Άρθρο

Ημερομηνία: 10 Σεπτεμβρίου 2024
Επικοινωνία: Κωνσταντίνα Λογοθέτη (+357-22555108) email: konstantina.logotheti@pwc.com

Πλοήγηση στο τελικό στάδιο συμμόρφωσης με την οδηγία NIS2

Του Μιχαήλ Σόλων Κασίνη, Διευθυντής, Υπηρεσίες Διασφάλισης Κινδύνων - Ψηφιακή Εμπιστοσύνη, PwC Κύπρου

Στο ταχέως εξελισσόμενο τοπίο των κυβερνοαπειλών, η Ευρωπαϊκή Ένωση κάνει ένα αποφασιστικό βήμα προς την ενίσχυση της κυβερνοασφάλειας και την προστασία της ψηφιακής της υποδομής με τη νέα Οδηγία για την Ασφάλεια Δικτύων και Πληροφοριών (NIS2). Αυτή η νέα οδηγία στοχεύει στη δημιουργία ενός ισχυρού πλαισίου κυβερνοασφάλειας, αντιμετωπίζοντας την επείγουσα ανάγκη για ισχυρότερη άμυνα, σε μια εποχή όπου οι επιθέσεις στον κυβερνοχώρο έχουν αυξηθεί δραματικά.

Σε αντίθεση με την προηγούμενη εκδοχή της NIS1, η βελτιωμένη οδηγία NIS2 καλύπτει ένα ευρύτερο φάσμα οργανισμών και επιβάλλει αυστηρότερες απαιτήσεις ασφαλείας. Η νέα οδηγία δεν περιορίζεται μόνο σε κρίσιμους οργανισμούς εντός της Ευρωπαϊκής Ένωσης, αλλά περιλαμβάνει και εξωτερικές οντότητες που συνεργάζονται με αυτούς. Έτσι, εξασφαλίζεται μια ολοκληρωμένη προστασία και ανθεκτικότητα. Το NIS2 θα επηρεάσει άμεσα τομείς που θεωρούνται απαραίτητοι για τη λειτουργία της κοινωνίας, διαχωρίζοντάς τους σε δύο κύριες κατηγορίες: «Υψηλής και κρίσιμης σημασίας» και «Άλλοι κρίσιμοι». Με αυτή την κίνηση, η Ευρωπαϊκή Ένωση αποσκοπεί στη δημιουργία ενός ισχυρού πλαισίου κυβερνοασφάλειας, το οποίο θα προσφέρει ουσιαστική προστασία σε ένα συνεχώς εξελισσόμενο και όλο και πιο απαιτητικό περιβάλλον κυβερνοαπειλών.

Υψηλής & κρίσιμης σημασίας τομείς	Άλλοι - κρίσιμοι τομείς
Ενέργεια	Ταχυδρομικές υπηρεσίες και υπηρεσίες Courier
Μεταφορές	Διαχείριση απορριμμάτων Υπηρεσίες που αφορούν στην αποκομιδή και διαχείριση απορριμμάτων
Τράπεζες	Κατασκευή/Παραγωγή και διανομή χημικών ουσιών

Υποδομή χρηματοπιστωτικής αγοράς	Παραγωγή/Επεξεργασία και διανομή τροφίμων
Υγεία	Κατασκευή/παραγωγή Συμπεριλαμβανομένης της παραγωγής βασικών αγαθών
Πόσιμο νερό Φορείς που ασχολούνται με την παροχή και διανομή πόσιμου νερού	Ψηφιακοί πάροχοι Πάροχοι διαδικτυακών αγορών, μηχανών αναζήτησης και υπηρεσιών κοινωνικής δικτύωσης
Λύματα Υπηρεσίες λυμάτων που ασχολούνται με την επεξεργασία και διάθεση λυμάτων	Έρευνα
Ψηφιακή υποδομή Συμπεριλαμβανομένων σημείων ανταλλαγής διαδικτύου, παρόχων υπηρεσιών συστήματος ονομάτων τομέα και υπηρεσιών υπολογιστικού νέφους	
Διαχείριση Τεχνολογιών (Β-2-Β)	
Δημόσια Διοίκηση	
Διάστημα	

Η Οδηγία εισάγει μια νέα κατηγοριοποίηση για τις επιχειρήσεις, διακρίνοντάς τις σε «Ζωτικής» σημασίας και «Σημαντικές» οντότητες. Αυτή η διάκριση καθορίζει τον τρόπο με τον οποίο οι οργανισμοί οφείλουν να πληρούν τις απαιτήσεις ασφαλείας, καθώς και τον τρόπο εποπτείας και επιβολής κυρώσεων σε περιπτώσεις μη συμμόρφωσης.

Ένας οργανισμός κατατάσσεται ως «Ζωτικής» σημασίας όταν δραστηριοποιείται σε ένα εξαιρετικά σημαντικό τομέα και υπερβαίνει τα όρια που καθορίζουν τις μεσαίες επιχειρήσεις. Οι μεσαίες επιχειρήσεις περιλαμβάνουν εκείνες που απασχολούν λιγότερα από 250 άτομα και έχουν ετήσιο κύκλο εργασιών που δεν υπερβαίνει τα 50 εκατομμύρια ευρώ ή/και ετήσιο σύνολο ισολογισμού που δεν υπερβαίνει τα 43 εκατομμύρια ευρώ.

Η NIS2 προωθεί μια ολιστική προσέγγιση για την προστασία των συστημάτων δικτύων και πληροφοριών, καθώς και του φυσικού τους περιβάλλοντος, λαμβάνοντας υπόψη όλους τους πιθανούς κινδύνους. Τα μέτρα που προβλέπονται περιλαμβάνουν συγκεκριμένες ενέργειες που πρέπει να λάβουν οι οργανισμοί για να διασφαλίσουν την ασφάλεια και τη συνέχεια των υπηρεσιών του όπως:

- Πολιτικές για την ανάλυση κινδύνων και την ασφάλεια του συστήματος πληροφοριών
- Διαχείριση περιστατικών

- Επιχειρησιακή συνέχεια, όπως είναι η διαχείριση αντιγράφων ασφαλείας και η ανάκτηση από καταστροφές, καθώς και η διαχείριση κρίσεων
- Ασφάλεια της εφοδιαστικής αλυσίδας, συμπεριλαμβανομένων των πτυχών που σχετίζονται με την ασφάλεια που αφορούν τις σχέσεις μεταξύ κάθε οντότητας και των άμεσων προμηθευτών ή παρόχων υπηρεσιών της
- Ασφάλεια στην απόκτηση, ανάπτυξη και συντήρηση των δικτύων και των συστημάτων πληροφοριών, συμπεριλαμβανομένης της διαχείρισης και της αποκάλυψης τρωτών σημείων
- Πολιτικές και διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων στον κυβερνοχώρο
- Βασικές πρακτικές κυβερνο-υγιεινής και εκπαίδευση στην κυβερνοασφάλεια
- Πολιτικές και διαδικασίες σχετικά με τη χρήση κρυπτογραφίας και, όπου κρίνεται σκόπιμο, την κρυπτογράφηση
- Ασφάλεια του ανθρώπινου δυναμικού, πολιτικές ελέγχου πρόσβασης και διαχείριση περιουσιακών στοιχείων
- Χρήση πολυπαραγοντικού ελέγχου ταυτότητας ή λύσεων συνεχούς ταυτοποίησης, ασφαλείς επικοινωνίες φωνής, βίντεο και κειμένου, καθώς και ασφαλή συστήματα έκτακτης επικοινωνίας εντός της οντότητας, όπου κρίνεται σκόπιμο

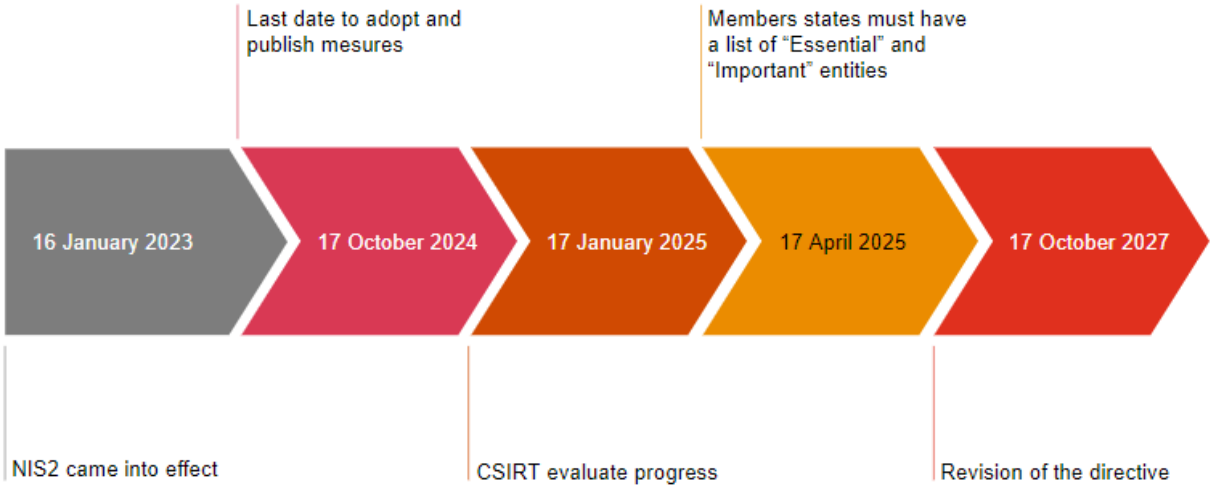
Η νέα Οδηγία εισάγει νέες αυστηρότερες υποχρεώσεις αναφοράς σε περίπτωση περιστατικών ασφάλειας. Οι οργανισμοί υποχρεούνται να ενημερώνουν άμεσα την τοπική CSIRT (Ομάδα Αντιμετώπισης Συμβάντων Ασφαλείας) ή, όπου αυτό είναι δυνατό, την αρμόδια Αρχή. Η έγκαιρη προειδοποίηση πρέπει να περιλαμβάνει ένδειξη για το αν το περιστατικό ενδέχεται να οφείλεται σε παράνομες ή κακόβουλες ενέργειες και εάν μπορεί να έχει διασυνοριακό αντίκτυπο.

Οι οργανισμοί καλούνται επίσης να πραγματοποιούν τακτικούς ελέγχους, σαρώσεις ασφαλείας, επιθεωρήσεις επιτόπου και εξ αποστάσεως καθώς και να παρέχουν δεδομένα και τεκμηρίωση όταν τους ζητηθεί. **Η Οδηγία NIS2 σηματοδοτεί μια σημαντική στροφή από την πιο εθελοντική προσέγγιση της προηγούμενης νομοθεσίας, με τη μη συμμόρφωση να επιφέρει αυστηρές κυρώσεις.** Αυτές περιλαμβάνουν **εντολές συμμόρφωσης, δεσμευτικές οδηγίες, ποινικές κυρώσεις για τα διοικητικά στελέχη, καθώς και οικονομικές κυρώσεις, παρόμοιες με εκείνες του GDPR**, σε περίπτωση που δεν τηρηθούν οι απαιτήσεις εντός των προβλεπόμενων χρονικών πλαισίων.

Οι βασικές οντότητες αντιμετωπίζουν **πρόστιμα ύψους τουλάχιστον 10 εκατομμυρίων ευρώ ή το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών τους**, όποιο από τα δύο είναι υψηλότερο. Οι σημαντικές επιχειρήσεις κινδυνεύουν με πρόστιμα ύψους τουλάχιστον 7 εκατομμυρίων ευρώ ή 1,4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών, όποιο από τα δύο είναι υψηλότερο.

Αξίζει να σημειωθεί ότι για τα **υψηλόβαθμα στελέχη σε οργανισμούς που δεν συμμορφώνονται** με την Οδηγία NIS2, οι συνέπειες μπορεί να είναι σοβαρές, όπως η **απώλεια της δυνατότητας να κατέχουν θέσεις σε εκτελεστικά συμβούλια. Για να προετοιμαστούν κατάλληλα, οι οργανισμοί πρέπει να λάβουν μια σειρά από μέτρα:**

- Προσδιορισμός της ανάγκης συμμόρφωσης με την οδηγία
- Εκτέλεση αξιολόγησης κινδύνου για τον εντοπισμό κενών ασφαλείας
- Εφαρμογή των απαραίτητων μέτρων ασφαλείας
- Επαλήθευση της συμμόρφωσης των προμηθευτών για την ασφάλεια
- Δοκιμή και αξιολόγηση των μέτρων για να διασφαλιστεί ότι λειτουργούν όπως προβλέπεται και πραγματοποίηση αλλαγών όπου αυτό είναι απαραίτητο
- Προώθηση της ευαισθητοποίησης για την ασφάλεια στο ανθρώπινο δυναμικό



Η νέα Οδηγία NIS2, η οποία φέρνει σημαντικές αλλαγές στον τομέα της κυβερνοασφάλειας, αναμένεται να τεθεί **σε ισχύ στις 17 Οκτωβρίου 2024**. Με λιγότερο από τέσσερις μήνες να απομένουν για την προετοιμασία, οι οργανισμοί καλούνται να προσαρμοστούν στις νέες απαιτήσεις, οι οποίες θα επηρεάσουν άμεσα τις δομές και τις διαδικασίες τους.

Πώς μπορεί να σας βοηθήσει η PwC

Με την επίσημη έγκριση της NIS2, οι οντότητες που εμπίπτουν στο πεδίο εφαρμογής της πρέπει να προετοιμαστούν για τα επερχόμενα εθνικά μέτρα μεταφοράς. Η προηγούμενη εμπειρία με άλλους κανονισμούς έδειξε ότι η προληπτική αντιμετώπιση πιθανών ζητημάτων αποφέρει καλύτερα αποτελέσματα από την προσπάθεια διόρθωσης προβλημάτων εκ των υστέρων. Ο έγκαιρος σχεδιασμός επιτρέπει τον έγκαιρο εντοπισμό και την ιεράρχηση των περιοχών που χρειάζονται σημαντικές επενδύσεις.

Ενώ η NIS2 εναρμονίζει τις απαιτήσεις διαχείρισης κινδύνων στον κυβερνοχώρο και αυτές της αναφοράς, πολλές υποχρεώσεις ευθυγραμμίζονται με τους υπάρχοντες κανονισμούς και πρότυπα. Αυτό επιτρέπει μια προληπτική προσέγγιση που θα συνδυάζει την αξιολόγηση της ετοιμότητας και που θα μπορεί να χειρίζεται τις πολλαπλές απαιτήσεις του πολύπλοκου ρυθμιστικού περιβάλλοντος.

Εμπειρία και εξειδίκευση

Διαθέτουμε εμπειρογνώμονες υψηλής ειδίκευσης στους τομείς του ελέγχου συστημάτων πληροφορικής, της ασφάλειας πληροφοριών, της νομικής υποστήριξης και της συμμόρφωσης. Η ομάδα μας είναι σε θέση να παρέχει ολοκληρωμένες λύσεις που ανταποκρίνονται στις ιδιαίτερες ανάγκες κάθε οργανισμού.

Τεχνογνωσία του κλάδου

Προσφέρουμε εξατομικευμένες λύσεις προσαρμοσμένες σε κρίσιμους και εξαιρετικά κρίσιμους τομείς, εξασφαλίζοντας ότι οι πελάτες μας μπορούν να ανταποκριθούν αποτελεσματικά στις απαιτήσεις της NIS2 και να ενισχύσουν την ανθεκτικότητά τους απέναντι σε κυβερνοαπειλές.

Ολοκληρωμένη προσέγγιση

Από την αρχική ανάλυση των επιπτώσεων μέχρι την εφαρμογή των απαραίτητων μέτρων, η PwC βρίσκεται δίπλα σας σε κάθε βήμα της διαδικασίας. Προσφέρουμε πλήρη υποστήριξη για να διασφαλίσουμε ότι η μετάβασή σας στις νέες απαιτήσεις είναι ομαλή και αποτελεσματική.

Παγκόσμιο Δίκτυο

Με την υποστήριξη του παγκόσμιου δικτύου EMEA NIS2, η PwC διαθέτει πρόσβαση σε πόρους και τεχνογνωσία σε ολόκληρη την Ευρωπαϊκή Ένωση και πέραν αυτής. Αυτό μας επιτρέπει να βοηθήσουμε τους πελάτες μας να επιτύχουν διασυνοριακή συμμόρφωση με την οδηγία, ανταποκρινόμενοι στις προκλήσεις ενός ολοένα και πιο διασυνδεδεμένου κόσμου.