

Številka: 0910-3/2022-42

Datum: 21. februar 2023

Finančni sektor med najpogostejšimi tarčami hakerjev

Zavarovalnice so priljubljene tarče kibernetских napadalcev, saj delajo z občutljivimi podatki. Z naraščajočimi geopolitičnimi tveganji se je v zadnjem obdobju raven globalnih kibernetских tveganj še povečala. Po podatkih spletne strani Hackmageddon.com se je v globalnem smislu v letu 2022, v primerjavi s predhodnim letom, število kibernetских incidentov povečalo za 21 %. Finančni sektor (skupaj z zavarovalnicami) je peta najbolj pogosta tarča napadov, takoj za proizvodnimi dejavnostmi, zdravstvenem sektorjem, javno administracijo in prebivalstvom, kažejo statistike.

Zakaj so zavarovalnice tako pogosta tarča?

Zavarovalnice zbirajo ogromno podatkov o posameznikih, ki zajemajo njihovo zdravje, premoženje, vozila in celo hišne ljubljence. Zato se mora zavarovalniški sektor po najboljših močeh potruditi za zaščito podatkov strank. Da bi zagotovile varnost osebnih podatkov zavarovancev, mora zavarovalniški sektor upoštevati stroge zahteve glede njihovega varstva. Te zahteve zavezujejo podjetja k izvajanju najboljših praks kibernetiske varnosti; v nasprotnem primeru se lahko zavarovalnice soočijo z globami.

Kibernetски napadi v zavarovalniškem sektorju pogosto ne ciljajo na ranljivosti sistema, ampak namesto tega na nepredvidne zaposlene in zunanje sodelavce (npr. zavarovalne posrednike). Statistični podatki kibernetских napadov v finančnem sektorju kažejo, da so najpogostejši tipi napadov prevare, napadi z lažnim predstavljanjem (phishing attacks) in napadi s pretvezo (pretexting attacks).

V zaščito podatkov strank je med drugim usmerjena Splošna uredba o varstvu podatkov (GDPR). Dodatno pa morajo zavarovalnice vzpostaviti mehanizme za ravnanje z osebnimi podatki zavarovancev, s čimer zmanjšajo izpostavljenost kibernetским in drugim tveganjem povezanim z osebnimi podatki. Ti mehanizmi vključujejo:

1. imenovanje pooblaščenca za osebne podatke - odgovoren za nadzor ukrepov varstva osebnih podatkov,
2. spremljanje aktivnosti zaposlenih, ki imajo dostop do osebnih podatkov,
3. šifriranje občutljivih podatkov - tako med prenosom, kot med hranjenjem,
4. upravljanje z uporabniškimi profili z dostopom do posebej občutljivih podatkov - redno spremljanje aktivnosti teh profilov, vzpostavitev dostopanja z enkratnimi gesli,
5. zmanjšanje tveganja pri dostopanju do podatkov s strani zunanjih sodelavcev - omejitev dostopa samo do najnujnejših podatkov za opravljanje nalog teh sodelavcev, pregled aplikacij, ki jih sodelavci uporabljajo, uporaba orodij za kibernetisko varnost.
6. sprejetje načrta za odziv v primeru kibernetiskega napada.

Zaupanje v zavarovalništvo torej zavarovalnice v pomembni meri ustvarjajo s tem, da skrbno ravnaajo s podatki in zagotavljajo najvišjo raven njihove zaščite. H krepitvi zaupanja pa prispeva tudi AZN kot regulator z zakonsko določenimi nalogami in pooblastili. Med dobre prakse med drugim uvrščamo:

- Redno (kvartalno) spremljanje ravni kibernetских tveganj za slovenski zavarovalniški trg s strani regulatorja. Na AZN smo v okviru metodologije za spremljanje tveganj trga določili nabor kazalcev s katerimi ocenjujemo reven tveganj in (med-kvartalne) spremembe v ravni kibernetских tveganj.

- Medsebojno sodelovanje in izmenjavo informacij z drugimi sektorskimi finančnimi nadzorniki (Banka Slovenije, Agencija za trg vrednostnih papirjev in AZN) pri nadzoru nad kibernetскими tveganji - v okviru delovanja skupine Odbora za finančno stabilnost za kibernetска tveganja. Poleg boljše obravnave kibernetских tveganj za relevanten del trga s strani nadzornika, je naloga delovne skupine priprava enotnega sistema za obravnavo kibernetских tveganj za celotni finančni sistem v Sloveniji, kar bo dodatno okrepilo kakovost spremljanja teh tveganj, povečalo možnost za hitro odzivanje ter varnost za zavarovalniški trg.

Pojasnilo: vsebino smo pripravili na podlagi strokovnega prispevka, ki ga je imel direktor AZN mag. Gorazd Čibej na poslovni konferenci Gospodarsko povezani, regijsko močnejši, ki je 21. februarja potekala v organizaciji Inštituta za strateške rešitve in partnerjev v Podgorici v Črni gori.

Agencija za zavarovalni nadzor

KONTAKTI:

telefon: + 386 (1) 2528 600

telefaks: + 386 (1) 2528 630

e-mail: agencija@a-zn.si

www: <http://www.a-zn.si/>

Twitter: [@AZN_PR](https://twitter.com/AZN_PR)

O Agenciji za zavarovalni nadzor

Agencija je bila ustanovljena junija 2000 na podlagi Zakona o zavarovalništvu. Cilj državne nadzorne institucije na področju zavarovalništva je zmanjševanje in odpravljanje nepravilnosti v zavarovanju, varovanje interesov zavarovalcev in omogočanje delovanja zavarovalnega gospodarstva ter pozitivnega vplivanja le-tega na celotno gospodarstvo. Agencija je pri svojem delu neodvisna in samostojna.



Naložbo sofinancirata Republika Slovenija in Evropska unija iz Evropskega socialnega sklada