Studija slučaja – upravljanje IT sigurnošću / kibernetičkom sigurnošću

„Medicine for future" najveća je medicinska organizacija u javnom sektoru koja surađuje s brojnim znanstvenim institutima i laboratorijima u svrhu stvaranja cjepiva protiv bolesti COVID-19. „Medicine for future" djeluje uz dozvolu i nadzor državnog Ministarstva zdravstva.

„Medicine for future" nastoji poštovati sve regulatorne zahtjeve i najbolje prakse u području zdravstvene skrbi te su uvedene gotovo sve politike i postupci u pogledu zaštite podataka i privatnosti klijenata.

Upravni odbor organizacije „Medicine for future" sastoji se od sedmero članova koji su nadležni za upravljanje, praćenje i nadzor radnih aktivnosti institucije. Šestero članova renomirani su liječnici, a jedan od članova ima iskustva u području unutarnje revizije i upravljanja rizikom.

Uspostavljen je i odjel za unutarnju reviziju čiji je glavni cilj procjenjivati procese unutarnje revizije.

U organizaciji „Medicine for future" postoji Odbor za reviziju i rizik koji je najaktivniji odbor institucije. Jedan od članova Upravnog odbora, koji je član i prethodno spomenutog Odbora, poznat je stručnjak u zemlji i ima više od 20 godina stručnog iskustva u upravljanju rizikom.

Ne postoji odbor za upravljanje sigurnošću IT-a i kibersigurnošću, a za nadzor nad rizicima u tom području bio je nadležan Upravni odbor.

ODJEL IT-a

„Medicine for future" posjeduje relativno veliku količinu resursa u tehnologija u području IT-a. Odjel IT-a sastoji se od četiri pododjela:

1. Upravljanje mrežama i sustavima,
2. Upravljanje bazama podataka i aplikacijama,
3. Razvoj bankarske tehnologije
4. Informacijska sigurnost

Iako je voditelj Odjela IT-a dobro upoznat s međunarodnim najboljim praksama i standardima u pogledu pružanja IT usluga i upravljanja IT-em, imao je vlastitu viziju o strateškom razvoju institucije.

Odjel IT-a nedavno je razvio strateški plan koji je podijelio s voditeljima poslovanja, međutim, nije uspostavljen formalan proces pregleda i pružanja povratnih informacija. Odgovorilo je samo dvoje voditelja od ukupno 15. Ostali su poslali kratku poruku da čitanje strategije IT-a *(dokumenta vrlo tehničke naravi)* i pružanje povratnih informacija nije njihova dužnost.

U posljednjih godinu dana organizacija „Medicine for future" bila je meta dvaju hakerskih napada u kojima su ukradeni čitavi gigabajti osjetljivih podataka. Iako su uspostavljeni plan i postupci izrade sigurnosnih kopija, Odjel IT-a nije uspio na vrijeme oporaviti poslovne procese jer su sigurnosne kopije bile zastarjele, te je u značajnoj mjeri bilo potrebno ručno unositi neke važne podatke za oporavak temeljnih poslovnih procesa. Neki su podaci bili dostupni na

internetu, što je stvorilo velike probleme za organizaciju „Medicine for future”, kao i za Ministarstvo zdravstva.

Ministarstvo zdravstva upozorilo je Upravni odbor da će ukinuti dozvolu instituciji ako ne poduzme ozbiljne mjere.

Upravni odbor razriješilo je dužnosti izvršnog direktora organizacije i imenovao je novu osobu za tu funkciju. Među članovima Upravnog odbora vodila se rasprava o tome bi li trebalo razriješiti dužnosti i osoblje Odjela za unutarnju reviziju, no neki su se članovi odbora, koji su istovremeno bili članovi Odbora za reviziju i rizik, tome usprotivili te su izjavili da je u prethodnim izvješćima o reviziji Odjela za unutarnju reviziju naveo nekoliko visokih rizika koji bi mogli uzrokovati ozbiljne probleme. Neki su se članovi odbora na to iznimno naljutili, pitajući se **zašto nisu o tome obaviješteni** te, ako je Odjel za unutarnju reviziju otkrio ozbiljne rizike, koje je radnje poduzelo rukovodstvo.

Nakon vrlo teške rasprave odbor je odlučio razriješiti dužnosti samo voditeljicu Odjela za unutarnju reviziju i imenovati novu osobu koja trenutačno nije zaposlenik organizacije „Medicine for future”.

Novi je izvršni direktor razriješio dužnosti prethodnog izvršnog direktora za sigurnost informacijskih sustava jer je on bio nadležan za kontinuitet poslovanja, te je na tu funkciju imenovao novu osobu.

Pitanje:

1. Na temelju okvira za kibernetičku sigurnost instituta NIST i COBIT, koje su ključne radnje novog izvršnog direktora za sigurnost informacijskih sustava?
2. Koje je pogreške počinila bivša voditeljica Odjela za unutarnju reviziju? Snosi li ona krivnju?
3. Što bi trebao poduzeti novi glavni revizor?
4. Koji su problemi u pogledu upravljanja postojali u organizaciji „Medicine for future”?
5. Što ste još uočili na temelju pruženih informacija?

Okvir kibernetičke sigurnosti instituta NIST *COBIT*