Sažetak za upravu

Ovo je jasno označen uzorak, ne izvještaj stvarnog klijenta niti dokaz provedenog angažmana. Nalazi i rokovi služe samo kao ilustracija; nisu procjena Vaših sustava ni potvrda usklađenosti.

Ilustrativna tvrtka i opseg

Izmišljena hrvatska tvrtka s 30 zaposlenih prodaje proizvode putem interneta i obrađuje narudžbe u uredskom timu. Primjer obuhvaća tri poslovno kritična sustava: web-trgovinu, bazu narudžbi i zaliha te internu aplikaciju za obradu narudžbi. Sustave održava postojeći vanjski IT partner u unajmljenoj infrastrukturi. Nisu uključena korisnička računala ni aktivna sigurnosna testiranja.

Ukupni pregled rizika

U demonstracijskom scenariju poslovanje ima sigurnosne kopije, ali nema dokaza da se ključni podaci i aplikacije mogu uspješno vratiti. Zajednički pristup i nepotpuna dokumentacija dodatno otežavaju reakciju. Stanje zahtijeva ciljanu provjeru, ne automatsku zamjenu sustava ili dobavljača.

Tri najvažnija nalaza i poslovni učinak

1. Oporavak nije provjeren: narudžbe se možda ne mogu nastaviti obrađivati nakon kvara. 2. Zajednički administratorski račun: teško je utvrditi tko je mijenjao sustav i kome treba ukinuti pristup. 3. Nema usklađenog održavanja i karte ovisnosti: promjena ili kvar mogu trajati dulje jer tim nema jasan redoslijed postupanja.

Preporuke za prvih 30 dana

Uprava imenuje vlasnike triju sustava i s IT partnerom dogovara prihvatljiv gubitak podataka i trajanje oporavka. IT partner provodi izolirani test vraćanja i bilježi rezultat. Zajednički pristup zamjenjuje se imenovanim računima gdje je izvedivo. Sve promjene prolaze dogovoreni plan, odobrenje i mogućnost povratka.

Prioritizirani registar rizika

Kako čitati registar

P1 označava prvi val aktivnosti, P2 planirano poboljšanje. Ozbiljnost opisuje ilustrativni poslovni učinak, ne potvrđenu ranjivost. Odgovorne uloge i rokovi su primjeri za dogovor, a ne preuzete obveze. Svaki nalaz u stvarnom izvještaju imao bi izvor dokaza i granice provjere.

ID	Opis rizika	Ozbiljnost	Poslovni učinak	Preporučena mjera	Prioritet	Odgovorna uloga
R-01	Vraćanje sigurnosnih kopija nije provjereno	Visoka	Narudžbe i podaci možda se neće moći vratiti nakon ispada.	Test vraćanja u izolirano okruženje i zapis rezultata.	P1 · prvih 30 dana	Vlasnik aplikacije + IT partner
R-02	Zajednički administratorski pristup	Visoka	Nije jasno tko je napravio promjenu; pristup se teško pojedinačno ukida.	Imenovani računi, višefaktorska prijava i pregled ovlasti.	P1 · prvih 30 dana	IT partner + odgovorna osoba
R-03	Nema dogovorenog rasporeda sigurnosnih ažuriranja	Srednja	Poznati nedostaci ostaju otvoreni; neplanirano ažuriranje može prekinuti rad.	Popis verzija, testiranje, termin održavanja i plan povratka.	P2 · do 60 dana	IT partner
R-04	Ovisnosti infrastrukture nisu dokumentirane	Srednja	Oporavak kasni kad nije poznat redoslijed pokretanja ili kontakt dobavljača.	Karta ovisnosti, odgovorne osobe i postupak eskalacije.	P2 · do 60 dana	Voditelj poslovanja + IT partner

Sve ocjene, dokazi, sustavi i rokovi u ovom izvještaju su demonstracijski. U stvarnom angažmanu ozbiljnost i prioriteti ovise o provjerenim dokazima, poslovnom učinku i dogovorenom opsegu. Nije provedeno testiranje stvarne tvrtke.

Tehnički nalaz R-01

Sigurnosne kopije postoje, ali vraćanje nije provjereno.

Opažanje: u demonstracijskoj dokumentaciji postoji raspored kopiranja baze i aplikacijskih podataka, ali ne i zapis uspješnog vraćanja u odvojeno okruženje.

Ilustrativni dokazi i rizik

Izmišljeni dokazi: raspored dnevnog kopiranja i popis datoteka; nije dostavljen zapis testa, provjera integriteta ni izmjereno trajanje. Postojanje datoteke ne potvrđuje mogućnost oporavka: kopija može biti nepotpuna, nečitljiva ili nepovezana s potrebnom konfiguracijom.

Poslovni učinak

Nakon ispada moguće je da tim ne može obraditi narudžbe ili potvrditi stanje zaliha. Stvarno dopušteno trajanje prekida i gubitak podataka mora odrediti vlasnik poslovnog procesa; primjer ne tvrdi koliko bi stvaran prekid trajao.

Preporučeno otklanjanje

Sastavite popis podataka, konfiguracije, verzija i pristupa potrebnih za oporavak. Dogovorite cilj vremena oporavka (RTO) i dopušteni gubitak podataka (RPO). Vratite odabranu kopiju u izolirano okruženje, bez slanja stvarnih poruka ili naplate. Zaštitite osobne podatke i nakon testa sigurno uklonite privremene kopije.

Kriteriji prihvaćanja

Baza prolazi provjeru integriteta; aplikacija se pokreće i probna narudžba radi bez učinka na produkciju. Vlasnik procesa potvrđuje potpunost dogovorenog uzorka podataka. Izmjereno trajanje i starost vraćenih podataka uspoređuju se s dogovorenim RTO/RPO. Postupak i nedostaci su zapisani, s imenovanim vlasnikom.

Koraci provjere

1. Odaberite i zabilježite datum kopije. 2. Pripremite odvojeno okruženje i ograničen pristup. 3. Vratite podatke i konfiguraciju prema uputi. 4. Provjerite integritet i funkcije aplikacije na odobrenom uzorku. 5. Zabilježite početak, završetak i pogreške. 6. Vlasnik potvrđuje rezultat, a IT partner uklanja testne podatke i dogovara sljedeći test.

Plan poboljšanja · 30 / 60 / 90 dana

0–30 dana · provjeriti i razjasniti

Dodijelite vlasnike sustava, provjerite vraćanje kopije i pregledajte administratorske pristupe. Hitne promjene provodite uz odobrenje, zapis i plan povratka. Rezultat: dokumentiran test, popis ovlasti i dogovoreni ciljevi oporavka.

31–60 dana · planirati i provesti

IT partner priprema raspored ažuriranja s testiranjem i terminima održavanja. Tim dopunjava kartu ovisnosti, kontakte dobavljača i upute za oporavak. Rezultat: dogovoren plan promjena i postupak eskalacije; bez neplaniranih zahvata u produkciji.

61–90 dana · uvesti redovitu praksu

Provedite stolnu vježbu ispada s upravom i IT partnerom. Dogovorite ponavljanje testova oporavka, pregleda ovlasti i provjera ažuriranja prema riziku i nakon većih promjena. Rezultat: operativni raspored, odgovorne osobe i evidencija provjera.

Primjer suradnje RTFM-a s postojećim IT partnerom

RTFM pojašnjava prioritete s upravom, s IT partnerom dogovara kriterije prihvaćanja i redoslijed aktivnosti te pregledava dostavljene dokaze nakon provedbe. IT partner izvodi dogovorene promjene; vlasnik procesa potvrđuje poslovnu funkcionalnost. Dodatni rad i opseg koordinacije posebno se ugovaraju. RTFM ne preuzima automatski operativnu podršku.

Ograničenja i zaključivanje nalaza

Nalaz se zatvara tek kad dogovoreni dokazi zadovolje kriterije prihvaćanja. Preostali rizik i odstupanja prihvaća odgovorna osoba tvrtke. Ovaj primjer nije certifikacija, zakonska revizija, jamstvo usklađenosti ni jamstvo neprekinutog rada.