



Asigurarea Cyber Lev Business – Medie

Programul Cyber Lev Umbrella dedicat întreprinderilor mijlocii membre CCIR

1. Introducere

Asigurarea Cyber Lev Business oferă și plătește pentru serviciile unui expert cibernetic, alături de o serie de alte cheltuieli, pentru a vă ajuta să vă recuperați în urma unei amenințări cibernetice, a unui atac cibernetic sau furt cibernetic descoperite în perioada de asigurare, sau pentru o cerere de despăgubire privind răspunderea dumneavoastră în legătură cu compromiterea sistemelor informatice ale afacerii dumneavoastră, formulată împotriva dumneavoastră în perioada de asigurare, acestea constituind obiectul condițiilor și excluderilor prezentei asigurări și a plății primei de asigurare. În cadrul acestei polițe beneficiați și de o licență EDR (Endpoint Detection and Response) pentru server inclusă gratuit. Serviciile furnizate și quantumul plăților sunt stabilite în Secțiunea 4 - „Pentru ce sunteți acoperit”.

2. Cum formulați o cerere de despăgubire

În cazul în care doriți să formulați o cerere de despăgubire, vă rugăm să vă adresați inspectorilor de daună la numărul de telefon indicat în poliță.

3. Definiții

Următoarele cuvinte vor avea același înțeles indiferent unde vor apărea în prezenta poliță.

Atac cibernetic înseamnă un atac digital deliberat conceput pentru a deteriora, șterge, corupe, distruge sau perturbă sistemul informatic sau activele dumneavoastră digitale, inclusiv virusurile informatice și atacurile hackerilor.

Active digitale înseamnă programele software și toate datele electronice stocate pe / sau în sistemul dumneavoastră informatic.

Răspundere față de terți înseamnă o cerere scrisă de despăgubire, dispoziții sau alte solicitări de despăgubire formulate împotriva dvs. de către un terț pentru daunele suferite și care rezultă direct în urma obținerii accesului neautorizat la conținutul sistemului dvs. informatic de către un hacker.

Expert cibernetic înseamnă orice specialist în securitate cibernetică desemnat de către gestionarul de daune pentru a vă oferi asistența din partea unui expert în securitate cibernetică.

Furt cibernetic înseamnă orice furt al activelor dvs. digitale de către un hacker.

Amenințare cibernetică înseamnă orice amenințare din partea unui terț în scopul deteriorării, ștergerii, coruperii, distrugerii sau perturbării prin orice mijloace a sistemului dvs. informatic sau a activelor dvs. digitale.

Hacker înseamnă un terț ale cărui acțiuni care vă vizează în mod rău intenționat și obține acces neautorizat la sistemul dvs. informatic numai prin evitarea sistemelor de securitate existente destinate protejării împotriva unui astfel de acces neautorizat.

Birou înseamnă sediul biroului dvs., utilizat de dvs. pentru activități comerciale / profesionale la adresa menționată în poliță.

Sistem informatic înseamnă orice computer, hardware, software care se conectează la internetul din biroul dvs., deținut de dvs. și utilizat în scopuri comerciale / profesionale și se află localizat în biroul dvs..

Incident înseamnă o amenințare cibernetică, atac cibernetic, furt cibernetic sau o cerere de despăgubire de răspundere civilă.

Perioadă de asigurare înseamnă perioada stabilită în poliță.

Gestionar de daună înseamnă reprezentantul de despăgubiri desemnat de către Asigurătorul responsabil de soluționarea daunelor conform prezentei polițe de asigurare. Datele de contact ale gestionarului de daune pot fi regăsite în poliță.

Noi, a noastră, noi, asigurător înseamnă Societatea de Asigurare Lev Ins AD autorizată și reglementată de Comisia de Supraveghere Financiară din Bulgaria.

Dumneavoastră, a dumneavoastră înseamnă entitatea denumită Asigurat în poliță.

4. Pentru ce sunteți acoperiți:

4.1. Amenințare cibernetică sau atac cibernetic

Dacă sunteți victima unei amenințări cibernetică sau a unui atac cibernetic în perioada de asigurare, noi vă vom:

4.1.1 Oferi asistență din partea unui expert, după cum urmează:

Consultanță și asistență inițială specializată prin intermediul liniei noastre de asistență telefonică disponibilă non-stop. Ulterior, vă vom oferi consultanță suplimentară și asistență specializată, fie prin telefon, fie prin intermediul unui program software de acces la distanță, acolo unde este posibil:

- investigarea amenințării sau atacului cibernetic și identificarea naturii acesteia;
- restaurarea sistemul informatic și a activelor digitale utilizând propriile dvs. backup-uri.

Vă vom furniza până la 25 de ore de asistență de specialitate.

4.1.2 Plăți ceea ce este rezonabil și necesar:

- costul reparării sau înlocuirii sistemului dvs. informatic, în cazul în care asistența noastră specializată furnizată potrivit art. 4.1.1 nu a putut soluționa atacul cibernetic, până la limita maximă stabilită în poliță;

Pentru ca asigurătorul să vă plătească costurile rezonabile și necesare menționate anterior, în conformitate cu prezenta secțiune, fără a exclude niciuna dintre condițiile menționate mai jos în secțiunea 6. „Condiții”, este necesar ca dvs. să fi instalat sau să fi permis accesul la distanță pentru instalarea unei soluții de securitate recomandate de asigurător de tip EDR (Endpoint detection and response). (instalarea poate fi realizată de dvs. sau de un expert cibernetic desemnat de noi).

Vă vom rambursa sumele aferente până la limita maximă, astfel cum este prevăzut în total în polița dvs. pentru perioada de asigurare.

Este obligatoriu ca, în cazul în care deveniți victima unui atac al unui hacker, să anunțați de îndată poliția și gestionarul de daună.

4.2. Furt cibernetic

Dacă sunteți victima furtului cibernetic în perioada de asigurare, noi vom:

4.2.1 Oferi asistență specializată, după cum urmează:

Consultanță și asistență inițială specializată prin intermediul liniei noastre de asistență telefonică disponibilă non-stop. Ulterior, vom oferi consultanță suplimentară și asistență din partea specializată, fie prin telefon, dacă este posibil;

Vă vom oferi până la 25 de ore de asistență de specialitate.

4.2.2 Consultanță de specialitate în scopul prevenirii sau minimizării potențialelor efecte adverse ale unui eveniment cibernetic semnificativ.

4.2.3 Asistență la notificarea persoanelor vizate care ar putea fi afectate de breșa de securitate.

4.3. Restricționarea accesului

Consultanță cu privire la evitarea potențialelor restricții sau barierelor de acces la sistemele informatice ale afacerii.

Pentru ca asiguratorul să vă furnizeze asistența specializată menționată anterior, în conformitate cu prezenta secțiune, fără a exclude niciuna dintre condițiile menționate mai jos în secțiunea 6. „Condiții”, este necesar ca dvs. să fi instalat sau să fi permis accesul la distanță pentru instalarea unei soluții de securitate recomandate de asigurator de tip EDR (Endpoint detection and response). (instalarea poate fi realizată de dvs. sau de un expert cibernetic desemnat de noi).

4.4. Răspunderea față de terți

În cazul în care vi se solicită soluționarea unei cereri de despăgubire sau executarea unei hotărâri judecătorești ce decurge dintr-o cerere de răspundere civilă formulată pentru inițial împotriva dumneavoastră în perioada de asigurare, noi:

Vă vom oferi până la 25 de ore de asistență de specialitate.

4.4.1 Vă vom asista în apărarea unei cereri sau în judecată până la o sublimită de până la 20% din limita maximă prevăzută în poliță. Este obligatoriu să respectați recomandările și soluțiile gestionarului de daune.

4.5. EDR pentru server

În cadrul acestei asigurari beneficiati de o licență gratuită EDR (Endpoint Detection and Response) pentru server. EDR este un software de securitate mult mai performant decât un antivirus, oferind o securitate puternică, cu vizibilitate cuprinzătoare în toate punctele finale (endpoints) ale rețelei și permitând automatizarea sarcinilor de descoperire, prioritizare, investigare și neutralizare a amenințărilor complexe și atacurilor de tip ATP.

4.5.1 Va vom transmite licența EDR pentru server în maxim 24 ore de la data plății primei de asigurare, însoțită de instrucțiunile de instalare.

4.5.2 Va vom facilita achiziția cu preț redus și instalarea de EDR pentru maxim 250 de computere (o licență pentru varianta server fiind inclusă gratuit) în cadrul programului Cyber Lev Umbrella pus la dispoziția membrilor CCIR. Pentru a accesa aceasta facilitare vizitați pagina <https://cyberlevins.com/ro/cyber-umbrella#> și selectați varianta Medie (pentru întreprinderi mijlocii).

5. Pentru ce nu sunteți acoperit:

Noi nu acoperim:

- 5.1. pieirea fizică sau deteriorarea bunurilor corporale, altele decât deteriorarea sistemului dvs. informatic cauzată de un atac cibernetic sau al unui hacker;
- 5.2. pierderi provenind din neîndeplinirea sau îndeplinirea defectuoasă a serviciilor de către orice furnizor terț de servicii;
- 5.3. orice pierdere sau daună sau răspundere, intervenită în legătură cu obiectul meseriei, afacerii sau profesiei dvs.;
- 5.4. costurile sau recuperarea, repararea sau înlocuirea oricăror date digitale personale, inclusiv, dar fără a se limita la fotografii, videoclipuri sau piese muzicale;
- 5.5. orice cauză care precede data de început a prezentei polițe și pe care o cunoașteți sau ar fi trebuit să o cunoașteți în mod rezonabil și care ar putea duce la o cerere de despăgubire sau la o daună acoperită;
- 5.6. orice costuri care decurg din orice fel de întrerupere a activității;
- 5.7. orice costuri care decurg din amenzi și sancțiuni de reglementare, inclusiv, dar fără a se limita la încălcări GDPR, reglementări privind protecția datelor etc.
- 5.8. În niciun caz, Asigurătorul nu va putea fi ținut răspunzător pentru îndeplinirea defectuoasă sau pentru vreo întârziere în îndeplinirea obligațiilor sale decurgând din sau cauzate de, direct sau indirect, forțe care nu pot fi controlate de către acesta, inclusiv, fără a se limita la, greve, opriri de activitate, accidente, acte de război sau terorism, tulburări civile sau militare, catastrofe nucleare sau naturale sau de forță majoră și întreruperi, pierderi sau disfuncționalități ale utilităților, comunicațiilor sau serviciilor informatice (software și hardware); se înțelege faptul că Asigurătorul va depune eforturi rezonabile care sunt în acord cu practicile acceptate în industria asigurărilor pentru a se relua activitatea cât mai curând posibil în respectivele condiții.
- 5.9. orice confiscare, expropriere, naționalizare forțată, deteriorare / confiscare a bunurilor prin dispoziția unui guvern sau autoritate în funcție; confiscarea, impusă ca sancțiune sau pedeapsă pentru o infracțiune săvârșită prevăzută de Codul penal și dezactivarea sau blocarea accesului la activele dvs. digitale sau la sistemele informatice sau atribuibile oricăror erori sau omisiuni în legătură cu activitatea dvs. profesională;
- 5.10. orice confiscare, expropriere, naționalizare forțată, deteriorare / confiscare a bunurilor prin dispoziția unui guvern sau autoritate în funcție; confiscarea, impusă ca sancțiune sau pedeapsă pentru o infracțiune săvârșită prevăzută de Codul penal și dezactivarea sau blocarea accesului la activele dvs. digitale sau la sistemele informatice sau atribuibile oricăror erori sau omisiuni în legătură cu activitatea dvs. profesională;
- 5.11. orice incident survenit în afara țării în care se află localizată afacerea dumneavoastră. La cerere, este disponibilă extinderea acoperirii pentru Uniunea Europeană;
- 5.12. încălcarea oricăror drepturi de proprietate intelectuală.

6. Condiții

Condiții prelabile de răspundere pentru furnizarea serviciului și plată:

Constituie condiții prelabile ale poliței de asigurare Cyber Lev Business pentru furnizarea serviciilor și a plăților cele menționate mai jos:

- a. Să fi plătit prima menționată în poliță la data intervenirii oricărui incident;
- b. Să vă asigurați că protecția prin parolă este activată, toate actualizările de software sunt instalate în termen de 90 de zile de la data la care acestea au devenit disponibile, că toate firewall-urile sunt active, iar software-ul antivirus este actualizat și activ pe toate sistemele informatice, dispozitivele portabile utilizate, deținute sau controlate de dvs.
- c. Pentru ca asiguratorul să efectueze plata în conformitate cu secțiunile 4.1.2 și 4.3., fără a exclude oricare dintre condiții, astfel cum a fost menționat în prezenta secțiune 6. „Condiții”, este necesar ca dumneavoastră să fi instalat sau să fi permis accesul la distanță pentru instalarea unei soluții de securitate recomandate de asigurator de tip EDR (Endpoint detection and response) (instalarea poate fi efectuată de dvs. sau de un expert cibernetic desemnat de noi).
- d. Este obligatoriu să sesizați poliția și gestionarul de daune cu privire la orice incident descoperit în perioada de asigurare, într-un termen cât mai scurt. În sensul prezentei condiții:
 - i. „descoperit” înseamnă să se afle la cunoștința dvs. sau a oricărui angajat al dvs.;
 - ii. sesizarea trebuie trimisă către gestionarul de daune prin intermediul liniei telefonice de urgență indicată în poliță.
- e. Nu veți fi de acord cu nicio răspundere sau cu soluționarea vreunei cereri de despăgubire, fără consimțământul nostru prealabil scris. În cazul în care veți proceda astfel, noi vom avea posibilitatea să refuzăm sau să diminuăm orice despăgubire pe care o datorăm conform Poliței.

7. Subrogare

Asiguratorul se subrogă în drepturile asiguratului, în toate cazurile în care se asigură plata costurilor sau rambursarea acestora.

8. Fraudă

În cazul în care dumneavoastră sau oricare altă persoană, în numele dvs., vor încerca să înșele Asiguratorul prin furnizarea, în mod deliberat, de informații false sau prin formularea unei cereri de despăgubire frauduloase în temeiul prezentei polițe de asigurare Cyber Lev Business, noi vom fi avea dreptul de a transmite o notificare de reziliere a prezentei polițe de asigurare cu efect de la data furnizării informațiilor neadevărate sau a formulării cererii de despăgubire frauduloase.

Asiguratorul va avea dreptul de a reține toate plățile anterioare de prime și nu va efectua nicio plată pentru nicio cerere de despăgubire efectuată după data rezilierii. În acest caz, dumneavoastră sunteți obligat să returnați orice plăți deja efectuate în temeiul prezentei polițe de asigurare Cyber Lev Business, în legătură cu orice cerere de despăgubire efectuată după data rezilierii acesteia.

9. Cum să formulați o reclamație

În cazul în care doriți să formulați o reclamație/petiție cu privire la prezenta poliță de asigurare Cyber Lev Business, vă rugăm să luați legătura cu Asigurătorul.

Reclamațiile care nu pot fi soluționate pot fi transmise autorității de reglementare a serviciilor financiare din țara în care este localizat riscul.

Drepturile dvs. nu vor fi afectate de prezenta procedură de reclamații.

10. Notificare privind Protecția Datelor

Noi și gestionarul de daune colectăm și procesăm informații despre dvs. pentru a furniza și administra polițe de asigurare și pentru a procesa daunele.

Noi și gestionarul de daune putem înregistra apeluri telefonice pentru a ajuta la monitorizarea și îmbunătățirea serviciului oferit.

11. Legea aplicabilă

Cu excepția cazului în care este convenită în scris aplicabilitatea unei alte legi, prezenta poliță de asigurare Cyber Lev Business va fi guvernată de legea română.

12. Promisiunea noastră

În schimbul primei plătite de dumneavoastră, suntem de acord să vă asigurăm în conformitate cu termenii și condițiile prezentei Polițe de asigurare Cyber Lev Business - Medie (în cadrul programului Cyber Lev Umbrella oferit întreprinderilor mijlocii membre CCIR).

Termenii și Condițiile generale prezente au fost adoptate de Consiliul de administrație al Societății de asigurări LEV INS AD, prin intermediul Procesului-verbal din data de 19.03.2021. Societatea de asigurări Lev Ins AD este înregistrată în Registrul Comerțului bulgar sub Nr. 121130788, Licența № 98/06.01.2000. LEV INS AD este înregistrată ca asigurător autorizat de ASF în baza principiului liberei circulații a serviciilor sub numărul de înregistrare RX-2125.