



Keep your data insured,
so your business growth
is secured.

Get insured at [cyberlevins.com](https://www.cyberlevins.com)
00800 10 200 000

cyberlev^{ins}

Cybersecurity Insurance for Everyone



Asigurare Cibernetică pentru Corporații

Lumea funcționează online și digitalizarea este inevitabilă. Suntem convinși că gestionați oportunitățile afacerii dvs. cu măiestrie. Sunteți, însă, complet pregătiți să învingeți toate amenințările?

Potrivit unui studiu realizat în 2020 de Verizon, 72% dintre breșele de securitate au vizat companiile mari. Infractorii cibernetici urmăresc sursele financiare, astfel că marile corporații de succes constituie o țintă.

Ce credeți că se va întâmpla în 2022? Criminalitatea cibernetică este în plină expansiune, iar **pierderile generale cauzate de atacuri cibernetice la nivel global vor ajunge la 6 trilioane \$** (sursa: Cyber Crime Magazine). Din păcate, nu există încă nici un "vaccin" împotriva amenințărilor cibernetice.

Cu cât este mai mare și mai complexă o organizație, cu atât este mai mare pericolul. Acest lucru se datorează pur și simplu faptului că majoritatea breșelor de securitate sunt cauzate de o eroare umană. Nouă din zece incidente cibernetice sunt o consecință a acțiunii sau inacțiunii angajaților unei companii.

Implementarea soluției de asigurare potrivite în structurile companiei dvs. vă va garanta prevenirea unor astfel de erori, deoarece rețeaua dvs. va fi securizată.

La Cyber Lev Ins **tratăm compania dumneavoastră într-un mod individual și proiectăm pentru dvs. o poliță cibernetică personalizată, care să se potrivească nevoilor dumneavoastră specifice.**

Ne străduim în mod constant să creștem gradul de conștientizare a securității cibernetice și să oferim o protecție proactivă. Soluțiile noastre complete de asigurare vă garantează securitatea.

Get insured at [cyberlevins.com](https://www.cyberlevins.com)
00800 10 200 000

cyberlevins

Cybersecurity Insurance for Everyone



Care sunt cele mai frecvente amenințări cibernetice?

Phishing
orice membru al
corporației dvs.
poate primi un
e-mail cu infor-
mații dăunătoa-
re.

**Denial of
Service
(DoS)**
sistemele dvs.
pot fi blocate în
totalitate.

**Încălcarea
securității
datelor**
organizațiile care
gestionează date
cu caracter perso-
nal pot fi grav
afectate

Malware
ar putea deteri-
ora sistemele
dvs.

Toate activitățile dăunătoare menționate mai sus pot duce la o întrerupere a activității dvs., la pierderi financiare semnificative, procese, la furturi de date, precum și la multe altele. Și asta fără a menționa repercusiunile asupra reputației mărcii dvs.

Cine sunt infractorii cibernetici?

Infractorii cibernetici pot fi persoane din interior, concurenți, clienți dezamăgiți, spioni și teroriști. Desigur, aceștia pot fi doar niște terți rău intenționați care încearcă să fure din compania dvs. Cel mai îngrijorător factor este acela că orice persoană rău intenționată vă poate compromite datele sau poate deveni hacker. Nu sunt necesare aptitudini speciale sau sofisticate.

Cum vă ajutăm noi?

Efectuăm un **test de penetrare amănunțit** creat special pentru compania dvs. după ce am analizat domeniul de activitate al afacerii dvs. Deținem un instrument puternic de mitigare a riscurilor - **Centrul nostru intern de operațiuni de securitate**.

Am creat un **pachet de asigurări complet personalizat** ce integrează Servicii de securitate gestionate (MSS) specifice, în funcție de nevoile companiei dumneavoastră.

Get insured at [cyberlevins.com](https://www.cyberlevins.com)
00800 10 200 000

cyberlevins

Cybersecurity Insurance for Everyone



Suntem o companie de asigurări cu peste 20 de ani de experiență. **În prezent, suntem pionieri în crearea de soluții de securitate cibernetică.** Produsul nostru este construit în colaborare cu unii dintre cei **mai renumiți experți în securitate cibernetică din lume.** Suntem la dispoziția dvs. non-stop și vă oferim **3 niveluri de asistență.** De asemenea, **vă reasigurăm pentru acoperirea completă a pierderilor/cheltuielilor** dvs.. Partenerul nostru de reasigurare este **al treilea cel mai mare reasigurător din lume - Hannover Re.**

Beneficii, beneficii, beneficii

Test de penetrare - Vă puteți baza pe expertiza și resursele noastre pentru o verificare completă a sistemelor dvs. și detectarea vulnerabilităților acestora.

Personalizare - Vă vom oferi o soluție de asigurare cibernetică personalizată compatibilă cu aspectele specifice ale afacerii dvs.

Centru operațional de securitate intern (SOC) - Soluția de asigurare cibernetică conține Servicii de securitate gestionate de ultimă generație.

Professionalism. Vă puteți baza pe specialiștii noștri din Centrul operațional de Securitate instruiți Mashav, precum și pe Oren Elimech, un expert de anvergură în securitatea cibernetică, cu autoritate în domeniu, căruia i-au acordat încrederea organizații precum CERN și Vodafone.

Reasigurare. Hannover Re, o companie de reasigurare cu prime subscrise de peste 24 miliarde EUR, vă garantează acoperirea completă.

Call Center. Puteți contacta call-center-ul nostru non-stop și beneficiați de trei niveluri de asistență.

Consultanță și investigații. Centrul operațional de securitate din Israel are capacitatea de a efectua investigații de tip criminalistic aprofundate pentru dvs..

Răspunderea față de terți. Polița dvs. cibernetică acoperă cererile de despăgubire ale partenerilor dvs.

Get insured at [cyberlevins.com](https://www.cyberlevins.com)
00800 10 200 000

cyberlevins

Cybersecurity Insurance for Everyone



Serviciile noastre de securitate gestionate

SafeNet - Safe Net reprezintă un serviciu de control al conținutului și protecție împotriva malware-ului dedicat afacerilor. Acest serviciu web de filtrare în cloud vă permite să monitorizați, să controlați și să vă protejați afacerea, precum și pe utilizatorii dvs. împotriva amenințărilor din mediul online. Serviciul vă permite crearea unei politici granulare, astfel încât utilizatorii dvs. să controleze accesul la Internet și să blocheze accesarea domeniilor rău intenționate de către organizația dvs.

SIEM – Securitatea informațiilor și managementul evenimentelor. Acest serviciu este conceput pentru a oferi echipelor de securitate o viziune de ansamblu asupra securității datelor la nivelul întregii companii, precum și informații utile cu privire la amenințările de maximă prioritate.

EDR - Serviciul Endpoint Threat Detection and Response oferă o securitate puternică cu o viziune de ansamblu la toate punctele finale din cadrul rețelei corporative, cu un nivel superior de protecție, permițând automatizarea sarcinilor de rutină de descoperire, prioritizare, investigare și neutralizare a amenințărilor complexe și a atacurilor de tip APT.

SafeMail - Un serviciu complet de filtrare a e-mailului, amplasat în cloud, care vă protejează afacerea, angajații și clienții. Soluția de cloud privat care poate fi configurată în cloud sau în propriul dvs. centru de date este extrem de simplu de gestionat și oferă detectarea spam-ului în proporție de 99,97%, blocarea virușilor și a programelor malware, controlul autentificării, scanarea la ieșire, precum și structuri robuste de raportare.

EP - Managed Endpoint Protection, o soluție completă de protecție și remediere a malware-ului cu detectarea predictivă a amenințărilor, blocare proactivă a amenințărilor și protecție integrată end-to-end.

Rămâneți în siguranță

Liniștea dvs. reprezintă prima noastră prioritate. Protejarea completă a afacerii dvs. reprezintă succesul nostru. Prin urmare, vă respectăm și vă garantăm confidențialitatea absolută.

Get insured at [cyberlevins.com](https://www.cyberlevins.com)
00800 10 200 000

cyberlev^{ins}

Cybersecurity Insurance for Everyone



Ce acoperă asigurarea cibernetică?

- ➔ Deteriorarea activelor digitale
- ➔ Întreruperea afacerii în urma unui atac cibernetic
- ➔ Extorcare cibernetică
- ➔ Restricționarea accesului
- ➔ Răspuns la încălcarea securității datelor
- ➔ Terorism cibernetic
- ➔ Acoperirea reputației personale

Acoperire față de terți

- ➔ Cereri de despăgubire privind răspunderea pentru confidențialitate
- ➔ Cereri de despăgubire privind răspunderea media pe internet
- ➔ Cheltuieli generate de posibila încălcare a standardelor de securitate PCI
- ➔ Cheltuieli cu apărarea și sancțiunile administrative

Încă ezitați?
Completați chestionarul nostru pentru a începe procesul de obținere a soluției personalizate de asigurări cibernetică.

Get insured at [cyberlevins.com](https://www.cyberlevins.com)
00800 10 200 000

cyberlev^{ins}

Cybersecurity Insurance for Everyone