

## **Zavarovanje kibernetских tveganj**

### **A. Zavarovane nevarnosti**

(1) V zavarovanje kibernetске zaštite so vključene vse spodaj navedene zavarovane nevarnosti:

- 1) odziv na incident,
- 2) stroški ponovne vzpostavitve sistema,
- 3) obratovalni zastoj,
- 4) kibernetско izsiljevanje,
- 5) kibernetски kriminal,
- 6) kritje škode na strojni opremi zavarovanca,
- 7) odgovornost za kršitve zaupnosti in zasebnosti,
- 8) odgovornost za omrežno varnost.

### **B. Opredelitev zavarovanih nevarnosti**

(1) Lastna škoda zavarovanca:

- 1) Odziv na incident: zavarovalnica krije vse razumne in nujne stroške, nastale zaradi kibernetskega varnostnega incidenta ali domnevnega kibernetskega varnostnega incidenta, in sicer:
  - a. stroške strokovnjaka za izvedbo preiskave in pripravo poročila o kibernetskem varnostnem incidentu;
  - b. stroške izpolnitve zahtev veljavne zakonodaje s področja varstva osebnih podatkov (npr. obveščanje informacijskega pooblaščenca ali posameznikov, na katere se nanašajo osebni podatki). Ti stroški so kriti tudi v primeru, če pride do kršitve varstva podatkov ali kraje, ne glede na to ali gre za kibernetски varnostni incident;
  - c. stroške svetovanja strokovnjaka za upravljanje in varovanje ugleda zavarovanca do konca obdobja varovanja ugleda po kršitvi varstva podatkov ter
  - d. pravne stroške zoper morebitni ukrep informacijskega pooblaščenca,

Krite so vse globe in kazni, ki jih izreče informacijski pooblaščenec zaradi kršitve varstva podatkov, če to ni v nasprotju s pravnim redom, ki velja za to zavarovalno polico in na območju pristojnosti, v katerem je treba izvesti plačilo,

- 2) Stroški ponovne vzpostavitve sistema: zavarovalnica krije vse razumne in nujne stroške za ponovno vzpostavitev podatkov in programske opreme po kibernetskem varnostnem incidentu v stanje, ki je najbližje, kolikor je mogoče, stanju, v kakršen so bili tik pred kibernetским varnostnim incidentom, v soglasju z zavarovalnico pa tudi nadgradnjo ali izboljšavo programske opreme, v obsegu, v katerem je takšen popravek smiselno potreben za preprečitev morebitnega prihodnjega kibernetskega varnostnega incidenta.

- 3) Obratovalni zastoj: zavarovalnica krije škodo zaradi izgube kosmatega dobička v obdobju prekinitev poslovanja zaradi kibernetnega varnostnega incidenta.
- 4) Kibernetko izsiljevanje: zavarovalnica krije stroške odkupnine, ki jo plača zavarovanec (če je to predhodno pisno odobrila zavarovalnica), ter vse razumne in nujne stroške za razrešitev kibernetnega izsiljevanja. Zavarovanec je dolžan na zahtevo zavarovalnice o kibernetnem izsiljevanju obvestiti pristojni državni organ.
- 5) Kibernetni kriminal: zavarovalnica povrne zavarovancu vsa nezakonito odvzeta denarna sredstva zaradi dejanj kibernetnega kriminala.
- 6) Kritje škode na računalniški strojni opremi zavarovanca: zavarovalnica povrne zavarovancu stroške za odpravo škode na strojni opremi zavarovanca nastale zaradi kibernetnega varnostnega incidenta, ne povrne pa kakršneoli izboljšave strojne opreme. Zavarovalna vrednost strojne opreme je nabavna vrednost novih stvari, zmanjšana za vrednosti, izgubljene zaradi obrabe, starosti in ekonomske ter tehnične zastarelosti (amortizirana vrednost).

## (2) Odškodninski zahtevki tretjih oseb

- 1) Odgovornost za kršitve zaupnosti in zasebnosti: zavarovalnica povrne vse stroške, nastale zaradi odškodninskih zahtevkov tretjih oseb ali zaposlenih, zaradi kraje ali kršitve varstva podatkov v zvezi z zaupnimi podatki ali osebnimi podatki ali zaradi kršitve veljavne zakonodaje o varstvu osebnih podatkov, in pravne stroške, ob predhodnem soglasju zavarovalnice.
- 2) Odgovornost za omrežno varnost: zavarovalnica povrne vse stroške, nastale zaradi odškodninskih zahtevkov tretjih oseb, zaradi kibernetnega varnostnega incidenta, kraje podatkov ali napada za nedosegljivost/ohromitev storitve (DOS napad) na računalniške sisteme tretje osebe, ki je povzročen neposredno zaradi zlonamernega dejanja ali zlonamernih programov na informacijski sistemih zavarovanca, ki jih ni uspelo ustaviti, in pravne stroške, ob predhodnem soglasju zavarovalnice.

## **C. Zavarovalni primer**

- (1) Zavarovalni primer je kršitev varstva podatkov, kibernetni varnostni incident, odškodninski zahtevek tretje osebe, kibernetko izsiljevanje ali kibernetni kriminal.
- (2) Za lastno škodo (opredeljena v točkah 1) do 6) v (1) odstavku poglavja »Opredelitev zavarovanih nevarnosti« te dokumentacije) velja, da je kritje podano, če je zavarovalni primer odkrit med veljavnostjo police.
- (3) Za kritje odškodninskih zahtevkov tretjih oseb (opredeljeno v točkah 1) in 2) v (2) odstavku poglavja »Opredelitev zavarovanih nevarnosti« te dokumentacije) velja, da mora biti odškodninski zahtevek tretje osebe proti zavarovancu ali zavarovalnici vložen med veljavnostjo police oziroma v roku 30 dni po izteku veljavnosti police ali prekinitve police s strani zavarovalnice (samodejno podaljšano obdobje prijave zavarovalnega zahtevka). Zahtevki vloženi v podaljšanem obdobju prijave zavarovalnega zahtevka morajo biti odkriti pred potekom veljavnosti zavarovalne police.
- (4) Zavarovanec lahko obdobje prijave zavarovalnega primera iz prejšnjega odstavka tega sklopa podaljša za največ pet let (opsijsko podaljšano obdobje prijave zavarovalnega zahtevka) s plačilom dodatne premije v roku 30 dni po izteku veljavnosti police ali prekinitve police s strani zavarovalnice. Dogovorjenega opsijskega podaljšanega obdobja prijave zavarovalnega zahtevka ni mogoče prekiniti. Če prekinitev ali neobnovitev zavarovanja uveljavlja zavarovalnica zaradi neplačila

premije, zavarovalec ali zavarovanec izgubi možnost do opsijskega podaljšanja obdobja prijave zavarovalnega zahtevka. Doplačilo za opsijsko podaljšano obdobje prijave zavarovalnega zahtevka se dogovori ob sklenitvi zavarovanja. Prvih 30 dni opsijskega podaljšane obdobja poročanja bo potekalo hkrati s samodejno podaljšanim obdobjem prijave zavarovalnega zahtevka.

Zahtevki vloženi v podaljšanem obdobju prijave zavarovalnega zahtevka morajo biti odkriti pred potekom veljavnosti zavarovalne police.

(5) Zavarovalni primeri, ki izhajajo iz istega vzroka, se obravnavajo kot en zavarovalni primer, odkrit ob prvem dogodku iz niza. To pravilo se upošteva ob določanju soudeležbe in zavarovalne vsote.

## **Č. Razlaga izrazov**

Vsi izrazi v tej Zavarovalno tehnični dokumentaciji, so opredeljeni izrazi in so opisani v tem poglavju.

- Časovna soudeležba - obdobje, navedeno na polici. Teči začne z odkritjem kibernetnega varnostnega incidenta, ki neposredno povzročil, da so informacijski sistemi zavarovanca delno ali v celoti nedosegljivi.
- Človeška napaka - vsaka napaka v delovanju informacijske in/ali komunikacijske tehnologije, ki je posledica ravnanja zaposlenih (npr. izbira programske opreme, napaka pri namestitvi ali vsaka neprimerna uporaba).
- Elektronski mediji -vsaka informacijsko-tehnološka naprava (npr. zunanji disk, CD, DVD, magnetni trak ali disk, USB-pomnilnik), ki se uporablja za snemanje in hranjenje podatkov.
- Informacijski sistemi - informacijsko-tehnološki in komunikacijski sistemi (npr. strojna oprema, infrastruktura, programska oprema ali elektronski mediji), ki se uporabljajo za ustvarjanje, dostop, obdelavo, zaščito, spremljanje, shranjevanje, ponovno iskanje, prikaz ali prenos podatkov.
- Informacijsko omrežje - eden ali več informacijskih sistemov, ki so medsebojno povezani ali si lahko kako drugače izmenjujejo podatke.
- Infrastruktura - vsakršna komunikacijska oprema, klimatske naprave, napeljava za neprekinjeno napajanje z elektriko, samostojni generatorji, frekvenčni pretvorniki, transformatorji in druge naprave, ki se uporabljajo za vzdrževanje delovanja elektronskih naprav, ki podpirajo informacijske sisteme in podatke.
- Informacijski pooblaščenec - pristojni državni organi s področja varstva osebnih podatkov.
- Informacijski sistemi zavarovanca - informacijski sistemi pod nadzorom zavarovanca, ki jih ima zavarovanec v lasti, zakupu, ima zanje licenco ali jih najema.
- Internetne storitve-storitve, ki omogočajo uporabo interneta, kot so (1) ponudniki internetnih storitev, ki zagotavljajo storitve, strojno in tehnično opremo za dostop in uporabo interneta; (2) ponudniki storitev domene; (3) drugi ponudniki internetnih storitev in storitev zunanjega omrežja, odgovorni za izmenjavo na internetu, ponudniki internetnega omrežja prve ravni; ter (4) operaterji kabelskega, satelitskega in radijskega komunikacijskega omrežja.
- Intranet - zasebno ali zaprto podatkovno omrežje.

- IT storitev - storitev obdelave, vzdrževalna, delovanja, zaščite ali hranjenja strojne opreme zavarovanja, infrastrukture, elektronskih podatkov ali računalniške programske opreme ter IT storitve v oblaku (npr. IaaS, PaaS and SaaS), ki pa ne vključuje zunanjih telekomunikacijskih storitev.
- Izguba kosmatega dobička - zavarovanje krije izgubo kosmatega dobička (tj. seštevek fiksnih stroškov in dobička iz poslovanja (EBIT), korigiran za spremembo zalog končane in nedokončane proizvodnje v poslovnem letu pred škodnim dogodkom), ter upravičeno nastalih dodatnih stroškov za preprečevanje ali zmanjšanje izpada prihodkov stroškov, ki nastajajo zaradi ukrepov preprečevanja ali zmanjšanja izpada prihodkov in katerih obseg ne sme preseči t. i. ekonomskega limita, ki predstavlja izgubo kosmatega dobička, če ti ukrepi ne bi bili izvedeni) v času jamčevalne dobe. Kalkulacijo škode predstavlja razlika med dokazljivimi, predvidenimi prihodki in dejanskimi prihodki v času jamčevalne dobe, pomnožena s stopnjo kosmatega dobička (tj. razmerje med kosmatim dobičkom in prihodki v poslovnem letu pred škodnim dogodkom).
- Kibernetski kriminal - nepooblaščen elektronski prenos zavarovančevih denarnih sredstev z njegovega bančnega računa, ki ga stori tretja oseba.
- Kibernetski varnostni incident - zlonamerno dejanje, zlonamerni programi, človeška napaka, napad za nedosegljivost/ohromitev storitve (DOS napad) ali kraja podatkov oziroma nepooblaščen pridobitev podatkov, ki vplivajo na zaupnost, celovitost in razpoložljivost informacijskega sistema zavarovanca ali ponudnika storitev, ali utemeljen sum o teh dejanjih.
- Kibernetsko izsiljevanje - resna grožnja tretje osebe, da bo storila dejanje, ki predstavlja zavarovalni primer, če ne bo plačana odkupnina, in zahteva tretje osebe za plačilo odkupnine, da bi se končal kibernetski varnostni incident.
- Kraja - zlonamerno dejanje nezakonitega kopiranja ali pridobivanja, npr. zaupnih podatkov, podatkov ali osebnih podatkov iz informacijskih sistemov.
- Kršitev varstva podatkov - kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščen razkritje ali dostop do osebnih podatkov ali zaupnih podatkov, poslanih, shranjenih ali kako drugače obdelanih na informacijskih sistemih zavarovanca ali informacijskih sistemih ponudnika storitev.
- Napad za nedosegljivost/ohromitev storitve (DOS napad) - zlonamerno dejanje, ki s preobremenitvijo informacijskih sistemov ali informacijskega omrežja zavarovanca z neprekinjenim tokom vhodnih zahtev (vključno z razpršenim napadom za nedosegljivost/ohromitev storitve - DOS napad) povzroči popolno ali delno prikrajšanost, motnjo v delovanju in/ali nedostopnost informacijskih sistemov in informacijskega omrežja.
- Obdobje prekinitve delovanja - nastopi po časovni soudeležbi, v katerem so informacijski sistemi zavarovanca v celoti ali delno nedelujoči, in se zaključi, ko so informacijski sistemi zavarovanca znova v celoti dosegljivi, ali po izčrpanju zavarovalnega kritja.
- Obdobje varovanja ugleda - obdobje, v katerem strokovnjak skrbi za ugled zavarovanca. Obdobje varovanja ugleda je časovno omejeno na 90 (z besedo devetdeset) dni.
- Odškodninski zahtevek tretje osebe - kakršen koli sodni, izvršilni ali arbitražni postopek, sprožen proti zavarovancu ali zavarovalnici, na podlagi katerega bi bil lahko zavarovanec spoznan za odgovornega za nastalo škodo ali kakršno koli pisno obvestilo naročnika storitve zavarovancu ali

zavarovalnici o tem, da meni, da je zaradi strokovne napake pri opravljanju registrirane dejavnosti zavarovanec odgovoren za nastalo škodo.

- Podatki - digitalna informacija, ne glede na namen, na kakršnega se uporablja ali prikazuje (besedilo, številke, podobe, video posnetki ali programska oprema), ki se hrani zunaj bralno-pisalnega pomnilnika(RAM).
- Ponudnik storitev - tretja oseba, ki za zavarovanca opravlja IT storitve v skladu s pisno sklenjeno pogodbo.
- Ponudnik storitev odziva na incident - pravna oseba, pooblaščen za zagotavljanje storitve odziva na incident, imenovana s strani ali s soglasjem zavarovalnice.
- Pravni stroški - vsi stroški plačil za strokovnjake, raziskave, prisotnost na sodišču ali postopke, ki so potrebni za civilno, gospodarsko ali kazensko pravno zastopanje zavarovanca. Splošni stroški zavarovanca (npr. plač in režijskih stroškov) niso predmet pravnih stroškov,
- Programska oprema - vsak digitalni standard, prilagojen ali individualno razvit program ali aplikacija, ki jo ima ali uporablja informacijski sistem, kateri je sestavljen iz navodil, ki so naložena na mediju, v napravi, zmožni obdelave podatkov, in ki povzročijo izvajanje ali doseganje neke funkcije, naloge ali rezultata.
- Soudležba - delež škode po zavarovalnem primeru, ki ga zavarovalnica ne krije in bremeni zavarovanca, bodisi v znesku bodisi v določenem časovnem obdobju.
- Strojna oprema - fizične komponente informacijskih sistemov, ki se uporabljajo za shranjevanje, prenos, obdelavo, branje, prilagajanje ali nadzor podatkov, vključno z elektronskimi mediji.
- Strokovnjak - fizična ali pravna oseba, imenovana s strani ali s soglasjem zavarovalnice, in/ali ponudnik storitve odziva na incident (npr. informacijski varnostni strokovnjak, forenzični računovodja, odvetnik ali svetovalec za odnose z javnostmi).
- Terorizem - dejanje, storjeno iz političnih, verskih, ideoloških ali podobnih namenov ali zaradi vplivanja na vladajoče organe ali ustrahovanja javnosti.
- Vodilni delavci - vsi pretekli, sedanji ali bodoči vodilni zaposleni (direktorji, odgovorne osebe, višji managerji in drugi zaposleni) z visoko odgovornostjo in avtoriteto odločanja v imenu zavarovanca.
- Zaposleni - vse osebe, ki delajo za zavarovanca ali izvajajo storitve v skladu s pogodbo o zaposlitvi, vključno z zunanjimi sodelavci, ki jih je zavarovanec najel za opravljanje storitev ter ki delo opravljajo znotraj organizacijske strukture in pod nadzorom zavarovanca. Vodilni delavci zavarovanca se ne štejejo za zaposlene.
- Zaupni podatki - vsaka oblika občutljivih podatkov, ki ni dostopna javnosti, ne glede na to, ali je opredeljena kot »zaupna« ali ne.
- Zavarovanec - zavarovanec, kot [e naveden na polici, in/ali njegovi vodilni delavci.
- Zavarovalna vsota - najvišji znesek, do katerega jamči zavarovalnica in je naveden na zavarovalni polici.
- Zlonamerni program - vsaka nedovoljena ali nezakonita programska oprema ali koda (npr. virusi, vohunsko programje, računalniški črvi, trojanski konji, izsiljevalsko programje,

beležniki tipkanja (ki beležijo zaporedje uporabljenih znakov na tipkovnici), samodejni izbirniki (programi za klicanje) in goljufiva varnostna programska oprema), ustvarjena za povzročanje škode ali dostopanje ali motenje Informacijskih sistemov ali informacijskih omrežij.

#### **D. Nezavarovane nevarnosti**

(1) Zavarovalno kritje ni podano za zahteve, ki neposredno ali posredno izvirajo iz naslednjega:

- 1) zlonamerno ali nepošteno ravnanje zavarovanca;
- 2) odškodninski zahtevki tretjih oseb, vloženi v Združenih državah Amerike ali Kanadi ali na ozemljih Združenih držav Amerike (Portoriko, Ameriška Samoa, Severni Marijanski otoki, Guam in Deviški otoki Združenih držav):
- 3) odpoved, prekinitev, poslabšanje ali izpad infrastrukture tretje osebe, ki ni pod nadzorom zavarovanca, in sicer za telekomunikacijske, satelitske in kabelske storitve, storitve interneta, elektrike, plina ali vode;
- 4) terorizem;
- 5) stavka, izgred ali javni nered;
- 6) vojna, vključno z vsakim stanjem sovražnega konflikta (napovedanim ali nenapovedanim), ki se izvaja z orožjem in/ali nasiljem, da bi se razrešil spor med dvema ali več državami ali narodi, vključno z vojnimi dejanji (npr. vpadi, vstaje, revolucije ali vojaški udari);
- 7) odvajanje, razpršitev, pronicanje, pretok, sproščanje ali uhajanje nevarnih snovi ter kontaminantov;
- 8) zaseg, zaplenba, zahteva, uničenje ali poškodovanje informacijskih sistemov zavarovanca zaradi ukrepa, zahteve ali ukaza vladnega, nadzornega, sodnega ali drugega organa, ki deluje v skladu z zakonskimi pooblastili;
- 9) uporaba nelegalne ali programske opreme brez licence;
- 10) napaka, okvara, pomanjkljivost ali opustitev v obliki, načrtu ali specifikaciji informacijskih sistemov zavarovanca, zaradi česar niso primerni za predviden namen uporabe;
- 11) škoda na stvarnem premoženju in kakršna koli iz tega izvirajoča posledična škoda, vključno z izgubo uporabe stvarnega premoženja. Podatki, strojna oprema in programska oprema se za ta primer ne obravnavajo kot stvarno premoženje;
- 12) če je zavarovalnici prepovedano plačevanje. zavarovanje in/ali nudenje kakršne koli koristi zavarovancu zaradi pravnih ali regulatornih sankcij, prepovedi ali omejitev;
- 13) če zavarovanec ni ustrezno sodeloval z informacijskim pooblaščencom ali je preprečil izvršitev ukaza, navodila ali usmeritve, ki je neposredno ali posredno izhajal/a iz zavarovalnega primera;
- 14) globe, kaznovalne odškodnine ali kazni (razen v primeru iz 1) točke (1) odstavka poglavja B-Opredelitev zavarovanih nevarnosti te dokumentacije);
- 15) izgube pri naložbah ali trgovanju, vključno z nezmožnostjo prodaje, prenosa ali drugega razpolaganja z vrednostnimi papirji;
- 16) načrtovani izpadi, zastoji ali načrtno obdobje neobratovanja informacijskih sistemov ali delov

informacijskih sistemov;

17) če zavarovanec ali ponudnik storitev ne plača ali ne obnovi ali ne podaljša najema, pogodbe ali licence ali ne naroči blaga ali storitev;

18) škoda na osebah zaradi telesne poškodbe, prizadetega zdravja, invalidnosti ali smrti;

19) kraja, kršitev ali razkritje intelektualne lastnine (kot so patenti, blagovne znamke, avtorske pravice). Ta izključitev ne velja za 1) točko (2) odstavka poglavja B- Opredelitev zavarovanih nevarnosti (Odgovornost za kršitve zaupnosti in zasebnosti) te dokumentacije, pri čemer je kraja, kršitev ali razkritje patentov vedno izključena iz kritja;

20) odškodninski zahtevki tretjih oseb s strani ali v imenu: pravne osebe, ki ima učinkovit nadzor nad zavarovancem; podrejene družbe zavarovanca; katere koli pravne osebe, nad katero ima nadzor zavarovanec ali zavarovančeva podrejena družba: katere koli osebe, ki ima večinski delež v podjetju zavarovanca; pravne osebe, v kateri ima zavarovanec finančni interes ali partnerstvo ali skupni podvig, v katerega je vpleten zavarovanec;

21) pogodbeni odgovornost ali odgovornost po posebnem dogovoru, ki presega obseg obveznosti, ki izvira iz pravnih predpisov o odgovornosti;

22) nenatančen, neustrezen ali nepopoln opis blaga ali storitev ali njihovih cen;

23) ex gratis ali diskrecijske poravnave ali izrazi dobre volje, namenjeni tretjim osebam, vključno s popusti, dobropisi za storitve, rabati, znižanji cen, kuponi, nagradami ali drugimi pogodbenimi ali ne pogodbenimi spodbudami in promocijami;

24) objava na spletni strani, kjer je mogoče objaviti vsebino brez registracije, ali spletni strani, kjer vsebine ne nadzira zavarovanec neposredno;

25) dogodki s katerim je bil vodilni delavec seznanjen, ali bi moral biti z njimi seznanjen na podlagi utemeljene preiskave pred začetkom veljavnosti police.