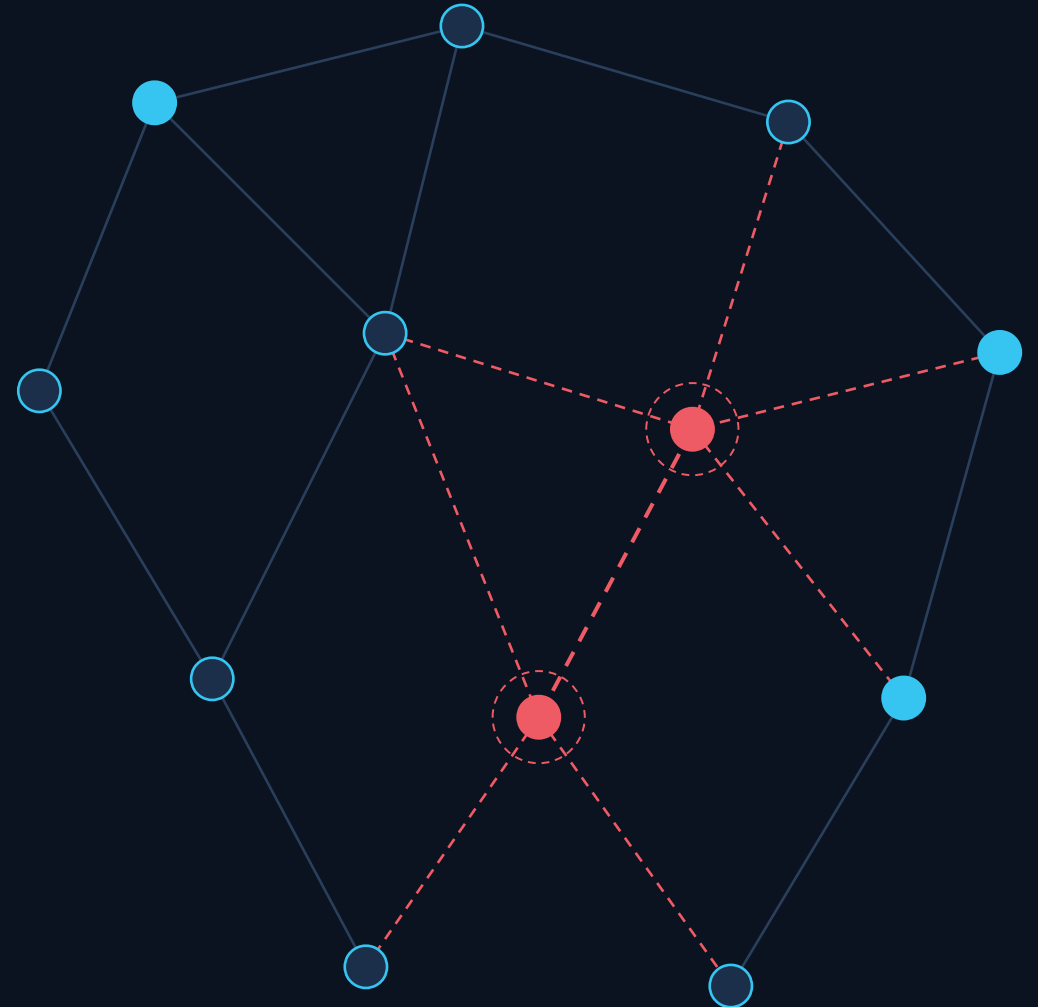


ADRIA LOGISTIKA d.o.o.

72 SATA NAKON RANSOMWARE NAPADA

Simulacija incidenta, poslovnih posljedica i oporavka sustava

FIKTIVNA STUDIJA SLUČAJA



Prezentacija za upravu. Tvrtka, iznosi, vremenski tijek i ocjene rizika su ilustrativni.

Napad u jednoj minuti

18

pogođenih uređaja zaposlenika

3

potencijalno pogođena poslužitelja

72 h

do uglavnom vraćenih osnovnih operacija

€140.000

procijenjeni kratkoročni učinak

*Ilustrativni podaci scenarija***Što se dogodilo**

Ransomware (zlonamjerni program koji šifrira datoteke i traži otkupninu) zahvatio je dio radnih stanica i poslužitelja. Početni put ulaska nije utvrđen; kompromitirani korisnički račun i udaljeni pristup glavni su trag.

Što je poremećeno

Obrada narudžbi i otprema iz skladišta pale su na oko 35 % kapaciteta; dio dijeljenih datoteka bio je nedostupan.

Prvi koraci

Izolacija pogođenih uređaja, blokada sumnjivog udaljenog pristupa, čuvanje dokaza i krizni tim.

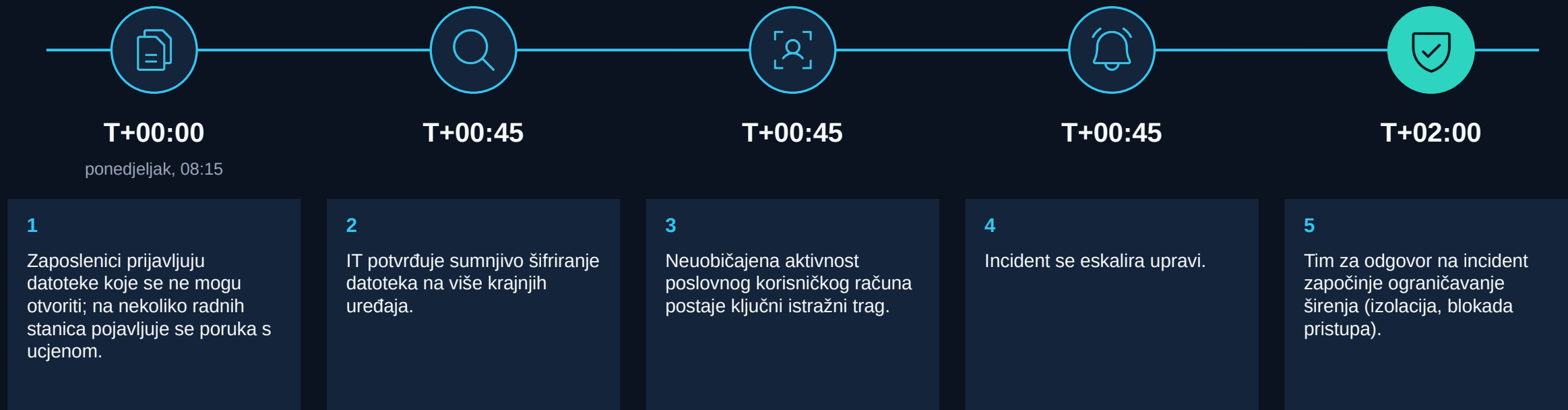
Stanje nakon 72 h

Osnovne operativne funkcije uglavnom su vraćene, uz pojačan nadzor. Incident nije zatvoren.

Što je otvoreno

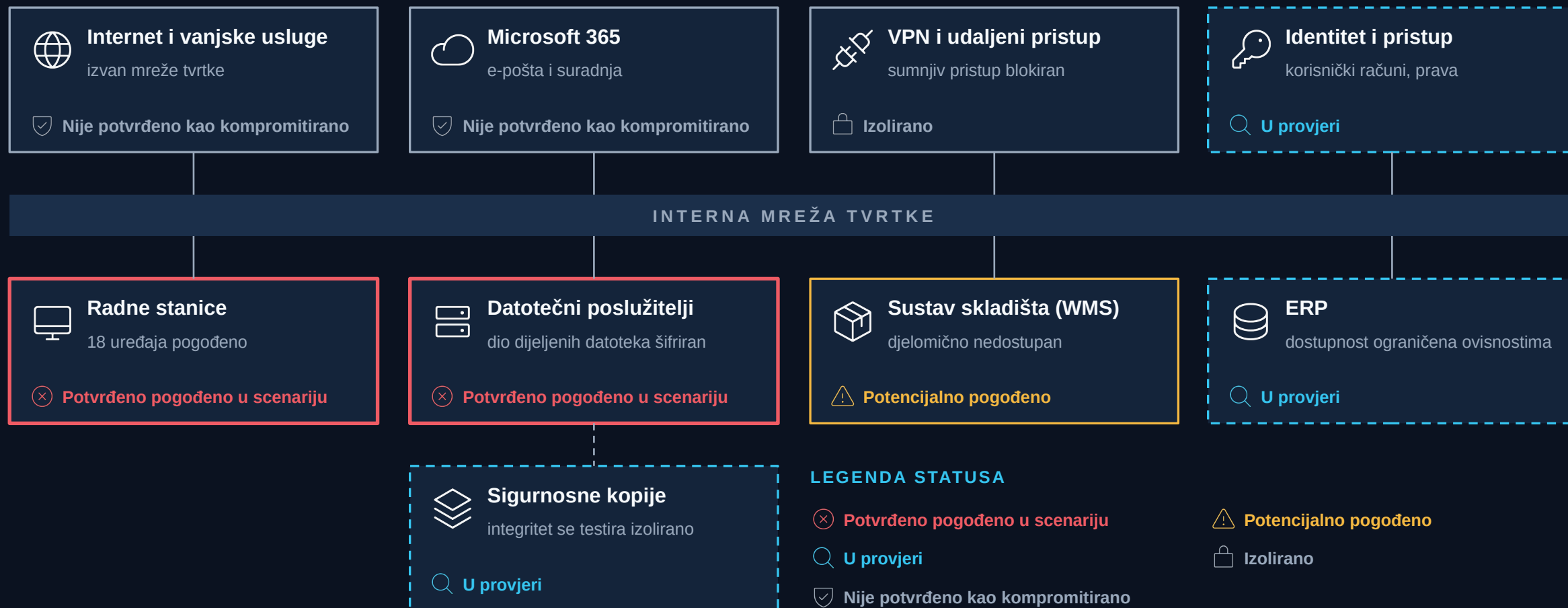
Forenzička istraga, moguća izloženost podataka (nije potvrđena), komunikacija s kupcima i dugoročne mjere.

Kako je incident otkriven: prvih 120 minuta



Početni put ulaska nije utvrđen. Kompromitirani račun i udaljeni pristup radna su hipoteza istrage, ne dokazani uzrok. Krajnji uređaj (endpoint) je svako računalo ili uređaj koji se spaja na mrežu tvrtke.

Što je pogođeno? Stanje sustava oko T+08:00



3 potencijalno pogođena poslužitelja: datotečni poslužitelji i aplikacijski poslužitelj WMS-a. Ilustrativni prikaz.

Prvih 8 sati: zaustaviti širenje, sačuvati dokaze

VRIJEME	MJERA	ZAŠTO (ZA UPRAVU)
T+02:00	Izolirati pogođene uređaje	Odspajanjem samo pogođenih uređaja sprječava se širenje, a ostatak poslovanja može raditi.
T+02:00	Ograničiti sumnjive račune i udaljeni pristup	Ako je napadač ušao preko računa, zatvaranje tog puta prekida njegov pristup.
T+02:00 – 04:00	Sačuvati zapise i dokaze	Zapisi (logovi) pokazuju što se dogodilo; brisanjem ili ponovnim pokretanjem gube se tragovi.
T+04:00 – 08:00	Utvrđiti potencijalno pogođene sustave	Uprava mora znati koji su sustavi sigurni za rad, a koji nisu.
T+04:00	Uspostaviti krizni tim i zapovjedni lanac	IT, operacije, uprava, pravna podrška i komunikacije odlučuju zajedno i brzo.
T+02:00 →	Spriječiti nesigurno vraćanje sustava	Vraćanje prije čišćenja može ponovno unijeti napadača u sustav.

Ne gase se svi sustavi bez razlike: ciljana izolacija štiti dokaze i dio poslovanja koji nije pogođen. T+04:00: proglašen veliki kibernetički incident.

Od 8. do 24. sata: što znamo, što pretpostavljamo, što ne znamo

☒ Poznato
 ☒ Radna hipoteza
 ☐ Nepoznato

Simulirani prikaz za upravu, ilustrativan, nije stvarni nadzorni sustav

POZNATO

Pogođeni sustavi

18 radnih stanica i dio dijeljenih datoteka šifrirano.

Operativna ograničenja

Obrada narudžbi oko 35 % kapaciteta; T+12:00 dio skladišta prelazi na ručne postupke.

Ovisnosti

Otprema ovisi o WMS-u; WMS je djelomično nedostupan.

RADNE HIPOTEZE

Put ulaska

Kompromitirani račun i udaljeni pristup (nije dokazano).

Izloženost podataka

Sumnja na iznošenje podataka (exfiltration), nije potvrđeno.

Opseg

Izloženost odabranih dijeljenih servisa, T+08:00.

NEPOZNATO

Sigurnosne kopije

Jesu li kopije čiste i potpune? Test u tijeku.

Puni opseg izloženosti

Koji podaci, čiji i u kojem obujmu.

Prisutnost napadača

Ima li još neotkrivenih točaka pristupa.

KLJUČNA PITANJA ZA SLJEDEĆIH 24 SATA

› Mogu li se kritični sustavi vratiti iz provjerenih kopija?

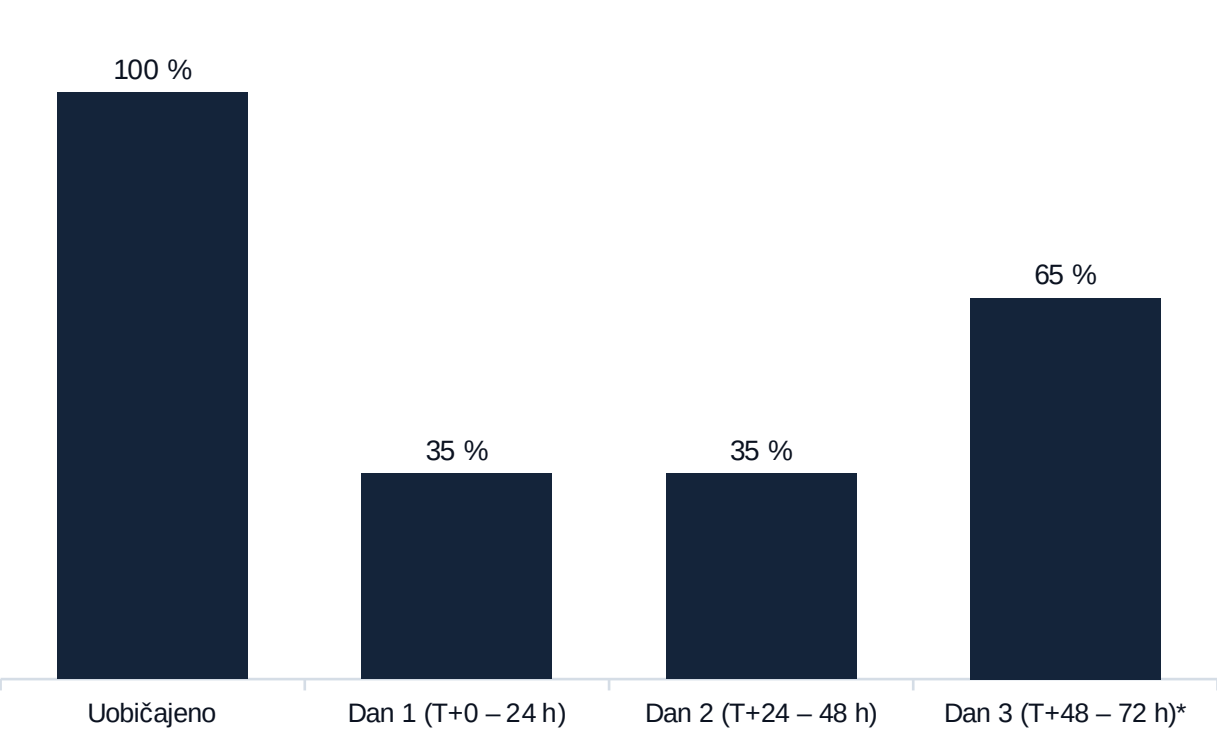
› Jesu li podaci kupaca ili zaposlenika mogli biti izneseni?

› Koji su računi i prava pristupa sigurni?

› Što kupcima reći danas, a što nakon provjere?

Kapacitet obrade narudžbi pao je na 35 % tijekom dva dana

Kapacitet obrade narudžbi (% uobičajenog)



*Dan 3: pretpostavka postupnog oporavka (oko 65 %) za ilustraciju; nije izmjereni podatak. Pri 35 % obrađuje se oko 420 od uobičajenih 1.200 narudžbi dnevno.

UČINAK PO POSLOVNIM FUNKCIJAMA



Obrada narudžbi

Dio ručno, smanjena propusnost

⊗ **Potvrđen učinak**



Otprema iz skladišta

Kašnjenja zbog djelomično nedostupnog WMS-a

⊗ **Potvrđen učinak**



Korisnička služba

Više upita kupaca, ograničene informacije

⚠ **Mogući učinak**



Pouzdanost isporuka

Rizik kašnjenja ugovorenih isporuka

⚠ **Mogući učinak**



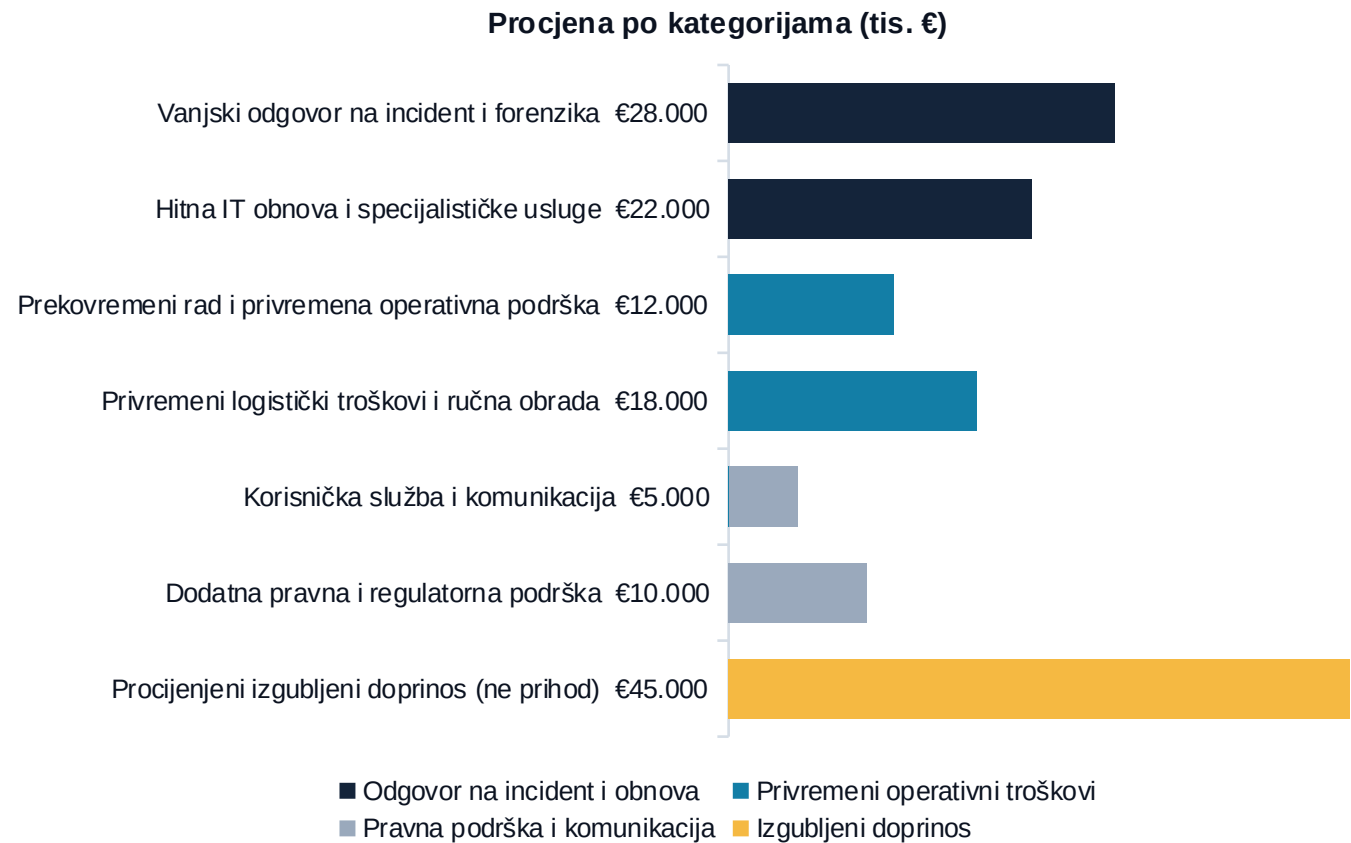
Financije i administracija

Otežan pristup dijeljenim datotekama

⚠ **Mogući učinak**

Ne procjenjujemo broj trajno izgubljenih narudžbi ni kupaca.

Procijenjeni kratkoročni učinak: €140.000



PO SKUPINAMA

Odgovor na incident i obnova	€50.000
Privremeni operativni troškovi	€30.000
Pravna podrška i komunikacija	€15.000
Procijenjeni izgubljeni doprinos	€45.000

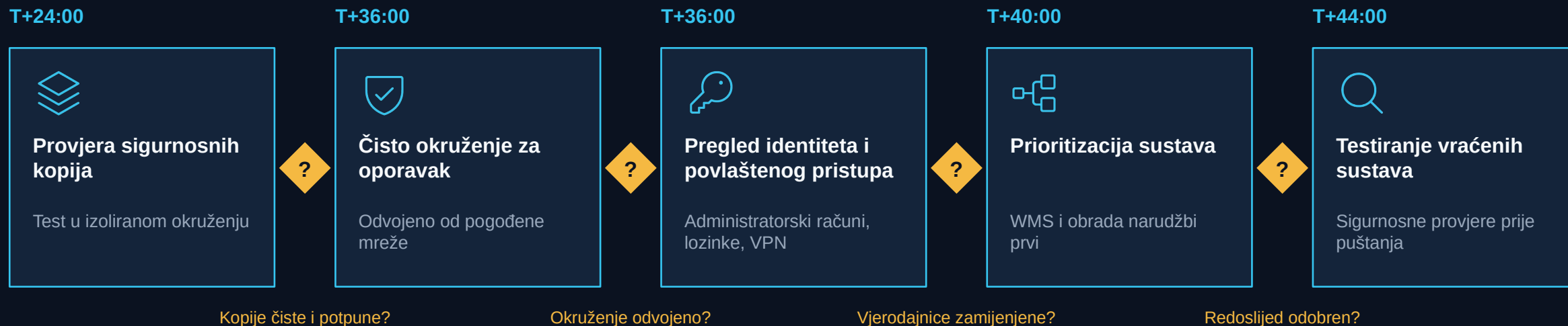
Ukupno (ilustrativno) €140.000

Izravni novčani izdaci (€95.000) su stvarna plaćanja. **Izgubljeni doprinos** (€45.000) je procjena marže koja nije ostvarena zbog poremećaja; nije izgubljeni prihod ni neto dobit.



Početna procjena scenarija, ne konačni trošak. Ne uključuje dugoročni gubitak kupaca, štetu ugledu, moguće kazne, sporove, franšize i sporove s osiguranjem, neutvrđenu izloženost podataka, dugoročnu sanaciju ni otkupninu (nije plaćena ni uključena).

Od 24. do 48. sata: najprije čisto okruženje, zatim vraćanje



Romb = točka odluke: ako je odgovor "ne", ne ide se dalje dok se uvjet ne ispuni.

KOORDINACIJA TIMOVA

IT i sigurnost pripremaju sustave; operacije određuju redoslijed poslovnih usluga; uprava odobrava rizik i resurse. Odluke se bilježe s vremenom i obrazloženjem.



Zašto ne vratiti sustave odmah? Vraćanje iz neprovjerene kopije ili u okruženje gdje je napadač još prisutan može ponovno pokrenuti napad. Kopije se provjeravaju prije vraćanja, ne poslije.

Od 48. do 72. sata: postupni povratak uz pojačan nadzor



T+48:00 vraćanje iz provjerenih kopija · T+60:00 dio skladišta i obrade narudžbi radi pod pojačanim nadzorom · T+72:00 osnovne funkcije uglavnom vraćene

STANJE U T+72:00

Obrada narudžbi Uglavnom vraćena, pojačan nadzor Vraćeno, uz nadzor	Otprema iz skladišta Osnovna funkcija radi; provjera tijekova u tijeku Vraćeno, uz nadzor
ERP U radu; integritet podataka u provjeri U provjeri	Dijeljene datoteke Djelomično vraćene Otvoreno pitanje
Forenzička istraga U tijeku U provjeri	Izloženost podataka Nije potvrđena; procjena u tijeku Otvoreno pitanje

Incident nije zatvoren. Poslovanje radi, ali istraga, procjena izloženosti podataka, komunikacija s kupcima i dugoročne mjere se nastavljaju. Nije vraćen svaki sustav ni svaka datoteka.

Što ako sigurnosne kopije nisu upotrebljive?



Konceptualni plan za nepredviđene okolnosti. Za scenarij B ne navodimo točne rokove: ovise o stanju sustava i dostupnim izvorima. U ovom scenariju kopije su se pokazale upotrebljivima (scenarij A).

Podaci, kupci i regulatorne obveze: pitanja za upravu

☒ Poznato ☒ Radna hipoteza ☐ Nepoznato

☐ Jesu li zahvaćeni osobni podaci?

☒ Je li neovlašteni pristup ili iznošenje podataka potvrđeno?

☐ Koji kupci ili partneri mogu biti pogođeni?

☒ Koje dokaze treba sačuvati?

☐ Koje ugovorne obveze obavješćavanja vrijede?

☐ Je li potrebno obavijestiti nadzorno tijelo?

Dokazi: zapisi, pogođeni uređaji i komunikacija napadača čuvaju se za istragu i moguće pravne postupke.



GDPR: rok od 72 sata, ali samo kad su ispunjeni uvjeti

Ako je riječ o povredi osobnih podataka koja vjerojatno predstavlja rizik za pojedince, voditelj obrade nadzorno tijelo (u Hrvatskoj AZOP) obavještava bez nepotrebnog odgađanja i, gdje je izvedivo, najkasnije 72 sata nakon što je saznao za povredu.

- Ransomware ne znači automatski povredu osobnih podataka.
- Rok od 72 sata nije univerzalni rok za svaki kibernetički incident.
- Primjena ovisi o činjenicama i pravnoj procjeni.
- Ovisno o djelatnosti i veličini, mogu vrijediti i obveze iz propisa o kibernetičkoj sigurnosti (NIS2) s vlastitim rokovima, te ugovorne obveze prema kupcima.

Preporuka: odmah uključiti kvalificiranog pravnog savjetnika i službenika za zaštitu podataka. Ova prezentacija ne daje pravni zaključak.

Gdje su kontrole mogle zakazati? Područja za provjeru

KONTROLE ZA PROCJENU, NE POTVRĐENI PROPUSTI

Područje kontrole	Pitanje za istragu	Mogući poslovni učinak	Preporučeno poboljšanje
Identitet i povlašteni pristup	Tko je imao administratorska prava i zašto?	Napadač s pravima može doći do više sustava	Najmanja potrebna prava, pregled računa
Višefaktorska autentifikacija (MFA)	Je li MFA bila uključena za pogođeni račun?	Ukradena lozinka dovoljna je za ulazak	MFA za sve udaljene i administratorske pristupe
Ograničenja udaljenog pristupa	Tko i odakle smije pristupiti preko VPN-a?	Širok ulaz u internu mrežu	Ograničen i nadziran udaljeni pristup
Zaštita krajnjih uređaja (EDR)	Je li šifriranje otkriveno i zaustavljeno na vrijeme?	Kasno otkrivanje, više pogođenih uređaja	Provjera pokrivenosti i pravila EDR-a
Segmentacija mreže	Je li se napad mogao proširiti između zona?	Jedan upad pogađa i skladište i ured	Odvajanje skladišnih i uredskih sustava
Izolacija i testiranje kopija	Jesu li kopije bile odvojene i testirane?	Duži oporavak ili gubitak podataka	Izolirane kopije i redoviti testovi vraćanja
Zapisi i upozorenja	Jesu li postojali signali prije T+00:00?	Propušteni rani znakovi	Centralizirani zapisi i pragovi upozorenja
Postupci odgovora na incident	Jesu li uloge i koraci bili dokumentirani?	Sporije i neusklađene odluke	Ažuriran plan i vježbe
Prijavljivanje i svijest zaposlenika	Koliko su brzo zaposlenici prijavili problem?	Kasnija reakcija	Jednostavan kanal prijave i edukacija

Prvih 90 dana: od istrage do provjerene otpornosti

DANI 1 – 15	DANI 16 – 30	DANI 31 – 60	DANI 61 – 90
Utvrđiti činjenice	Zatvoriti ulaz	Testirati oporavak	Dokazati učinak
Dovršiti forenzičku procjenu	Ojačati MFA i udaljeni pristup	Vježbe vraćanja iz kopija	Simulacijska vježba incidenta za upravu
Pregledati kompromitirane račune i povlašteni pristup	Pregledati zaštitu uređaja i zapise	Poboljšati nadzor i eskalaciju upozorenja	Provjeriti učinkovitost mjera
Provjeriti kopije i dokumentirati rezultate oporavka	Provjeriti segmentaciju mreže	Testirati postupke kontinuiteta poslovanja	Ažurirati izvještavanje i ciljeve oporavka
Potvrditi status izloženosti podataka	Ažurirati postupke odgovora na incident	Pregledati pristup dobavljača i trećih strana	Dokumentirati preostale rizike i nositelje
Procijeniti obavijesti i komunikaciju			

Predloženi plan. Bez odobrenih budžeta i imenovanih nositelja; uprava ih određuje.

Što uprava mora odlučiti?

- 1 Odobriti resurse za odgovor na incident i oporavak
- 2 Odrediti prioritete vraćanja poslovnih usluga
- 3 Odrediti pravni pristup i komunikaciju s kupcima
- 4 Financirati najvažnija sigurnosna poboljšanja
- 5 Tražiti izvještavanje o oporavku i preostalom riziku na temelju dokaza

Aktivnost	Uprava	IT i sigurnost	Operacije	Pravna podrška	Komunikacije
Resursi za odgovor i oporavak	A	R	C	C	I
Prioriteti vraćanja usluga	A	R	R	I	I
Pravni pristup i obavijesti	A	C	I	R	C
Komunikacija s kupcima	A	C	C	C	R
Sigurnosna poboljšanja	A	R	C	I	I
Izvještavanje o preostalom riziku	A	R	C	C	I

R = provodi · A = odgovara i odobrava · C = savjetuje · I = informiran. Predložena podjela, ne potvrđena organizacijska zaduženja.

„Brz oporavak nije dovoljan ako sigurnosni rizik ostane nepromijenjen.”

Nakon 72 sata: što dalje?



Oporavak

Vratiti kritične sustave i potvrditi integritet podataka.



Otpornost

Ukloniti uzroke i zatvoriti prioritetne sigurnosne nedostatke.



Odgovornost

Dokumentirati odluke, procijeniti obveze i pratiti provedbu.



72 sata

Osnovne operacije uglavnom vraćene

Stanje scenarija



30 dana

Prioritetne korektivne mjere u provedbi

Predloženi cilj



90 dana

Učinkovitost mjera provjerena

Predloženi cilj

„Cilj nije samo vratiti sustave u rad, nego osigurati da sljedeći incident ne proizvede isti poslovni učinak.”

Fiktivni scenarij. Podaci, procjene i vremenski tijek služe isključivo ilustraciji.