστωτικές υπηρεσίες και του Κανονισμού για την Κυβερνοανθεκτικότητα, που στοχεύει στην καθιέρωση του νομικού πλαισίου της ΕΕ για τις οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία.

ΣΚΟΠΟΣ ΚΑΙ ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η Οδηγία NIS2 στοχεύει στη βελτίωση της ανθεκτικότητας των δικτύων, πληροφοριακών συστημάτων και πληροφοριών και στην αντιμετώπιση περιστατικών κυβερνοασφάλειας στον δημόσιο και τον ιδιωτικό τομέα στην ΕΕ. Η προηγούμενη οδηγία (ΕΕ) 2016/1148 (Οδηγία NIS), η οποία τέθηκε σε ισχύ το 2016, καθόρισε για πρώτη φορά ενιαίες απαιτήσεις κυβερνοασφάλειας σε ολόκληρη την ΕΕ. Ωστόσο, σύμφωνα με την Ευρωπαϊκή Επιτροπή, η εφαρμογή της Οδηγίας NIS στα κράτη μέλη δεν έχει οδηγήσει σε επαρκές και ενιαίο επίπεδο κυβερνοασφάλειας, θεωρώντας το επίπεδο κυβερνοασφάλειας σε κοινωνικά σημαντικούς τομείς της οικονομίας παραμένει πολύ χαμηλό. **Η οδηγία NIS2 στοχεύει να διορθώσει αυτήν την κατάσταση** και να αυξήσει το επίπεδο ασφάλειας στον κυβερνοχώρο, επιφέροντας τις ακόλουθες βελτιώσεις:

- Δημιουργία της απαραίτητης δομής διαχείρισης κυβερνοκρίσεων (CyCLONe).
- Αύξηση του επιπέδου εναρμόνισης όσον αφορά τις απαιτήσεις ασφαλείας και τις υποχρεώσεις αναφοράς.
- Ενθάρρυνση των Κρατών Μελών να εισαγάγουν νέους τομείς ενδιαφέροντος, όπως η αλυσίδα εφοδιασμού, η διαχείριση ευπαθειών, το βασικό διαδίκτυο και η κυβερνοϋγιεινή στις εθνικές τους στρατηγικές κυβερνοασφάλειας.
- Εισαγωγή νέων ιδεών όπως οι ομότιμες αξιολογήσεις για την ενίσχυση της συνεργασίας και της ανταλλαγής γνώσεων μεταξύ των Κρατών Μελών.
- Κάλυψη μεγαλύτερου μέρους της οικονομίας και της κοινωνίας με την συμπερίληψη περισσότερων τομέων, που σημαίνει ότι περισσότερες οντό-

τητες είναι υποχρεωμένες να λάβουν μέτρα για να αυξήσουν το επίπεδο της κυβερνοασφάλειάς τους.

Για το σκοπό αυτό, η Οδηγία NIS2 βασιζόμενη στην αρχική Οδηγία NIS, **διευρύνει τις κατηγορίες οντοτήτων** που εμπίπτουν στο πεδίο εφαρμογής της, και επεκτείνει έτσι σημαντικά το φάσμα των καλυπτόμενων φορέων. Τα σχετικά κριτήρια για τον καθορισμό της εφαρμοσιμότητας είναι η κατηγορία μεγέθους της οντότητας και ο τομέας (ή η κρισιμότητα του αντίστοιχα) στον οποίο δραστηριοποιείται η οντότητα. Πιο συγκεκριμένα, η Οδηγία NIS2 **κατηγοριοποιεί τις οντότητες βάσει μεγέθους**, αναφερόμενη στο Άρθρο 2 του Παραρτήματος της Σύστασης 2003/361/ΕΚ. (βλέπε ΠΙΝΑΚΑΣ 1)

Με βάση την κατηγοριοποίηση, η Οδηγία NIS2 καθιερώνει ένα ρυθμιστικό καθεστώς βασισμένο στην παρακάτω διαστρωματική προσέγγιση.

1.Οντότητες που Επηρεάζονται βάσει Μεγέθους και Τομέα

Μεγάλες και μεσαίες εταιρείες ή άλλες οντότητες από τους τομείς που αναφέρονται στο Παράρτημα I ή II της Οδηγίας NIS2, που παρέχουν τις υπηρεσίες τους ή ασκούν τις δραστηριότητές τους στην ΕΕ (Άρθρο 3(1) της Οδηγίας NIS2), εμπίπτουν στο πεδίο εφαρμογής της Οδηγίας NIS2, αν ανήκουν στους εμπλεκόμενους τομείς. (βλέπε ΠΙΝΑΚΑΣ 2)

2. Οντότητες που Επηρεάζονται Ανεξαρτήτως Μεγέθους

Ανεξαρτήτως μεγέθους, ορισμένες οντότητες εμπίπτουν στο πεδίο εφαρμογής της νέας Οδηγίας NIS2. Αυτές είναι ουσιαστικά οντότητες που ανήκουν στους παρακάτω τομείς (Άρθρο 3(2) της Οδηγίας NIS2):

- Πάροχοι δημόσιων ηλεκτρονικών δικτύων επικοινωνίας ή δημόσια διαθέσιμων υπηρεσιών ηλεκτρονικών επικοινωνιών

ΠΙΝΑΚΑΣ 1

Κατηγορία Μέγεθους	Αριθμός εργαζομένων	Ετήσιες Πωλήσεις	Ετήσιος Ισολογισμός
Μικρές Εταιρίες	<50	< 10.000.000	< 10.000.000
Μεσαίες Εταιρίες	<250	< 50.000.000	< 43.000.000
Μεγάλες εταιρίες	>250	> 50.000.000	> 43.000.000

- Πάροχοι υπηρεσιών εμπιστοσύνης
- Μητρώα ονομάτων κορυφαίου επιπέδου (TLD) και πάροχοι υπηρεσιών DNS (εξαιρούνται οι διαχειριστές root name server, Άρθρο 6 No. 20 της Οδηγίας NIS2)
- Οντότητες που είναι οι μοναδικοί πάροχοι σε ένα κράτος μέλος μιας υπηρεσίας απαραίτητης για τη διατήρηση κρίσιμων κοινωνικών ή οικονομικών δραστηριοτήτων
- Πάροχοι υπηρεσιών των οποίων η διακοπή θα μπορούσε να έχει σημαντική επίδραση στη δημόσια ασφάλεια, δημόσια τάξη, δημόσια υγεία ή να δημιουργήσει συστημικό κίνδυνο

3. Οντότητες που Επηρεάζονται Έμμεσα από την Εφοδιαστική Αλυσίδα

Οι μικρές εταιρείες ή άλλες οντότητες γενικά δεν καλύπτονται άμεσα από την Οδηγία NIS2, με τις παραπάνω εξαιρέσεις των επηρεαζόμενων οντοτήτων ανεξαρτήτως μεγέθους. Ωστόσο, οι πάροχοι υπηρεσιών και οι προμηθευτές των επηρεαζόμενων οντοτήτων πρέπει επίσης να συμμορφώνονται με τα μέτρα ασφαλείας, στο βαθμό που τα μέτρα διαχείρισης κινδύνων που πρέπει να εφαρμόσουν οι επηρεαζόμενες οντότητες μπορεί επίσης να καλύπτουν την ασφάλεια της εφοδιαστικής αλυσίδας, συμπεριλαμβανομένων των πτυχών ασφαλείας των σχέσεων μεταξύ κάθε οντότητας και των άμεσων προμηθευτών ή παρόχων υπηρεσιών της (Άρθρο 21(3) της Οδηγίας NIS2). Οι μικρές οντότητες μπορεί, επομένως, να επηρεαστούν από την Οδηγία NIS2 μέσω της εφοδιαστικής αλυσίδας.

Εκτός από τις κατηγοριοποιήσεις βάσει μεγέθους, η Οδηγία NIS2 διακρίνει με-

ΠΙΝΑΚΑΣ 2

Τομείς Υψηλής Κρισιμότητας (Παράρτημα I)	Άλλοι Κρίσιμοι Τομείς (Παράρτημα II):
• Ενέργεια • Μεταφορές • Τραπεζικός Τομέας • Υποδομές Χρηματοοικονομικών Αγορών • Υγεία • Πόσιμο Νερό • Αποχέτευση • Ψηφιακή Υποδομή • Διαχείριση Υπηρεσιών Πληροφορικής (B2B) • Δημόσια Διοίκηση • Διάστημα	• Ταχυδρομικές και Ταχυμεταφορές • Διαχείριση Αποβλήτων • Χημικά • Τρόφιμα • Βιομηχανία Επεξεργασίας/ Παραγωγής • Ψηφιακοί Πάροχοι • Έρευνα

ταξύ των κατηγοριών ουσιαστικών και σημαντικών οντοτήτων:

- Οι μεγάλες οντότητες από τομείς υψηλής κρισιμότητας θεωρούνται ουσιαστικές (Παράρτημα I).
- Οι μεγάλες και μεσαίες οντότητες από άλλους κρίσιμους τομείς θεωρούνται σημαντικές (Παράρτημα II).

Αν μια εταιρεία ή άλλη οντότητα ταξινομείται ως κρίσιμη ή σημαντική υπό την Οδηγία NIS2, δεν κάνει διαφορά ως προς τις υποχρεώσεις που πρέπει να τηρηθούν και τα μέτρα που πρέπει να εφαρμοστούν.

ΝΕΕΣ ΥΠΟΧΡΕΩΣΕΙΣ ΠΟΥ ΑΠΟΡΡΕΟΥΝ ΑΠΟ ΤΗΝ ΟΔΗΓΙΑ NIS2

Όπως είδαμε, χτίζοντας πάνω στη βάση που έθεσε η προκάτοχος, η Οδηγία NIS2 δεν είναι απλώς μια ενημέρωση· είναι μια σημαντική επέκταση του πεδίου εφαρμογής και της φιλοδοξίας για την αντιμετώπιση του εξελισσόμενου τοπίου των κυβερνοαπειλών. Μία από τις κύριες βελτιώσεις είναι η συμπερίληψη των **αλυσίδων εφοδιασμού**, ένας **κρίσιμος τομέας ευπάθειας** στο σημερινό διασυνδεδεμένο ψηφιακό οικοσύστημα. Επιπλέον, το NIS2 στοχεύει στην τυποποίηση της αναφοράς περιστατικών, δημιουργώντας ένα ενιαίο πλαίσιο που ενισχύει την εθνική ορατότητα στις κυβερνοεπιθέσεις και τις επιπτώσεις τους σε διάφορους τομείς. Μια αξιοσημείωτη αλλαγή είναι η **προληπτική στάση της Οδηγίας, αναφορικά με την παρακολούθηση της ασφάλειας.** Η οδηγία επιβάλλει την ενεργή παρακολούθηση των πληροφοριακών συστημάτων για την ανίχνευση ανωμαλιών και πιθανών απειλών, προχωρώντας πέρα από τους παθητικούς αμυντικούς μηχανισμούς. Επιπλέον, περιλαμβάνει τη διοίκηση των εταιρειών στη διαχείριση της κυβερνοασφάλειας, καθιερώνοντας την ευθύνη και ενσωματώνοντας τη διαχείριση της κυβερνοασφάλειας στη γενικότερη δομή εταιρικής διακυβέρνησης. Επιπλέον, η οδηγία NIS2 επιβάλλει νέες, ενισχυμένες υποχρεώσεις στις καλυπτόμενες οντότητες και θεσπίζει **αυστηρότερο καθεστώς επιβολής.** Στον πυρήνα των νέων υποχρεώσεων, βρίσκεται η απαίτηση για ολοκληρωμένα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας. Οι βασικές και κρίσιμες οντότητες πρέπει να εφαρμόζουν κατάλληλα, αναλογικά και αποτελεσματικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα για την προστασία των δικτύων, των συστημάτων πληροφορικής και των διαδικασιών, διασφαλίζοντας την ασφάλεια των υπηρεσιών τους και ελαχιστοποιώντας τις επιπτώσεις των περιστατικών ασφαλείας στους χρήστες τους (Άρθρο 21(1) της Οδηγίας NIS2). Τα μέτρα διαχείρισης κινδύνων πρέπει να βασίζονται σε μια **πολυπαραγοντική προσέγγιση** και να περιλαμβάνουν τουλάχιστον τα ακόλουθα στοιχεία:

- Σχέδιο για την ανάλυση κινδύνων και την ασφάλεια των πληροφοριακών συστημάτων.
- Διαχείριση περιστατικών ασφαλείας.
- Επιχειρησιακή συνέχεια και διαχείριση κρίσεων.
- Ασφάλεια της αλυσίδας εφοδιασμού.
- Μέτρα ασφαλείας για την απόκτηση, ανάπτυξη και συντήρηση των ΤΠΕ.
- Σχέδια και διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων.
- Κυβερνοϋγιεινή και εκπαίδευση στην κυβερνοασφάλεια.
- Κρυπτογραφία και κρυπτογράφηση, όπου είναι εφαρμόσιμο.
- Ασφάλεια προσωπικού, σχέδια για τον έλεγχο πρόσβασης.
- Πολυπαραγοντική ταυτοποίηση.

Η αξιολόγηση κινδύνου πρέπει να λαμβάνει υπόψη την έκθεση σε κίνδυνο και το μέγεθος της οντότητας, αφενός, και την πιθανότητα εμφάνισης περιστατικού ασφάλειας, τον βαθμό σοβαρότητας και την επίπτωση, αφετέρου. Για να ορίσει ακόμη πιο συγκεκριμένες τεχνικές και μεθοδολογικές προδιαγραφές για τα παραπάνω υποχρεωτικά στοιχεία, η Ευρωπαϊκή Επιτροπή μπορεί να εκδώσει δεσμευτικές εφαρμοστικές πράξεις (Άρθρο 21(2) 2 της Οδηγίας NIS2). Μια ακόμα σημαντική παράμετρος του καταλόγου υποχρεώσεων της Οδηγίας NIS2 είναι η **υποχρέωση ειδοποίησης και αναφοράς**.

Οι επηρεαζόμενες οντότητες πρέπει να αναφέρουν σημαντικά περιστατικά ασφάλειας στην εθνική **Ομάδα Αντί-**

δρασης σε Περιστατικά Πληροφορικής Ασφάλειας (CSIRT), η οποία θα οριστεί βάσει της Οδηγίας NIS2 ή, όπου κατάλληλο, στην αρμόδια τοπική αρχή (στη συνέχεια αναφέρονται συλλογικά ως "αρχή") εντός καθορισμένων χρονικών ορίων και με σταδιακές αναφορές. Ο ακριβής χρόνος για την αναφορά σε μια CSIRT ή σε άλλη αρχή θα γίνει σαφέστερος καθώς προχωρά η εθνική εφαρμογή της Οδηγίας NIS2. Βάσει της Οδηγίας NIS2, ένα περιστατικό ασφάλειας ουσιαστικά είναι οποιοδήποτε γεγονός που επηρεάζει τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των αποθηκευμένων ή αλλιώς επεξεργασμένων δεδομένων ή των υπηρεσιών που προσφέρονται μέσω δικτύου και πληροφοριακών συστημάτων (Άρθρο 6 Αρ. 6 της Οδηγίας NIS2). Το περιστατικό θεωρείται σημαντικό αν:

- Έχει προκαλέσει ή ενδέχεται να προκαλέσει σοβαρή διαταραχή στη λειτουργία των υπηρεσιών ή οικονομική ζημιά στην ενδιαφερόμενη εταιρεία.
- Έχει επηρεάσει αρνητικά ή ενδέχεται να επηρεάσει αρνητικά άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντική υλική ή άυλη ζημιά (Άρθρο 23(3) (α) και (β) της Οδηγίας NIS2).

Για να διευκρινιστεί, η υποχρέωση ειδοποίησης ενεργοποιείται χωρίς την ανάγκη να εμπλέκεται η επεξεργασία ή η αποκάλυψη προσωπικών δεδομένων. Υπάρχουν τρεις **κατηγορίες υποχρεωτικών ενεργειών ειδοποίησης και αναφοράς** προς την αρχή σε περίπτωση σημαντικού περιστατικού ασφάλειας:

- **Προειδοποίηση:** Οι ουσιώδεις και σημαντικές οντότητες πρέπει να αναφέρουν μια προειδοποίηση στην αρχή χωρίς καθυστέρηση, αλλά όχι αργότερα από 24 ώρες, σε περίπτωση σημαντικού περιστατικού ασφάλειας. Αυτή η αναφορά πρέπει να υποδεικνύει εάν υπάρχει υποψία ότι το περιστατικό ασφάλειας είναι πιθανό να οφείλεται σε παράνομη ή κακόβουλη ενέργεια ή μπορεί να έχει διασυνοριακές επιπτώσεις (Άρθρο 23(4) της Οδηγίας NIS2).
- **Εκτεταμένη ειδοποίηση:** Πρέπει επίσης να υποβληθεί μια πιο λεπτομερής ειδοποίηση στην αρχή εντός 72 ωρών, ενημερώνοντας την προειδοποίηση και παρέχοντας μια πρώτη αξιολόγηση του περιστατικού ασφάλειας. Αυτή πρέπει να αναφέρει τη σοβαρότητά του, την επίδρασή του και, εφόσον είναι εφαρμόσιμο, ενδείξεις παραβιάσεων.
- **Ενδιάμεση/τελική αναφορά:** Σε περίπτωση που το αρμόδιο όργανο το ζητήσει, οι επηρεαζόμενες οντότητες πρέπει να παρέχουν μια ενδιάμεση αναφορά, εάν είναι εφαρμόσιμο, και μια τελική αναφορά μέχρι ένα μήνα το αργότερο. Η τελική αναφορά πρέπει να περιλαμβάνει λεπτομερείς πληροφορίες σχετικά με το περιστατικό ασφάλειας, συμπεριλαμβανομένης της επίπτωσής του, των αιτιών του και των ληφθέντων μέτρων επίλυσης, μεταξύ άλλων (Άρθρο 23(5) της Οδηγίας NIS2).

Οι αρχές θα πρέπει να παρέχουν ανατροφοδότηση στις αναφερθείσες εταιρείες για το αναφερθέν περιστατικό ασφάλειας και, κατόπιν αιτήματος της εταιρείας, να προσφέρουν καθοδήγηση ή λειτουργική συμβουλή για πιθανά μέτρα αντιμετώπισης (Άρθρο 23(5) της Οδηγίας NIS2). Αυτές οι υποχρεώσεις ειδοποίησης είναι παρόμοιες, αν και όχι ταυτόσημες, με τις απαιτήσεις ειδοποίησης για περιστατικά προστασίας δεδομένων σύμφωνα με **τον Γενικό Κανονισμό Προστασίας Δεδομένων της ΕΕ (Κανονισμός (ΕΕ) 2016/679) (GDPR)** και περιστατικά ασφάλειας σύμφωνα με τους εθνικούς νόμους τηλεπικοινωνιών που εφαρμόζουν τον Ευρωπαϊκό Κώδικα Ηλεκτρονικών Επικοινωνιών (EECC). Ως αποτέλεσμα, οι εταιρείες πρέπει να αξιολογήσουν εάν οι υπάρχουσες εταιρικές δομές και διαδικασίες μπορούν να χρησιμοποιηθούν εν μέρει για την εκπλήρωσή τους. Υπάρχουν υποχρεώσεις για **ειδοποίηση των παρόχων υπηρεσιών και του κοινού.** Εάν ένα σημαντικό περιστατικό ασφάλειας επηρεάζει την παροχή υπηρεσιών, η ενδιαφερόμενη εταιρεία πρέπει να ειδοποιήσει άμεσα τους παραλήπτες των υπηρεσιών. Το ίδιο ισχύει εάν

οι παραλήπτες επηρεάζονται από μια σημαντική κυβερνοαπειλή. Οι αρμόδιες αρχές μπορεί επίσης να απαιτήσουν από τις εταιρείες να ενημερώσουν το κοινό για ένα σημαντικό περιστατικό ασφάλειας, ειδικά όταν η δημόσια ενημέρωση είναι απαραίτητη για την πρόληψη ή την αντιμετώπιση του περιστατικού ασφάλειας.

ΕΠΙΒΟΛΗ ΚΑΙ ΚΥΡΩΣΕΙΣ

Τα άρθρα 31 έως 37 περιγράφουν το πλαίσιο εποπτείας και επιβολής, χορηγώντας στις εθνικές αρχές εξουσίες για τη διασφάλιση της συμμόρφωσης. Μέσα σε αυτά τα πλαίσια, το Άρθρο 32 παρέχει εξουσίες για την εφαρμογή μέτρων που είναι αποτελεσματικά, αναλογικά και αποτρεπτικά για τις οντότητες εντός του πεδίου εφαρμογής της Οδηγίας. Αυτά δυνητικά περιλαμβάνουν εποπτεία επί τόπου και εκτός τόπου, τυχαίους ελέγχους και στοχευμένους ελέγχους ασφαλείας, όπως φαίνεται αναλυτικότερα (βλέπε ΠΙΝΑΚΑΣ 3)

Επιπρόσθετα, η Οδηγία NIS2 **δίνει στις εθνικές αρχές ένα φάσμα εξουσιών επιβολής**, που περιλαμβάνουν τη δυνατότητα έκδοσης προειδοποιήσεων για μη συμμόρφωση, δεσμευτικών οδηγιών προς τις οργανώσεις, εξουσιών για την επιβολή της διαχείρισης κινδύνου και της εφαρμογής προτάσεων. Ένα νέο στοιχείο είναι η προσωπική ευθύνη των ανώτερων μελών της διοίκησης (π.χ., μέλη του διοικητικού συμβουλίου, διευθύνοντες σύμβουλοι) που πρέπει να εγκρίνουν και να παρακολουθούν

τα μέτρα διαχείρισης κινδύνου στον τομέα της κυβερνοασφάλειας. Η Οδηγία δίνει, εξουσίες στην εθνική αρχή για την επιβολή της ευθύνης της διοίκησης. Σαν αποτέλεσμα, σε ακραίες περιπτώσεις, ο Διευθύνων Σύμβουλος ή ο νομικός αντιπρόσωπος μπορεί να απαγορευθεί προσωρινά από την εκτέλεση των διοικητικών του καθηκόντων.

ΕΠΙΠΤΩΣΕΙΣ ΚΑΙ ΣΥΜΒΟΥΛΕΣ ΣΥΜΜΟΡΦΩΣΗΣ

Για τους οργανισμούς, η μετάβαση στην Οδηγία NIS2 φέρνει μια σειρά νέων ευθυνών και προκλήσεων. Η οδηγία περιλαμβάνει ένα ευρύτερο φάσμα τομέων, συμπεριλαμβανομένων προηγουμένως παραβλεπόμενων περιοχών, όπως τα δημόσια δίκτυα πληροφοριών, η παραγωγή τροφίμων και η δημόσια διοίκηση. Επιπλέον, εισάγει αυστηρές απαιτήσεις αναφοράς, με την πρώτη ειδοποίηση περιστατικών που απαιτείται εντός 24 ωρών και ένα λεπτομερές αναλυτικό σχέδιο δράσης που πρέπει να υποβληθεί μέσα σε ένα μήνα. Η Οδηγία NIS2 επίσης **τονίζει τη σημασία της ασφάλειας της αλυσίδας εφοδιασμού**, αναγνωρίζοντας τις αλυσιδωτές επιπτώσεις που μπορούν να έχουν οι ευπάθειες σε μια περιοχή της αλυσίδας εφοδιασμού σε άλλες. Αυτή η **ολιστική προσέγγιση** επεκτείνεται στις βέλτιστες πρακτικές τεχνολογίας πληροφορικής, απαιτώντας από τις οργανώσεις να υιοθετήσουν μια ολοκληρωμένη ασφαλή στάση που καλύπτει τα πάντα από τη διαχείριση περιουσιακών στοιχείων μέχρι την κρυπτογράφηση και τους ανθρώπινους πόρους. Με την προθεσμία υλοποίησης να πλησιάζει και χωρίς περίοδο μετάβασης, οι οργανισμοί πρέπει να δράσουν γρήγορα για να ευθυγραμμίσουν τις πρακτικές ασφάλειάς τους με τις απαιτήσεις της Οδηγίας NIS2. Η εφαρμογή ή η αναθεώρηση ενός συστήματος κυβερνοασφάλειας είναι μια τεράστια εργασία λαμβάνοντας υπόψη την πολυπλοκότητα της νομοθεσίας. Ως εκ τούτου, οι οργανισμοί θα πρέπει να αρχίσουν να προετοιμάζονται από τώρα:

- αξιολογώντας εάν και, εάν ναι, σε ποιο βαθμό θα υπόκεινται στις (νέες) κυβερνοασφαλειακές υποχρεώσεις σύμφωνα με την Οδηγία NIS2 και προετοιμαζόμενοι για τις απαραίτητες προσαρμογές.
- όπου είναι εφαρμοστέο, σχεδιάζοντας επαρκείς οικονομικούς και ανθρώπινους πόρους για την εφαρμογή, ορίζοντας έναν υπεύθυνο πρόσωπο και εμπλέκοντας αρμόδιους εξωτερικούς συνεργάτες εγκαίρως για την υποστήριξη στην εφαρμογή.

ΠΙΝΑΚΑΣ 3

Ουσιαστικές Οντότητες	Σημαντικές Οντότητες
• Τακτικοί και στοχευμένοι έλεγχοι ασφαλείας (προληπτικοί) • Έλεγχοι επιτόπου • Πρόστιμα έως 2% του ετήσιου παγκόσμιου τζίρου, ή 10.000.000 ελάχιστο	• Έλεγχοι μόνο σε περίπτωση βάσιμων υποψιών (εκ των υστέρων) • Επιτόπιες επιθεωρήσεις και εξωτερικά μέτρα επιβολής εκ των υστέρων • Πρόστιμα έως 1,4% του ετήσιου παγκόσμιου τζίρου, ή 7.000.000 μέγιστο

Cover Issue

- εντοπίζοντας και εφαρμόζοντας κατάλληλα μέτρα, συμπεριλαμβανομένης της προσαρμογής των εσωτερικών διαδικασιών της εταιρείας και των κυβερνοασφαλειακών διατάξεων ανάλογα.

Αναλυτικότερα, οι οργανισμοί θα πρέπει να υιοθετήσουν μια **προληπτική προσέγγιση για τη συμμόρφωση με την Οδηγία NIS2**, εκμεταλλευόμενοι τον πολύτιμο χρόνο πριν επιβληθούν πλήρως οι απαιτήσεις, που θα περιλαμβάνει κατ' ελάχιστο:

1. **Κατανόηση του νομικού πλαισίου που διέπει την λειτουργία του οργανισμού**

Καταρχάς, οι οργανισμοί θα πρέπει να κατανοήσουν εάν εμπίπτουν στο πεδίο εφαρμογής της Οδηγίας NIS2. Αν ναι, οι επιχειρήσεις πρέπει να γνωρίζουν εάν θα υπόκεινται σε προληπτική ρυθμιστική επίβλεψη (βασικά οντότητες) ή όχι (σημαντικές οντότητες). Εκτός από το πεδίο εφαρμογής Οδηγίας NIS2, η αναγνώριση άλλων πιθανών κανονιστικών πλαισίων στα οποία ο οργανισμός ίσως χρειαστεί να συμμορφωθεί στο μέλλον, όπως η Οδηγία Ανθεκτικότητας Κρίσιμων Οντοτήτων (CER) και ο Κανονισμός για την Τεχνητή Νοημοσύνη της ΕΕ (EU AI Act), μπορεί επίσης να ωφελήσει μακροπρόθεσμα.

2. **Αξιολόγηση της ικανότητάς συμμόρφωσης**

Η κατανόηση του βαθμού συμμόρφωσης του οργανισμού με την Οδηγία NIS2 θα βοηθήσει στην καθορισμό μιας βάσης συμμόρφωσης και θα καθοδηγήσει τις προσπάθειες για το κλείσιμο των πιθανών κενών. Ένα χρήσιμο εργαλείο είναι ένα πλαίσιο ελέγχου κυβερνοασφάλειας - η αντιστοίχιση συγκεκριμένων ελέγχων που εφαρμόζονται εντός του οργανισμού σε κάθε άρθρο της Οδηγίας NIS2 μπορεί να βοηθήσει σε μεγάλο βαθμό στον καθορισμό των κενών. Οι αξιολογήσεις της τρέχουσας κατάστασης πρέπει να καλύπτουν τους τομείς της κυβερνοασφάλειας, από τη διακυβέρνηση και την αναφορά έως τους τεχνικούς ελέγχους προστασίας δεδομένων, αξιολογώντας τη λειτουργική αποτελεσματικότητα των ελέγχων που έχουν τεθεί σε εφαρμογή και εντοπίζοντας πιθανά κενά ελέγχου.

3. **Ενεργή δοκιμή των διαδικασιών αντίδρασης σε περιστατικά**

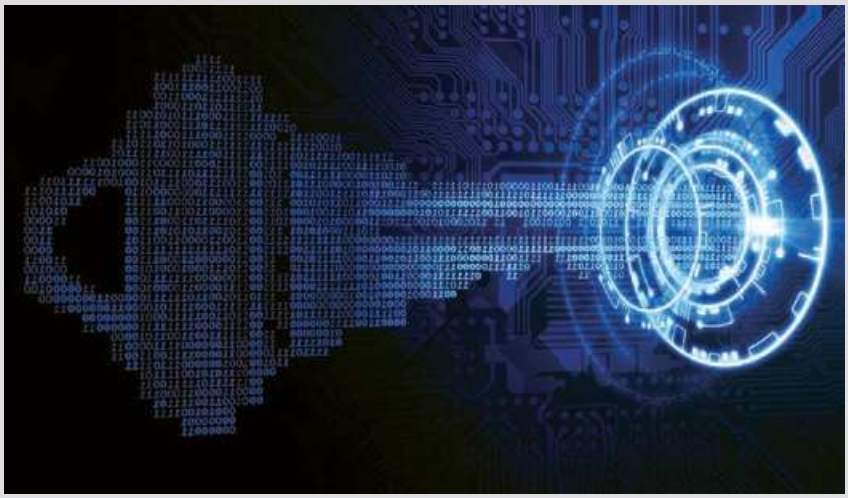
Οι ανασκοπήσεις και οι εκτενείς δραστηριότητες προσομοίωσης κρίσης είναι αποτελεσματικοί τρόποι για την περιοδική αξιολόγηση της ικανότητας του οργανισμού να αντιδράσει σε κυβερνοεπιθέσεις. Όλοι οι εμπλεκόμενοι, συμπεριλαμβανομένων των υψηλών στελεχών και τρίτων μερών, πρέπει να γνωρίζουν τις ευθύνες τους κατά τη διάρκεια ενός περιστατικού για να διευκολυνθεί η γρήγορη, ασφαλής ανάκαμψη. Επιπλέον, η ευθύνη για την αναφορά στις αρχές και τους εξωτερικούς φορείς είναι κρίσιμη για τη συμμόρφωση - η Οδηγία NIS2 ορίζει αυστηρές απαιτήσεις αναφοράς περιστατικών με σφιχτές προθεσμίες. Η ενεργή δοκιμή της ικανότητας του οργανισμού να επικοινωνεί αποτελεσματικά εσωτερικά και εξωτερικά κατά τη διάρκεια και μετά από ένα περιστατικό είναι σημαντική, όπως και η αποτελεσματική αντιμετώπιση της ρίζας του προβλήματος του περιστατικού.

4. **Ενσωμάτωση δοκιμών ανθεκτικότητας**

Οι αρχές έχουν δώσει έμφαση στην κυβερνοανθεκτικότητα. Η Οδηγία NIS2 θεσπίζει ένα κοινό πλαίσιο για τους οργανισμούς σε όλη την Ευρωπαϊκή Ένωση όσον αφορά την ικανότητά τους να αντέχουν σε κυβερνοεπιθέσεις. Οι οργανισμοί πρέπει να εφαρμόσουν ένα πρόγραμμα δοκιμής ανθεκτικότητας σε όλες τις κύριες ψηφιακές τους πλατφόρμες και υπηρεσίες για να επιβεβαιώσουν σε ποιο βαθμό μπορούν να διατηρηθούν οι λειτουργίες σε δυσμενείς συνθήκες. Οι δοκιμές πρέπει να πραγματοποιούνται τακτικά με προσέγγιση βασισμένη στον κίνδυνο αναφορικά με το εύρος και συχνότητα τους. Οι οργανισμοί πρέπει να ορίσουν τους Στόχους Χρόνου : Ανάκαμψης (Recovery Time Objective - RTO) και τους Στόχους Σημείου Ανάκαμψης (Recovery Point Objective - RPO) για τα κρίσιμα τους συστήματα για να θέσουν τις ελάχιστες προσδοκίες για την ανάκτηση των κύριων ψηφιακών υπηρεσιών.

5. **Ανάπτυξη ενός προγράμματος διαχείρισης απειλών και ευπάθειας end-to-end**

Παράλληλα με τις δοκιμές ανθεκτικότητας, η κατανόηση των ανοιχτών ευπαθειών του οργανισμού στα πληροφοριακά συστήματα του θα βοηθήσει στην αποτελεσματική διαχείριση του κυβερνοκινδύνου. Ασκήσεις όπως σάρωση ευπαθειών πρέπει να συμπληρώνονται από χειροκίνητες δοκιμές παρείσδυσης από έμπειροι επαγγελματίες κυβερνοασφάλειας σε κύρια συστήματα. Επιπλέον, η δοκιμή ευπαθειών πρέπει να καλύπτει όλους τους τομείς που σχετίζονται με την κυβερνοασφάλεια, όχι μόνο τα παραδοσιακά συστήματα πληροφορικής. Η λειτουργική τεχνολογία (OT) μπορεί να αποτελέσει σημαντικό μέρος του ψηφιακού αποτυπώματος και της επιφάνειας επίθεσης ενός οργανισμου. Πρέπει να καθιερωθούν διαδικασίες για την τακτική δοκιμή ευπαθειών, με τα αποτελέσματα των δοκιμών να περιλαμβάνουν σχέδια αντιμετώπισης για την διόρθωση των εντοπισμένων αδυναμιών. Ο όγκος και η κρισιμότητα των ανοικτών ευπαθειών πρέπει να επικοινωνούνται μέσα στον οργανισμό ώστε να επιτευχθεί η ενίσχυση της απαραίτητης ευαισθητοποίησης των εμπλεκόμενων και η ανάληψη της ευθύνης για την ασφάλεια του οργανισμού.



6. **Αναθεώρηση των διαδικασιών διαχείρισης κινδύνων κυβερνοασφάλειας του οργανισμού**

Η τακτική αναθεώρηση και ενημέρωση των διαδικασιών διαχείρισης κινδύνων κυβερνοασφάλειας για την αντιμετόπηση των εξελισσόμενων απειλών και ευπαθειών των συστημάτων, είναι απαραίτητη. Πιθανά σημεία αδυναμίας πρέπει να αναλύονται, και να αξιόπιστα μέτρα για την προστασία ευαίσθητων πληροφοριών. Η προώθηση μιας κουλτούρας επίγνωσης και επαγρύπνησης μεταξύ των μελών της ομάδας προκειμένου να ενισχυθεί η συνολική ανθεκτικότητα της κυβερνοασφάλειας και να μειωθούν οι πιθανοί κίνδυνοι είναι επίσης επιτακτική, για την απρόσκοπτη συμμόρφωση με τις απαιτήσεις της οδηγίας.

7. **Αναθεώρηση των διαδικασιών Διαχείρισης Κινδύνων Τρίτων (TPRM) του οργανισμού**

Οι διαδικασίες Διαχείρισης Κινδύνων Τρίτων (TPRM) του οργανισμού επιβάλλεται να αξιολογούνται εκτενώς προκειμένου να ενισχυθεί η ασφάλεια και η συμμόρφωση με τις απαιτήσεις της Οδηγίας NIS2. Πρέπει να αξιολογούνται οι σχέσεις με τους προμηθευτές, να αναγνωρίζονται πιθανές ευπαθείες, και βεβαιώνεται η εφαρμογή αξιόπιστων στρατηγικών μείωσης κινδύνου. Η διαδικασία TPRM πρέπει να ενημερώνεται και να προσαρμόζεται τακτικά ώστε να συμμορφώνεται με τις βέλτιστες πρακτικές του κλάδου, με στόχο τη μείωση των πιθανών απειλών και τη βελτίωση της συνολικής λειτουργικής ανθεκτικότητας. Οι τακτικές αναθεωρήσεις είναι αναγκαίες προκειμένου να διατηρηθεί μια προληπτική προσέγγιση στην προστασία ευαίσθητων πληροφοριών και να διατηρηθεί η εμπιστοσύνη των ενδιαφερομένων.

8. **Αναθεώρηση της κουλτούρας και των τρόπων εργασίας σας για την αναγνώριση κινδύνων στη συμμόρφωση με τις απαιτήσεις της Οδηγίας NIS2**

Η κατανόηση της κουλτούρας και των τρόπων εργασίας έχει καίρια σημασία για τον προσδιορισμό των κινδύνων που μπορεί να αντιμετωπίσει ο οργανισμός σας στο πλαίσιο της συμμόρφωσης με το NIS2. Η εισαγωγή προηγούμενης κοινοτικής νομοθεσίας όπως ο GDPR έχει δείξει ότι η αλλαγή συμπεριφοράς είναι απαραίτητη για τη μείωση κινδύνων και την αποτροπή εκθέσεως του οργανισμού σε αποφεύγονται κινδύνους και κυρώσεις. Με δεδομένη την εισαγωγή της "προσωπικής ευθύνης" ως μέρους του NIS2, η αντιμετώπιση των απαιτήσεων αλλαγής συμπεριφοράς της διοίκησης αποτελεί έναν κύριο οικοδόμο μιας αποτελεσματικής στρατηγικής για την ανταπόκριση στο NIS2.

Οι προετοιμασίες δεν πρέπει να καθυστερούν από το γεγονός ότι οι λεπτομέρειες των κυβερνοασφαλειακών υποχρεώσεων θα διευκρινιστούν στους εθνικούς νόμους που εφαρμόζουν την Οδηγία NIS2. Προς αυτήν την κατεύθυνση, οι επηρεαζόμενες εταιρείες και φορείς θα πρέπει να συνεχίσουν να παρακολουθούν προσεκτικά τις περαιτέ-

ρω εξελίξεις και να προσαρμόζουν τον σχεδιασμό της κυβερνοασφάλειας τους όπως απαιτείται για να αποφεύγουν πιθανά κανονιστικά μέτρα, ειδικά σημαντικές διοικητικές πρόστιμα.

Η πιθανή άμεση ευθύνη των μελών της διοίκησης λειτουργεί ως πρόσθετο κίνητρο. Είναι σημαντικό για τις εταιρείες και τους φορείς να διατηρούν την ενημέρωση και τη συμμόρφωσή τους με τις νέες κυβερνοασφαλειακές απαιτήσεις προκειμένου να προστατεύουν τα δεδομένα και την ορθή λειτουργία των υπηρεσιών τους. Επιπλέον, η επενδυτική προσπάθεια και η προσήλωση στην κυβερνοασφάλεια μπορεί να αποτελέσουν ένα ανταγωνιστικό πλεονέκτημα, ενισχύοντας την εμπιστοσύνη των πελατών και των συνεργατών.

Συνολικά, η προετοιμασία για τις νέες κυβερνοασφαλειακές υποχρεώσεις είναι μια αναγκαιότητα που απαιτεί προσεκτικό σχεδιασμό, εφαρμογή και συνεχή παρακολούθηση.

ΠΡΟΚΛΗΣΕΙΣ ΚΑΙ ΕΥΚΑΙΡΙΕΣ

Οι προκλήσεις και οι ευκαιρίες που σχετίζονται με τη συμμόρφωση στις απαιτήσεις της Οδηγίας NIS2 μπορούν **να κατηγοριοποιηθούν σε διάφορες διαστάσεις**. Κυρίως, η εκπλήρωση αυστηρών απαιτήσεων ασφαλείας, η συμμόρφωση με αυστηρές αναφορές περιστατικών και η διασφάλιση της ασφάλειας της αλυσίδας εφοδιασμού αποτελούν σημαντικές προκλήσεις. Ωστόσο, η αποδοχή αυτών των απαιτήσεων προσφέρει μια ευκαιρία συμμόρφωσης μέσω της διαμόρφωσης μιας πιο ανθεκτικής κυβερνοασφάλειας και, τελικά, της μείωσης του κινδύνου διαρροής δεδομένων.

Επιπλέον, η πτυχή της **επένδυσης πόρων,** ιδιαίτερα σε τεχνολογία και εμπειρογνωμοσύνη, αποτελεί μια πρόκληση, ειδικά για μικρότερες επιχειρήσεις. Ωστόσο, η μετατροπή αυτής της πρόκλησης σε ευκαιρία μπορεί να οδηγήσει σε λειτουργικές αποδοτικότητες και καινοτομία, με τελικό όφελος για τον οργανισμό.

Επιπλέον, οι **τακτικοί και ειδικοί έλεγχοι και αξιολογήσεις που διενεργούν ανεξάρτητοι φορείς** αποτελούν προκλήσεις όσον αφορά τον πιθανό έλεγχο και τη διάθεση πόρων. Ωστόσο, αυτές οι διαδικασίες παρέχουν πολύτιμες ευκαιρίες συμμόρφωσης με το να εντοπίζουν περιοχές προς βελτίωση, βελτιώνοντας έτσι την αξιοπιστία και την ασφάλεια του οργανισμού.Η **επίδραση στους οργανισμούς**, συμπεριλαμβανομένης της πιθανής πίεσης στους πόρους και της ανάγκης προσαρμογής σε νέα πρότυπα, είναι επίσης μια αδιαμφισβήτητη πρόκληση. Ωστόσο, η επιτυχής πλοήγηση στις απαιτήσεις συμμόρφωσης μπορεί να οδηγήσει σε μια βελτιωμένη φήμη, εμπιστοσύνη και ανταγωνιστικό πλεονέκτημα στην αγορά.

Τέλος, στη βιομηχανία της κυβερνοασφάλειας, η προσαρμογή στα εξελισσόμενα πρότυπα συμμόρφωσης και η ενσωμάτωσή τους στις προσφορές υπηρεσιών αποτελούν μια σημαντική πρόκληση. Ευτυχώς, αυτή η πρόκληση δημιουργεί ευκαιρίες με το να ανοίγει νέες αγορές για λύσεις και υπηρεσίες συμμόρφωσης, επιτρέποντας στις εταιρείες κυβερνοασφάλειας να παραμείνουν μπροστά σε ένα δυναμικό και πολλές φορές μεταβαλλόμενο τοπίο.

ΕΠΙΛΟΓΟΣ

Για τους οργανισμούς, ο δρόμος προς τη συμμόρφωση με την **Οδηγία NIS2** μπορεί να είναι προκλητικός, αλλά αποτελεί μια κρίσιμη επένδυση στην ασφάλεια και την αξιοπιστία των λειτουργιών τους και, με επέκταση, του ευρύτερου ψηφιακού οικοσυστήματος.

Καθώς πλησιάζει η προθεσμία, το μήνυμα είναι σαφές: ο χρόνος για δράση είναι τώρα. Αυτό περιλαμβάνει τη διενέργεια λεπτομερών αναλύσεων κινδύνου, την εγκαθίδρυση ικανοτήτων διαχείρισης περιστατικών και τη διασφάλιση ότι όλα τα τεχνικά μέτρα, από τη διαχείριση ενημερώσεων έως την πολυπαραγοντική ταυτοποίηση, είναι σε εφαρμογή.

Αναλαμβάνοντας το πνεύμα του NIS2, οι οργανισμοί μπορούν να συμμορφωθούν με τη νέα οδηγία και να ενισχύσουν τις αμυντικές τους ικανότητες ενάντια στις διαρκώς εξελισσόμενες απειλές της ψηφιακής εποχής.

Η **συνεργασία και η κοινή εμπειρία θα είναι ζωτικής σημασίας για την πλοήγηση αυτής της μετάβασης**. Για παράδειγμα, η εκμετάλλευση υπαρχουσών διαστάσεων κυβερνοασφάλειας όπως ο ISO 27001 ή το Πλαίσιο Κυβερνοασφάλειας του NIST μπορεί να παρέχει μια στέρεα βάση για την εκπλήρωση των απαιτήσεων της Οδηγίας NIS2. Επιπλέον, η συνεχής εκπαίδευση του προσωπικού και τα προγράμματα ευαισθητοποίησης είναι ουσιώδη για την προώθηση μιας κουλτούρας ασφάλειας και προετοιμασίας σε όλα τα επίπεδα του οργανισμού.


ΝΙΚΟΣ ΓΕΩΡΓΟΠΟΥΛΟΣ
Digital Risk Insurance Broker, **Cromar Insurance Brokers** – Co founder DPO Academy, https://www.linkedin.com/in/nikos-georgopoulos/

NIS 2 & CYBER INSURANCE ΕΝΙΣΧΥΟΥΝ ΤΗΝ ΑΝΘΕΚΤΙΚΟΤΗΤΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Ο ψηφιακός μετασχηματισμός έχει δημιουργήσει μια σειρά προκλήσεων και κινδύνων για τις επιχειρήσεις τις κυβερνήσεις και τους ιδιώτες. Για την αντιμετώπιση αυτών υιοθετήθηκε η οδηγία NIS 2 που στοχεύει στην ενίσχυση της ασφάλειας στον κυβερνοχώρο και τη διασφάλιση της ανθεκτικότητας σε όλους τους κρίσιμους τομείς. Η ασφάλιση **Cyber Insurance παρέχει ένα δίχτυ οικονομικής προστασίας** και αυξάνει την δυνατότητα διαχείρισης του κινδύνου.

Η **ανθεκτικότητα στον κυβερνοχώρο** αναφέρεται στην ικανότητα ενός οργανισμού να προετοιμάζεται, να ανταποκρίνεται και να ανακάμπτει από κυβερνοεπιθέσεις. Η NIS 2 τονίζει την ανάγκη για ισχυρή ανθεκτικότητα στον κυβερνοχώρο, προτρέποντας τους οργανισμούς να υιοθετήσουν **ολοκληρωμένες στρατηγικές κυβερνοασφάλειας**. Αυτό περιλαμβάνει τακτικές αξιολογήσεις κινδύνου, εφαρμογή μέτρων ασφαλείας, όπως κρυπτογράφηση και έλεγχο ταυτότητας πολλαπλών παραγόντων, και διασφάλιση ότι υπάρχουν και δοκιμάζονται σχέδια αντιμετώπισης περιστατικών. Μια σημαντική πτυχή της ανθεκτικότητας στον κυβερνοχώρο στο πλαίσιο της NIS 2 είναι η έμφαση στην **ασφάλεια της αλυσίδας εφοδιασμού**. Οι οργανισμοί πρέπει να διασφαλίζουν ότι οι προμηθευτές και οι συνεργάτες τους τηρούν επίσης αυστηρά πρότυπα κυβερνοασφάλειας, αναγνωρίζοντας ότι τα τρωτά σημεία στην αλυσίδα εφοδιασμού μπορούν να αξιοποιηθούν για να θέσουν σε κίνδυνο τον πρωταρχικό οργανισμό.

Ο ΡΟΛΟΣ ΤΗΣ ΑΣΦΑΛΙΣΗΣ CYBER INSURANCE

Ενώ η NIS 2 παρέχει ένα κανονιστικό πλαίσιο για την ασφάλεια στον κυβερνοχώρο, η ασφάλιση Cyber Insurance προσφέρει **οικονομική προστασία** και υπηρεσίες διαχείρισης περιστατικών παραβίασης ασφάλειας μειώνοντας σημαντικά τον αντίκτυπο μιας επίθεσης και επιταχύνοντας την ανάκαμψη. Η ασφάλιση Cyber Insurance καλύπτει συνήθως το κόστος που συνδέεται με περιστατικά παραβίασης ασφάλειας, απώλειας δεδομένων, επιθέσεις ransomware μεταφοράς χρημάτων μετά από παραπλάνηση και άλλα περιστατικά στον κυβερνοχώρο. Οι ασφαλιστές συχνά απαιτούν από τους αντισυμβαλλόμενους να πληρούν συγκεκριμένα πρότυπα κυβερνοασφάλειας ως προϋπόθεση για να παρέχουν ασφαλιστική κάλυψη. Αυτό αναγκάζει τους οργανισμούς να υιοθετούν βέλτιστες πρακτικές (χρήση MFA for Remote access, εκπαίδευση του ανθρώπινου δυναμικού, τεσταρισμένες διαδικασίες ανάκτησης δεδομένων κ.α.), να διενεργούν τακτικούς ελέγχους ασφαλείας και να διατηρούν ενημερωμένα σχέδια αντιμετώπισης περιστατικών. Ο **συνδυασμός NIS 2 και Cyber Insurance**, σχηματίζει μια **άμυνα δύο επιπέδων**, διασφαλίζοντας ότι οι οργανισμοί όχι μόνο συμμορφώνονται με τους κανονισμούς αλλά και είναι προετοιμασμένοι να μετριάσουν και να ανακάμψουν αποτελεσματικά από τις απειλές στον κυβερνοχώρο. Η σύγκλιση ρυθμιστικών πλαισίων όπως η NIS 2 και των μέτρων που απαιτεί η ασφάλιση Cyber Insurance είναι ζωτικής σημασίας στο σημερινό τοπίο απειλών. Η συμμόρφωση με την NIS 2 και η επένδυση στην κυβερνοασφάλεια και στην ασφάλιση Cyber Insurance μπορούν να ενισχύσουν την ανθεκτικότητά των οργανισμών στον κυβερνοχώρο, διασφαλίζοντας τις δραστηριότητές τους και διατηρώντας την εμπιστοσύνη στην ψηφιακή εποχή.