

Risk Management & Remediation Plan

Από πού πρέπει να ξεκινήσει ένας οργανισμός;

Ένας οργανισμός, πριν σχεδιάσει τις επενδύσεις του στην κυβερνοασφάλεια, οφείλει να γνωρίζει την πραγματική κατάσταση της πληροφοριακής του υποδομής.

Η Διαχείριση Κινδύνων (Risk Management) αποτελεί το σημείο εκκίνησης. Μέσα από την αποτύπωση των υποδομών, τον εντοπισμό των ευπαθειών και την αξιολόγηση των κινδύνων, ο οργανισμός αποκτά σαφή εικόνα:

Πού βρίσκεται σήμερα → Ποιοι είναι οι πραγματικοί κίνδυνοι → Τι πρέπει να αντιμετωπιστεί κατά προτεραιότητα

Έτσι, οι επόμενες επενδύσεις στην κυβερνοασφάλεια μπορούν να σχεδιαστούν με βάση τις πραγματικές ανάγκες και τους κινδύνους, και όχι μέσα από αποσπασματικές επιλογές τεχνολογιών.

Από το Risk Assessment στο Remediation Plan

Δεν αρκεί ο εντοπισμός των προβλημάτων. Είναι απαραίτητο να υπάρχει ένα σαφές πλάνο για την αντιμετώπισή τους.

Γι' αυτό δίνεται ιδιαίτερη βαρύτητα στο Remediation Plan, το οποίο αποτελεί βασικό παραδοτέο της προσέγγισής μας.

Τα ευρήματα του Risk Assessment οργανώνονται, αξιολογούνται και ιεραρχούνται, και μετατρέπονται σε ένα συγκεκριμένο και εφαρμόσιμο πλάνο διορθωτικών ενεργειών.

Τι πρέπει να γίνει → Τι προηγείται → ΠΟΤΕ πρέπει να γίνει → ΠΩΣ θα επαληθευτεί

Έτσι, ο οργανισμός δεν παραλαμβάνει απλώς μια τεχνική αναφορά ευρημάτων, αλλά έναν πρακτικό οδικό χάρτη για τη μείωση του πραγματικού κινδύνου.

2310 590 196

More Info:

www.bluevalue.gr

info@bluevalue.gr



Risk Management & Remediation Plan

Από το πλάνο στην πράξη

Η υποστήριξή μας δεν χρειάζεται να σταματήσει στην παράδοση της μελέτης.

Η τεχνική μας ομάδα διαθέτει την τεχνογνωσία για να υποστηρίξει, όπου απαιτείται, την υλοποίηση των διορθωτικών ενεργειών και στη συνέχεια την επαλήθευση της αποκατάστασης.

Οι ενέργειες μπορούν να υλοποιηθούν από την ομάδα IT του οργανισμού, από υφιστάμενους συνεργάτες ή με τη δική μας τεχνική υποστήριξη.

ASSESS → PRIORITISE → REMEDIATE → VERIFY →
MONITOR

Πέρα από τη μελέτη

Στο πλαίσιο της υπηρεσίας, παρέχεται, χωρίς επιπλέον κόστος, πλατφόρμα Endpoint Management για:

Patch Management • Hardware & Software Inventory •
CVE Visibility • Remote Management

δημιουργώντας, παράλληλα, έναν μηχανισμό συνεχούς παρακολούθησης και αντιμετώπισης ευπαθειών στα endpoints.

Κατανοούμε τον κίνδυνο.

Οργανώνουμε την αντιμετώπισή του.

Επενδύουμε εκεί που πραγματικά χρειάζεται.

Ας συζητήσουμε πού βρίσκεται, σήμερα, ο δικός σας οργανισμός.

Προγραμματίστε μια σύντομη συνάντηση μέσω Microsoft Teams με την ομάδα
Cloud Services & Cyber Security.

2310 590 196

More Info:

www.bluevalue.gr

info@bluevalue.gr



Risk Management & Remediation Plan

Η υπηρεσία περιλαμβάνει:

1. Προετοιμασία και Καθορισμό Πλαισίου

- Ορισμός αντικειμένου Risk Management (υποδομές, υπηρεσίες, κρίσιμες λειτουργίες)
- Ορισμός κριτηρίων αποδοχής κινδύνου και risk appetite
- Συγκρότηση Ομάδας Διαχείρισης Κινδύνων
- Παραδοτέα: Risk Management Plan, Scope & Context Document

2. Αναγνώριση Υποδομών, Απειλών και Αδυναμιών

- Καταγραφή assets (λογισμικό, υλικό, υπηρεσίες)
- Αναγνώριση απειλών (φυσικές, τεχνικές, ανθρωπογενείς)
- Vulnerability Assessment και Penetration Testing (Qualys, Nessus, Metasploit, Nmap)
- Παραδοτέα: Asset Inventory, Threat Catalogue, Vulnerability Report

3. Εκτίμηση Κινδύνου (Risk Assessment)

- Ανάλυση κινδύνων με βάση πιθανότητα και αντίκτυπο
- Δημιουργία Risk Matrix
- Παραδοτέα: Risk Register, Risk Matrix Report

4. Αντιμετώπιση Κινδύνου (Risk Treatment)

- Προτάσεις μέτρων αποδοχής, αποφυγής, μετριασμού ή μεταφοράς κινδύνων
- Συσχέτιση λύσεων με πρότυπα (ISO 27001 Annex A, ENISA controls)
- Παραδοτέα: Risk Treatment Plan

5. Σχέδιο Απόκρισης σε Περιστατικά (Incident Response Plan)

- Ανάπτυξη διαδικασιών ανίχνευσης, αναφοράς και απόκρισης σε περιστατικά ασφάλειας
- Παραδοτέα: Incident Response Plan

6. Επικοινωνία Κινδύνων (Risk Communication Plan)

- Καθορισμός τρόπων ενημέρωσης διοίκησης και εποπτικών αρχών σε περίπτωση κινδύνου ή περιστατικού
- Παραδοτέα: Risk Communication Framework

7. Παρακολούθηση και Επανεξέταση (Monitoring & Review)

- Καθορισμός KPIs για risk management
- Ετήσιος επανέλεγχος και επικαιροποίηση των αναλύσεων
- Παραδοτέα: Monitoring Reports, Updated Risk Register

8. Εκπαίδευση και Ευαισθητοποίηση Χρηστών (User Training and Awareness)

- Διεξαγωγή εκπαιδευτικών σεμιναρίων για την ενημέρωση των χρηστών σχετικά με τις διαδικασίες διαχείρισης κινδύνων, την αναγνώριση απειλών και τη σωστή αντίδραση σε περιστατικά ασφάλειας
- Ανάπτυξη υλικού εκπαίδευσης (guides, manuals, quick reference cards)
- Ενίσχυση κουλτούρας ασφάλειας στον Οργανισμό
- Παραδοτέα: User Training Plan, Εκπαιδευτικό Υλικό, Attendance Reports

9. Παροχή Πλατφόρμας Διαχείρισης Τερματικών (Endpoint Management)

Στο πλαίσιο της υπηρεσίας Risk Management παρέχεται, χωρίς επιπλέον κόστος, η εγκατάσταση και παραμετροποίηση πλατφόρμας διαχείρισης τερματικών, με στόχο την άμεση εφαρμογή βασικών μέτρων μείωσης των κινδύνων που θα αναδειχθούν κατά την αξιολόγηση.

Η πλατφόρμα παρέχει ενδεικτικά:

- Κεντρική διαχείριση ενημερώσεων Windows και εφαρμογών τρίτων
- Αυτόματη απογραφή υλικού (Hardware Inventory)
- Αυτόματη απογραφή λογισμικού (Software Inventory)
- Εντοπισμό γνωστών ευπαθειών (CVE Exposure)
- Απομακρυσμένη πρόσβαση (Remote Support)
- Κεντρική εικόνα της κατάστασης όλων των τερματικών

Παραδοτέα:

- Εγκατεστημένη και παραμετροποιημένη πλατφόρμα
- Dashboard απογραφής εξοπλισμού
- Dashboard ευπαθειών
- Dashboard ενημερώσεων