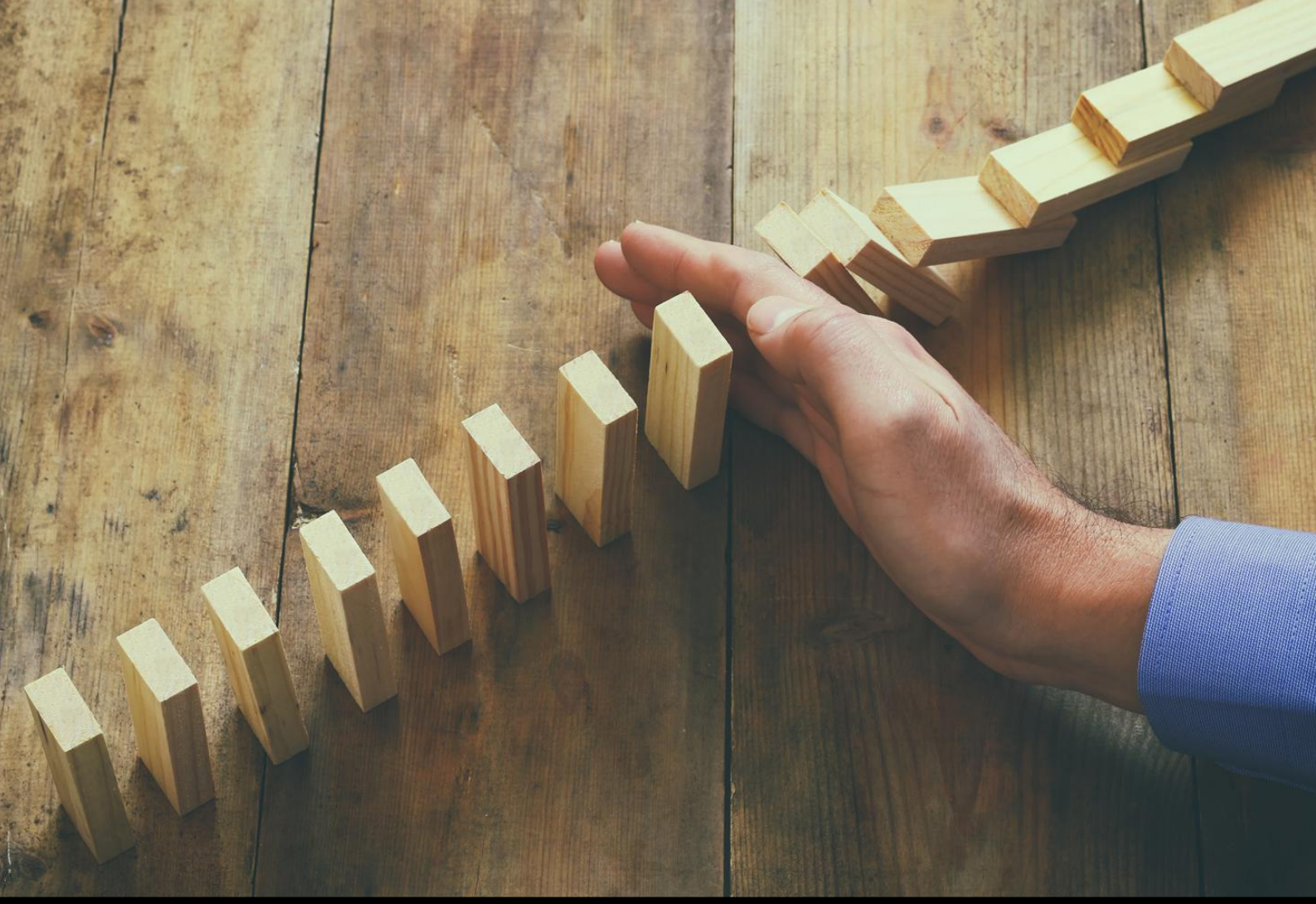


NOVA REALNOST – KIBERNETSKA TVEGANJA

Kratka predstavitev kibernetskih zavarovanj

LIBRA PREMIA

»Risk comes from not knowing what you're doing.«

december 2020

ZA UVOD - MITI IN RESNICE O KIBERNETSKI VARNOSTI IN ZAVAROVANJIH

Ne glede na to, koliko podjetje investira v svojo IT varnost, ne more biti 100 % varno. Namen zavarovanja je ravno v tem, da zagotavlja finančno zaščiti v najneugodnejših scenarijih, ki lahko močno prizadanejo podjetje.

Drži, da investicije v IT varnost zmanjšujejo ranljivost podjetja glede kibernetskih napadov. Vendar nekaj tveganja vedno ostaja. Ob tem je potrebno upoštevati, da se tudi kibernetski napadalci ves čas izpopolnjujejo in iščejo nove ranljivosti pri podjetjih ter svoje priložnosti za nove napade.

K vsemu skupaj je potrebno dodati še človeške napake, ki zelo

Mit o kibernetskem zavarovanju

» Ne potrebujemo kibernetskega zavarovanja, saj investiramo v IT varnost… «

Ranljivost in tveganje sta dve različni stvari.

Mit o kibernetskem zavarovanju

» Kibernetski napadi resno prizadenejo le velika podjetja in državne organizacije. Mi smo premajhni… «

Kibernetski napadalci napadajo najbolj ranljive.

Multinacionalke in velika podjetja veliko investirajo v svojo IT varnost, zato je vdor v njihove sisteme praviloma zahtevnejši.

Manjša podjetja, ki jim pogosto primanjkuje sredstev za IT varnost, so zato lažja tarča za kibernetske napade.

Zaupanje izvajanja IT opravil zunanjim izvajalcem lahko spremeni izpostavljenost podjetja kibernetskim tveganjem, nikakor pa jih ne izniči.

Iz naslova kibernetskih tveganj lahko izhajajo tako odgovornostne škode kot tudi škode na lastnem premoženju. Z vidika odgovornostnih škod je podjetje, ki je svoja IT opravila zaupalo zunanjim izvajalcem, v skladu z zakonom še vedno odgovorno za škode, ki so nastale tretjim osebam ali poslovnim partnerjem. V povezavi s škodami na premoženju podjetja pa je zelo tvegano predpostavljati, da bo možno vso nastalo škodo izterjati od izvajalca, kateremu je podjetje zaupalo izvajanje svojih IT opravil.

Mit o kibernetskem zavarovanju

» Celoten IT smo zaupali zunanjim izvajalcem, zato nimamo kibernetskega tveganja…«

Tveganje ostaja tudi če IT zaupamo zunanjim izvajalcem.

MANIFESTACIJA ŠKOD IZ NASLOVA KIBERNETSKIH TVEGANJ

Poslovanje večine podjetij temelji na takšni ali drugačni računalniški podpori. Programi ali sistemi lahko poganjajo in nadzorujejo celotno avtomatizirano proizvodnjo, lahko pa računalniški sistemi služijo za hranjenje in obdelavo velike količine (tudi zelo občutljivih) podatkov o strankah.

Škode, povezane s kibernetskimi tveganji, se lahko v podjetju manifestirajo v različnih oblikah, in sicer lahko podjetje utrpi škodo na svojem premoženju (tako imenovana lastna škoda) ali pa se sooči z odgovornostnimi odškodninskimi zahtevki tretjih oseb ali poslovnih partnerjev.

Vsako podjetje ali organizacija, ki pri svojem delovanju uporablja računalniški sistem, je izpostavljeno kibernetskim tveganjem.

HOTEL

Na osnovi hekerskega vdora v računalniški sistem hotelske verige so storilci pridobili občutljive podatke o gostih hotelov (kot na primer imena in priimke gostov, podatke iz njihovih osebnih dokumentov, podatke o njihovih plačilnih karticah ipd.). Preden je hotel ugotovil, da je prišlo do vdora v njegov računalniški sistem, so bile nekatere plačilne kartice že uporabljene za spletne nakupe.

Škoda, ki nastane podjetju:	Stroški ugotavljanja izvora vdora virusa (IT forenzika), stroški obveščanja strank, stroški spremljanja dogajanja z računi strank, katerih podatki o plačilnih karticah so bili ukradeni, izguba ugleda hotelske verige, neposredno odškodninski zahtevki gostov, katerih podatki so bili ukradeni ali kontaminirani, kazni ipd.

Podobni primeri so možni oziroma pogosti tudi drugje v turizmu in gostinstvu, v zdravstvu, finančnem sektorju, storitveni dejavnosti, spletnih trgovinah ipd. – **torej povsod tam, kjer so velike količine (občutljivih / osebnih) podatkov**…

Zelo pogosto so škode iz naslova kibernetskih tveganj povezane s preprostimi človeškimi napakami. Velika verjetnost je, da bodo zaposleni pritisnili na nekaj, na kar ne bi smeli (npr. elektronsko sporočilo, ki vsebuje zlonamerno kodo ipd.).

PROIZVODNO PODJETJE

Virus, ki je prišel v podjetje preko elektronske pošte, ki jo je odprl eden od »radovednih« uslužbencev podjetja, povzroči poškodovanje procesnih podatkov in zaustavitev avtomatiziranega sistema proizvodnje. Podjetje se sooči z izgubljenimi prihodki, posledično pa ima lahko takšen dogodek dolgoročnejši vpliv na pogodbene obveznosti.

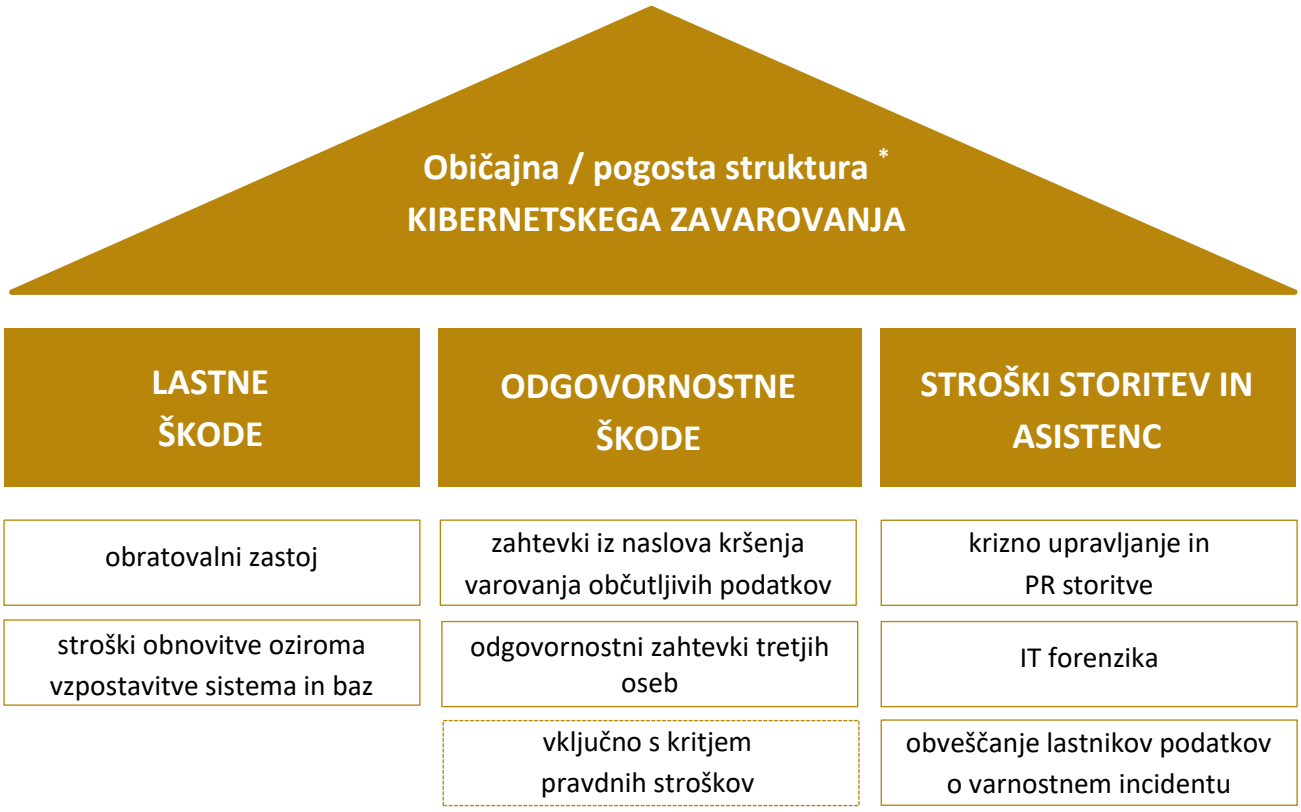
Škoda, ki nastane podjetju:	Stroški ugotavljanja izvora vdora virusa (IT forenzika), stroški ponovne vzpostavitev sistema oziroma obnovitve procesnih podatkov, škoda v obliki obratovalnega zastoja, ker podjetje do končanja procesa obnovitve sistema ne more poslovati ipd.

Zelo pogosto se kibernetska tveganja povezuje s kršenjem zaupnosti občutljivih podatkov. A je kibernetsko tveganje bistveno več kot to – zastoji v obratovanju oziroma poslovanju, odkrivanje vdorov ipd. pogosto vodijo v še večje škode oziroma izgube.

Mnoga (proizvodna in storitvena) podjetja največjo grožnjo vidijo ravno v škodah zaradi **obratovalnih zastojev**.

KIBERNETSKA ZAVAROVANJA

Kljub temu, da so kibernetska zavarovanja zelo daleč od tega, da bi zanje lahko dejali, da so standardizirana, je med različnimi ponudniki na trgu vseeno možno povleči določene skupne točke. Praviloma so oblikovana v treh stebrih.

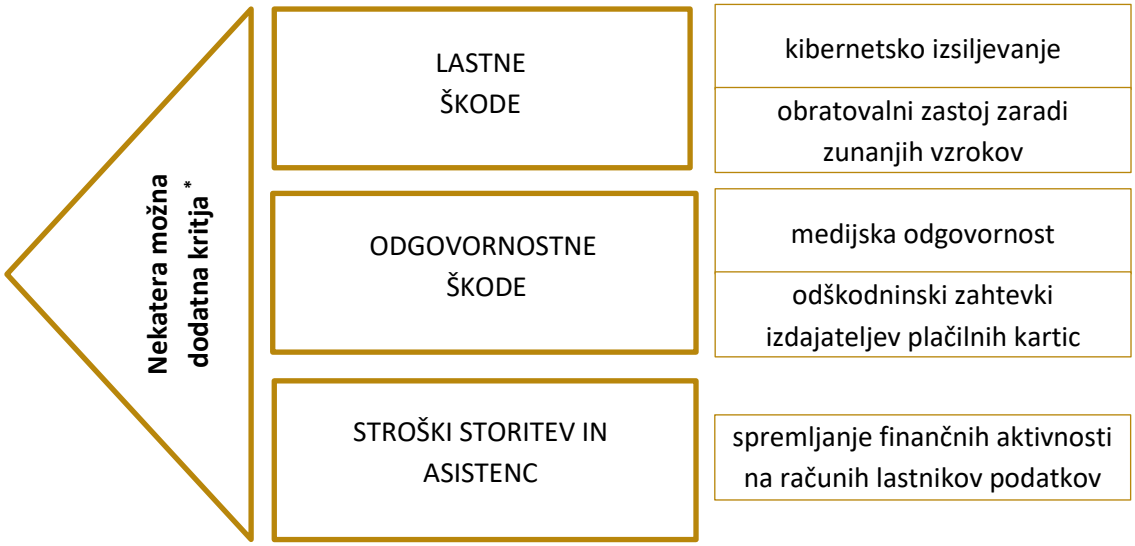


obratovalni zastoj: Zavarovanje krije škodo v obliki kosmatega dobička** (oziroma fiksnih stroškov in čistega dobička), ki ga podjetje zaradi zastoja, ki je bil posledica kibernetskega dogodka, ni moglo pokrivati oziroma dosegati.

stroški obnovitve oziroma vzpostavitve sistema in baz: Stroški, ki so po varnostnem incidentu oziroma kibernetskem napadu potrebni za ponovno vzpostavitev poškodovanih sistemov (kot na primer ponovno nalaganje operacijskih sistemov in drugih sistemov, konfiguriranje sistemov za avtomatiziran sistem proizvodnje ipd.) ter ponovno vzpostavitev baz podatkov (kot na primer nalaganje varnostnih kopij podatkov, njihovo prepisovanje, preverjanje ipd.).

zahtevki iz naslova kršenja varovanja občutljivih podatkov: Odgovornostni odškodninski zahtevki »lastnikov« občutljivih podatkov, s katerimi je razpolagal zavarovanec in ki so bili v varnostnem incidentu oziroma kibernetskem napadu izpostavljeni ali domnevno izpostavljeni storilcem. Lastnikom podatkov je lahko dejansko nastala finančna škoda, ker so na primer storilci uporabili njihove plačilne kartice, lahko so le doživeli stres, ker so na primer podatki o njihovem zdravstvenem stanju postali javni ali je bila ukradena njihova identiteta in uporabljena za sumljive zadeve ipd.

odgovornostni zahtevki tretjih oseb:	Odgovornostni zahtevki (pravnih ali fizičnih) oseb, ki so utrpele varnostni incident oziroma kibernetski napad in s tem določeno škodo, pri čemer je bil takšen incident oziroma napad izveden iz oziroma preko ali s pomočjo naprav in / ali omrežja zavarovanega podjetja. Oškodovanci torej zavarovancu očitajo premajhno skrbnost pri zagotavljanju kibernetske varnosti svojih naprav in / ali omrežja.
krizno upravljanje in PR storitve:	Stroške povezane s kriznim upravljanjem in stroške povezane s svetovalci s področja odnosov z javnostjo, ki nastanejo z namenom, da se prepreči ali ublaži škoda iz naslova zavarovančevega ugleda.
kritje pravdnih stroškov:	V okviru odgovornostnih zahtevkov zavarovanje krije tudi pravdne stroške, ki jih ima zavarovanec v povezavi z zahtevki iz naslova kršenja varovanja občutljivih podatkov, odgovornostnih zahtevkov tretjih in (v nekaterih primerih) tudi regulatornih organov.
IT forenzika:	Stroški, povezani z varnostnimi strokovnjaki, ki poizkušajo ugotoviti vzrok, identiteto storilca in dejansko nastalo škodo zaradi varnostnega incidenta oziroma hekerskega napada.
obveščanje lastnikov podatkov o varnostnem incidentu:	Stroški, povezani s pripravo, pošiljanjem in upravljanjem obvestil osebam, za katere se ve ali predvideva, da so bili njihovi podatki ukradeni, spremenjeni ali na kakšen drugačen način ogroženi zaradi varnostnega incidenta oziroma kibernetskega napada.



Klasična zavarovanja (kot na primer požarno zavarovanje, zavarovanje splošne odgovornosti ipd.) praviloma krijejo le majhen delež ali celo nič, kar je povezanega s kibernetskimi tveganji.

** Dejanski zavarovalni produkti posameznih zavarovalnic, se lahko med seboj razlikujejo.*

*** Zavarovalniška kategorija (ne enačiti z dobičkom pred obdavčitvijo – računovodsko kategorijo).*

LIBRA
PREMIA

KAKŠNA JE IZPOSTAVLJENOST PO DEJAVNOSTIH

ZDRAVSTVO

obratovalni zastoj **5**

varovanje občutljivih podatkov **5**

Motnje pri naročanju in posegih.
Kraja občutljivih informacij o pacientih vodi v obsežno obveščanje, odškodnine prizadetih pacientov, kazni ipd.

PROIZVODNO PODJETJE

obratovalni zastoj **5**

varovanje občutljivih podatkov **1**

Zaradi problemov na računalniških sistemih v samem podjetju ali pri dobaviteljih se zaustavi proizvodnja oziroma se v proizvodnji pojavljajo motnje.

TRANSPORTNO / LOGISTIČNO PODJETJE

obratovalni zastoj **5**

varovanje občutljivih podatkov **3**

Napad z odkupnino prepreči podjetju uporabo sistema za sledenje tovora / prevoza, kar vodi v velike zamude, izgube tovorov, povišane stroške dela ipd.

TRGOVSKO PODJETJE

obratovalni zastoj **4**

varovanje občutljivih podatkov **5**

Zaradi nedelovanja sistema ne deluje spletna ali klasična trgovina, stranke izgubijo zaupanje, po drugi strani pa so velike škode zaradi ukradenih podatkov strank.

ŠOLSTVO

obratovalni zastoj **2**

varovanje občutljivih podatkov **5**

Kibernetski napadalci ukradejo podatke o učencih, vključno z njihovimi zdravstvenimi stanji, ocenami ipd. Prihaja do velikih stroškov obveščanja, možni so odškodninski zahtevki.

JAVNE USTANOVE

obratovalni zastoj **5**

varovanje občutljivih podatkov **4**

Zaradi nedelovanja sistema pride do zaustavitve izvajanja ključnih operacij v javnem sektorju. Občutljive informacije o prebivalstvu so objavljene na spletu – sledijo tožbe…

TEHNOLOŠKA PODJETJA

obratovalni zastoj **3**

varovanje občutljivih podatkov **5**

Ukradeni so podatki strank, ki bi jih moralo tehnološko podjetje (npr. programersko podjetje) ustrezno varovati. Sledijo odškodninski zahtevki.

PODJETJA, KI IZVAJA STROKOVNE STORITVE

obratovalni zastoj **3**

varovanje občutljivih podatkov **3**

Ukradeni so podatki strank, ki bi jih moralo podjetje (npr. računovodski servis, odvetniška pisarna ipd.) ustrezno varovati. Sledijo odškodninski zahtevki.

** Povzeto po CFC (5 – največja izpostavljenost … 1 – najmanjša izpostavljenost).*

LIBRA PREMIA, zavarovalno posredniška družba, **d.o.o.**

Podkraj 35G, 3320 Velenje, Slovenija

e-mail: jaka.dolenc@libra-premia.si

telefon: +386 (0)41 333 989

spletna stran: www.libra-premia.si

Dovoljenje Agencije za zavarovalni nadzor za opravljanje dejavnosti zavarovalnega posredovanja številka: ***40111-40/2018-2****.*

MATIČNA ŠTEVILKA: 6072402000 | DAVČNA ŠTEVILKA: SI51637596 | IBAN: SI56 3500 1000 0524 876, BKS BANK AG

LIBRA
PREMIA

RISK COMES FROM NOT KNOWING WHAT YOU'RE DOING.

Warren Buffet