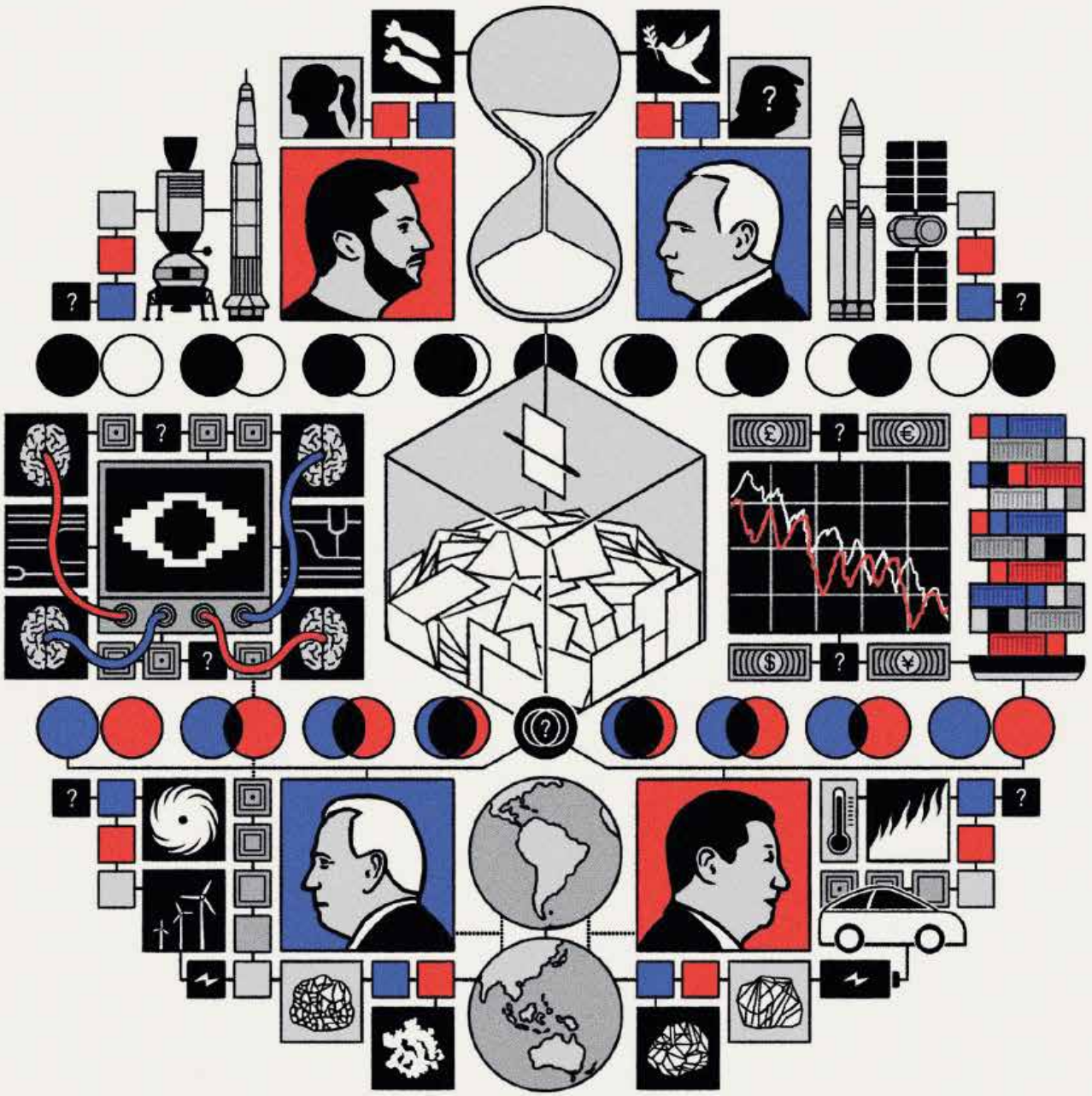
The Economist

Εκδόθηκε με την αποκλειστική άδεια
του *The Economist* από τη:
hazlis & rivas

ΟΚΟΣΜΟΣ ΤΟ 2024



9 772585 343001

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΤΗΝ ΕΠΟΧΗ ΤΗΣ ΑΒΕΒΑΙΟΤΗΤΑΣ

Ο ΡΟΛΟΣ ΤΩΝ ΑΝΘΡΩΠΩΝ, ΤΩΝ ΔΙΑΔΙΚΑΣΙΩΝ ΚΑΙ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

Σε ένα συνεχώς μεταβαλλόμενο και εξελισσόμενο κόσμο, με απρόβλεπτες αλλαγές που χαρακτηρίζονται από αστάθεια, αβεβαιότητα, πολυπλοκότητα αλλά και ασάφεια, η άνοδος του ψηφιακού μετασχηματισμού, η μετάβαση στο cloud, το υβριδικό μοντέλο εργασίας και η Τεχνητή Νοημοσύνη, έχουν αλλάξει ριζικά το ψηφιακό οικοσύστημα. Με τη διεύρυνση της ψηφιακής περιμέτρου και τη δημιουργία νέων σημείων ευπάθειας, όλοι οι οργανισμοί ανεξαρτήτως μεγέθους και τομέα δραστηριότητας καθίστανται πιθανοί στόχοι.

Με την κυβερνοασφάλεια να είναι πιο επίκαιρη από ποτέ, οι οργανισμοί καλούνται όχι μόνο να ενισχύσουν την κυβερνοασφάλεια, αλλά και την κυβερνοανθεκτικότητα τους, δηλαδή να μπορούν να προβλέπουν, να προσαρμόζονται, να ανταποκρίνονται και να ανακάμπτουν γρήγορα. Για να μπορέσει όμως μια στρατηγική κυβερνοασφάλειας να είναι αποτελεσματική και εφαρμόσιμη πρέπει να βασίζεται σε όλες τις λειτουργικές πτυχές του οργανισμού: Άνθρωπους, Διαδικασίες και Τεχνολογία.

ΑΝΘΡΩΠΟΙ - Η πρώτη γραμμή άμυνας

Στον τομέα της διαχείρισης των ψηφιακών απειλών, η εκπαίδευση και η καλλιέργεια αισθήματος ευθύνης και κουλτούρας υπέρ της κυβερνοασφάλειας, μεταξύ των εργαζομένων δημιουργεί ένα ισχυρό ανθρώπινο τείχος προστασίας έναντι πιθανών απειλών. Η εκπαίδευση όμως, δεν περιορίζεται μόνο στην πρόληψη των απειλών, αλλά περιλαμβάνει επίσης τη διαχείριση των περιστατικών εφόσον αυτά συμβούν. Ένα σωστά ενημερωμένο και καταρτισμένο προσωπικό, μπορεί να αντιληφθεί και να αναφέρει αυτά τα περιστατικά άμεσα, δίνοντας την δυνατότητα για ταχύτερη αντιμετώπιση τους, μειώνοντας τις αρνητικές συνέπειες που μπορεί να επιφέρουν για τον εκάστοτε οργανισμό.

ΔΙΑΔΙΚΑΣΙΕΣ - Η Βάση της Ψηφιακής Ασφάλειας

Τα διοικητικά συμβούλια των οργανισμών πρέπει να καθιερώσουν μια συνολική διαδικασία διαχείρισης κινδύνων που να περιλαμβάνει τον εντοπισμό, την αξιολόγηση και την αντιμετώπιση των κινδύνων. Αυτές οι διαδικασίες πρέπει να είναι ευθυγραμμισμένες με την επιχειρηματική στρατηγική του οργανισμού και τις νομικές απαιτήσεις του. Μέσω της τακτικής αξιολόγησης των κινδύνων, οι οργανισμοί μπορούν να εντοπίσουν πιθανά τρωτά σημεία στις υποδομές τους και να λάβουν προληπτικά μέτρα για την αντιμετώπισή τους. Επιπλέον, θεσπίζοντας σαφείς διαδικασίες αντίδρασης σε περιστατικά και διαδικασίες κλιμάκωσης, ελαχιστοποιούν επιπτώσεις σε τυχόν κυβερνοεπίθεση.

ΤΕΧΝΟΛΟΓΙΑ – Η Ασπίδα Προστασίας

Με το ψηφιακό τοπίο να εξελίσσεται πιο γρήγορα από ποτέ, η εφαρμογή προηγμένων αλλά και προσαρμοσμένων λύσεων ασφάλειας που μπορούν να ανιχνεύουν και να αντιδρούν σε απειλές σε πραγματικό χρόνο, κρίνεται αναγκαία. Αυτό περιλαμβάνει από την εγκατάσταση firewalls, συστημάτων ανίχνευσης και πρόληψης κακόβουλων ενεργειών, λογισμικού προστασίας τερματικών ως και λύσεις διαχείρισης πληροφοριών και συμβάντων ασφάλειας (SIEM). Είναι σημαντικό οι οργανισμοί να υιοθετήσουν συστήματα συνεχούς προσομοίωσης επιθέσεων και ευπαθειών (Continuous Threat Exposure Management (CTEM)) για να μπορούν να αναγνωρίσουν και διαγνώσουν πιθανές απειλές για τα δίκτυα και τα συστήματα τους.

Συνδυάζοντας λοιπόν, αυτά τα τρία στοιχεία ο οργανισμός δημιουργεί ένα ολοκληρωμένο πλαίσιο διαχείρισης κινδύνου, συμπεριλαμβανομένου του εντοπισμού, της αξιολόγησης και του μετριασμού του, ενισχύοντας έτσι την κυβερνοανθεκτικότητα του.

> **Η ραγδαία αύξηση των κυβερνοεπιθέσεων ως παγκόσμιο φαινόμενο, δεν αφήνει ανεπηρέαστη την Ελλάδα, με την κυβερνοανθεκτικότητα να αποτελεί βασικό μέρος της ατζέντας του διοικητικού συμβουλίου του κάθε οργανισμού**
>
> **Απόστολος Πανδρούλας**
> Γενικός Διευθυντής Ελλάδος