10. 11. 2023 **Slovensko bančništvo - priloga** Stran/Termin: 12

Naslov: Finančna panoga se pripravlja na krepitev kibernetske odpornosti

Avtor: Jakob Žorž

Rubrika/Oddaja: / Žanr: POROČILO

Površina/Trajanje: 548,01 Naklada: 8.240,00

Gesla: SID BANKA

FINANČNA PANOGA SE PRIPRAVLJA NA KREPITEV KIBERNETSKE ODPORNOSTI

Celoten finančni sektor v Evropski uniji se bo moral prilagoditi uredbi o digitalni operativni odpornosti (DORA), katere cilj je okrepiti odpornost proti resnim operativnim motnjam, ki so lahko posledica hudih kibernetskih napadov.

Jakob Žorž

Čez dobro leto dni, 17. januarja 2025, se bo v Evropski uniji začela uporabljati uredba o digitalni operativni odpornosti (DORA - Digital Operational Resilience Act). V njej so določene zahteve, ki jih morajo finančne institucije izpolnjevati, da lahko prenesejo, se odzovejo in si opomorejo od vseh vrst motenj in groženj, povezanih z informacijsko-komunikacijsko tehnologijo (IKT). DORA je hkrati del širše digitalne strategije Evropske unije, ki zagotavlja varno in zanesljivo delovanje digitalnih sistemov v finančni industriji. V uradnem listu EU je bila objavljena 27. decembra 2022, veljati pa je začela 16. januarja letos.

Enotne zahteve za vse udeležence v finančni panogi

Kot je povedala Aleksandra Žibrat iz Združenja bank Slovenije (ZBS), DORA vzpostavlja enotne zahteve za varnost omrežij in informacijskih sistemov podjetij in organizacij, ki delujejo v finančnem sektorju, ter ključnih tretjih strani, ki jim zagotavljajo storitve, povezane z IKT. Tu gre, na primer, za ponudnike programske opreme, platform v oblaku, storitev podatkovne analitike, v prihodnje pa verjetno tudi za storitve s področja umetne inteligence. Vsa podjetja morajo zagotoviti, da lahko vzdržijo vse vrste motenj in groženj, povezanih z IKT, ter se nanje ustrezno odzovejo in si opomorejo.

Kot so poudarili v ZBS, DORA bankam postavlja pet glavnih zahtev:

- uvesti morajo celosten sistem upravljanja IKT-tveganj, ki vključuje oceno IKT-tveganj, politike in postopke za preprečevanje, odkrivanje in odpravljanje IKT-incidentov ter načrte za obvladovanje in okrevanje;
- izvajati morajo redna testiranja IKT-odpornosti, ki simulirajo različne scenarije IKT-motenj in groženj ter preverjajo učinkovitost;
- uskladiti in poenostaviti morajo mehanizme poročanja o IKT-incidentih, ki znižujejo stroške institucij in povečujejo vpogled nadzornikov z dostopom do relevantnih informacij;
- okrepiti morajo nadzor in spremljanje tretjih strank, ki zagotavljajo IKT-storitve, kot so ponudniki računalništva v oblaku in programske opreme;
- ozaveščati morajo o IKT-tveganjih in jih minimizirati z izmenjavo informacij, ki institucijam omogoča izmenjavo obveščevalnih podatkov o kibernetskih grožnjah.

Tri najpomembnejše novosti

Igor Jarc, direktor oddelka za informacijsko varnost v SID banki, poudarja tri glavne zahteve, s katerimi DORA v splošnem razširja nadzor in kibernetsko varovanje. Prva je neposreden nadzor nad zunanjimi izvajalci, kot so dobavitelji programske opreme, oblačnih storitev in IKT-sistemov. Evropska komisija želi vzpostaviti neposreden nadzor nad njimi. »Prej se, recimo, Banka Slovenije ni mogla kar pojaviti pri večjem tujem IT-ponudniku, ki je ključen za poslovanje slovenskih bank, in izvesti nadzor. Zdaj DORA omogoča ustanovitev skupne pregledniške ekipe, ki bo lahko opravila inšpekcijski pregled večjega IT-ponudnika,« je pojasnil Jarc.

Medtem ko so ponudniki finančnih storitev nadzora že vajeni, bodo imeli večji izziv njihovi dobavitelji, ki še niso uskladili svojega poslovanja z zahtevami informacijske varnosti, na primer s standardom ISO 27001. Kot pravi Jarc, se bodo zavezanci za nadzor obravnavali glede na vpliv, ki ga ima tak dobavitelj na finančno panogo, pri čemer se bo gledala tudi vrednost pogodb. Za ponudnike, ki bodo predmet nadzora, sicer ne bodo veljale enake zahteve kot za banke, vsekakor pa bodo morali izpeljati dodatne naložbe v organizacijske, procesne in tehnične ukrepe.

Druga pomembna novost, ki je neposredna posledica naraščajočih kibernetskih groženj, je zahteva po povečanju uporabe proaktivnega odzivanja s preizkušanjem odpornosti in odzivnih načrtov. »Do zdaj so se regulatorji v finančnem sektorju zadovoljili z načrtom neprekinjenega poslovanja. Šlo je za bolj reaktiven pristop, zdaj pa bomo morali delovati zelo proaktivno, na primer spremljati grožnje in potencialne ranljivosti, delati načrte in validacije, da smo sposobni imaginarno grožnjo obvladati tako, da bo poslovanje potekalo nemoteno,« je povedal Jarc.

Tretja večja novost pa je obveznost poročanja o incidentih, ki je bilo do zdaj silosno oziroma parcialno. Če se na neki banki zgodi incident, mora banka o tem poročati Banki Slovenije. Če bi se podoben incident zgodil še pri nekem drugem subjektu iz druge veje finančne industrije, bi bilo vprašanje, ali bi obveščanje in odziv na oba dogodka prišla na skupni imenovalec in ali bi bil o tem incidentu obveščen celoten finančni sektor. »Poročanje, kot ga vzpostavlja DORA, odkriva, kakšna je bila ranljivost in kakšna grožnja se je uresničila, tako da bo tudi odziv verjetno bolj obsežen in usklajen,« je dodal Jarc.

Obvezno poročanje o incidentih tudi za zavarovalnice

Zavarovalnice in pokojninske družbe trenutno o incidentih lahko poročajo nacionalnemu odzivnemu centru za kibernet-

10. 11. 2023 **Slovensko bančništvo - priloga** Stran/Termin: 12

Naslov: Finančna panoga se pripravlja na krepitev kibernetske odpornosti

Avtor: Jakob Žorž

Rubrika/Oddaja: / Žanr: POROČILO

Površina/Trajanje: 548,01 Naklada: 8.240,00

Gesla: SID BANKA

Uredba o digitalni operativni odpornosti vzpostavlja enotne zahteve za varnost omrežij in informacijskih sistemov podjetij in organizacij, ki delujejo v finančni panogi, ter ključnih tretjih strani, ki jim zagotavljajo storitve, povezane z IKT.

sko varnost SI-CERT, kar je njihova prostovoljna odločitev. V skladu z DORA bodo morale o vsakem večjem incidentu obvezno poročati agenciji za zavarovalni nadzor. Slavko Kavšek, področni sekretar na tej agenciji, poudarja, da bodo zavarovalnice, vključno s pokojninskimi družbami, prisiljene v testiranje operativne kibernetske odpornosti. »Zdaj to počnejo, vendar ne še zares sistematično. Pripraviti bodo morale letne načrte, izvajati testiranje in najemati usposobljene izvajalce. Precej bolj bo predpisano, kako bodo morali to početi. Uporabljalo se bo načelo proporcionalnosti.«

»Zdaj bodo morali vsi poročati o incidentih in najmanj enkrat na leto tudi o tretjih ponudnikih IKT-storitev,« je dejal Slavko Kavšek. Kot pravi, bodo merila za poročanje določili vsi trije ključni nadzorniki, in sicer Evropski bančni organ (EBA) za banke, Evropski organ za zavarovanja in poklicne pokojnine (EIOPA) za zavarovalnice ter Evropski organ za vrednostne papirje in trge (ESMA) za borznoposredniške družbe in družbe za upravljanje. Predloge regulativnih in izvedbenih standardov bodo vse tri nadzorne ustanove uskladile na skupnem odboru. V letu 2024 tako lahko pričakujemo končne različice teh standardov, ki bodo finančnim ustanovam omogočili uskladitev z zahtevami DORA.

Kateri bodo glavni izzivi

Uredba DORA lahko po besedah Aleksandre Žibrat pomeni več morebitnih izzivov za finančne institucije. »Težko bo uporabiti enoten okvir za subjekte, ki se razlikujejo po velikosti, kompleksnosti in poslovnem modelu. Poleg tega v regulativni obseg vključuje ponudnike programske opreme in druge ponudnike storitev, kar pomeni, da bodo morali sodelovati z nadzorniki in izpolnjevati njihove zahteve,« je dejala sogovornica. Poudarila je tudi, da bo uredba zahtevala visoko stopnjo usklajenosti med različnimi deležniki, kot so poslovne enote, funkcije tveganja in skladnosti, IT-oddelki in zunanji partnerji, pri čemer bo prinesel dodatne stroške in administrativno breme za finančne institucije, ki bodo morale prilagoditi svoje procese, sisteme in poročila.

»Že zdaj uporabljamo nekatera orodja za preverjanje ranljivosti, zdaj pa bo to treba izvajati v širšem obsegu. To pomeni vzpostaviti proaktivnost pri odkrivanju in obravnavi groženj. Neposreden nadzor bo od bančnih zunanjih izvajalcev zahteval tudi dokazila neodvisnih pregledovalcev oziroma revizorjev, kako izvajajo posamezne procese zagotavljanja kibernetske odpornosti - do zdaj se je to izvajalo večinoma prek vprašalnikov,« je razložil Jarc. Opozoril je tudi na kadrovske izzive, s katerimi se bodo srečali predvsem zunanji izvajalci, ki bodo morali skrbeti za nove vidike skladnosti. Same banke se bodo pri preverjanju zunanjih izvajalcev sicer predvidoma obrnile na uveljavljene revizorske hiše in preizkušene revizorje informacijskih sistemov.

»Zavarovalnice imajo težavo predvsem pri izhodnih strategijah, ko pretrgajo pogodbo s tretjim ponudnikom. Vprašanje je, kako bodo zagotovile nadaljevanje poslovanja na tistem področju. Naslednji izziv je obvladovanje sredstev. Če hočeš obvladovati tveganja, je treba imeti popisana vsa IT-sredstva,« je poudaril Kavšek.

Z vidika obvladovanja tveganja bodo morale zavarovalnice spremljati dejavnosti v njihovem omrežju v režimu 24/7, kar narekuje uporabo storitev varnostno-operativnega centra. Tega velike zavarovalce že imajo oziroma ga dopolnjujejo s storitvami zunanjih izvajalcev. Manjše zavarovalnice bodo morale tovrstne storitve najemati na trgu, da bodo po eni strani zagotovile neprekinjeno spremljanje stanja varnosti, po drugi pa omogočale ustrezno odzivanje in okrevanje po incidentih.