Raport privind analiza tematică referitoare la asigurarea de risc cibernetic

1. FUNDAMENTARE

Autoritatea de Supraveghere Financiară asigură protejarea şi apărarea drepturilor consumatorilor de servicii și produse de asigurare împotriva practicilor incorecte şi frauduloase, prin colectarea şi analizarea datelor şi informaţiilor despre produsele, serviciile şi furnizorii de pe piaţa asigurărilor şi reasigurărilor, efectele inovaţiei financiare pe plan european şi naţional asupra consumatorilor, despre activităţi, tendinţe, programe şi alte aspecte relevante domeniului protecţiei consumatorilor de asigurări.

Conform Geneva Association (Understanding and Addressing Global Insurance Protection Gaps, Geneva Association, aprilie 2018) ***riscul cibernetic*** este cu siguranță cea mai mare provocare cu care se confruntă economiile moderne. Acesta poate fi definit ca orice risc care decurge din utilizarea tehnologiei informațiilor și a comunicațiilor care compromite confidențialitatea, disponibilitatea sau integritatea datelor sau a serviciilor, ducând la întreruperea activităților/afacerilor, întrerupând infrastructurile critice (servicii publice, energie, transport, financiar etc) și afectând oameni și proprietăți.

Noțiunea de risc cibernetic cuprinde o multitudine de riscuri care amenință bunurile firmelor, guvernelor sau persoanelor fizice, pierderile în general incluzând active financiare sau nefinanciare, identități, divulgarea de informații sensibile și întreruperea activităților/afacerii.

La nivel mondial se estimează pierderi cauzate de riscuri cibernetice la aproape 0,5 % din PIB-ul mondial și aproape de două ori mai mult decât media anuală a pierderilor datorate dezastrelor naturale. Se estimează că aproximativ 90% din piața asigurărilor de risc cibernetic se află în SUA și doar aproximativ 5-9% în Europa. Conform EIOPA nevoia unei înțelegeri mai profunde a riscului cibernetic este provocarea principală pentru industria europeană de asigurări cibernetice. O dificultate recunoscută la nivel european este lipsa elementelor comune în limbajul de evaluare a riscurilor, care devine evidentă în diferite aspecte - de la riscurile acoperite la chestionarele de subscriere.

La nivel european, industria asigurărilor de risc cibernetic se așteaptă la o creștere progresivă a cererii de astfel de asigurări, datorată noilor reglementări, creșterea conștientizării riscului și frecvenței crescute a evenimentelor cibernetice.

Impactul financiar principal care poate fi acoperit de asigurările de risc cibernetic este rezultat în principal din furtul de active (financiare sau nefinanciare), întreruperea activităților/afacerii cu afectarea veniturilor/cifrei de afaceri, costurile pentru protecție și despăgubiri, costuri adiționale cu investigarea pierderilor, costurile de comunicare (autorități, clienți, păgubiți) și de reparare. Ca

urmare a aplicării Regulamentului GDPR costuri majore, suplimentare, pot fi generate de afectarea datelor cu caracter personal.

2. OBIECTIVUL ACTIVITĂȚII DE SUPRAVEGHERE TEMATICĂ

Din perspectiva prevenirii **riscurilor cibernetice**, ASF a luat măsuri încă din 2015, emițând *Normă privind gestionarea riscurilor operaționale generate de sistemele informatice utilizate de entitățile reglementate, autorizate/avizate şi/sau supravegheate de Autoritatea de Supraveghere Financiară*, prin care asigurătorii trebuie să aplice procese cu puncte de control foarte bine definite în vederea implementării corecte și sănătoase a tehnologiilor informatice. ASF susține implementarea noilor tehnologii în beneficiul consumatorilor, tot în 2015 emițând o normă referitoare la permiterea și susținerea vânzării de produse de asigurare în mod on-line, inclusiv permițând soluțiile biometrice. Noua normă RCA din 2017 prevede utilizarea tehnologiilor pentru avizarea și soluționarea electronică a dosarelor de daună.

Unul din obiectivele grupului InsurTech Hub, înființat la data de 26.04.2018, este atât susținerea dezvoltării tehnologice inovatoare în mod controlat și în avantajul consumatorilor cu protecția drepturilor și intereselor acestora din perspectiva identității digitale, a activelor dematerializate pe care le dețin și a datelor cu caracter personal, cât și **dezvoltarea produselor de asigurare de risc cibernetic**, aceasta fiind una din prioritățile InsurTech Task Force al EIOPA.

Supravegherea tematică a urmărit gradul de dezvoltare a acestui produs pe piața românească pentru a stabili dacă asigurații români pot beneficia de asigurări împotriva riscurilor cibernetice, inclusiv gradul de acoperire a acestor produse.

Pe piață sunt promovate produse ale unor companii din spațiul UE, prin intermediul FOS/FOE, dar acești asigurători nu intră în zona de supraveghere a ASF și nu au fost incluși în analiză.

3. PREZENTAREA PROIECTULUI

În contextul în care amenințările cibernetice se află într-un trend de creștere, atât din punct de vedere al numărului, cât şi al complexității, a fost elaborat un chestionar cu 33 de întrebări, care a fost transmis societăților de asigurare autorizate de ASF să practice asigurări generale.

Chestionarul a fost structurat în 3 părți, prima parte fiind destinată societăților de asigurare care dețin în portofoliu sau distribuie produse de asigurare de risc cibernetic, cea de a doua parte

societăților care nu au în portofoliu astfel de produse iar ultima parte cuprinde întrebări generale referitoare la acest tip de produs de asigurare.

În urma analizării de către Serviciul Supraveghere și Control Reguli de Conduită (SSCRC) din cadrul Direcției Supraveghere, Control Intermediari și Reguli de Conduită (DSCIRC) a răspunsurilor primite de la cele 16 societăți, se constată că **doar 2 societăți dețin în portofoliu produse de asigurare de risc cibernetic**, pentru persoane juridice.

- **Societatea de asigurare 1** deține în portofoliu asigurarea de risc cibernetic destinată **persoanelor juridice și instituțiilor publice**, motivul lansării acestui produs fiind cererile din piață formulate prin intermediul brokerilor de asigurare.
- **Societatea de asigurare 2** deține în portofoliu **asigurarea de răspundere profesională**, care acoperă parțial în cadrul BBB, uz fraudulos de carduri, un produs destinat **persoanelor juridice**, respectiv **unui număr de unități bancare** cu care colaborează pe canal de bancassurance sau peer to peer.

Pe lângă cele 2 societăți de asigurare, s**ocietatea de asigurare 3** comunică faptul că până în prezent nu au încheiat nicio poliță Cyber însă **sunt în discuții** cu potențiali clienți, având în vedere că **produsul este disponibil la nivel de grup**, analiza riscului și stabilirea termenilor de asigurare fiind făcută de către entitatea din grup responsabilă de produs.

<u>În general riscurile acoperite</u> prin asigurare de societăți înregistrate în România sunt:

- răspundere pentru scurgerea de informații, inclusiv pierderea datelor personale colectate;
- costuri generate de scurgerile de informații - inclusiv costuri legate de notificări și analiză criminalistică;
- răspundere pentru securitatea rețelelor - pentru sisteme compromise, inclusiv cauzate de atacuri DOS;
- răspundere media - pentru publicații digitale;
- întreruperea afacerii cauzată de un incident informatic;
- costuri de restaurare a datelor și a aplicațiilor rezultate în urma unui incident de natură să afecteze funcționarea afacerii;
- comunicare de criză pentru reducerea riscului reputațional;
- răspundere pentru plăți electronice, inclusiv amenzi și penalități;
- pierderile generate de furtul de proprietate intelectuală.

<u>Principalele excluderi</u> din asigurare sunt în general:

- Pierderi auto-provocate;
- Acte de terorism;
- Altele: Încălcarea obligațiilor profesionale; Deficiențe ale furnizorilor de servicii; Patent sau secret comercial; Hacking săvârșit de directori sau parteneri; Distrugerea bunurilor corporale; Vătămare corporală; Sechestru și confiscare; Război, terorism și riscuri nucleare; Declarații defăimătoare; Insolventa; Probleme pre-existente; Acte abuzive și penale; Conduită iresponsabilă; Cereri de despăgubire cu privire la răspunderea media formulate de angajați; Amenzi, penalități și sancțiuni; Cereri de despăgubire în afara instanțelor competente.

În cazul producerii unui eveniment asigurat, viteza de reacție a societății de asigurare poate fi de 4 ore de la sesizarea evenimentului.

La proiectarea acestor produse, se ține cont de evenimentele precedente, dimensiunea firmei, maturitatea informatică a companiei, portofoliul de clienți, prezența online și tipul de date colectate și păstrate.

Principalii factori luați în considerare la stabilirea prețului, în cazul asigurărilor de risc cibernetic sunt: tipul de industrie, dimensiunea companiei, evenimentele precedente, prezența online, procesator de date cu caracter personal senzitiv.

Înainte de încheierea unui contract de asigurare, societatea de asigurare solicită o declarație/chestionar în format fizic și electronic din partea asiguratului, cu posibilitatea punctuală de a solicita efectuarea unor teste de penetrabilitate și/sau vulnerabilitate, inspecția de risc incluzând și consultanță înaintea preluării în asigurare și o evaluare/auditare a managementului securității informației din cadrul companiei.

Principalele provocări la proiectarea acestor produse sunt: lipsa datelor statistice privind evenimentele de risc pentru proiectarea produsului precum și a celor privind evenimentele de risc pentru subscriere și stabilirea prețului, lipsa de maturitate informatică a companiilor și lipsa personalului specializat.

A doua parte a chestionarului a fost completată de majoritatea societăților de asigurare, având în vedere faptul că doar două din societățile chestionate dețin în portofoliu produse de asigurare de risc cibernetic.

Din analiza răspunsurilor primite de la cele 14 societăți de asigurare care nu dețin în portofoliu astfel de produse, s-au desprins următoarele:

- **principalele <u>motive</u> pentru care societățile de asigurare respondente nu au în portofoliu aceste produse sunt:**

- reglementările în vigoare
- impredictibilitatea expunerii la risc
- lipsa datelor statistice privind evenimentele de risc pentru proiectare produs
- lipsa datelor statistice privind evenimentele de risc pentru subscriere și stabilire preț
- lipsa cerințelor obligatorii de raportare a incidentelor cibernetice
- lipsa sistemelor de evaluare a riscurilor cibernetice
- lipsa de maturitate informatică a companiilor
- lipsa standardelor și a reglementărilor în domeniul securității IT
- lipsa cererii

- **principalele probleme/provocări cu care se confruntă societățile de asigurare și care îi împiedică să lanseze astfel de produse de asigurare**:

- nu face parte din strategia companiei
- societate mică, nu poate dezvolta produsul
- asigurarea de răspundere civilă profesională, ce acoperă inclusiv componenta de risc cibernetic, sunt în curs de lansare a unui produs specific, iar pentru asigurarea de risc cibernetic, provocările cu care se confruntă vizează adaptarea pentru piața locală a mecanismului de funcționare a acoperirii.
- lipsa datelor statistice privind evenimentele, lipsa unor informații minime de evaluare a expunerii și de stabilire a prețului riscului
- imposibilitatea calculării de acumulări ale expunerilor
- lipsa personalului de specialitate
- lipsa cererii
- lipsa predictibilității evoluției portofoliului de riscuri
- lipsa cadrului legislativ specific
- lipsă know-how, lipsă date și informații statistice necesare estimării expunerii și a daunelor maxime posibile/probabile, lipsa unui model actuarial de stabilire a primei de risc, lipsa unui apetit deosebit din partea pieței internaționale pentru preluarea în reasigurare a acestor riscuri, dificultăți în administrarea acestui tip de asigurări (necesitatea unui parteneriat cu un furnizor

de servicii IT capabil să evalueze riscurile și să intervină imediat în cazul unui eveniment cibernetic, pentru stoparea / diminuarea efectelor).

- lipsa tratatului de reasigurare și dezvoltarea produsului la nivelul grupului.

➢ În ceea ce privește **lansarea unor astfel de produse de asigurare**, 5 societăți de asigurare au în vedere lansarea acestora într-o perioadă mai mică de 1 an, 2 societăți de asigurare într-o perioadă cuprinsă între 1-2 ani, 3 societăți de asigurare în 3-4 ani, 2 societăți de asigurare își propun lansarea acestora peste 5 ani, în timp ce 2 societăți de asigurare nu intenționează să lanseze astfel de produse.

➢ **Principalele riscuri** care ar putea fi acoperite în condițiile lansării unor produse de asigurare de risc cibernetic sunt:

- Răspundere pentru scurgerea de informații, inclusiv pierderea datelor personale colectate
- Răspundere pentru securitatea rețelelor - pentru sisteme compromise, inclusiv cauzate de atacuri DOS
- Întreruperea afacerii cauzată de un incident informatic
- Costuri de restaurare a datelor și a aplicațiilor rezultate în urma unui incident de natură să afecteze funcționarea afacerii
- Comunicare de criză pentru reducerea riscului reputațional
- Acoperire a riscului de sustragere informatică a activelor financiare
- Pierderile generate de furtul de proprietate intelectuală
- Costuri cu experții, înlocuire soft, emiterea de noi carduri, șantaj cibernetic, altele.

➢ **Excluderile** din polița de asigurare ar/vor fi:

- Pierderi auto-provocate
- Accesarea site-urilor / link-urilor nesigure
- Acte de terorism
- Altele: Vătămări corporale și pagube la bunuri, răspundere contractuală, daune preexistente încheierii poliței, război, solicitări de despăgubire în legătura cu tranzacții de titluri de valoare și alte valori mobiliare, poluare, riscuri naturale, orice acțiune guvernamentală, utilizare ilegală de software/software fără licență.

➢ Majoritatea societăților de asigurare consideră necesară crearea unor competențe specifice în ingineria riscurilor cibernetice.

- În cazul persoanelor juridice, **la proiectarea acestor produse** de asigurare, societățile de asigurare ar/vor ține cont de: evenimente precedente, dimensiunea firmei, maturitatea informatică a companiei (procese, definire management securitate, poziție CISO, implementare standarde gen ISO 27000, ISO 20000 etc.), portofoliul de clienți, prezență online, tipul de date colectate și păstrate, industria în care activează, țara de origine a companiei "mamă", modalități de protejare a datelor etc.

A treia parte a chestionarului (5 întrebări) a cuprins întrebări generale referitoare la produsele de asigurare de risc cibernetic, respectiv:

- *Înființarea unui Pool de Asigurare Împotriva Riscurilor Cibernetice*

5 Societăți de asigurare consideră benefică înființarea unui Pool de Asigurare Împotriva Riscurilor Cibernetice, în timp ce celelalte societăți chestionate, nu consideră necesară o astfel de acțiune.

- ***Măsurile pe care ar trebui să le ia Guvernul pentru a preveni riscurile cibernetice*** *și pentru a susține asigurarea de risc cibernetic, necesitatea emiterii unor cerințe obligatorii de asigurare a riscului cibernetic*

- organizarea unor campanii mai ample de conștientizare asupra riscurilor cibernetice, cu invitarea asigurătorilor/experților în domeniul securității datelor și sistemelor informatice;
- respectarea Directivelor Europene;
- cerințe obligatorii de securitate IT;
- încheierea de acorduri la nivel internațional pentru schimbul de date și informații în domeniul securității cibernetice;
- investirea de resurse într-un centru specializat în combaterea infracționalității cibernetice (exista deja, în cadrul Poliției Române, Serviciul de Combatere a Criminalității Informatice și un portal efrauda.ro insuficient funcțional și popularizat);
- programe de educație și training în domeniul securității informatice;
- suport și verificare în aplicarea regulamentului GDPR la nivelul companiilor;
- elaborarea unor metodologii de informare asupra domeniilor de activitate cu riscuri ridicate urmând ca ulterior să se analizeze maniera în care asigurații potențiali au conștientizat acest

risc și au considerat să îl protejeze printr-o poliță de asigurare. Necesitatea introducerii unor cerințe minime obligatorii de asigurare a riscului cibernetic ar putea fi decisă în urma acestor analize (pentru domeniile cu impact social);

- la nivel local este necesară luarea tuturor măsurilor "specifice" unui risc, respectiv realizarea cadrului legislativ, inclusiv a celui specific asigurărilor;
- măsuri de minimizare a riscurilor privind anumite domenii industriale, unde efectele unui atac cibernetic ar putea fi catastrofice;

➢ ***Ce ar trebui să facă industria de asigurări*** *pentru a reduce impactul riscurilor cibernetice și pentru a susține asigurarea de risc cibernetic?*

- împărtășirea în cadrul unor sesiuni de comunicare/training-uri a experienței acumulate, precum și a celor mai bune practici cu intermediarii în asigurări, reasigurătorii, A.S.F., companii private;
- colaborarea cu companii de specialitate din domeniul IT, care să ofere cunoștințele aplicate privind producerea acestor riscuri specifice;
- asigurătorii locali trebuie să țină pasul cu trendul acestor asigurări pe piața internațională, să folosească know-how-ul și datele pieței internaționale, ca să-și dezvolte propriile structuri specializate pe acest tip de asigurări;
- informarea publicului asupra riscurilor și a posibilelor moduri de acoperire ale acestuia;
- realizarea de produse de asigurare destinate nevoilor reale de protecție a clienților este doar un pas care poate fi întreprins de industria de asigurări din România, însă având în vedere complexitatea riscului și mai ales a posibilelor consecințe, este necesară o colaborare strânsă a mai multor instituții ale statului român împreună cu jucătorii din piața de asigurări;
- întocmirea unei metodologii / unui ghid de reacție imediată a companiilor atunci când sunt victimele unui atac cibernetic ar putea fi o soluție ce să minimizeze impactul riscurilor cibernetice.

➢ *Care sunt **viitoarele direcții de exploatare** în ceea ce privește riscurile cibernetice și asigurarea de risc cibernetic?*

- odată cu dezvoltarea exponențială a majorității afacerilor pe baza unor soluții digitale, se estimează creșterea interesului potențialilor clienți pentru un produs de asigurare împotriva riscurilor cibernetice, pentru securizarea riscurilor remanente;

- creșterea cererii de produse de asigurare a riscului cibernetic, în special pe fondul intrării în vigoare a regulamentului GDPR și pe fondul popularizării tot mai crescute în media a riscurilor cibernetice;
- includerea acestui risc în condițiile de asigurare ale altor produse de asigurare sau lansarea de produse independente, axate doar pe riscurile cibernetice;
- produsele trebuie dezvoltate gradual, începând cu produse standard simplificate (acoperiri limitate) și continuând, pe măsura acumulării de know-how și experiență.

➢ *Care sunt **costurile și consecințele** cauzate de riscurile cibernetice?*

- întreruperea activității companiilor afectate, generarea de cheltuieli de restabilire a sistemelor informatice afectate și de recuperare a datelor pierdute ar putea fi dintre cele mai riscante consecințe ale riscurilor cibernetice;
- luând în considerare cerințele GDPR, companiile încep să investească în securitatea datelor terțelor persoane; aceste investiții și cheltuieli pot fi amenințate în cazul unor atacuri cibernetice (putând fi mult mai mare luând în considerare atacurile cibernetice asupra unor infrastructuri critice precum aeroporturi, porturi, autostrăzi etc.).

CONCLUZII

Riscurile cibernetice sunt în responsabilitatea atât a managementului instituțiilor și companiilor, cât și la nivel de angajați, asigurările cibernetice putând acoperi și riscurile profesionale generate de riscurile cibernetice.

Instituțiile/companiile au nevoie de o strategie cuprinzătoare de management al riscului cibernetic asigurând revenirea la operațiunile normale cât mai repede posibil, cu costuri cât mai reduse. Asigurările pot avea un rol esențial în a prelua/transfera riscurile la care companiile sunt expuse și pot fi un instrument care completează (și nu înlocuiește) cadrul de gestionare a riscurilor pe care fiecare organizație ar trebui să îl aibă și ar trebui să fie un element de stabilitate economică și socială, atât pentru infrastructurile critice, guvernamentale, cât și pentru cele comerciale și personale, inclusiv pentru sectorul financiar și ar trebui să fie utilizat în evaluarea solidității/sănătății financiare și a susținerii activității prin recuperarea rapidă a pierderilor și continuarea activității.

Piața de asigurări din România necesită susținere în dezvoltarea produselor de asigurare cibernetică, atât prin politici la nivel național, cât și la nivel sectorial.

InsurTech Hub constituie deja aplicarea unei astfel de politici la nivelul ASF, asigurând suport know-how și de educație în domeniu**, dar sunt necesari pași suplimentari pentru eliminarea barierelor legislative și aplicarea cerințelor europene la nivel național împotriva riscurilor cibernetice, prin sincronizare cu demersurile realizate la nivel european în domeniu, inclusiv prin educarea companiilor românești asupra riscurilor și a beneficiilor unor astfel de asigurări.**