					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P40					Τίτλος εγγράφου: **Πολιτική δοκιμών ασφάλειας και ασκήσεων Red Team**							
Έκδοση: 1.0		Ημερομηνία έναρξης ισχύος: 01.01.2025			Ιδιοκτήτης εγγράφου:							
X	Πολιτική		Πρότυπο		Διαδικασία		Έντυπο		Μητρώο		Άλλο	

Ιστορικό αναθεωρήσεων				
Αριθμός αναθεώρησης	**Ημερομηνία αναθεώρησης**	**Αλλαγές**	**Ελέγχθηκε από**	**Ιδιοκτήτης διεργασίας**

Εγκρίσεις			
Όνομα	**Θέση**	**Ημερομηνία**	**Υπογραφή**

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	9.1, 9.2, 9.3	
ISO/IEC 27002:2022	5.7, 5.36, 8.8, 8.29, 8.30, 8.1	
NIST SP 800-53 Rev.5	CA-2, CA-7, CA-8, RA-5	
ΓΚΠΔ της ΕΕ	Άρθρο 32(1)(d)	
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(f)	
Κανονισμός DORA της ΕΕ	Άρθρα 25–27	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Σκοπός

1 Καθορίζει ένα δομημένο πρόγραμμα τακτικών δοκιμών ασφάλειας για τα δίκτυα, τα συστήματα και τις εφαρμογές του οργανισμού, συμπεριλαμβανομένων αξιολογήσεων ευπαθειών, δοκιμών διείσδυσης και ασκήσεων Red Team, ώστε να ικανοποιούνται οι απαιτήσεις του άρθρου 21(2)(f) της Οδηγίας NIS2 της ΕΕ σχετικά με την αξιολόγηση της αποτελεσματικότητας των μέτρων κυβερνοασφάλειας.

1.1 Διασφαλίζει ότι αδυναμίες στα τεχνικά και οργανωτικά μέτρα εντοπίζονται και αποκαθίστανται προληπτικά μέσω ελεγχόμενων δοκιμών, με στόχο τη διαρκή βελτίωση του προφίλ κινδύνου του οργανισμού.

2. Πεδίο εφαρμογής

2 Η παρούσα πολιτική καλύπτει όλα τα κρίσιμα πληροφοριακά συστήματα, τις εφαρμογές και την υποστηρικτική υποδομή που ανήκουν στον οργανισμό ή τελούν υπό τη λειτουργική του ευθύνη. Περιλαμβάνει επίσης δοκιμές φυσικής ασφάλειας εγκαταστάσεων, στον βαθμό που σχετίζονται με την κυβερνοασφάλεια, όπως κοινωνική μηχανική ή φυσικές δοκιμές διείσδυσης, εφόσον αυτές εμπίπτουν στο πεδίο των ασκήσεων Red Team.

2.1 Η πολιτική εφαρμόζεται στις εσωτερικές ομάδες ασφάλειας πληροφοριών, σε κάθε εξωτερικό πάροχο υπηρεσιών δοκιμών ασφάλειας που έχει συμβληθεί με τον οργανισμό και στους σχετικούς Ιδιοκτήτες Συστημάτων/Ιδιοκτήτες Εφαρμογών. Όλες οι δραστηριότητες δοκιμών πρέπει να είναι εξουσιοδοτημένες και να ακολουθούν τις παρούσες διαδικασίες, ώστε να αποφεύγονται ακούσιες διακοπές λειτουργίας.

3. Στόχοι

3 Επαληθεύει την αποτελεσματικότητα των εφαρμοσμένων ελέγχων κυβερνοασφάλειας, σε τεχνικό, επιχειρησιακό και οργανωτικό επίπεδο, μέσω περιοδικών δοκιμών και προσομοιώσεων, σε ευθυγράμμιση με την απαίτηση της Οδηγίας NIS2 της ΕΕ για μέτρηση της αποτελεσματικότητας.

3.1 Εντοπίζει ευπάθειες ή κενά που ενδέχεται να διαφεύγουν από τις τακτικές επιχειρησιακές διαδικασίες, συμπεριλαμβανομένων ευπαθειών μηδενικής ημέρας και ζητημάτων παραμετροποίησης, υπό ρεαλιστικά σενάρια επίθεσης μέσω ασκήσεων Red Team, πριν αυτά αξιοποιηθούν από φορείς απειλής.

3.2 Παρέχει στη διοίκηση διασφάλιση και εφαρμόσιμες συστάσεις μέσω της αναφοράς των ευρημάτων των δοκιμών, ώστε να υποστηρίζεται η λήψη αποφάσεων για την αντιμετώπιση κινδύνων και η συνεχής βελτίωση του προγράμματος ασφάλειας.

4. Ρόλοι και αρμοδιότητες

4 Συντονιστής Δοκιμών Ασφάλειας (STC): Ορίζεται από τον Επικεφαλής Ασφάλειας Πληροφοριών (CISO) και είναι υπεύθυνος για τον σχεδιασμό και την εποπτεία όλων των δραστηριοτήτων δοκιμών ασφάλειας. Διασφαλίζει ότι οι δοκιμές έχουν σαφώς καθορισμένο πεδίο εφαρμογής, είναι εξουσιοδοτημένες και ότι τα αποτελέσματα αναφέρονται και αξιοποιούνται.

4.1 Εσωτερική Ομάδα Ασφάλειας (Blue Team): Συμμετέχει στις δοκιμές, παρέχοντας ενδεικτικά πληροφορίες για τον καθορισμό του πεδίου εφαρμογής και παρακολουθώντας τα συστήματα κατά τη διάρκειά τους. Στις ασκήσεις Red Team, η Blue Team αποκρίνεται στις προσομοιωμένες επιθέσεις και αξιολογείται η ικανότητα ανίχνευσης και απόκρισής της.

4.2 Red Team / Δοκιμαστές Διείσδυσης: Μπορεί να είναι εσωτερική επιθετική ομάδα ασφάλειας ή εξωτερικοί σύμβουλοι. Εκτελούν τις δοκιμές βάσει συμφωνημένων κανόνων εμπλοκής, τεκμηριώνουν όλες τις ευπάθειες και τις διαδρομές εκμετάλλευσης που εντοπίζονται και τηρούν την εμπιστευτικότητα.

[... Οι ενότητες 4.3–8 δεν περιλαμβάνονται σε αυτή την προεπισκόπηση. Αγοράστε το πλήρες έγγραφο για πρόσβαση στο πλήρες περιεχόμενο. ...]

9. Παρακολούθηση και έλεγχος

9 Ο STC οφείλει να τηρεί ημερολόγιο και αρχείο καταγραφής όλων των δραστηριοτήτων δοκιμών ασφάλειας που διενεργούνται. Το αρχείο αυτό πρέπει να περιλαμβάνει την ημερομηνία, το πεδίο εφαρμογής, τον εκτελούντα τη δοκιμή και συνοπτική αποτύπωση των αποτελεσμάτων. Ανασκοπείται ώστε να διασφαλίζεται η τήρηση του απαιτούμενου προγράμματος, για παράδειγμα ότι κανένα κρίσιμο σύστημα δεν παραμένει χωρίς δοκιμή πέραν του ετήσιου κύκλου.

9.1 Η πρόοδος της αποκατάστασης των ευρημάτων των δοκιμών παρακολουθείται και αναφέρεται σε μηνιαία βάση. Εκκρεμή ζητήματα υψηλής σοβαρότητας ανασκοπούνται σε συναντήσεις διοίκησης έως το κλείσιμό τους.

9.2 Ο Εσωτερικός Έλεγχος ή ανεξάρτητος ελεγκτής ανασκοπεί ετησίως το πρόγραμμα δοκιμών ασφάλειας, ώστε να επαληθεύεται ότι οι δοκιμές είναι δεόντως εξουσιοδοτημένες, διενεργούνται και αναφέρονται ορθά, ότι τα κρίσιμα ευρήματα έχουν αντιμετωπιστεί και ότι το πρόγραμμα καλύπτει τις κανονιστικές προσδοκίες. Για παράδειγμα, οι ελεγκτές μπορεί να επαληθεύουν ότι διενεργήθηκε δοκιμή διείσδυσης πριν από την έναρξη λειτουργίας νέας διαδικτυακής υπηρεσίας, όπου αυτό απαιτείται. Τυχόν αποκλίσεις οδηγούν σε σχέδια διορθωτικών ενεργειών.

10. Ανασκόπηση και συντήρηση

10 Η παρούσα πολιτική και το συνολικό σχέδιο δοκιμών ανασκοπούνται τουλάχιστον μία φορά ετησίως. Η ανασκόπηση λαμβάνει υπόψη μεταβολές στο τοπίο απειλών, όπως η εμφάνιση νέων τεχνικών επίθεσης που ενδέχεται να μην καλύπτονται από τις ισχύουσες δοκιμές, και προσαρμόζει αναλόγως το πεδίο εφαρμογής ή τη συχνότητα.

10.1 Μετά από κάθε μείζον περιστατικό κυβερνοασφάλειας ή παραβίαση, η πολιτική πρέπει να επανεξετάζεται ώστε να προσδιορίζεται αν πρόσθετες ή συχνότερες δοκιμές θα μπορούσαν να είχαν αποτρέψει ή εντοπίσει το ζήτημα. Η πολιτική επικαιροποιείται στη συνέχεια ώστε να ενσωματώνονται οι σχετικές προσαρμογές, όπως η προσθήκη νέου σεναρίου σε ασκήσεις Red Team βάσει των μοτίβων επίθεσης που παρατηρήθηκαν.

10.2 Οι επικαιροποιήσεις της παρούσας πολιτικής πρέπει να εγκρίνονται από τον Επικεφαλής Ασφάλειας Πληροφοριών (CISO) και να τίθενται υπόψη του Διοικητικού Συμβουλίου. Όλο το σχετικό προσωπικό ενημερώνεται για τις αλλαγές και οι εξωτερικοί συνεργάτες δοκιμών ειδοποιούνται εάν οποιαδήποτε αλλαγή επηρεάζει τους όρους ανάθεσής τους.

11. Συναφείς πολιτικές και διασυνδέσεις

11.1 P06 – Πολιτική Διαχείρισης Κινδύνων. Τα αποτελέσματα των δοκιμών τροφοδοτούν την αξιολόγηση και την αντιμετώπιση κινδύνων.

11.2 P22 – Πολιτική Καταγραφής και Παρακολούθησης. Επικυρώνει την κάλυψη ανίχνευσης κατά τη διάρκεια των ασκήσεων.

11.3 P24 – Πολιτική Ασφαλούς Ανάπτυξης. Ενσωματώνει τα ευρήματα των δοκιμών στους ελέγχους του Κύκλου Ζωής Ανάπτυξης Λογισμικού (SDLC).

11.4 P25 – Πολιτική Απαιτήσεων Ασφάλειας Εφαρμογών. Διασφαλίζει ότι οι απαιτήσεις αποτυπώνουν τα διδάγματα από τις δοκιμές.

11.5 P30 – Πολιτική Αντιμετώπισης Περιστατικών (P30). Τα σενάρια Red Team βελτιώνουν τα εγχειρίδια ενεργειών και την απόκριση.

11.6 P31 – Πολιτική Συλλογής Τεκμηρίων και Ψηφιακής Εγκληματολογίας. Συλλέγει τεχνουργήματα κατά τις δοκιμές με ασφαλή τρόπο.

11.7 P32 – Πολιτική Επιχειρησιακής Συνέχειας και Ανάκαμψης από Καταστροφή. Οι ασκήσεις επαληθεύουν την ανθεκτικότητα υπό συνθήκες επίθεσης.

11.8 P33 – Πολιτική Ελέγχων και Παρακολούθησης Συμμόρφωσης. Παρέχει ανεξάρτητη εποπτεία της αποτελεσματικότητας του προγράμματος δοκιμών.

12. Αναφορές

12.1 Οδηγία NIS2 (ΕΕ 2022/2555), άρθρο 21(2), σημείο (f) (πολιτικές και διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας)

12.2 Εκτελεστικός Κανονισμός της Επιτροπής (ΕΕ) 2024/2690, Παράρτημα, Ενότητα 7 (απαιτήσεις για την παρακολούθηση, τις δοκιμές και την αξιολόγηση της αποτελεσματικότητας των μέτρων κυβερνοασφάλειας)

12.3 Τεχνική καθοδήγηση ENISA (2025) – Παράρτημα για δοκιμές ασφάλειας και έλεγχο (οδηγίες για τη διεξαγωγή ασκήσεων κυβερνοασφάλειας και τεχνικών δοκιμών)

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:

12.5 Βέλτιστες πρακτικές του κλάδου: OWASP Testing Guide, NIST SP 800-115 (Technical Guide to Security Testing), CBEST/GREEN Team (πλαίσια ασκήσεων red teaming του χρηματοοικονομικού τομέα για σκοπούς αναφοράς)