



01. LISTOPADA 2026. · 10:20 — 11:10 · MAGUS CYBER WORLD

DIGITALNA TRANSFORMACIJA BEZ PAUZE

Kibernetska sigurnost kao temelj svake digitalne transformacije
NIS2 u praksi - regulatorni zahtjevi i priprema organizacija

Maja Krejči - Matija Matijevac



KAKO ULAZE

napad više ne traži lozinku

31 %

kroz ranjivost

Iskorištavanje ranjivosti prvi je put u devetnaest godina preteklo ukradene vjerodajnice kao najčešći ulaz.

56 %

uspješno šifriranje

Više od polovice napada uspije šifrirati podatke. Obrana ih zaustavi u manje od pola slučajeva.

48 %

preko treće strane

Gotovo polovica povreda uključuje treću stranu - dobavljača, partnera ili pružatelja usluge. Godinu prije: 30 %.

Napad ne mora doći na vas. Dovoljno je da dođe na nekoga vašeg.

VERIZON DBIR 2026 (PODACI ZA 2025.) · SOPHOS: STATE OF RANSOMWARE 2026



KOLIKO KOŠTA PAUZA

cijena zastoja, ne cijena otkupnine

1,7

milijuna dolara

Prosječan trošak oporavka od ransomware napada - odvojeno od otkupnine.

769

tisuća dolara

Medijan plaćene otkupnine. Prosjek je viši jer ga podižu rijetke goleme isplate.

28 %

žrtava plati

Najniži udio ikad zabilježen. Preostalih 72 % samo oporavak plaća samo - iznos lijevo.

Većina ne plati otkupninu. Svi plate zastoj.

SOPHOS: STATE OF RANSOMWARE 2026 · CHAINALYSIS 2026 (PODACI ZA 2025.)



Transformacija bez otpornosti nije
napredak. To je veća površina za napad.



ZAŠTO TO NIJE ADMINISTRATIVNI TERET

regulativa ne traži papir, traži sposobnost

Ne traži politiku sigurnosti - traži da znate što imate i tko tome pristupa.

Ne traži plan oporavka - traži da ste ga isprobali i da znate koliko traje.

Ne traži registar dobavljača - traži da vas dobavljač obavijesti prije nego vama istekne rok.

Ujedno 3 ključne stvari za svaki projekt digitalne transformacije.



OKOSNICA

tri skupine mjera, jedan sustav

organizacija

Tko odlučuje, tko odgovara, tko je osposobljen - i gdje to piše.

tehnika

Što stvarno mora raditi u IT-u i u OT-u, uključujući fizički pristup.

lanac

Dobavljači, ugovorni rokovi i vaš vlastiti položaj dobavljača.

ZKS traži sve tri. DORA također. Nijedna se ne preskače.



01

organizacijske mjere



ŠTO TRAŽI ZKS ČL. 30

nisu sve mjere tehnologija

- (1) Politike analize rizika i sigurnosti informacijskih sustava.
- (2) Postupanje s incidentima - tko, kada, kome.
- (3) Kontinuitet poslovanja, upravljanje pričuvcama i krizom.
- (7) Osnovna higijena i osposobljavanje zaposlenika.

Ove četiri ne kasne zbog novca. Kasne jer se ne zna čiji su posao.



UPRAVA · NIS2 ČL. 20, ZKS ČL. 29

odluka koja mora imati potpis

Uprava odobrava mjere, nadzire njihovu provedbu i odgovara za propuste.

Odluka uprave o mjerama upravljanja rizicima - s datumom i potpisom, ne zapisnik sa sastanka.

Točka na dnevnom redu uprave barem jednom godišnje, s pisanim tragom.

Evidencija osposobljavanja članova uprave - ime, datum, sadržaj.

Imenovana osoba odgovorna za provedbu, s ovlastima i proračunom.

Bez potpisa mjere nisu obveza organizacije, nego prijedlog informatike.



ODLUKA · NIS2 ČL. 23, UREDBA ČL. 58-67

tko u 03:47 smije reći da je značajno

Ime i prezime, ne odjel.

Broj telefona koji se javlja izvan radnog vremena - provjeren pozivom, ne dokumentom.

Pragovi na jednoj stranici: 20 % korisnika kroz sat, 100.000 € ili 5 % prihoda, dva incidenta u šest mjeseci.

Ista osoba istodobno procjenjuje jesu li dirnuti osobni podaci - drugi okidač, drugo tijelo.

Financijski subjekti: DORA traži prvu obavijest u 4 sata od klasifikacije incidenta kao velikog.

Ako odgovor nije ime nego odjel - nemate odluku, imate sastanak.



ROKOVI · UREDBA ČL. 66, 67, 70

tri broja koja se znaju napamet

24 h Rano upozorenje CSIRT-u, od saznanja.

72 h Početna obavijest s procjenom. Isti rok vrijedi i prema AZOP-u (osobni podaci).

30 dana Završno izvješće, od početne obavijesti.

Financijski subjekti: DORA - 4 sata od klasifikacije, najkasnije 24 sata od saznanja.



Organizacijska mjera je jedina koja se ne može naručiti. I ona koju nadzor provjerava prvo.



02

tehničke mjere: IT i OT

Isti propis, dvije potpuno različite izvedbe. I jedan popis koji mora obuhvatiti oboje.



POPIS IMOVINE · ZKS ČL. 30 T. 9

pet stupaca koji moraju postojati

KONKRETNO

Vlasnik - ime osobe, ne odjela.

Koju uslugu nosi - bez toga ne možete procijeniti značaj incidenta.

Verzija i datum zadnje provjere - za OT uključujući firmver.

Tko i kako pristupa - lokalno, daljinski, preko dobavljača.

Je li u opsegu vaših kontrola - i ako nije, zašto.

Popis bez stupca „koju uslugu nosi” ne pomaže u 03:47.



IT MJERE · ZKS ČL. 30 T. 5, 9, 10

pet stvari koje moraju raditi

KONKRETNO

Višestruka autentifikacija na svemu što je dostupno izvana - bez iznimki za upravu.

Odvojeni povlašteni računi, bez dijeljenih administratorskih lozinki.

Segmentacija mreže, s pisanim popisom dopuštenih prijelaza između segmenata.

Središnje prikupljanje zapisa, s rokom čuvanja duljim od 72 sata.

Upravljanje ranjivostima s rokom za kritične zakrpe i evidentiranim iznimkama.

Zapis koji se čuva sedam dana ne pomaže kad je napadač bio unutra tri tjedna.



ZAKRPE · ZKS ČL. 30 T. 5

31 % ulaza kroz ranjivost - i gotovo sve imaju zakrpu

Rok za kritične ranjivosti izražen u danima, zapisan i mjeran.

Popis opreme koja se ne smije zaustaviti - s kompenzacijskom kontrolom umjesto zakrpe.

Svaka iznimka ima vlasnika, razlog i datum ponovnog razmatranja.

Provjera da je zakrpa doista primijenjena - ne da je objavljena.

Popis iznimaka koji nitko ne pregledava s vremenom postaje popis ulaza.



KRIPTOGRAFIJA · ZKS ČL. 30 T. 8

politika postoji, primjena se ne provjerava

KONKRETNO

Popis gdje su podaci šifrirani u mirovanju, a gdje samo u prijenosu.

Tko ima pristup ključevima - i što se događa kad ta osoba ode iz organizacije.

Pričuve su šifrirane, a ključ nije na istom mjestu kao pričuva.

Certifikati imaju vlasnika i rok - istek certifikata je zastoj bez napadača.

Šifrirana pričuva čiji ključ leži uz nju jednako je korisna kao nešifrirana.



OT MJERE · ZKS čl. 30 t. 9 i 10 · rječnik: IEC 62443

zone, prijelazi i odvojene vjerodajnice

KONKRETNO

Podjela na zone s popisom dopuštenih prijelaza - i nijedan prijelaz bez zapisa.

Nijedan uređaj u OT-u nije izravno dostupan s interneta, uključujući telemetriju.

Odvojene vjerodajnice za OT - administrator iz IT-a nije automatski administrator u OT-u.

Inventar firmvera s verzijama, jer se ranjivosti objavljuju po verziji.

Tvorničke lozinke promijenjene i evidentirane, uključujući opremu koju je ugradio dobavljač.

OT se ne štiti kopijom IT pravila, nego njihovim prijevodom.



DALJINSKI PRISTUP · ZKS ČL. 30 T. 4 I 9

trajni tunel prema dobavljaču

KONKRETNO

Pristup se otvara na zahtjev i zatvara sam od sebe, s rokom u satima.

Imenovana osoba kod dobavljača, ne zajednički račun tvrtke.

Višestruka autentifikacija i zapis sjednice koji preživi brisanje kod dobavljača.

Popis svih postojećih trajnih pristupa - i datum kad se svaki ukida.

Svaki trajni pristup je odluka. Provjerite tko ju je donio i kada.



KONTINUITET · ZKS čl. 30 t. 3

pričuva koja nije vraćena nije pričuva

KONKRETNO

Barem jedna kopija izvan dosega mreže - odvojena od domene i od administratorskih računa.

Izmjereno vrijeme povrata za svaku ključnu uslugu, izraženo u satima.

Vraćanje isprobano na pravom sustavu, ne na testnom, barem jednom godišnje.

Plan rada bez sustava: što se radi ručno i tko to zna napraviti.

Uprava ne razumije postotke. Razumije broj sati do povratka usluge.



OCJENA DJELOTVORNOSTI · ZKS čl. 30 t. 6 i čl. 31

mjera koja nije isprobana je namjera

KONKRETNO

Tablična vježba s upravom jednom godišnje - scenarij, sat, odluke.

Vježba obavješćivanja: napisati i poslati probnu obavijest u roku od 24 sata.

Provjera da kontrola doista blokira - jedan pokušaj, jedan zapis, jedan zaključak.

Nalaz svake vježbe ulazi u plan postupanja iz samoprocjene.

Financijski subjekti: DORA čl. 24-27 - obvezan program testiranja, za dio subjekata i TLPT (Threat-Led Penetration Testing).

Razlika između uvedene i djelotvorne mjere je jedna vježba.



UMJETNA INTELIGENCIJA

AI nije uvijek čarobni štapić

SVI GA KORISTE, NO

AI + SaaS + no-code omogućili su svakom zaposleniku da postane vlastiti IT odjel

AI alat nije samo alat - može postati novi obrađivač vaših osobnih podataka

Shadow AI je Shadow IT na steroidima

Za curenje podataka više nije potreban napadač

Odgovor nije zabraniti AI već ga kontrolirati, klasificirati i njime ispravno upravljati

Ne znate koji AI koristi vaše podatke? Nimate inventar informacijskog sustava.



03

lanac opskrbе



RAČUNICA · UREDBA ČL. 66-67

vaš sat pokreće tuđi incident

24 h

Vaš zakonski rok za rano upozorenje, od trenutka saznanja.

8 h

Rok koji dobavljač treba imati u ugovoru da vam ostane vremena za odluku.

0 h

Koliko imate ako ugovor o tome ne kaže ništa.

Ako rok dobavljača nije kraći od vašeg, matematika ne radi.



UGOVOR · ŠEST KLAUZULA

što mora biti u ugovoru

KONKRETNO

Rok obavješćivanja o incidentu, kraći od vašeg zakonskog.

Pravo na provjeru - dokumentacijom, upitnikom ili nalazom treće strane.

Popis podizvođača i obveza najave promjene.

Pravila daljinskog pristupa: imenovane osobe, rok, zapis sjednice.

Izlazna strategija: povrat podataka, brisanje, rok.

Obveza sudjelovanja u vašoj vježbi oporavka barem jednom godišnje.

Financijski subjekti: DORA čl. 30 ove odredbe propisuje, a čl. 28. st. 3. traži registar svih ugovora.



REGISTAR · TRI POGLEDA

jedan registar dobavljača, tri pitanja

Tko nosi dio ključne usluge - i što se događa ako stane.

Tko ima pristup OT-u ili prostorima s opremom - i je li taj pristup trajan.

Tko obrađuje osobne podatke - jer to pokreće i drugi rok.

Tri tablice u tri odjela nisu registar.



04

bez pauze



ZAŠTO BEZ PAUZE

tri stvari koje regulativa daje svakom projektu

Pregled umjesto pretpostavke. Nema “crne kutije” - znate što je pušteno u rad i što možete vratiti.

Zahtjeve umjesto dorade. Sigurnost ulazi u projekt na početku, a ne nakon primopredaje.

Dokaz umjesto tvrdnje. Da mjere rade, a ne samo da su uvedene.

Otpornost nije trošak projekta digitalizacije. Ona je razlika između isporučenog i upotrebljivog.



pitanja