TLP:CLEAR

Εθνική Αρχή Κυβερνοασφάλειας
Γενική Διεύθυνση Επιχειρησιακού Σχεδιασμού
EL-CSIRT
Χανδρή 1, 18346 Μοσχάτο

EL-CSIRT RFC 2350

Version 1.0 - 2025-04-14

1 Σχετικά με αυτό το έγγραφο

Αυτό το έγγραφο περιγράφει τις λειτουργίες της ομάδας απόκρισης συμβάντων ασφάλειας υπολογιστών (CSIRT) της Ελληνικής Εθνικής Αρχής Κυβερνοασφάλειας (EL-CSIRT) σύμφωνα με τις προδιαγραφές RFC 2350. Παρέχει βασικές πληροφορίες για το EL-CSIRT και περιγράφει τις αρμοδιότητες και υπηρεσίες που προσφέρονται.

1.1 Ημερομηνία τελευταίας ενημέρωσης

- **Τίτλος**: EL-CSIRT RFC 2350
- **Έκδοση**: 1.0
- **Ημερομηνία Έκδοσης**: 2025-04-14
- **Λήξη**: Αυτό το έγγραφο είναι έγκυρο έως ότου αντικατασταθεί από μεταγενέστερη έκδοση

1.2 Λίστα διανομής για ειδοποιήσεις

Οι αλλαγές σε αυτό το έγγραφο κοινοποιούνται στην παρακάτω διεύθυνση του ιστότοπου της Ελληνικής Εθνικής Αρχής Κυβερνοασφάλειας: https://cyber.gov.gr/el-csirt/

Ερωτήματα σχετικά με ενημερώσεις μπορούν να αποσταλούν μέσω ηλεκτρονικού ταχυδρομείου, όπως αναφέρεται στην παράγραφο 2.7.

1.3 Τοποθεσίες όπου μπορεί να βρεθεί αυτό το έγγραφο

Η τρέχουσα έκδοση αυτού του εγγράφου περιγραφής του EL-CSIRT διατίθεται από τον ιστότοπο της Ελληνικής Εθνικής Αρχής Κυβερνοασφάλειας, στην παρακάτω ηλεκτρονική διεύθυνση: https://cyber.gov.gr/el-csirt/

Βεβαιωθείτε ότι χρησιμοποιείτε την πιο πρόσφατη έκδοσή του.

2 Στοιχεία επικοινωνίας

2.1 Όνομα της ομάδας

- **Πλήρες Όνομα**: Ομάδα απόκρισης για συμβάντα που αφορούν στην ασφάλεια υπολογιστών (CSIRT) της Ελληνικής Εθνικής Αρχής Κυβερνοασφάλειας
- **Σύντομο Όνομα**: EL-CSIRT

2.2 Διεύθυνση

Εθνική Αρχή Κυβερνοασφάλειας

Χανδρή 1, Μοσχάτο 18346, Ελλάδα

2.3 Ζώνη Ώρας

UTC+2 (EET – Eastern European Time) κατά τη χειμερινή περίοδο (από την τελευταία Κυριακή του Οκτωβρίου έως την τελευταία Κυριακή του Μαρτίου).

UTC+3 (EEST – Eastern European Summer Time) κατά τη θερινή περίοδο (από την τελευταία Κυριακή του Μαρτίου έως την τελευταία Κυριακή του Οκτωβρίου).

2.4 Αριθμός τηλεφώνου

+30 210 4802166

2.5 Αριθμός Φαξ

Μη διαθέσιμο

2.6 Άλλες Τηλεπικοινωνίες

Κανένα διαθέσιμο.

2.7 Διεύθυνση Ηλεκτρονικού Ταχυδρομείου

Επικοινωνήστε μαζί μας στη ηλεκτρονική διεύθυνση: csirt@cyber.gov.gr . Εάν χρειαστεί να ειδοποιήσετε για ένα περιστατικό ασφάλειας πληροφοριών ή μια απειλή στον κυβερνοχώρο της αρμοδιότητάς μας χρησιμοποιήστε την ηλεκτρονική διεύθυνση: incident@cyber.gov.gr

2.8 Δημόσια κλειδιά και άλλες πληροφορίες κρυπτογράφησης

Το EL-CSIRT χρησιμοποιεί PGP για την ανταλλαγή πληροφοριών (ειδοποιήσεις, αναφορές περιστατικών κ.λπ.) με τους ομότιμους, συνεργάτες και ενδιαφερόμενους φορείς.

- Χρήστης: el-csirt <csirt@cyber.gov.gr>
- Αποτύπωμα PGP: CD5B138D39005BB715714003C639A0184948BBAA
- Τοποθεσία: : https://cyber.gov.gr/el-csirt/

2.9 Μέλη της Ομάδας

Η ομάδα EL-CSIRT αποτελείται από ειδικούς σε θέματα ασφάλειας πληροφοριών. Η λίστα των μελών της ομάδας EL-CSIRT δεν είναι δημόσια διαθέσιμη. Η ταυτότητα των μελών της ομάδας EL-CSIRT ενδέχεται να αποκαλυφθεί κατά περίπτωση, σύμφωνα με τους περιορισμούς της ανάγκης για γνώση.

2.10 Άλλες πληροφορίες

Γενικές πληροφορίες για το EL-CSIRT της Ελληνικής Εθνικής Αρχής Κυβερνοασφάλειας, καθώς και σύνδεσμοι σε διάφορους προτεινόμενους ιστότοπους ασφάλειας πληροφοριών είναι διαθέσιμα στο https://cyber.gov.gr/ .

Το EL-CSIRT είναι μέλος του ΕΕ Δικτύου CSIRT (EU CNW), το οποίο δημιουργήθηκε σύμφωνα με την οδηγία NIS (Network and Information Systems Directive) της Ευρωπαϊκής Ένωσης.

2.11 Σημεία επικοινωνίας

Η προτιμώμενη μέθοδος επικοινωνίας με το EL-CSIRT της Ελληνικής Εθνικής Αρχής Κυβερνοασφάλειας είναι η ηλεκτρονική αλληλογραφία στη διεύθυνση που αναφέρεται στην παράγραφο 2.7. Παρακαλώ χρησιμοποιήστε το κρυπτογραφικό κλειδί PGP του EL-CSIRT της παραγράφου 2.8 για τη διασφάλιση της ακεραιότητας και της εμπιστευτικότητας. Σε περίπτωση έκτακτης ανάγκης, χρησιμοποιήστε την ετικέτα [ΕΠΕΙΓΟΝ] στο πεδίο θέματος του e-mail σας.

3 Καταστατικός Χάρτης

3.1 Δήλωση αποστολής

Με το νόμο 5086/2024 άρθρο 10 παρ.1.γ, στη Γενική Διεύθυνση Επιχειρησιακού Σχεδιασμού της Εθνικής Αρχής Κυβερνοασφάλειας, ανατίθεται η διαχείριση περιστατικών στον κυβερνοχώρο και η λειτουργία της Ομάδας Απόκρισης Συμβάντων στον Κυβερνοχώρο (CSIRT).

Με το νόμο 5160/2024, η Εθνική Αρχή Κυβερνοασφάλειας, ορίζεται ως η αρμόδια αρχή, το ενιαίο σημείο επαφής και η ομάδα απόκρισης για συμβάντα που αφορούν στην ασφάλεια υπολογιστών (CSIRT) βασικών και σημαντικών οντοτήτων. Το CSIRT της Εθνικής Αρχής Κυβερνοασφάλειας επιτελεί συντονιστικό ρόλο των CSIRTs στην Ελλάδα για την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας.

3.2 Πεδίο αρμοδιότητας

Το πεδίο αρμοδιότητας του EL-CSIRT της Ελληνικής Εθνικής Αρχής Κυβερνοασφάλειας περιλαμβάνει:

- Κρίσιμες, βασικές και σημαντικές οντότητες όπως καθορίζονται από την ελληνική νομοθεσία
- Ειδικότερα, για τις οντότητες του Δημοσίου Τομέα, αυτές υπάγονται στο Εθνικό CERT (NCERT-GR) της Εθνικής Υπηρεσίας Πληροφοριών.

Επίσης το EL-CSIRT της Εθνικής Αρχής Κυβερνοασφάλειας, αποτελεί το συντονιστικό CSIRT της Ελλάδας.

3.3 Υπαγωγή

Το EL-CSIRT λειτουργεί στη Γενική Διεύθυνση Επιχειρησιακού Σχεδιασμού της Εθνικής Αρχής Κυβερνοασφάλειας και υποστηρίζεται οικονομικά από την Εθνική Αρχή Κυβερνοασφάλειας.

3.4 Νομική Βάση

Οι αρμοδιότητες και η εξουσιοδότηση του EL-CSIRT της Εθνική Αρχή Κυβερνοασφάλειας, καθορίζονται από τους ακόλουθους εθνικούς νόμους:

- Ν.5086/2024, ΦΕΚ 23 τ. Α΄ / 14-02-2024
- Ν.5160/2024, ΦΕΚ 195, τ. Α΄ / 27-11-2024.

4 Πολιτικές

4.1 Τύποι συμβάντων και επίπεδο υποστήριξης

Το επίπεδο υποστήριξης που παρέχεται από το EL-CSIRT ποικίλλει ανάλογα με τον τύπο και τη σοβαρότητα του περιστατικού ή της κυβερνοαπειλής, το είδος της επηρεαζόμενης βασικής ή σημαντικής οντότητας, τη σημασία της επίπτωσης του σε κρίσιμη βασική υποδομή ή υπηρεσία και τους διαθέσιμους πόρους του EL-CSIRT τη δεδομένη χρονική στιγμή. Το EL-CSIRT παρέχει προληπτικές υπηρεσίες κυβερνοασφάλειας, καθώς και υπηρεσίες απόκρισης σε περιστατικά κυβερνοασφάλειας, όπως οι παρακάτω:

- Λήψη αναφορών περιστατικών
- Παρακολούθηση και ανάλυση κυβερνοαπειλών, ευπαθειών και περιστατικών σε εθνικό επίπεδο, αποκλειστικά για τους τομείς και οργανισμούς αρμοδιότητάς του
- Παροχή έγκαιρων προειδοποιήσεων, ειδοποιήσεων, ανακοινώσεων και πληροφοριών σε εμπλεκόμενες βασικές και σημαντικές οντότητες, καθώς και σε αρμόδιες αρχές και άλλα σχετικά ενδιαφερόμενα μέρη, σχετικά με κυβερνοαπειλές, ευπάθειες και περιστατικά, ει δυνατόν σε σχεδόν πραγματικό χρόνο
- Παροχή, κατόπιν αιτήματος βασικής ή σημαντικής οντότητας, προληπτικής σάρωσης των συστημάτων δικτύου και πληροφοριακών συστημάτων της οικείας οντότητας για τον εντοπισμό ευπαθειών με δυνητικό σημαντικό αντίκτυπο
- Προληπτική μη παρεμβατική σάρωση των δημοσίως προσβάσιμων συστημάτων δικτύου και πληροφοριακών συστημάτων βασικών και σημαντικών οντοτήτων, εφόσον δεν έχει αρνητικές συνέπειες για τη λειτουργία των υπηρεσιών των οντοτήτων
- Αντιμετώπιση περιστατικών και παροχή συνδρομής στις επηρεαζόμενες βασικές και σημαντικές οντότητες, κατόπιν αιτήματός τους
- Συλλογή και ανάλυση εγκληματολογικών δεδομένων και δυναμική ανάλυση κινδύνων και περιστατικών και επίγνωση της κατάστασης σε θέματα κυβερνοασφάλειας

4.2 Συνεργασία, αλληλεπίδραση και αποκάλυψη πληροφοριών

Πληροφορίες που σχετίζονται με περιστατικά, όπως ονόματα και τεχνικές λεπτομέρειες, δεν δημοσιεύονται χωρίς σύμφωνη γνώμη των εμπλεκόμενων οντοτήτων. Εάν δεν συμφωνηθεί διαφορετικά, οι πληροφορίες που γνωστοποιούνται στο EL-CSIRT διατηρούνται εμπιστευτικές. Το EL-CSIRT δεν θα διαβιβάσει ποτέ πληροφορίες σε τρίτους εκτός αν αυτό απαιτείται από το νόμο.

Το EL-CSIRT, χειρίζεται τις πληροφορίες που του διαβιβάζονται ανάλογα με τη διαβάθμισή τους και βάσει της αρχής της ανάγκης για γνώση. Επομένως η εκάστοτε διαβίβαση πληροφοριών περιλαμβάνει μόνο συγκεκριμένα σχετικά και ανωνυμοποιημένα αποσπάσματα.

Πληροφορίες που σχετίζονται με περιστατικά, ενδέχεται να διαβιβαστούν σε οντότητες όπως:

- Τεχνικούς εμπειρογνώμονες της Ελληνικής Εθνικής Αρχής Κυβερνοασφάλειας
- Επηρεαζόμενες οντότητες αρμοδιότητας του EL-CSIRT
- Ελληνικές υπηρεσίες επιβολής του νόμου (εάν απαιτείται από το νόμο ή κατόπιν αιτήματος)
- Ομάδες και δίκτυα συνεργασίας CERT/CSIRT

Το EL-CSIRT συνεργάζεται στενά με ομάδες σε εθνικό, ευρωπαϊκό και διεθνή επίπεδο και υποστηρίζει σθεναρά την εθελοντική συνεργασία μεταξύ των CSIRT σε όλα τα επίπεδα. Για το σκοπό αυτό, το EL-CSIRT διασφαλίζει παρουσία και δικτύωση με τους εταίρους του μέσω της ενεργού συμμετοχής σε ομάδες εργασίας και διεθνείς συναντήσεις και συνέδρια.

Όταν παρέχονται πληροφορίες στο EL-CSIRT με χρήση του Πρωτοκόλλου Φωτεινού Σηματοδότη (Traffic Light Protocol - TLP), το EL-CSIRT σέβεται την πολιτική ανταλλαγής πληροφοριών όπως αυτή ορίζεται από τον οργανισμό FIRST στο: https://www.first.org/tlp/.

4.3 Επικοινωνία και έλεγχος ταυτότητας

Η προτιμώμενη μέθοδος επικοινωνίας με το EL-CSIRT είναι η ηλεκτρονική αλληλογραφία, όπως αναφέρεται στην παράγραφο 2.7. Το EL-CSIRT χρησιμοποιεί το PGP για κρυπτογράφηση ή/και υπογραφή μηνυμάτων. Όλες οι ευαίσθητες επικοινωνίες με το EL-CSIRT θα πρέπει να είναι κρυπτογραφημένες. Τα μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται στο EL-CSIRT, προτείνεται να είναι κρυπτογραφημένα, αξιοποιώντας το δημόσιο κλειδί PGP του EL-CSIRT, όπως αυτό περιγράφεται στην παράγραφο 2.8 του παρόντος.

5 Υπηρεσίες

5.1 Αντιμετώπιση περιστατικού

Το EL-CSIRT παρέχει υπηρεσίες συντονισμού απόκρισης συμβάντων διαθέσιμες 24/7 βάσει του πεδίου αρμοδιότητας του (παρ. 3.2) σε εθνικό επίπεδο προς διευκόλυνση των άλλων CSIRT, και ανταλλάσσει πληροφορίες με βασικές και σημαντικές οντότητες και άλλους σχετικά ενδιαφερόμενους ώστε να διατηρήσουν τα συστήματα πληροφοριών και τα δίκτυά τους ασφαλή.

5.1.1 Διαλογή περιστατικών

- Παρακολούθηση και ανίχνευση πιθανών απειλών και ευπαθειών
- Διερεύνηση εάν όντως συνέβη περιστατικό ασφαλείας
- Προσδιορισμός της έκτασης του συμβάντος
- Ενημέρωση για αποφάσεις και μέτρα περιορισμού

5.1.2 Συντονισμός συμβάντων

Το EL-CSIRT υποστηρίζει τα βασικά ενδιαφερόμενα μέρη για την αντιμετώπιση περιστατικών ασφαλείας παρέχοντας υπηρεσίες συντονισμού όπως:

- Προσδιορισμός της αρχικής αιτίας του συμβάντος
- Διευκόλυνση επικοινωνίας των εμπλεκόμενων φορέων
- Διευκόλυνση επικοινωνίας με τις αρμόδιες αρχές επιβολής του νόμου, αν χρειαστεί
- Ανάλυση και δημιουργία αναφορών προς άλλα CSIRT
- Σύνταξη ανακοινώσεων

5.1.3 Χειρισμός Συμβάντων

Η ευθύνη για το σχεδιασμό, την ανάπτυξη και τη λειτουργία των συστημάτων και υπηρεσιών με ασφαλή τρόπο και την επίλυση συμβάντων ασφαλείας παραμένει πάντα στους κατόχους των εν λόγω συστημάτων και υπηρεσιών. Σε ορισμένες περιπτώσεις και κατόπιν αιτήματος, παρέχεται συνδρομή στις επηρεαζόμενες βασικές και σημαντικές οντότητες, ως κάτωθι:

- Καθοδήγηση ή επιχειρησιακές συμβουλές σχετικά με την εφαρμογή πιθανών ενεργειών μετριασμού
- Συλλογή και ανάλυση εγκληματολογικών δεδομένων
- Δυναμική ανάλυση κινδύνων και περιστατικών
- Λήψη σχετικών αναφορών
- Αποστολή σχετικών αναφορών

Η έκταση αυτής της υποστήριξης θα εξαρτηθεί από τον τύπο και τη σοβαρότητα του συμβάντος και τον τύπο της επηρεαζόμενης οντότητας.

5.2 Προληπτικές Υπηρεσίες

Το EL-CSIRT συντονίζει και διατηρεί τις ακόλουθες υπηρεσίες στο μέτρο του δυνατού ανάλογα με τους πόρους του:

- Παροχή έγκαιρων προειδοποιήσεων, ειδοποιήσεων, ανακοινώσεων και πληροφοριών σε εμπλεκόμενες βασικές και σημαντικές οντότητες, καθώς και σε αρμόδιες αρχές και άλλα σχετικά ενδιαφερόμενα μέρη σχετικά με κυβερνοαπειλές, ευπάθειες και περιστατικά
- Παροχή, κατόπιν αιτήματος, προληπτικής σάρωσης των συστημάτων δικτύου και πληροφοριακών συστημάτων για τον εντοπισμό ευπαθειών με δυνητικό σημαντικό αντίκτυπο
- Προληπτική μη παρεμβατική σάρωση των δημοσίως προσβάσιμων συστημάτων δικτύου και πληροφοριακών συστημάτων για τον εντοπισμό ευπαθών ή επισφαλώς διαμορφωμένων συστημάτων
- Υπηρεσίες ενημέρωσης μέσω του ιστότοπου https://www.cyber.gov.gr
- Παρακολούθηση των τάσεων της τεχνολογίας
- Συντονισμός γνωστοποίησης ευπαθειών (CVD) σε εθνικό επίπεδο
- Συμβολή στην ευαισθητοποίησης και εκπαίδευση για την ασφάλεια στον κυβερνοχώρο

6 Έντυπα Αναφοράς Συμβάντων

Η λήψη αναφορών περιστατικών ασφαλείας από βασικές και σημαντικές οντότητες αρμοδιότητας του EL-CSIRT, βασίζεται σε συγκεκριμένη διαδικασία αναφοράς που είναι διαθέσιμη στην ηλεκτρονική διεύθυνση: https://cyber.gov.gr/kyvernoepitheseis/anafora-symvanton/ .

7 Αποποίηση ευθυνών

Το EL-CSIRT λαμβάνει όλα τα απαραίτητα οργανωτικά και τεχνικά μέτρα προστασίας των πληροφοριών που του παρέχονται. Για οποιοδήποτε σφάλμα, παράλειψη ή ζημία που ενδεχομένως προκύψει από τη χρήση ή σε σχέση με τις πληροφορίες που της παρέχονται, δε φέρει καμία ευθύνη οποιασδήποτε απαίτησης αποζημίωσης.