

DTS

NIS2 & DTS IDENTITY

Σωστή και βιώσιμη εφαρμογή των απαιτήσεων για συμμόρφωση με τον ευρωπαϊκό κανονισμό ασφαλείας NIS2, με τη χρήση της πλατφόρμας ασφαλείας DTS-IDENTITY.

1. ΤΙ ΕΙΝΑΙ Η ΟΔΗΓΙΑ NIS2;

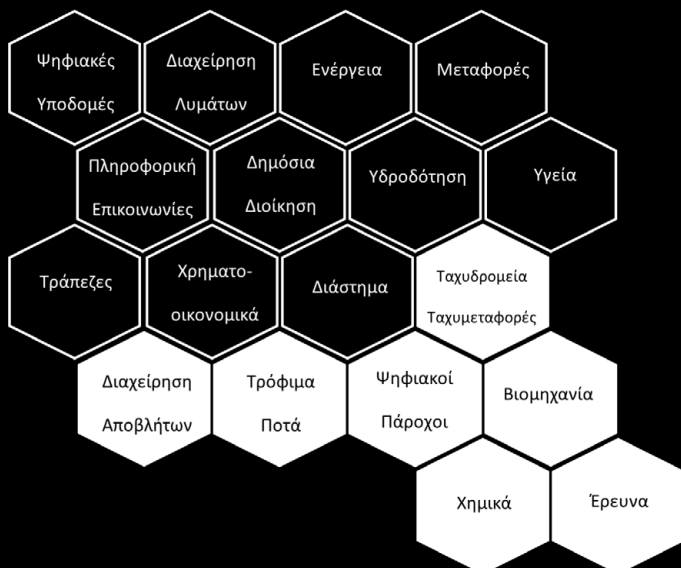
- Μια νέα οδηγία της Ε.Ε. για την προστασία των δικτύων & την αύξηση του βαθμού ασφάλειας των πληροφοριακών συστημάτων
- Χρησιμοποιείται, μαζί με τον Ευρωπαϊκό Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR), για την ενίσχυση της ασφάλειας στον τομέα πληροφορικής στην Ε.Ε.

2. ΠΟΤΕ ΤΙΘΕΤΑΙ ΣΕ ΙΣΧΥ Η NIS2;

- Ισχύει στην Ε.Ε. από την **1η Ιανουαρίου 2023**
- Η οδηγία ενσωματώθηκε στην Ελληνική εθνική νομοθεσία τον Νοέμβριο του 2024, μετά την οποία ισχύουν υποχρεωτικά τα μέτρα ασφαλείας

3. ΠΟΙΟΥΣ ΑΦΟΡΑ Η NIS2;

- Αφορά εταιρείες που έχουν περισσότερους από **50 εργαζομένους** ή ετήσιο κύκλο εργασιών άνω των **10 εκατομμυρίων ευρώ** και
- Ανήκουν σε έναν από τους εξής 18 τομείς:



4. ΑΠΑΙΤΗΣΕΙΣ ΣΥΜΦΩΝΑ ΜΕ ΤΗ NIS2:

- Διαχείριση περιουσιακών στοιχείων (Asset Management)
- Επιχειρησιακή συνέχεια & διαχείριση κρίσεων
- Διαχείριση ευπαθειών
- Ενσωμάτωση σύγχρονων μέτρων συμμόρφωσης
- Διαχείριση κινδύνων (αποτελεσματικά μέτρα ασφαλείας)
- Διαχείριση περιστατικών (Incident Management)
- Κρυπτογράφηση, ιδιαίτερα για την επικοινωνία
- Ασφάλεια στην εφοδιαστική αλυσίδα
- Ασφάλεια προσωπικού (εκπαίδευση, ελεγχόμενη πρόσβαση, πολιτική εξουσιοδοτήσεων)
- Υποχρέωση καταγραφής, υποχρέωση αναφοράς, κυρώσεις, ευθύνη

5. ΤΟΜΕΙΣ ΠΟΥ ΒΕΛΤΙΩΝΟΝΤΑΙ ΜΕ ΤΗΝ ΕΝΙΣΧΥΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ:

- Επιχειρησιακή συνέχεια: Διαχείριση αντιγράφων ασφαλείας, αποκατάσταση καταστροφών, διαχείριση κρίσεων
- Αποτελεσματικότητα: Προδιαγραφές για την αξιολόγηση των μέτρων αντιμετώπισης των κινδύνων στον κυβερνοχώρο
- Προμήθειες: Ασφάλεια στην προμήθεια συστημάτων πληροφορικής
- Διαχείριση περιστατικών: Πρόληψη, ανίχνευση & διαχείριση περιστατικών ασφαλείας
- Επικοινωνία: Ασφαλής μεταφορά φωνής, εικόνας & κειμένου
- Κρυπτογραφία: Κρυπτογράφηση όπου είναι δυνατόν
- Πολιτικές: Κατευθυντήριες γραμμές για κινδύνους
- Εφοδιαστική αλυσίδα: Ασφάλεια στην εφοδιαστική αλυσίδα
- Έλεγχος πρόσβασης: Χρήση MFA & SSO

Με την πλατφόρμα ταυτότητας DTS, σας βοηθάμε σημαντικά με τα απαραίτητα μέτρα!



6. ΤΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ DTS IDENTITY ΠΟΥ ΣΑΣ ΒΟΗΘΟΥΝ ΣΤΗ ΣΥΜΜΟΡΦΩΣΗ ΜΕ ΤΙΣ ΑΠΑΙΤΗΣΕΙΣ ΤΗΣ NIS2:

- ✓ Έλεγχος πρόσβασης, διαχείριση πρόσβασης & διαχείριση προφίλ:
 - Customer Identity & Access Management (IAM & CIAM) διασφαλίζει μέσω μιας κεντρικής πλατφόρμας, ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση στα πληροφοριακά συστήματα του κάθε οργανισμού. Επιπλέον, το DTS Identity προστατεύει τα ευαίσθητα δεδομένα σας και αυξάνει το συνολικό επίπεδο ασφάλειας.
 - Multi Factor Authentication (MFA) & Single-Sign-On (SSO), τόσο για τοπικές όσο και για cloud εφαρμογές: Συνδέστε μία φορά μέσω MFA και έχετε πρόσβαση για όλες τις προ-εγκεκριμένες εφαρμογές.
 - Κεντρικός εύχρηστος πίνακας ελέγχου για τη "self service" διαχείριση της πλατφόρμας και με δυνατότητα παραμετροποίησης ανάλογα με τις εκάστοτε απαιτήσεις.
- ✓ Πολιτικές:
 - Conditional Access: Καθορισμός δικαιωμάτων για το ποιος επιτρέπεται να έχει πρόσβαση σε συγκεκριμένες εφαρμογές και πληροφορίες, από πού και με ποιο MFA.
 - Role-based access control (RBAC): Δυνατότητα ανάθεσης ρόλων στους χρήστες, δίνοντας τους άμεσα τα προκαθορισμένα δικαιώματα πρόσβασης που χρειάζονται. Αυτό επιτρέπει τη διατήρηση εποπτείας και τον έλεγχο της πρόσβασης στις εφαρμογές.
- ✓ Διαχείριση περιστατικών:
 - Πρόληψη & ανίχνευση, δίνοντας τη δυνατότητα ιχνηλασιμότητα των δικαιωμάτων πρόσβασης και των συνδέσεων με μια ματιά.
 - Διαχείριση: Όλα τα δικαιώματα πρόσβασης μπορούν να ανακληθούν άμεσα.
- ✓ Κρυπτογραφία:
 - Κρυπτογράφηση: Κανένας κωδικός πρόσβασης δεν αποθηκεύεται στο DTS Identity και όλοι μεταβιβάζονται σε κρυπτογραφημένη μορφή.
 - Ανίχνευση παραβιασμένων κωδικών πρόσβασης: Η αναγνώριση παραβιασμένων κωδικών πρόσβασης επιτρέπει άμεση αντίδραση.
- ✓ Εφοδιαστική αλυσίδα: Ασφάλεια στην εφοδιαστική αλυσίδα με την ενσωμάτωση των συνεργατών στο DTS Identity μέσω κατάλληλων B2B αδειών.
- ✓ Αποτελεσματικότητα: Αξιολόγηση των μέτρων κυβερνοασφάλειας & διαχείρισης κινδύνων, καθώς το DTS Identity Reporting είναι διαθέσιμο ανά πάσα στιγμή.
- ✓ Επικοινωνία: Ασφαλής μεταφορά φωνής, εικόνας και κειμένου, μέσω ενσωμάτωσης στο DTS Identity.
- ✓ Ύψιστη ασφάλεια:
 - Αρχιτεκτονική Secure-by-Design, βασισμένη στην αρχή Zero Trust (περιβάλλον gclustered K8s ανθεκτικό σε επιθέσεις brute force, απειλές και DDoS).
 - Παρέχεται από τα δικά μας, πιστοποιημένα, συμβατά κατά GDPR και εντός E.E. data center.

ΕΠΙΧΕΙΡΗΜΑΤΙΚΗ ΕΥΕΛΙΞΙΑ

Η λύση είναι βασισμένη στο cloud, αυτό επιτρέπει την ευέλικτη προσαρμογή στις ατομικές απαιτήσεις. Μπορεί να υλοποιηθεί γρήγορα και είναι επεκτάσιμη, καθιστώντας ευκολότερη την προσαρμογή στις αλλαγές του επιχειρηματικού τοπίου.

ΑΥΞΗΜΕΝΗ ΑΣΦΑΛΕΙΑ

Η λύση μειώνει τον κίνδυνο κυβερνοεπιθέσεων και πιθανών περιστατικών ασφάλειας που θα μπορούσαν να βλάψουν τη φήμη της εταιρείας, βοηθώντας στην ενίσχυση της ασφάλειας και την προστασία ευαίσθητων δεδομένων.

ΜΕΙΩΣΗ ΚΟΣΤΟΥΣ & ΠΟΛΥΠΛΟΚΟΤΗΤΑΣ

Η ενσωμάτωση λειτουργιών ασφάλειας συνδυάζει ξεχωριστά προϊόντα ασφάλειας και καθιστά την κατανομή των αδειών χρήσης των διαφόρων εφαρμογών ορατή και ευκολότερη στον έλεγχο. Αυτό οδηγεί σε εξοικονόμηση κόστους και μείωση της πολυπλοκότητας.

ΑΥΞΗΣΗ ΠΑΡΑΓΩΓΙΚΟΤΗΤΑΣ ΧΡΗΣΤΩΝ

Καθώς είναι απλό και εύκολο στη χρήση αυξάνει την αποδοτικότητα των χρηστών, παρέχοντας τη δυνατότητα για γρήγορη και ασφαλή σύνδεση από οποιαδήποτε τοποθεσία, ανεξαρτήτως των συσκευών που χρησιμοποιούνται και για όλες τις εφαρμογές.

Επικοινωνήστε μαζί μας για μια λεπτομερή ενημέρωση.