



BLUE VALUE
training and operational services

NIS2

Ασφάλεια Δικτύων και Πληροφοριών

- Αξιολόγηση Κινδύνων και Συμμόρφωσης
- Προστασία από Κυβερνοεπιθέσεις
- Ανθεκτικότητα των Συστημάτων και Business Continuity
- Εκπαίδευση Ετοιμότητας Προσωπικού
- Συνεχής Συμμόρφωση και Αξιολόγηση

Contact Us

 bluevalue.gr  info@bluevalue.gr  2310 590196

Αξιολόγηση Κινδύνων και Συμμόρφωσης

Άρθρα 21, 32 και 85 της Οδηγίας NIS2

Για τη συμμόρφωση με τις απαιτήσεις της Οδηγίας NIS2 είναι απαραίτητο να κατανοηθούν, σε βάθος, οι υπάρχουσες απειλές αλλά και οι ευπάθειες ενός Οργανισμού. Για τον σκοπό αυτόν, αναπτύσσουμε διαδικασίες για τη διαχείριση και γνωστοποίηση ευπαθειών.

Η αξιολόγηση κινδύνου και συμμόρφωσης είναι το πρώτο βήμα για την ενίσχυση της κυβερνοασφάλειας. Επιπλέον, εφαρμόζουμε τεχνικές αξιολόγησης ευπαθειών.

Τι παρέχουμε

- **Gap Analysis:** Διενεργούμε αξιολόγηση της παρούσας κατάστασης του Φορέα, σύμφωνα με τις απαιτήσεις της Οδηγίας NIS2, αναδεικνύοντας τις περιοχές που χρειάζονται βελτίωση
- **Vulnerability Assessment και Penetration Testing:** Διενεργούμε αξιολόγηση ευπαθειών και προσομοιωμένες επιθέσεις, για να διασφαλίσουμε την ανθεκτικότητα των συστημάτων του Φορέα

Προστασία από Κυβερνοεπιθέσεις

Άρθρα 89 και 32 της Οδηγίας NIS2

Για την αποτελεσματική προστασία των συστημάτων ενός Φορέα από κυβερνοεπιθέσεις, το Άρθρο 89 της Οδηγίας NIS2 απαιτεί τη χρήση λύσεων, όπως το Endpoint Protection Platform (EPP) και τείχη προστασίας για τη δικτυακή τμηματοποίηση.

Το Άρθρο 32 ορίζει τη συνεχή παρακολούθηση και διαχείριση της ασφάλειας των συστημάτων, η οποία ενισχύεται με την υλοποίηση συστημάτων SIEM.

Τι παρέχουμε

- **Εγκατάσταση πλατφόρμας Endpoint Security (EPP):** Προσφέρουμε λύσεις προστασίας των Endpoints (π.χ. υπολογιστές, κινητά) από κακόβουλο λογισμικό και άλλες επιθέσεις

- **Εγκατάσταση και παραμετροποίηση Firewall:** Με τη χρήση τειχών προστασίας διασφαλίζουμε τη δικτυακή τμηματοποίηση και τη συνεχή παρακολούθηση της κυκλοφορίας
- **Εγκατάσταση Συστήματος PAM και SIEM:** Παρέχουμε λύσεις διαχείρισης προνομιακής πρόσβασης PAM και SIEM για ενίσχυση της ασφάλειας και άμεση ανίχνευση κυβερνοαπειλών

Ανθεκτικότητα των Συστημάτων και Business Continuity

Άρθρο 49 της Οδηγίας NIS2

Η Οδηγία NIS2 απαιτεί από τους Οργανισμούς να διασφαλίζουν την επιχειρησιακή συνέχεια και την ανθεκτικότητα των συστημάτων τους, όπως καθορίζεται από το Άρθρο 49.

Τι παρέχουμε

Προσφέρουμε λύσεις δημιουργίας και αποθήκευσης αντιγράφων ασφαλείας, διασφαλίζοντας την αποκατάσταση των δεδομένων σε περίπτωση καταστροφής:

- **Σύστημα Λήψης και Διαχείρισης Αντιγράφων Ασφαλείας:** Λύσεις για τη δημιουργία και διαχείριση αντιγράφων ασφαλείας δεδομένων, όπως απαιτείται από το Άρθρο 49
- **Αποθήκευση Δεδομένων σε Cloud:** Ασφαλής αποθήκευση στο Cloud για εξασφάλιση αποκατάστασης
- **Υπηρεσίες Αποκατάστασης Δεδομένων:** Λύσεις αποκατάστασης σε περίπτωση απώλειας δεδομένων

Εκπαίδευση Ετοιμότητας Προσωπικού

Άρθρο 21 της Οδηγίας NIS2

Το Άρθρο 21 της Οδηγίας NIS2 ορίζει την εκπαίδευση και ευαισθητοποίηση του προσωπικού σε θέματα κυβερνοασφάλειας.

Τι παρέχουμε

- **Προγράμματα Εκπαίδευσης:** Ολοκληρωμένα προγράμματα εκπαίδευσης (π.χ. Security Awareness Training, Phishing Simulation) για την ενίσχυση της ετοιμότητας του προσωπικού και για την αντιμετώπιση κυβερνοαπειλών

Συνεχής Συμμόρφωση και Αξιολόγηση

Άρθρο 32 της Οδηγίας NIS2

Σύμφωνα με το Άρθρο 32, η συμμόρφωση με την Οδηγία NIS2 απαιτεί συνεχή παρακολούθηση και αναβάθμιση των μέτρων ασφαλείας.

Τι παρέχουμε

- Διενεργούμε τακτικούς ελέγχους και αξιολογήσεις μέσω Vulnerability Assessments και Penetration Tests, διασφαλίζοντας την προστασία του Οργανισμού σας από νέες απειλές

Πίνακας Σύνδεσης Απαιτήσεων NIS2 Με Προτεινόμενες Λύσεις

Άρθρο NIS2	Περιγραφή Οδηγίας	Λύσεις, που καλύπτουν την απαίτηση
24	Διατήρηση ενός ελάχιστου συνόλου δεδομένων περιστατικών ασφάλειας	Σύστημα Διαχείρισης Συμβάντων Ασφάλειας (Security Information and Event Management - SIEM)
44	Ενθάρρυνση οντοτήτων για χρήση PAM	Διαχείριση Προνομιακής Πρόσβασης (Privileged Access Management - PAM)
48	Περιορισμοί σε λογαριασμούς με δικαιώματα διαχειριστή, τακτικές αλλαγές κωδικών πρόσβασης	Διαχείριση Προνομιακής Πρόσβασης (PAM)
49	Σύσταση για βασική γραμμή κυβερνοασφάλειας, συμπεριλαμβανομένων των ενημερώσεων λογισμικού	Προστασία Τελικού Σημείου (Endpoint Protection Platform - EPP)
55	Ενθάρρυνση χρήσης καινοτόμων τεχνολογιών, συμπεριλαμβανομένης της Τεχνητής Νοημοσύνης	Ανίχνευση και Αντίδραση Τελικού Σημείου (Endpoint Detection and

		Response - EDR), Προστασία E-mail
57	Πρόληψη, ανίχνευση, παρακολούθηση, ανάλυση και μετριασμός παραβιάσεων ασφαλείας δικτύου με ενεργό τρόπο	Προστασία Τελικού Σημείου (EPP), Ανίχνευση και Αντίδραση Σημείων Τερματισμού (EDR), Αξιολόγηση Τρωτότητας (Vulnerability Assessment), Δοκιμές Δεισδυσσης (Penetration Testing)
89	Υιοθέτηση αρχής Zero Trust, Διαχείριση ταυτότητας και πρόσβασης	Διαχείριση Προνομιακής Πρόσβασης (PAM)
89	Βασικές πρακτικές κυβερνο-υγιεινής, συμπεριλαμβανομένων των ενημερώσεων λογισμικού, της προστασίας συνεργατικών εφαρμογών και επικοινωνιών, καθώς και της εκπαίδευσης ετοιμότητας του προσωπικού σε θέματα κυβερνοασφάλειας	Προστασία Τελικού Σημείου (EPP), Προστασία Συνεργασίας για O365, Ενίσχυση ασφάλειας σε O365, Προστασία E-mail, Εκπαίδευση Ετοιμότητας Προσωπικού σε Θέματα Κυβερνοασφάλειας (Security Awareness Training)
89	Πρώθηση της ενσωμάτωσης τεχνολογιών, όπως η Τεχνητή Νοημοσύνη και η μηχανική μάθηση	Ανίχνευση και Αντίδραση Τελικού Σημείου (EDR)
89	Ασφάλεια Cloud περιβάλλοντων	Cloud Access Security Broker (CASB)
98	Πολιτική πρόσβασης, διαχείριση πρόσβασης και αυτοματοποιημένες αποφάσεις πρόσβασης	Διαχείριση Προνομιακής Πρόσβασης (PAM)
98	Κρυπτογράφηση από άκρο σε άκρο για την προστασία των ηλεκτρονικών επικοινωνιών	Προστασία απομακρυσμένης πρόσβασης και μετάδοση κρυπτογραφημένων δεδομένων