MICHAIL CHOURDAKIS
09/11/2025 09:31

ΧΟΥΡΔΑΚΗΣ Γ. ΜΙΧΑΗΛ

ΜΟΥΣΙΚΟΛΟΓΟΣ – ΕΚΠΑΙΔΕΥΤΙΚΟΣ
ΔΙΔΑΚΤΩΡ ΜΗΧΑΝΙΚΟΣ DSP
Ανδρόνικου 11, Μαρούσι, 15122
Τηλ.: 2155000007, 6944822488
e-mail: chourdakismichael@gmail.com

Άλιμος, 11 – 9 – 2025 09:30. Α.Π. 15777.

Αναλυτική έκθεση συμμόρφωσης των ηλεκτρονικών υπηρεσιών του Μουσικού Σχολείου Αλίμου με την οδηγία NIS2 – EU 2022/2555.

Το παρόν έγγραφο συντάσσεται στο πλαίσιο συμμόρφωσης με την Οδηγία (ΕΕ) 2022/2555 – NIS2 και τον Νόμο 4961/2022 για την κυβερνοασφάλεια. Σκοπός είναι η τεκμηρίωση των μέτρων ασφάλειας, πρόληψης και διαχείρισης περιστατικών των πληροφοριακών συστημάτων του Μουσικού Σχολείου Αλίμου.

ΑΡΘΡΟ 1 : Διαχείριση Ασφάλειας Πληροφοριών

Παράγραφος 1. Πολιτική Ασφαλείας.

Πρόσβαση στα ηλεκτρονικά συστήματα έχουν:

1. Ο κ. Χουρδάκης Μιχαήλ ως administrator και επόπτης της υπηρεσίας, καθολική πρόσβαση σε επίπεδο βάσης δεδομένων και Server.
2. Η Διεύθυνση του σχολείου σε όλες τις πληροφορίες που αφορούν το σχολείο και που προσφέρονται μέσω του msa-apps.com.
3. Οι εκπαιδευτικοί του σχολείου στα μέρη που τους αφορούν.
4. Οι γονείς των μαθητών του σχολείου στα μέρη που τους αφορούν.

Παράγραφος 2. Διαβαθμισμένη πρόσβαση.

Η διαβαθμισμένη πρόσβαση στα ηλεκτρονικά συστήματα πραγματοποιείται

- Με τους κωδικούς Taxisnet σύμφωνα με την ΥΑ
- Με τους κωδικούς δημόσιας διοίκησης σύμφωνα με την ΥΑ
- Με την υπηρεσία SSO του ΠΣΔ που διατίθεται σε όλους τους φορείς του
- Με βιομετρικά δεδομένα εφόσον ο χρήστης δώσει συγκατάθεση.

Σύμφωνα με την ΥΑ το σχολείο χρησιμοποιεί 2 factor authentication σε υπηρεσίες κρίσιμης σημασίας, ταυτοποιώντας τους χρήστες με SMS.

Όλοι οι χρήστες των υπηρεσιών (εκπαιδευτικοί, κηδεμόνες) έχουν ενημερωθεί για τους όρους διαβαθμισμένης πρόσβασης.

ΑΡΘΡΟ 2 : Τεχνικά Μέτρα Πρόληψης

Παράγραφος 1. Server-Side Configuration

Ο server χρησιμοποιεί λογισμικό που αναβαθμίζεται καθημερινά, τελευταίες εκδόσεις Alma Linux + nginx + PHP + SQLite με καθημερινά security + feature updates.

Η υποδομή του server είναι σε VPS που παρέχεται από την ΕΔΥΤΕ Α.Ε. (Ν.4727/2020).

Χρησιμοποιούνται τυπικές ενέργειες αποφυγής κοινών επιθέσεων, ενδεικτικά προστασία SQL Injection, nginx proxy κλπ. Σε κανένα σημείο της βάσης δεδομένων δεν αποθηκεύονται προσωπικοί κωδικοί χρήστη ούτε ως plaintext ούτε ως hashed data.

Γίνεται καθημερινό backup της βάσης δεδομένων. Τα backups φυλάσσονται σε offline αντίγραφο στο σχολείο.

Οι υπηρεσίες επιτηρούνται μέσω τα συστήματα Logging που υπάρχουν στο λειτουργικό. Υπάρχει ενεργή πολιτική ενημερώσεων και ανανέωσης SSL/TLS μέσω letsencrypt/certbot. Τα δεδομένα μεταφέρονται αποκλειστικά μέσω HTTPS (TLS 1.3).

Οι υπηρεσίες λειτουργούν αποκλειστικά μέσω TLS 1.2/1.3 με ενεργοποιημένο HSTS header και ισχυρές σουίτες κρυπτογράφησης (AES-256 GCM / ChaCha20). Η συμβατότητα με παλαιότερα συστήματα αξιολογείται περιοδικά ώστε να διατηρείται η ασφάλεια χωρίς να θίγεται η προσβασιμότητα.

Γίνεται τακτικός έλεγχος ασφάλειας του server με penetration testing εργαλεία καθώς και εργαλεία ελέγχου ασφαλείας εισόδου (ssllabs.com).

Παράγραφος 2. Client-Side Configuration

Χρησιμοποιούνται well-known βιβλιοθήκες για την προβολή των υπηρεσιών, (Bootstrap, Bulma, Foundation, jQuery κλπ.).

ΑΡΘΡΟ 3 : Εκπαίδευση Ανθρώπινου Δυναμικού

Οι εκπαιδευτικοί και η Διεύθυνση του σχολείου συμμετέχουν σε βασική εκπαίδευση κυβερνοασφάλειας (phishing awareness, διαχείριση δεδομένων κλπ.). Η εκπαίδευση πραγματοποιείται κάθε χρόνο, ιδίως σε νέους συναδέλφους.

Οι γονείς ενημερώνονται πριν ακόμα εισαχθούν τα παιδιά τους στο σχολείο μας (με τη διαδικασία των εισαγωγικών εξετάσεων) για την πολιτική απορρήτου, προστασίας προσωπικών δεδομένων και έννομες συνέπειες των ηλεκτρονικών ενεργειών τους.

Οι μαθητές ενημερώνονται για ασφαλή χρήση διαδικτύου και υπηρεσιών cloud ανά τακτά χρονικά διαστήματα είτε μέσω ημερίδων ασφαλούς χρήσης δικτύου είτε μέσω των τεχνολογικών μαθημάτων του σχολείου.

ΑΡΘΡΟ 4 : Διαχείριση Περιστατικών

Σύμφωνα με το καθορισμένο "Σχέδιο Αντιμετώπισης Περιστατικών Ασφάλειας", σε περίπτωση σοβαρού περιστατικού:

- Ενημερώνεται άμεσα ο διαχειριστής (κ. Χουρδάκης Μιχαήλ).
- Καταγράφεται το περιστατικό σε φόρμα συμβάντος.
- Ενημερώνεται η Διεύθυνση και, εφόσον απαιτείται, η ΕΔΥΤΕ Α.Ε. και η Εθνική Αρχή Κυβερνοασφάλειας.
- Ενημερώνεται το Υπουργείο Ψηφιακής Διακυβέρνησης
- Διενεργείται εσωτερική αξιολόγηση και προτείνεται διορθωτική ενέργεια.

Μέχρι σήμερα και από το 2016 που λειτουργούν τα ηλεκτρονικά συστήματα του σχολείου μας δεν έχουν αντιμετωπιστεί προβλήματα κυβερνοασφάλειας.

ΑΡΘΡΟ 5 : Καταγραφή και Τεκμηρίωση

Πραγματοποιείται συστηματική καταγραφή (logging) στις ενέργειες που πραγματοποιούνται στα ηλεκτρονικά συστήματα, ιδίως αυτά που συνεργάζονται με το Υπουργείο Ψηφιακής Διακυβέρνησης (Εθνικό Μητρώο Επικοινωνίας, Αποστολή SMS κλπ.). Οι βάσεις δεδομένων διατηρούνται επ' αόριστον. Τα αρχεία συμβάντων (logs) τηρούνται για τουλάχιστον 12 μήνες και είναι προσβάσιμα μόνο από εξουσιοδοτημένο προσωπικό.

ΑΡΘΡΟ 6 : Αξιολόγηση

Η συμμόρφωση με την οδηγία NIS2 αξιολογείται ετησίως και τυχόν αδυναμίες τεκμηριώνονται και προγραμματίζονται διορθωτικές ενέργειες.

Η πολιτική αναθεωρείται με βάση τις νέες τεχνολογικές εξελίξεις στον τομέα της κυβερνοασφάλειας.

Ο ΕΠΟΠΤΗΣ ΤΗΣ ΥΠΗΡΕΣΙΑΣ
Χουρδάκης Μιχαήλ