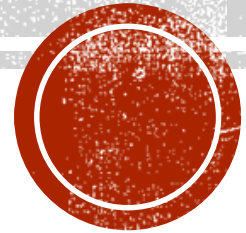
SAFETY AND BACKUP

Sugestii și recomandări legate de securitatea sistemului și a calculatoarelor în care rulează aplicația isoLEX



ROUTERUL

- Utilizarea unui router sigur de tip business (Cisco sau similar) – pentru utilizarea la distanță a isoLEX, echipamentul trebuie să dețină opțiunea „VPN Server”;
- Actualizarea la zi a firmware-ului acestuia;
- Verificarea atentă a setărilor acestuia pentru a închide orice portiță prin care un atacator poate intra în rețeaua locală;
- Firewall-ul să fie activ;
- Dezactivarea tuturor serviciilor care nu sunt absolut necesare;
- Instalarea unui server de logging extern pentru ca routerul să arhiveze pe acesta toate datele de logging (pe mai multe zile sau chiar luni) – informații care vor putea ajuta la investigații în cazul unui eveniment de penetrare a securității.

SERVERUL DE DATE

(BAZA DE DATE ISOLEX + DOCUMENTELE CLIENTULUI)

- Securizarea serverului pe care sunt păstrate datele și documentele clientului;
- Verificarea atentă a setărilor serverului pentru a închide orice portiță care ar permite un atac informatic;
- Actualizarea la zi a Windows-ului (în special a patch-urilor de securitate);
- Dezactivarea oricăror conturi Windows nefolosite, inclusiv a contului „Guest" dacă acesta este activ.
- Setarea unor parole corespunzătoare pe toate conturile de utilizator active;
- Rularea continuă a unui firewall (cel puțin Windows Firewall);
- Rularea continuă a unui antivirus performant (BitDefender sau similar) – se va excepta de la scanare baza de date isoLEX pentru a nu pierde din performanță!

BACKUP
(OBLIGATORIU)

- În ciuda măsurilor de siguranță luate, există posibilitatea ca un atacator să penetreze rețeaua locală și serverul de date. Pentru a evita pierderea datelor și a documentelor, este recomandat să se realizeze în fiecare zi o copie a datelor;
- Aplicația isoLEX ține datele in directorul "transfer", astfel că tot acest director trebuie arhivat;
- Datele se pot arhiva pe un alt server în cadrul rețelei, altul decât cel de date. Se dorește minimizarea riscului de pierdere a datelor arhivate dacă serverul de date este compromis;
- Este foarte recomandat să se organizeze arhivarea pe servere externe firmei (DropBox, Google Drive, Amazon S3 sau similar). Există și alte tipuri de aplicații care pot face astfel de operațiuni automate, în condițiile alese de către client;
- Varianta clasică și simplă constă în copierea manuală a datelor de pe server pe un HDD extern. Se recomandă în acest caz copierea datelor în directoare care să indice data când a fost realizată operațiunea pentru o identificare ulterioară mai ușoară a acestora.

UTILIZATORII RETELEI

- De cele mai multe ori virușii/malware intră în rețeaua locală prin intermediul calculatoarelor utilizatorilor care primesc dreptul de a se conecta la rețea, fie prin cablu, fie prin Wi-Fi sau VPN;
- Se recomandă limitarea drepturilor pe care aceștia le au în cadrul rețelei locale;
- Se recomandă rularea continuă a unui antivirus performant pe calculatoarele utilizatorilor;
- Folosirea unor conturi de e-mail care scanează e-mail-urile și marchează pe cele cu suspiciuni ca spam;
- Se recomandă educarea utilizatorilor în privința securității în așa fel încât aceștia să fie conștienți asupra pericolelor de securitate existente;
- Se recomandă instalarea și rularea de programe obținute doar din surse sigure, iar vizitarea site-urilor web făcându-se cu precauție;
- Cei mai mulți virușii/malware se răspândesc prin intermediul atașamentelor la e-mail-uri, prin site-uri web nesigure sau prin alte programe descărcate de pe asemenea site-uri nesigure. Recomandăm evitarea deschiderii unor atașamente din cuprinsul e-mail-urilor venite din partea unor persoane necunoscute și deschiderea cu precauție a mesajelor venite din partea persoanelor cunoscute, navigarea pe site-uri notorii și de încredere, respectiv împiedicarea download-urilor făcute de către utilizatori de pe site-uri care nu sunt de încredere sau care sunt făcute fără supraveghere specializată.

ASPECTE GENERALE

- Folosirea unor parole complexe generate de programe dedicate acestui scop;
- Păstrarea parolelor în locuri sigure, nu pe serverul de date sau pe laptopul de lucru;
- Folosirea unor programe de generare de parole aleatoriu și de administrare a acestora (LastPass sau similar). Acestea generează parole complexe și le păstrează criptate, salvându-le criptat pe servere online;
- Schimbarea regulată a parolelor;
- Folosirea dublei autentificări (parolă + telefon), în special pentru conturile esențiale (acolo unde este permisă posibilitatea);
- Rularea regulată sau chiar continuă a unui antivirus performant și a unui anti-malware (Malwarebytes sau similar).

NOTE

- *Aceste sugestii și/sau recomandări vin ca urmare a unei preocupări active a echipei isoLEX față de clienți și față de munca întregului colectiv al acestora;*
- *Aceste sugestii și/sau recomandări se aplică cel mai bine prin luarea lor împreună cu echipa de IT (rețea) a fiecărui client în parte;*
- *Aceste sugestii și/sau recomandări nu vizează în mod direct structura sau performanța sistemului isoLEX, ci au în vedere documentele generate prin intermediul acestui sistem.*