ΕΠΕΙΓΟΝ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ
Δ/ΝΣΗ ΥΠΗΡΕΣΙΑΣ ΣΥΝΤΟΝΙΣΜΟΥ
ΓΡΑΦΕΙΟ ΝΟΜΙΚΩΝ ΚΑΙ ΚΟΙΝΟΒΟΥΛΕΥΤΙΚΩΝ ΘΕΜΑΤΩΝ

Ταχ. Δ/νση: Αριστοτέλους 17
Τ.Κ.: 10433 Αθήνα
Τηλέφωνα: 2132161426, 2132161433
2132161428, 2132161429
E-mail: tke@moh.gov.gr

Αθήνα, 11.09.2025

Αρ. Πρωτ.: 28162

ΠΡΟΣ: **ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ**
Δ/νση Κοινοβουλευτικού Ελέγχου
Τμήμα Ερωτήσεων

ΘΕΜΑ: Απάντηση σε ερώτηση Βουλευτή

Σε απάντηση της με αρ. **6810/24.06.2025** ερώτησης, που κατατέθηκε στη Βουλή των Ελλήνων από τον Βουλευτή κ. Βελόπουλο Κ., με θέμα *«Ερωτήματα περί λειτουργίας συγκεκριμένων ιστότοπων Υπουργείων»*, σας γνωρίζουμε τα κάτωθι:

1. Το αρχικό κόστος κατασκευής του ιστοχώρου του Υπουργείου Υγείας (www.**moh.gov.gr**) ήταν περίπου 6.000€
2. Το κόστος τεχνικής υποστήριξης και φιλοξενίας ανέρχεται σε 12.000€/έτος
3. Η ιστοσελίδα του Υπουργείου Υγείας **δεν** βασίζεται σε κάποια έτοιμη πλατφόρμα ανοιχτού λογισμικού, βασίζεται σε προσαρμοσμένο προγραμματισμό (custom made) για μέγιστη ασφάλεια και ευελιξία λειτουργιών.
4. Μέτρα που λαμβάνονται για την προστασία του ιστοχώρου από κυβερνοεπιθέσεις περιλαμβάνουν:

   - Προστασία και ασφάλεια των servers
     - Software-based WAF & Proactive Defence

     Ειδικό λογισμικό Web Application Firewall σε μορφή software για την προστασία του site στον backend server από κακόβουλες επιθέσεις στο επίπεδο της εφαρμογής. Σε αντίθεση με τα παραδοσιακά firewalls που εστιάζουν στην προστασία του δικτύου, ένα WAF εστιάζει στην κυκλοφορία HTTP/S, δηλαδή σε αιτήματα που στέλνονται σε web εφαρμογές.

Συγκεκριμένα προστατεύει επιθέσεις από:

i SQL injection
ii. Cross-site scripting (XSS)
iii. Cross-site request forgery (CSRF)
iv. File inclusion attacks
v. Bot attacks (e.g., credential stuffing, scraping)
vi. Remote Code Execution
vii. Zero day exploit detection

- Antivirus & Malware detection
  - Λογισμικό για την προστασία του server από ιούς και malware. Αναλύει τα αρχεία του server και:
    - Ανιχνεύει κακόβουλο κώδικα
    - Καθαρίζει αυτοματοποιημένα τα μολυσμένα αρχεία
    - Διατηρεί log με τις επεμβάσεις

- Intrusion Detection & Prevention System (IDS/IPS)
  - Εντοπίζει και μπλοκάρει ύποπτη δραστηριότητα στο σύστημα, όπως:
    - Μη εξουσιοδοτημένες συνδέσεις SSH
    - Κακόβουλα scripts που εκτελούνται στον server
    - Exploit attempts

- Software-based WAF & DDOS Firewall
  - Σύστημα ασφαλείας σε μορφή hardware που παρέχεται από το datacenter για επιθέσεις που αφορούν:
    - DDOS Attacks
    - Web-based επιθέσεις
    - SQL injection, XSS, CSRF, LFI, RFI
    - Deep packet inspection σε HTTP/S traffic

- Dual proxy frontend με geo-location για ανακατεύθυνση της κίνησης
  - Ειδική υποδομή πολλαπλών DNS Servers με δυνατότητα geo-routing. Το σύστημα αυτό μας επιτρέπει την αυτόματη κατανομή της κίνησης ανάλογα με το σημείο πρόσβασης του χρήστη. Σε περιπτώσεις πολύ μεγάλων επιθέσεων (High volume

DDOS), οι επιθέσεις ανακατευθύνονται αυτόματα προς διαφορετικό proxy αφήνοντας ελεύθερο το σημείο που εξυπηρετεί το ελληνικό διαδίκτυο.

- Αναβαθμίσεις και ενημερώσεις
    - Σε επίπεδο λογισμικού (OS)
        - Security updates (Αναβαθμίσεις ασφαλείας)
        - Vulnerabilities (π.χ. CVEs)
        - Kernel patches ασφαλείας
        - Ενημερώσεις policies
        - Bug fixes (Διορθώσεις σφαλμάτων)
        - Package updates (Ενημερώσεις λογισμικού)
        - Minor Version Updates
        - Kernel updates
    - Σε επίπεδο web software
        - Αναβάθμιση εκδόσεων λογισμικού που χρησιμοποιείται για την ιστοσελίδα
        - Αναβαθμίσεις του site και του συστήματος διαχείρισης

- Πρόσβαση διαχειριστών με 2FA
    - Two-Factor Authentication – έλεγχος ταυτότητας δύο παραγόντων για την ενίσχυση της ασφάλειας κατά τη σύνδεση στους λογαριασμούς των διαχειριστών για την ανανέωση του περιεχομένου του site.

- Disaster Recovery plan
    - Δυνατότητα επαναφοράς των συστημάτων για άμεση λειτουργία σε εναλλακτικό κέντρο λειτουργίας (Failover datacenter) σε περίπτωση διακοπής όπως:
        - Φυσικές καταστροφές (σεισμός, πυρκαγιά, πλημμύρα)
        - Τεχνικές αποτυχίες (βλάβη server, διακοπή ρεύματος, καταστροφή δεδομένων)
        - Ανθρώπινα λάθη (διαγραφή δεδομένων, λάθος ρυθμίσεις)
        - Κυβερνοεπιθέσεις (ransomware, hacking, DDoS)
        - Προβλήματα τρίτων παρόχων (cloud outage, ISP failure)

5. Το site υποβάλλεται περιοδικά σε penetration test. Το τελευταίο τεστ (Ιούλιος 2025), όπως ενημερωθήκαμε από τον ανάδοχο, δεν έχει αναδείξει θέματα ασφάλειας καθώς λαμβάνονται όλα τα απαραίτητα μέτρα.

6. Είναι custom made.

7. Ο ιστοχώρος του Υπουργείου Υγείας βασίζεται σε custom made λύση.

ΚΟΙΝΟΠΟΙΗΣΗ:

Βουλευτή κ. Βελόπουλο Κ.

ΕΣΩΤ. ΔΙΑΝΟΜΗ:

1. Γρ. Υπουργού
2. Γρ. Αναπλ. Υπουργού
3. Γρ. Υφυπουργού
4. Γρ. Νομικών και Κοινοβουλευτικών Θεμάτων

Ο ΥΠΟΥΡΓΟΣ

ΣΠΥΡΙΔΩΝ-ΑΔΩΝΙΣ ΓΕΩΡΓΙΑΔΗΣ