

# Battlecard για τη Διοίκηση

Όσα αξίζει να κρατήσετε, και από πού να ξεκινήσετε · Ιούλιος 2026

**\$10,5 τρισ.**

η «οικονομία» του κυβερνο-εγκλήματος: 3η στον κόσμο

**< 60''**

από το κλικ σε phishing έως τη διαρροή κωδικού

**6 στις 10**

παραβιάσεις μέσω ανθρώπινου λάθους ή εξαπάτησης

**~30%**

των παραβιάσεων ξεκινούν από τρίτους / προμηθευτές

## ΟΙ 7 ΕΡΩΤΗΣΕΙΣ ΠΡΟΣ ΤΗΝ ΟΜΑΔΑ ΣΑΣ

- Πόσο γρήγορα εντοπίζουμε και περιορίζουμε ένα περιστατικό; (MTTD / MTTR)
- Πότε δοκιμάσαμε τελευταία φορά επαναφορά από backup; Όχι το backup, την επαναφορά.
- Ποιοι προμηθευτές και συνεργάτες έχουν πρόσβαση στα δεδομένα μας;
- Υπάρχει σχέδιο απόκρισης, και ποιος αποφασίζει σε κρίση, με τι όρια;
- Πόση κάλυψη έχουμε σε MFA, EDR και δοκιμασμένα backups, και ποιες είναι οι εξαιρέσεις;
- Ποια δεδομένα μας είναι ευαίσθητα, πού βρίσκονται, και τι μπορεί να «δει» ένα εργαλείο AI σήμερα;
- Ποιοι AI agents τρέχουν στα συστήματά μας, με ποια δικαιώματα, και ποιος απαντά για τις πράξεις τους;

## ΚΑΝΟΝΕΣ ΜΗΔΕΝΙΚΟΥ ΚΟΣΤΟΥΣ

- Καμία μεταφορά χρημάτων με εντολή από κλήση ή βίντεο χωρίς επιβεβαίωση από δεύτερο, ανεξάρτητο κανάλι. Τα deepfakes νικούν πλέον μάτι και αυτί.
- Το help desk ταυτοποιεί αυστηρά πριν από κάθε reset κωδικού. Το τηλεφώνημα παραμένει η πιο αποδοτική «επίθεση».
- Τίποτα ευαίσθητο σε μη εγκεκριμένα εργαλεία AI: το AI διαρρέει ό,τι βλέπει, όχι μόνο ό,τι του δίνετε.
- Όποιος αναφέρει το λάθος του δεν τιμωρείται: ο εργαζόμενος που φοβάται να μιλήσει είναι ο ακριβότερος.

## ΕΝΔΕΙΚΤΙΚΑ ΚΡΙΣ ΓΙΑ ΤΟ ΔΣ

### Ταχύτητα

MTTD / MTTR: πάντα με στόχο και τάση, όχι στιγμιότυπο

### Κλείσιμο εκθέσεων

% κρίσιμων ευπαθειών εντός SLA · ευρήματα εκτός προθεσμίας

### Κάλυψη βασικών

% phishing-resistant MFA · % EDR · % δοκιμασμένα backups

### Ανάκαμψη

τελευταίο επιτυχές restore test · χρόνος ανάκτησης vs RTO

### Ανθρώπινος παράγοντας

ποσοστά κλικ & αναφοράς στα phishing tests, ανά τρίμηνο

### Προμηθευτές

% κρίσιμων με αξιολόγηση · σχέδιο χειροκίνητης λειτουργίας

### Διακυβέρνηση AI

% χρήσης AI μέσα από εγκεκριμένα, εποπτευόμενα κανάλια

### Οικονομική διατύπωση

κόστος προστασίας έναντι ρίσκου που αποσύρει (Gartner ODM)

*Ποτέ ένας ενιαίος «βαθμός ασφάλειας»: ο μέσος όρος κρύβει τα κενά.*

## ΞΕΚΙΝΗΣΤΕ ΑΠΟ ΕΔΩ: πέντε κινήσεις μηδενικού κόστους

- Ρωτήστε: «πότε δοκιμάσαμε τελευταία φορά επαναφορά από backup;»
- Ζητήστε απογραφή: ποια εργαλεία AI χρησιμοποιούνται πραγματικά;
- MFA ανθεκτικό σε phishing παντού, εξαιρέσεις μόνο με ημερομηνία λήξης
- Προγραμματίστε άσκηση προσομοίωσης κρίσης, με ονόματα: ποιος αποφασίζει τι
- Ταξινομήστε πρώτα τα «πετράδια του στέμματος», όχι όλα τα δεδομένα

### ΛΕΞΙΛΟΓΙΟ

MFA: πολυπαραγοντική ταυτοποίηση · EDR: ανίχνευση & απόκριση σε τερματικά · MTTD / MTTR: μέσος χρόνος εντοπισμού / απόκρισης · ODM: μετρικές βάσει αποτελέσματος (Gartner) · RTO: μέγιστος αποδεκτός χρόνος επαναφοράς · SLA: συμφωνημένη προθεσμία