ΕΘΝΙΚΗ
ΥΠΗΡΕΣΙΑ
ΠΛΗΡΟΦΟΡΙΩΝ

CERT

Π. Κανελλοπούλου 4
Αθήνα – ΤΚ: 10177
210 697 3121
cert@nis.gr

RFC2350 - Λειτουργία Εθνικού CERT

1. Σκοπός εγγράφου

Το παρόν έγγραφο περιγράφει τη λειτουργία της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT σύμφωνα με το RFC2350.

1.1 Ημερομηνία τελευταίας αναθεώρησης

Η παρούσα έκδοση 1.1 αναθεωρήθηκε τον Ιούλιο 2022 και είναι σε ισχύ έως ότου υπερκαλυφθεί από νεότερη έκδοση.

1.2 Λίστα διανομής για ειδοποιήσεις

Οι αλλαγές σε αυτό το έγγραφο δεν θα διανεμηθούν μέσω λίστας ηλεκτρονικού ταχυδρομείου ή οποιουδήποτε άλλου μηχανισμού. Παρακαλούμε οποιεσδήποτε ερωτήσεις ή παρατηρήσεις να αποσταλούν μέσω ηλεκτρονικού ταχυδρομείου (όπως § 2.5).

1.3 Θέση που μπορεί να βρεθεί το έγγραφο

Η τρέχουσα έκδοση του κειμένου που περιγράφει το Εθνικό CERT είναι πάντα διαθέσιμη στην ιστοσελίδα της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικού CERT στο www.nis.gr. Παρακαλούμε να βεβαιωθείτε ότι χρησιμοποιείτε την τελευταία έκδοση.

2. Πληροφορίες σημείων επαφής

2.1 Όνομα ομάδας

Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT

Ομάδα Αντιμετώπισης Ηλεκτρονικών Επιθέσεων

Εθνικό CERT

NCERT-GR

2.2 Διεύθυνση

Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων

Π. Κανελλοπούλου 4, Αθήνα, Τ. Κ. Αθήνα, 10177, Ελλάδα

2.3 Ζώνη Ώρας

EET, Eastern European Time (UTC +2 μεταξύ τελευταίας Κυριακής του Οκτωβρίου και τελευταίας Κυριακής του Μαρτίου).

EEST, Eastern European Summer Time (UTC+3, μεταξύ τελευταίας Κυριακής του Μαρτίου και τελευταίας Κυριακής του Οκτωβρίου).

2.4 Αριθμός τηλεφώνου

+302106973121

2.5 Ηλεκτρονική Διεύθυνση

<cert@nis.gr>

Αυτή η ηλεκτρονική διεύθυνση χρησιμοποιείται για την αναφορά περιστατικού καθώς επίσης και για την συνολική επικοινωνία με την Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων - Εθνικό CERT.

Π. Κανελλοπούλου 4
Αθήνα – ΤΚ: 10177
210 697 3121
cert@nis.gr

2.6 Δημόσια Κλειδιά και άλλη πληροφορία Κρυπτογράφησης

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT χρησιμοποιεί PGP για την υπογραφή και την κρυπτογράφηση της ηλεκτρονικής αλληλογραφίας του. Τα στοιχεία του δημοσίου κλειδιού του Εθνικού CERT είναι:

KeyID: 0xFC196D8B

PGP Fingerprint: 8F58 C6C8 414D DA71 5D01 8310 54D1 3895 FC19 6D8B

Το δημόσιο κλειδί επισυνάπτεται στο παρόν έγγραφο.

2.7 Μέλη ομάδας

Δεν είναι διαθέσιμο.

2.8 Λοιπές Πληροφορίες

Γενικές πληροφορίες περί της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT, όπως επίσης και σύνδεσμοι για προτεινόμενα έγγραφα ασφαλείας, μπορούν να βρεθούν στην ιστοσελίδα της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT (όπως § 1.3).

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT είναι καταχωρημένο επίσημο μέλος του TF-CSIRT (Trusted Introducer).

2.9 Σημεία επαφής

Η προτεινόμενη μέθοδος για επαφή με την Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT είναι μέσω ηλεκτρονικού ταχυδρομείου (όπως § 2.5).

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT ενθαρρύνει τους ομολόγους της να χρησιμοποιούν ασφαλές e-mail όταν ανταλλάσσουν ευαίσθητες πληροφορίες.

Εναλλακτικά, μπορεί να χρησιμοποιηθεί ο τηλεφωνικός αριθμός της § 2.4.

Οι ώρες λειτουργίας της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT είναι οι ελληνικές εργάσιμες ώρες (07:30 – 15:30, Δευτέρα έως Παρασκευή, εκτός αργιών).

3 Καταστατικό

3.1 Δήλωση αποστολής

Αποστολή της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT είναι να μεριμνά για την πρόληψη, την έγκαιρη προειδοποίηση και την αντιμετώπιση κυβερνοεπιθέσεων εναντίον της κοινότητας αρμοδιότητάς της.

3.2 Κοινότητα Αρμοδιότητας

Σύμφωνα με τη νομοθεσία (π.δ. 1/2017 όπως τροποποιήθηκε με τα π.δ. 96/2020 και 33/2022), η κοινότητα αποδεκτών της Ομάδας Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (Εθνικό CERT), είναι κατά προτεραιότητα οι δημόσιοι φορείς της χώρας που δεν εμπίπτουν στην αρμοδιότητα της Διεύθυνσης Κυβερνοάμυνας του ΓΕΕΘΑ (CSIRT). Ειδικότερα, υποστηρίζει την Προεδρία της Κυβέρνησης, τα Υπουργεία και τους εποπτευόμενους φορείς τους, με εξαίρεση το Υπουργείο Εθνικής Άμυνας, για την πρόληψη, την έγκαιρη προειδοποίηση και την αντιμετώπιση κυβερνοεπιθέσεων εναντίον τους.

Π. Κανελλοπούλου 4
Αθήνα – ΤΚ: 10177
210 697 3121
cert@nis.gr

3.3 Υπαγωγή

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT υπάγεται στη Διεύθυνση Κυβερνοχώρου της Εθνικής Υπηρεσίας Πληροφοριών (ΕΥΠ).

3.4 Αρμοδιότητα

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT είναι αρμόδια για την αντιμετώπιση και την προστασία κυρίως του Δημόσιου τομέα και των κρίσιμων υποδομών, όπως ορίζεται στην παρ. 8 του άρθρου 4 του ν. 3649/2008, όπου για την εκπλήρωση της αποστολής της, η ΕΥΠ ασκεί τις αρμοδιότητες της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων, η οποία μεριμνά για την πρόληψη και τη στατική και την ενεργητική αντιμετώπιση ηλεκτρονικών επιθέσεων κατά δικτύων επικοινωνιών, εγκαταστάσεων αποθήκευσης πληροφοριών και συστημάτων πληροφορικής, σύμφωνα με τις διατάξεις της παρ. 3 του άρθρου 2 του π.δ. 325/2003. Ακολούθως, το π.δ. 1/2017 όπως τροποποιήθηκε με τα π.δ. 96/2020 και 33/2022, έδωσε την αρμοδιότητα στην Διεύθυνση Κυβερνοχώρου της ΕΥΠ ως Ομάδα Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (Εθνικό CERT).

4. Πολιτικές

4.1 Τύποι περιστατικών και επίπεδο υποστήριξης

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT συλλέγει πειστήρια για ηλεκτρονικές επιθέσεις/απειλές από δημόσιους και ιδιωτικούς οργανισμούς και κρίσιμες υποδομές και τους υποστηρίζει στην ανάκαμψη και πρόληψη.

Αναλύει και κατηγοριοποιεί τους τύπους των επιθέσεων/απειλών και τις αντιμετωπίζει σύμφωνα με τον τύπο τους.

Κατόπιν αιτήματος της κοινότητας αρμοδιότητάς της, παρέχει πληροφορίες και συμβουλές για την προστασία των Πληροφοριακών Συστημάτων (ΠΣ) από κυβερνοαπειλές.

Παρέχει υπηρεσίες που άπτονται του αντικειμένου της ασφάλειας των ΠΣ του ευρύτερου Δημόσιου Τομέα, όπως παρακάτω:

- Ενημέρωση Δημοσίων φορέων για περιστατικά ασφαλείας.
- Συντονισμό των εμπλεκόμενων για την αντιμετώπιση περιστατικών ασφαλείας.
- Ανάλυση και αξιολόγηση περιστατικών ασφαλείας.
- Πρόταση των μέτρων προστασίας που απαιτούνται για εξάλειψη των επιπτώσεων από ένα περιστατικό ασφαλείας.
- Ανάλυση κακόβουλων λογισμικών.
- Διενέργεια ελέγχων κυβερνοασφάλειας σε ΠΣ του Δημόσιου τομέα.
- Έκδοση γενικών οδηγιών για τη διασφάλιση των ΠΣ του Δημόσιου τομέα.

4.2 Συνεργασία, Αλληλεπίδραση και Αποκάλυψη Πληροφοριών

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT συνεργάζεται με άλλα CSIRT, Υπηρεσίες του Δημόσιου τομέα, καθώς και εθνικούς και διεθνείς φορείς, αρμόδιους για θέματα κυβερνοασφάλειας.

Επιπροσθέτως, η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT συνεργάζεται με άλλες αρμόδιες Αρχές στις ακόλουθες καταστάσεις:

Π. Κανελλοπούλου 4
Αθήνα – ΤΚ: 10177
210 697 3121
cert@nis.gr

- Για θέματα Εθνικής σημασίας – με την Κυβέρνηση, ειδικά την Εθνική Αρχή Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης.
- Για θέματα ασφαλείας που σχετίζονται στην Κυβερνητική υποδομή ή κρίσιμες υποδομές – με την Κυβέρνηση.
- Για θέματα προστασίας δεδομένων – με την Αρχή Προστασίας Προσωπικών Δεδομένων.
- Για ύποπτη εγκληματική δραστηριότητα – με την Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της ΕΛΑΣ.
- Για θέματα ΦΕΒΥ (οδηγία NIS) με το αρμόδιο CSIRT (Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ).

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT συντονίζει τις δράσεις σε περίπτωση κρίσιμων καταστάσεων και εφαρμόζει την Εθνική Στρατηγική σε εθνικό και διεθνές επίπεδο, σε ό,τι αφορά την αντιμετώπιση κυβερνοαπειλών.

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT τηρεί όλα τα απαραίτητα μέτρα ασφάλειας, ώστε να εξασφαλίζεται ότι τα εταιρικά και ιδιωτικά δεδομένα προστατεύονται. Οποιαδήποτε αποκάλυψη πληροφορίας πραγματοποιείται αποκλειστικά στα πλαίσια «ανάγκης γνώσης» και με την εξουσιοδότηση του ιδιοκτήτη της πληροφορίας.

4.3 Επικοινωνία και Αυθεντικοποίηση

Η προτεινόμενη μέθοδος επικοινωνίας είναι μέσω email (όπως §2.5).

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT ακολουθεί το Traffic Light Protocol (TLP) όπως ορίζεται στο πρότυπο του FIRST (https://www.first.org/tlp/). Το TLP είναι ένα σύνολο ορισμών που χρησιμοποιούνται για να διασφαλίσουν ότι η ευαίσθητη πληροφορία μπορεί να διαμοιραστεί στο σωστό κοινό.

Για χρήση από την κοινότητα αρμοδιότητας, επισυνάπτεται «ΕΝΤΥΠΟ ΑΝΑΦΟΡΑΣ ΠΕΡΙΣΤΑΤΙΚΟΥ» με τα ελάχιστα στοιχεία που απαιτείται να αποσταλούν Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT, ώστε να κινηθεί η διαδικασία διερεύνησης ενός κυβερνοπεριστατικού.

5. Υπηρεσίες

5.1 Αντίδρασης Περιστατικών

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT βοηθά τους διαχειριστές συστημάτων να χειριστούν τα τεχνικά και οργανωτικά θέματα των κυβερνοπεριστατικών. Συγκεκριμένα, παρέχει αρωγή και συμβουλές στα ακόλουθα θέματα διαχείρισης περιστατικών:

5.1.1 Διαλογή περιστατικού

Διακρίβωση της πραγματικής ύπαρξης περιστατικού ασφαλείας και καθορισμός των επιπτώσεών του.

5.1.2 Συντονισμός περιστατικού

- Ενέργειες καθορισμού της αρχικής αιτίας του περιστατικού (εκμετάλλευση ευπαθειών).
- Διευκόλυνση επαφών με κατάλληλους επιτελείς διωκτικών αρχών, εάν είναι απαραίτητο.
- Δημιουργία αναφορών προς άλλα CERTs/CSIRTs.
- Συντονισμός απαντήσεων σε περιστατικά κατανεμημένης επίθεσης.

Π. Κανελλοπούλου 4
Αθήνα – ΤΚ: 10177
210 697 3121
cert@nis.gr

- Δημιουργία ανακοινώσεων για τους χρήστες που εμπλέκονται στο περιστατικό.
- Παρακολούθηση της διαδικασίας επίλυσης του περιστατικού.
- Καταχώρηση και τήρηση αρχείου περιστατικών.

5.1.3 Ανάλυση περιστατικού

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT συλλέγει, διατηρεί, τεκμηριώνει και αναλύει τα στοιχεία από υπολογιστές που έχουν παραβιαστεί, για να καθοριστούν οι αλλαγές στο σύστημα και για να αναδομηθούν τα γεγονότα που οδήγησαν στην παραβίαση.

Η ευθύνη της λειτουργίας των συστημάτων με ασφαλή τρόπο και η επίλυση των περιστατικών ασφαλείας παραμένει πάντα στους ιδιοκτήτες των συστημάτων.

5.2 Πρόληψη

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT προσφέρει στην κοινότητα αρμοδιότητας τις παρακάτω υπηρεσίες πρόληψης:

- Εκδίδει ανακοινώσεις για απειλές, επιθέσεις και προτεινόμενα μέτρα πρόληψης.
- Προτείνει και επιδεικνύει τη χρήση εργαλείων ασφαλείας στην κοινότητα αποδεκτών της.
- Παράγει κανόνες/έγγραφα ασφάλειας που βοηθούν στο να ελαχιστοποιηθεί η εκμετάλλευση τρωτοτήτων από κυβερνοαπειλές.
- Διενεργεί αξιολόγηση τρωτοτήτων, κατόπιν αίτησης του ενδιαφερόμενου φορέα στα ΠΣ του.
- Διεξάγει εκπαιδεύσεις στα στελέχη πληροφορικής των κυβερνητικών φορέων για προστασία από κυβερνοαπειλές.

6. Φόρμες αναφορών περιστατικών

Οι αναφορές περιστατικών γίνονται με επίσημο ηλεκτρονικό μήνυμα (όπως ορίζεται στην § 2.5).
Σε κάθε περίπτωση, είναι υποχρεωτική η συμπλήρωση του εντύπου αναφοράς περιστατικών (όπως ορίζεται στην §4.3).

7. Αποποίηση ευθύνης

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT λαμβάνει όλα τα απαραίτητα μέτρα και προφυλάξεις στην επεξεργασία των πληροφοριών που της παρέχονται με οποιονδήποτε τρόπο (ιστοσελίδα, λίστες αλληλογραφίας κλπ).

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT δε φέρει καμία ευθύνη για οποιαδήποτε απαίτηση αποζημίωσης για σφάλματα, παραλείψεις, ζημιές, ή άλλες ευθύνες προκύψουν, από τη χρήση ή και σε σχέση με τις παραχθείσες πληροφορίες.

Π. Κανελλοπούλου 4
Αθήνα – ΤΚ: 10177
210 697 3121
cert@nis.gr

ΔΗΜΟΣΙΟ ΚΛΕΙΔΙ ΕΘΝΙΚΟΥ CERT

Διεύθυνση ηλεκτρονικού ταχυδρομείου: <cert@nis.gr>

PGP Fingerprint: 8F58 C6C8 414D DA71 5D01 8310 54D1 3895 FC19 6D8B

Δημόσιο κλειδί:

-----BEGIN PGP PUBLIC KEY BLOCK-----

xsBNBE9m5o8BCAC3aec1qPWwLT4+mave3oUL6uf6EXL5OF3Fy55geeLrbsifTVGx
Nt/ipqsWj9gsKqEScHtbI8BbuuiL3DM6Gs7SW6JWUM9GUXvCstrePxo7nHEQ5Fd1
+boOQEmPpsuAlXWivC3hjjaCAp9OhAQPAHqQfF3sdkVLLqSy9lJhC/MZuHpDyHzk
Y+vUZSFgHic69hpxToqo2tJRTi2qAzSGzlt5KnCilOe67wx8bWcUjuNSKlwBb3Db
ZQs5ZFIXJsDyhXCJJhazVmosmR6K5N5kQMJPvZzcUcnI+nyuQHIHVErsb1BBU3uH
faitWly3p1UoekCwpPHD/YX1zWppiM9OKHpxABEBAAHNFm4tY2VydCAxIDxjZXJo
QG5pcy5ncj7CwMwEEAECAHYFAlMqvLcwFIAAAAAAIAAHcHJlZmVycmVkLWVtYWls
LWVuY29kaW5nQHBncC5jb21wZ3BtaW1lCAsJCAcDAgEKAhkBGRhsZGFwOi8va2V5
c2VydmVyLnBncC5jb20oFGwMAAAAFFgADAgEFHgEAAAAGFQgJCgMCAAoJEFTROJX8
GW2LTbUH/1ORuOd6UK2LrL8+fYzDtt+vBw7ZJ7oohoULoRYbnrEkjByFUVGevO+X
qnl+aqz/miHRvALWNqH6V+zZhDp9OB+AjTouoyA+UfOwKR9y5Xm6GlKLox0SxIaR
vJV3eJ3HiwLl3ZDVT7uZB46+onhstFJ4WfPqSlPf1XTzjdI7hFWcs4iRTy0wywoC
cWqCPeO2iFjUPsI7thVk4wgTrRE1K2PhA5UL/Q5cFxlltbKU4AKgMdqHyrBfGeyL
i1AL9if6Ljum2/N4AsD/AlNd54EoNoWN9oFXAIJy52rzNuVqvTOj9LL3eUklU+7o
8vsD1rmU1ORfwb/630VPCv5xekGeFObNEmNlcnQgPGNlcnRAbmlzLmdyPsLAyQQQ
AQIAcwUCUyrB9TAUgAAAAAgAAdwcmVmZXJyZWQtZW1haWwtZW5jb2RpbmdAcGdw
LmNvbXBncG1pbWUICwkIBwMCAQoZGGxkYXA6Ly9rZXlzZXJ2ZXIucGdwLmNvbQUb
AwAAAAUWAAMCAQUeAQAAAAYVCAkKAwIACgkQVNE4lfwZbYuVnAf+JU9PlLZy490V
GrUBJUZoySQEzxSC9NQ+R3/tWMAujzBn8WO87Vsm9zhsIDh+EkDySnhrHAbKamxu
Vvg3f3L62TYkMW/nnN1tcrSHMC4LRTsjTmbM8xYfD65B51Qod/htzQxn7jiJY1VV
cJ2WyBlC+sJRGoWS2kHDGB1LMXZzNvvpJdCyLDi2iUU6EzGzoTQ+jHAa4qy8ciRG
NTjPEokwFf5NEJsrAweAs/3+Gun6fkz4VBpohkmccCAyqx7if3vLuu7VOtKKXgNF
wj461QLsZf4kayV4wUJWpYgIWeKPHrfD7AdAiCXftzKrQpDob5jgLHp7QvyZmjDr
PzIV69QFrM7ATQRPZudPAQgAwvFLmFmMu/+CHly9DV6DMN6DhTkVnvn4nKZkrZsC
ncjiaU1ZCpNUeojHplk+k3YGh1R8R6l8H36XeGnbl//HM7ruhColi9bctJoJXe6N
MkVg0243Y/AQr4FNCZDYmoQEESgqzH2apAeW8ll2qfgyttnFdZWi/CZFhee3J4iz
qUvxzCNSeoAEJLaPwd6NgqbBgrrc9xRJeCvQDilZsYxdoFms5EiCGN36bW2wH8GU
Z4bJwzJi4Nt8PTv94SYuKVjB4ou20WsPHt/Gu2gd9KtdQ5EdfBpvLNFHb6dWrHmF
83wcESqHUdIX+hjiFktVNFWhvnywD82PuRp4lNPr7llLFQARAQABwsGBBBgBAgEr
BQJPZudQBRsMAAAAwFogBBkBCAAGBQJPZudPAAoJEJdg5Q9CogGh12MIALJ7fGZu
VqRPVXV7ksxxrXTqg5q3LStpNVB8PcMiAeHXZ9nwvics+4JOfPhe5/fhw66j8v9d
RZL+rFzGedNTggINN/6n1t9dlnyn+vzwA2eBBdx2r2VCoXqqme+vlMydppQrpgw/
ga8obKncTMmWlNdOQoCa/jawwRYhuCxDBE8QQc8pUPRLQwZnBwLe4OyRuwnv7Nuv
/c8biNJsRoK4j5Ca3LK2Su6vou2IBQrRDzCxjJilxZt9AX6dxr3/epAX8B9mDag8
b1/r4YrkMQwPJwACSx6jQpiLDHpZ/VgNropuirAondQitJ+RmDYNobm0c1QiAusn
FTLtcG52zYleR1MACgkQVNE4lfwZbYuXJAf+NRBRroGkUHN16/CoBJ2asdhKeIzV
WeoHCr90AroobGkvrHO9lsd8wwow18kkW6lgTBGH6nwnVTO3shjUGN5Y5npvVw6v
4cvD/tOjyNkkvR9jrRrjp862BEx6+lJlv4BfyqpIoiLdxuQAPgApQn8Vjsw6Exho
NRy5srHwFZMnqatoLgk5nwG3vo//WoOxycnpf+NurLI9ktilo1bomiDAeG4R3z7E
pPQxClnyHBIn7uml+gk7+Y6q4jEhPh5dHIEoUbM+bNWpqyyM9TjT7SoF8nyV4ws6
wb+QozT6CdyZ15zRsVwb7TQdqOTJx5O/jJhmBE1nLUhcXaMplo9JwZetEA==
=Wah5
-----END PGP PUBLIC KEY BLOCK-----

ΕΘΝΙΚΗ ΥΠΗΡΕΣΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

CERT

Π. Κανελλοπούλου 4
Αθήνα – ΤΚ: 10177
210 697 3121
cert@nis.gr

ΕΝΤΥΠΟ ΑΝΑΦΟΡΑΣ ΠΕΡΙΣΤΑΤΙΚΟΥ

Παρακαλούμε συμπληρώσετε τα παρακάτω στοιχεία για την αναφορά περιστατικού και αποστείλετε στη διεύθυνση: **cert@nis.gr**

ΣΤΟΙΧΕΙΑ ΟΡΓΑΝΙΣΜΟΥ	
Όνομα οργανισμού/τομέα:	
Δνση/Πόλη:	
Τμήμα:	
email:	
Τηλέφωνο:	
Κινητό τηλέφωνο:	
Υπεύθυνος Ασφαλείας:	
Διαχειριστής:	
ΣΤΟΙΧΕΙΑ ΠΕΡΙΣΤΑΤΙΚΟΥ	
Αριθμός αναφοράς ref. #:	
Είδος περιστατικού (π.χ. σκουλήκι δικτύου, Δούρειος Ίππος, Botnet, μικτές επιθέσεις, ιστοσελίδα με ενσωματωμένο κακόβουλο κώδικα, κακόβουλος ιστότοπος φιλοξενίας, άρνηση υπηρεσίας, παράνομο περιεχόμενο κ.α.):	
Αρχή του περιστατικού:	
Αυτό είναι ένα συνεχές περιστατικό:	ΝΑΙ ☐ ΟΧΙ ☐
Λεπτομερής περιγραφή περιστατικού (Τι συνέβη, πως συνέβη, γιατί συνέβη, στοιχεία που επηρεάζονται, δυσμενείς επιπτώσεις, ευπάθειες):	
Αντίμετρα:	

ΕΘΝΙΚΗ ΥΠΗΡΕΣΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

CERT

Π. Κανελλοπούλου 4
Αθήνα – ΤΚ: 10177
210 697 3121
cert@nis.gr

ΕΝΤΥΠΟ ΑΝΑΦΟΡΑΣ ΠΕΡΙΣΤΑΤΙΚΟΥ

ΥΠΟΛΟΓΙΣΤΕΣ ΠΟΥ ΕΠΗΡΕΑΖΟΝΤΑΙ	
Αριθμός κεντρικών υπολογιστών:	
Λειτουργία του κεντρικού υπολογιστή:	
Ημερομηνία και ώρα του συμβάντος:	
Ημερομηνία και ώρα του συμβάντος που ανακαλύφθηκε το συμβάν:	
Έχει κλείσει η απάντηση σε αυτό το συμβάν;	ΝΑΙ ☐ ΟΧΙ ☐
Εάν ναι, καθορίστε πόσο διήρκησε το συμβάν (διάρκεια σε ημέρες/ώρες/λεπτά):	
Υλικό:	
Λειτουργικό σύστημα:	
Επηρεαζόμενο λογισμικό:	
Επηρεαζόμενα αρχεία:	
Όνομα κεντρικού υπολογιστή:	
Source IP(s):	
Destination IP:	
Πρωτόκολλο:	