Ένωση Πληροφορικών Ελλάδας
Λυκούργου 1 & Αιόλου (1ος όροφος)
ΤΚ 10551, Αθήνα
http://www.epe.org.gr
e-mail: info@epe.org.gr
Τηλέφωνο: (+30) 211 3332456

Δελτιο Τυπου

Ψηφιακή Ελλάδα 2.0 ή κυβερνητικό Denial of Service;

Αθήνα, 2-6-2023

Τις τελευταίες ημέρες η ελληνική ειδησεογραφία πραγματικά κατακλύστηκε από δημοσιεύματα όπως τα παρακάτω:

- 26/5/2023: *"Ολοκληρωμένο Πληροφοριακό Σύστημα Διαχείρισης Προσωπικού Εκπαίδευσης(ΟΠΣΥΔ) Ακούει κανείς; Ποιος θα αναλάβει την ευθύνη των λαθών; Είναι δυνατόν τόσοι εκπαιδευτικοί να έκαναν το ίδιο λάθος;"* (https://is.gd/TU1Abu)
- 29/5/2023: *"Άνω κάτω τα σχολεία: "Έπεσε" η Τράπεζα Θεμάτων! Μπλόκαραν οι εξετάσεις στα Λύκεια"* (https://is.gd/KRXDeb)
- 29/5/2023: *"Νέο "χάος" με την Τράπεζα Θεμάτων: Κληρώνει "λειψά" θέματα στα Λύκεια και "κλειδώνει" η πλατφόρμα"* (https://is.gd/MVHBu7)
- 30/5/2023: *"Τράπεζα Θεμάτων: "Κατέρρευσε" και σήμερα η ηλεκτρονική πλατφόρμα"* (https://is.gd/bK6Lwz)
- 30/5/2023: *"ΟΑΕΔ-ΔΥΠΑ:«Έπεσε» η πλατφόρμα του Κοινωνικού Τουρισμού"* (https://is.gd/824EdT)

Και μόνο το πρώτο από τα παραπάνω προβλήματα, αυτό της κατάρρευσης επί δύο ημέρες της Τράπεζας Θεμάτων στην πλατφόρμα του ΙΕΠ (https://trapeza.iep.edu.gr), ταλαιπώρησε χιλιάδες μαθητές Γενικών Λυκείων και ΕΠΑΛ, αρκετοί εκ των οποίων θα καλούνταν να συμμετάσχουν στις Πανελλήνιες Εξετάσεις της Γ' ΓΕΛ και ΕΠΑΛ ελάχιστες ημέρες μετά. Αυτό που ανακοινώθηκε επισήμως από τα συναρμόδια υπουργεία Παιδείας και Ψηφιακής Διακυβέρνησης για το συγκεκριμένο πρόβλημα ήταν ότι οι αντίστοιχοι servers φιλοξενίας είχαν γίνει στόχος πρωτοφανούς μαζικότατης επίθεσης τύπου άρνησης υπηρεσίας (Distributed Denial of Service attack - DDoS) από άγνωστους

hackers του εξωτερικού, με αποτέλεσμα την κατάρρευση της πλατφόρμας για πολλές ώρες επί δύο συνεχόμενες ημέρες.

Ως Ένωση Πληροφορικών Ελλάδας (ΕΠΕ) παρακολουθούμε διαρκώς τα ζητήματα που αφορούν την ασφάλεια, τη διαθεσιμότητα και την αξιοπιστία των βασικών υποδομών σε πληροφοριακά συστήματα, ειδικά στον ευρύτερο δημόσιο τομέα. Δυστυχώς, το φαινόμενο της επισφαλούς, πολύ κακής ως και εντελώς καταστροφικής τους λειτουργίας είναι συχνό και έχουμε αναγκαστεί να παρέμβουμε δημόσια πολλές φορές. Ενδεικτικά, μερικά παραδείγματα:

- 8/3/2023: *"Δελτίο Τύπου - Ανακοίνωση σχετικά με το πολύνεκρο δυστύχημα τρένων στα Τέμπη"* (https://is.gd/R2Pkjk)
- 3/2/2022: *"Δελτίο Τύπου - Θέματα σχετικά με την τελευταία κακοκαιρία και την διαχείριση του δικτύου Αυτοκινητόδρομων της Ελλάδας"* (https://is.gd/6rrAxZ)
- 25/5/2021: *"Δελτίο Τύπου - Διευκρινίσεις ως προς τη δημοσιοποίηση επιστολής σχετικά με σοβαρό πρόβλημα ασφάλειας στην πλατφόρμα gov.gr"* (https://is.gd/sAJ2cI)
- 21/5/2021: *"Σοβαρό πρόβλημα ασφάλειας στην πλατφόρμα gov.gr"* (https://is.gd/jz6Ycd)
- 26/3/2021: *"Δελτίο Τύπου - Επισημάνσεις σχετικά με τη σύμβαση Cisco-Webex με το υπουργείο Παιδείας"* (https://is.gd/VRSfjP)

Επίσης, είναι γνωστό ότι στο σχετικά πρόσφατο παρελθόν έχει αποδειχθεί η μαζική διαρροή προσωπικών δεδομένων από κεντρικούς οργανισμούς και συστήματα όπως το TAXISnet (https://is.gd/pEX9HP) και τα ΕΛΤΑ (https://is.gd/bTy5oJ), χωρίς ποτέ να δοθούν επαρκείς εξηγήσεις για τα ακριβή αίτια, ούτε όπως φαίνεται να έχουν αξιοποιηθεί τα αντίστοιχα περιστατικά ως μάθημα για το μέλλον.

Στο πιο πρόσφατο περιστατικό της κατάρρευσης της πλατφόρμας του ΙΕΠ, αντιλαμβάνεται κανείς εύκολα ότι γεννιούνται τα ακόλουθα ερωτήματα:

1. **Κατά τη σχεδίαση του όλου έργου είχαν ληφθεί τα απαραίτητα μέτρα θωράκισης από κακόβουλες ενέργειες;** Ποια ακριβώς ήταν αυτά, ποιες δοκιμές (stress tests) είχαν πραγματοποιηθεί και ποιος διασφάλισε το απαραίτητο επίπεδο αξιοπιστίας και διαθεσιμότητας της υπηρεσίας προτού τεθεί σε πραγματική χρήση; Θυμίζουμε πως η φετινή ήταν η δεύτερη χρονιά λειτουργίας της Τράπεζας Θεμάτων Διαβαθμισμένης Δυσκολίας (Τ.Θ.Δ.Δ.) απ' το Υπουργείο Παιδείας, ενώ μέχρι πριν τις 29/5 ο ιστότοπος δεν υποστήριζε καν τη λεγόμενη ασφαλή σύνδεση (HTTPS/SSL), όπως φαίνεται και από σχετικές εικόνες. Να υποθέσουμε λοιπόν πως οφείλεται καθαρά στην τύχη το ότι πέρυσι δεν είχε παρουσιαστεί καμία απολύτως δυσλειτουργία; Επίσης, γιατί δεν υπήρχε "Plan B" για τέτοιες περιπτώσεις κατάρρευσης ή -έστω- μη αποδεκτού downtime της πλατφόρμας; Θα μπορούσε π.χ. να επιτραπεί στους εκπαιδευτικούς να χρησιμοποιήσουν θέματα απ' τη σχετική

υπηρεσία του ΙΕΠ για το κοινό (public): https://trapeza.iep.edu.gr/public/subjects.php

2. Αφότου έγινε η φερόμενη "επίθεση" τη Δευτέρα 29/5, φαίνεται ότι ελήφθησαν κάποια μέτρα τελευταίας στιγμής και εξαιρετικά βιαστικά, ώστε αυτό να μην επαναληφθεί. Γνωρίζουμε ότι από την επόμενη ημέρα, Τρίτη 30/5, η βασική υποδομή της πλατφόρμας υποστηρίζεται από συγκεκριμένη διαδικτυακή υπηρεσία (Akamai cloudbase), η οποία προσφέρει πολύ αυξημένη εξειδίκευση και ανθεκτικότητα απέναντι σε τέτοιου είδους περιστατικά. **Παρόλα αυτά, το ίδιο πρόβλημα παρουσιάστηκε ξανά,** χωρίς ουσιαστική διαφοροποίηση σε σχέση με την προηγούμενη ημέρα, ενδεχομένως λόγω κακής ή ελλιπούς παραμετροποίησης για την ενεργοποίηση των πρόσθετων υπηρεσιών έναντι DDoS επιθέσεων. **Γιατί συνέβη αυτό;** Σημειώνουμε ότι σε τεχνικό επίπεδο οι επιθέσεις DDoS μπορούν να αντιμετωπιστούν με πολλαπλούς τρόπους και διαδικασίες, οι οποίες μάλιστα δεν είναι εξεζητημένες ή κοστοβόρες, όπως για παράδειγμα IP geolocation filtering, next generation firewalls (NGFW), πολλαπλές "εισόδους" με δυναμική ανάθεση server IP, κ.ο.κ. Γιατί δεν ήταν ενεργά τέτοια αντίμετρα ήδη πριν από τις 29/5;

3. **Πώς τεκμηριώνεται ότι πράγματι συνέβη τέτοιου είδους μαζική και "πρωτοφανής" επίθεση DDoS στις συγκεκριμένες δύο ημερομηνίες κατά της πλατφόρμας του ΙΕΠ;** Σημειώνεται ότι, με βάση τα δημόσια διαθέσιμα δεδομένα, αναφορές ασφάλειας και χάρτες αναφοράς τέτοιων καθημερινών περιστατικών διεθνώς, πουθενά δεν προκύπτει ότι υπήρξε κάποια εξαιρετικά αυξημένη κίνηση στοχευμένα προς την πλατφόρμα του ΙΕΠ σαν και αυτή που περιγράφηκε από τις ανακοινώσεις των αρμοδίων. Αντίθετα, φαίνεται πως η κίνηση δεδομένων που απεικονίζεται για παράδειγμα στις 29/5 δεν ήταν μεγαλύτερη από την αντίστοιχη των προηγούμενων ημερών, ενώ περιπτώσεις ακριβώς αντίστοιχης κίνησης λίγες μέρες νωρίτερα δε φαίνεται να είχαν δημιουργήσει κανένα πρόβλημα ή υποψία "επίθεσης" (https://is.gd/mSexNe , https://is.gd/lUD9Sz). Επίσης, η αναφερόμενη DDoS επίθεση στις 29-30/5 στην Ελλάδα δεν φαίνεται να εμφανίζεται σε διεθνείς υπηρεσίες καταγραφής παρόμοιων περιστατικών σε καθημερινή βάση, όπως αυτή του Cloudflare Radar (https://is.gd/Dx6TIf). Αξίζει να αναφερθεί ότι τόσο για την 1η ημέρα (29/5) στην υποδομή του GRnet, όσο και για τη 2η μέρα (30/5) στην υποδομή του Akamai, ροές δεδομένων αυτής της τάξης μεγέθους είναι εκατοντάδες φορές μικρότερη από αυτές που ιστορικά έχουν δεχτεί σε τέτοιους τύπου επιθέσεις και έχουν ανταπεξέλθει επιτυχώς (https://is.gd/JrqfY6). Συνεπώς, ακόμη και αν συνέβη επίθεση στην πλατφόρμα του ΙΕΠ όπως αυτή που αναφέρεται, δεν θα έπρεπε να εμφανιστεί πρακτικά κανένα σημαντικό πρόβλημα. Ενδεικτικά, η υπηρεσία Single-Sign-On (SSO) του Πανελλήνιου Σχολικού Δικτύου (ΠΣΔ), η οποία χρησιμοποιείται κάθε φορά που ένας εκπαιδευτικός ή μαθητής θα χρειαστεί να διαβάσει τα e-mails του ή να συνδεθεί σε eclass, e-me, WebEx κλπ. και την οποία επίσης χρησιμοποιεί το ΙΕΠ για σύνδεση και με την Τ.Θ.Δ.Δ., συχνά δέχεται σαφώς μεγαλύτερο αριθμό επισκέψεων από αυτόν που αναφέρουν στην ανακοίνωσή τους

τα Υπουργεία Παιδείας και Ψηφιακής Διακυβέρνησης (https://is.gd/d9tYoi) και όμως δεν καταρρέει. Να σημειώσουμε επίσης ότι το πλήθος των αιτημάτων που ανακοινώθηκε ότι δέχτηκαν τα συστήματα του ΙΕΠ, δε συνάδει με το προφίλ εξειδικευμένων επιθέσεων DDoS που εκμεταλλεύονται εγγενείς αδυναμίες κάποιων εγκαταστάσεων, όπως για παράδειγμα επιθέσεις Slow HTTP Attack (https://is.gd/Jr39P0).

Όλα τα παραπάνω, όχι μόνο για την περίπτωση της πλατφόρμας του ΙΕΠ, συνηγορούν ότι κατά πάσα πιθανότητα βρισκόμαστε και πάλι μπροστά στα αποτελέσματα της προχειρότητας, της έλλειψης σοβαρότητας, της έλλειψης σωστής μελέτης σχεδίασης και αποτίμησης ρίσκου, καθώς και της εν γένει αντιμετώπισης των έργων και υποδομών των Τεχνολογιών Πληροφορικής και Τηλεπικοινωνιών (ΤΠΕ) ως κάτι δευτερεύον, όχι και τόσο σημαντικό, κάτι που ακόμα και όταν αστοχεί δεν έγινε κάτι πολύ κακό.

Δυστυχώς, η Πληροφορική στην Ελλάδα εξακολουθεί να αντιμετωπίζεται ως μη-επιστήμη, χωρίς τεχνικές προδιαγραφές και απαιτήσεις αξιοπιστίας, η οποία δεν απαιτεί τίποτα παραπάνω από "μεράκι" και "τέχνη". Δεν είναι τυχαίο το ότι ακόμα και σήμερα η περιγραφή επαγγέλματος για τον τεχνικό δικτύων Η/Υ μεταλυκειακής βαθμίδας (π.χ. απόφοιτοι ΙΕΚ και ΕΠΑΛ) στο αντίστοιχο πλαίσιο του ΕΟΠΠΕΠ εντάσσεται στην κατηγορία 3, μαζί με Στυλίστες, Διακοσμητές, κτλ ("Γ: Επαγγέλματα για την άσκηση των οποίων δεν είναι απαραίτητη η κτήση τίτλου σπουδών" - https://is.gd/mj2jyg) - γεγονός που ως ΕΠΕ έχουμε καταγγείλει δημόσια εδώ και χρόνια ("Επαγγελματικά δικαιώματα πιστοποιημένων από τον ΕΟΠΠΕΠ αποφοίτων ΕΠΑΛ και ΙΕΚ ειδικοτήτων Πληροφορικής"- https://is.gd/HXhnD8 , https://is.gd/n9tpcy).

Είμαστε βέβαιοι ότι η ελληνική Δικαιοσύνη, με τη συνδρομή της Δίωξης Ηλεκτρονικού Εγκλήματος, θα εντοπίσει τα αίτια που προκάλεσαν το πρόβλημα. Καλούμε τους αρμόδιους φορείς να δημοσιοποιήσουν αναλυτικά τα ευρήματα της έρευνας όταν ολοκληρωθεί. Καλούμε επίσης όλους τους συναρμόδιους φορείς και υπηρεσίες να πράξουν τα δέοντα για την άμεση δημοσιοποίηση στοιχείων ως προς τα τεχνικά χαρακτηριστικά της φερόμενης επίθεσης μόλις αυτά γίνουν διαθέσιμα, όπως ενδεικτικά το είδος των αιτημάτων που έγιναν προς τους εξυπηρετητές - ενδεικτικά GET/POST/PATCH requests, είδος/μέγεθος και ταχύτητα μετάδοσης payload, προορισμός/endpoint διεύθυνσης προορισμού, κλπ. Τα στοιχεία αυτά θα επιτρέψουν τη μελέτη της περίπτωσης από τους τεχνικούς άλλων οργανισμών με σκοπό την κατανόηση των αδυναμιών και την υλοποίηση μεθόδων αποφυγής παρόμοιων προβλημάτων στο μέλλον.

Παρόλα αυτά, είναι βέβαιο ότι δυσλειτουργίες ψηφιακών υπηρεσιών θα εξακολουθούν να παρουσιάζονται, είτε λόγω αστοχίας υλικού, είτε λόγω κακού σχεδιασμού, είτε λόγω δολιοφθοράς, είτε για δεκάδες ακόμη λόγους, όσο δεν διαμορφώνεται το κατάλληλο θεσμικό πλαίσιο. Είμαστε αναγκασμένοι να επαναλάβουμε ξανά τις πάγιες θέσεις και προτάσεις μας για:

ΕΝΩΣΗ ΠΛΗΡΟΦΟΡΙΚΩΝ ΕΛΛΑΔΑΣ

1. Τον καθορισμό κανόνων ανάπτυξης λογισμικού για τις υπηρεσίες του ευρύτερου δημοσίου τομέα.
2. Τον καθορισμό κανόνων διασφάλισης ποιότητας, βάσει των οποίων θα γίνονται όλα τα έργα ΤΠΕ και οι προμήθειες λογισμικού.
3. **Την ίδρυση Εθνικού Επιμελητηρίου Επικοινωνιών και Πληροφορικής (ΕΘΕΕΠ) το οποίο θα είναι υπεύθυνο για τον καθορισμό των παραπάνω κανόνων.**
4. Την ενίσχυση των ΤΠΕ ειδικά στη Δημόσια Διοίκηση, τόσο σε υποδομές όσο και σε κατάλληλο επιστημονικό προσωπικό.

Παραμένουμε στη διάθεση της Πολιτείας και των αρμόδιων Αρχών, εφόσον ζητηθεί η συνδρομή μας σε σχέση με τα παραπάνω.

Το Διοικητικό Συμβούλιο
της Ένωσης Πληροφορικών Ελλάδας

URL: http://www.epe.org.gr , mailto:info@epe.org.gr