UNIUNEA NAŢIONALĂ A BAROURILOR DIN ROMÂNIA
CONSILIUL UNIUNII

H O T Ă R Â R E A nr. 80
13 iunie 2024

În conformitate cu dispozițiile art. 65 lit. a), c) d) și ș) din Legea nr. 51/1995 privind organizarea și exercitarea profesiei de avocat, cu modificările și completările ulterioare,

Având în vedere demersurile dispuse de Comisia Permanentă a Uniunii Naționale a Barourilor din România (în continuare, UNBR), ca urmare a informațiilor apărute în spațiul public cu privire la o pretinsă breșă de securitate a platformei IFEP,

Văzând Raportul Evaluare Răspuns la Incident Cibernetic și Analiză Digital Forensics și Raportul Teste de penetrare pentru Platforma IFEP înaintate de SC CYBERWALL SRL, care a fost angajată să analizeze situația;

Ținând cont de avizul favorabil al Comisiei Permanente, acordat în ședința din 12 iunie 2024

*Consiliul UNBR, întrunit în ședința din **13 iunie 2024**,*

H O T Ă R Ă Ș T E:

Art. 1 – (1) Se aprobă *Raportul Evaluare Răspuns la Incident Cibernetic și Analiză Digital Forensics* și *Raportul Teste de penetrare pentru Platforma IFEP* înaintate de SC CYBERWALL SRL.

(2) Se aprobă Recomandările propuse în cele 2 rapoarte, inclusiv în ce privește testarea periodică, la 6 luni, a platformei.

(3) Concluziile și recomandările indicate în cele 2 rapoarte și aprobate de Consiliul UNBR sunt cuprinse în anexa la prezenta hotărâre.

Art. 2 – Se aprobă continuarea relațiilor contractuale cu SC INTRACONECT SRL, în ce privește aplicația informatică Tabloul național al avocaților și a tuturor celorlalte aplicații ce au legătură cu aceasta, deținute pe platforma ifep.ro.

Art. 3 – Se mandatează Comisia Permanentă ca, împreună cu Șeful Serviciului IT și Administrativ din cadrul UNBR, să prezinte un raport privind costurile și implicațiile asupra aplicației informatice pentru ipoteza creării unei platforme similare IFEP.ro, proprietate a UNBR.

Art. 4 – Prezenta hotărâre se comunică membrilor Consiliului UNBR și Barourilor și se afișează pe website-ul www.unbr.ro .

C O N S I L I U L U.N.B.R.

1. Raport Evaluare Răspuns la Incident Cibernetic și Analiză Digital Forensics

Concluzii:

Raportul concluzionează că, în prezent, platforma este securizată conform rezultatelor recente ale testelor de penetrare, care indică faptul că o breșă similară cu cea presupusă nu ar putea avea loc în configurația actuală a platformei. Aceasta nu exclude posibilitatea unui incident anterior, ci subliniază limitările tehnice ale echipamentelor și procedurilor de logare folosite în momentul presupusului incident.

Recomandări:

1. Implementarea unui Protocol Standard de Răspuns la Incidente:

Este esențial să se dezvolte și să se implementeze un protocol standardizat de răspuns la incidente, conform cu standardul ISO / IEC 27001 : 2022 – MANAGEMENTUL SECURITĂȚII INFORMATIEI. Acesta ar trebui să includă:

• *Proceduri Clare de Notificare și Escaladare***:** Stabilirea unor canale de comunicare rapide și eficiente, cu instrucțiuni specifice privind cine, când și cum trebuie să fie notificat în caz de incident.

• *Roluri și Responsabilități:* Definirea clară a rolurilor și responsabilităților pentru fiecare membru implicat în răspunsul la incidente.

• *Planuri de Acțiune:* Elaborarea planurilor de acțiune specifice pentru diferite tipuri de incidente de securitate, asigurându-se că sunt acoperite toate scenariile posibile.

• *Revizuire și Testare Periodică:* Protocolul ar trebui revizuit și testat periodic pentru a asigura eficiența și actualizarea acestuia în conformitate cu evoluțiile tehnologice și amenințările emergente.

2. Configurarea Detaliată a Logurilor:

Pentru a asigura o monitorizare eficientă și o capacitate de audit conformă cu standardul ISO/IEC 27001:2022 - MANAGEMENTUL SECURITĂȚII INFORMATIEI, configurarea logurilor trebuie să fie exhaustivă și detaliată:

• *Detalii Complete de Logare:* Logurile ar trebui să includă informații detaliate privind traficul de rețea (intrare și ieșire), autentificările utilizatorilor, accesul la sisteme și modificările de configurare.

• *Monitorizare Continuă:* Implementarea unor soluții de monitorizare în timp real pentru a detecta și alerta comportamente neobișnuite sau suspecte.

• *Păstrarea și Protejarea Logurilor:* Asigurarea integrității logurilor prin măsuri de securitate fizică și digitală, și stabilirea unei politici de retenție a datelor care să respecte cerințele legale și operaționale.

3. Păstrarea de Imagini ale Sistemului:

Crearea și păstrarea periodică a imaginilor de sistem sunt esențiale pentru recuperarea datelor și analiza incidentelor:

• *Crearea Regulată a Imaginilor de Backup:* Stabilirea unui program de backup regulat care să includă toate componentele critice ale sistemului.

• *Stocare Securizată:* Imaginile sistemului ar trebui stocate în locații securizate, fizic și digital, și ar trebui să fie accesibile doar personalului autorizat.

• *Testarea Recuperării:* Periodic, ar trebui efectuate teste de recuperare pentru a verifica capacitatea de a restaura sistemul din imagini la un punct anterior în timp, asigurându-se că procesul de recuperare este eficient și complet.

2. Raport Teste de penetrare pentru Platforma IFEP

Concluzii și Recomandări

Vulnerabilitățile minore identificate și natura dinamică a dezvoltării platformei reamintesc necesitatea unei vigilențe continue și a îmbunătățirii procedurilor de securitate pentru a ține pasul cu amenințările emergente și evoluțiile tehnologice.

Pentru a asigura un nivel optim de securitate pentru platforma IFEP și a proteja datele sensibile, recomandăm următoarele acțiuni specifice care ar trebui luate de către administratorul platformei, Intra Connect SRL:

1. *Implementarea Mesajelor de Eroare Personalizate:* Se recomandă configurarea unor mesaje de eroare care să fie informative pentru utilizator fără a dezvălui detalii tehnice ale infrastructurii sau ale aplicației. Aceasta va reduce semnificativ riscul ca informațiile expuse să fie folosite de atacatori pentru a identifica vulnerabilități.
2. *Eliminarea Paginilor Implicite ale Serverului:* Paginile default ale serverului web ar trebui eliminate sau înlocuite, deoarece pot conține informații utile pentru potențialii atacatori. Acest pas simplu poate preveni expunerea neintenționată a detaliilor de configurare.
3. *Gestionarea Corectă a Erorilor la Nivel de Cod:* Este crucială revizuirea modului în care aplicația gestionează și raportează erorile. Eroarea trebuie tratată într-un mod care să protejeze informațiile sensibile, preferabil printr-un mecanism centralizat care să permită și ajustări ușoare pe viitor.
4. *Limitarea Detaliilor în Mesajele de Eroare:* Evitarea includerii în mesajele de eroare a traseelor de execuție, a numelor de fișiere sau a altor detalii care ar putea fi folosite de atacatori pentru a găsi puncte vulnerabile în sistem.
5. *Stabilirea unei Politici Uniforme de Tratare a Erorilor:* Adoptarea unui set standard de practici pentru gestionarea erorilor. Trebuie determinat clar ce informații sunt adecvate pentru a fi afișate utilizatorilor finali și ce informații ar trebui să fie înregistrate doar intern, pentru analiza echipei tehnice.

   Prin aplicarea acestor măsuri, Intra Connect SRL va putea îmbunătăți securitatea platformei IFEP, protejând atât integritatea sistemului, cât și confidențialitatea datelor utilizatorilor. Aceste practici reprezintă un pas esențial în consolidarea apărării împotriva potențialelor atacuri cibernetice.

În concluzie, activitățile desfășurate până în prezent au demonstrat că Intra Connect SRL menține un nivel bun de protecție a informațiilor și a infrastructurii IT. Recomandăm continuarea acestor eforturi și actualizarea periodică a protocoalelor de securitate pentru a menține aceste standarde ridicate.