CIRED HRVATSKI OGRANAK

ACCREDI®

SIGURNOST I OTPORNOST:

Integracija zahtjeva CER, NIS2 i DORA-e u sigurnosne strategije kritične infrastrukture

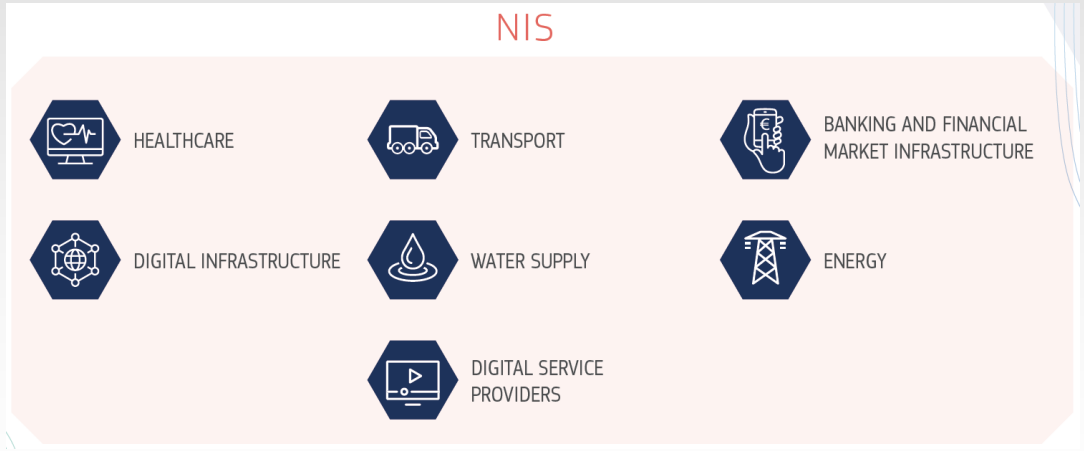
dr. sc. Natalija Parlov Una

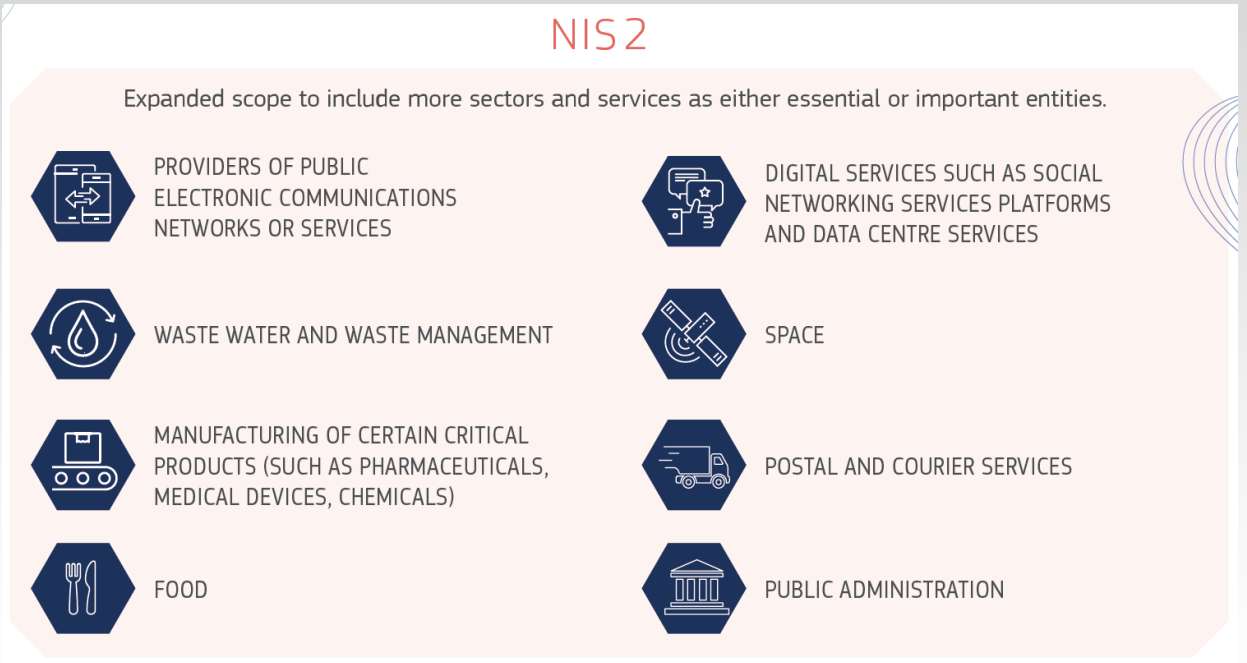
Authorised IRCA Lead Tutor & Senior Lead Certification Auditor

ACCREDI | TÜV NORD Adriatic

Sadržaj

NIS > NIS2
ZKS > ZKS(2)





Izvor: Europska Komisija ***(2020)*** *Factsheet hitting the refresh button on cybersecurity rules,* ***NIS2: Proposal for a Directive on measures for high common level of cybersecurity across the Union***

NIS2 Direktiva, ZKS(2)

- ✓ **Upravljanje informacijskom sigurnošću i kontinuitetom poslovanja – OTPORNOST**
- ✓ **Konkretno upravljanje rizicima**
- ✓ Odgovor na **incidente** i izvješćivanje
- ✓ **Sigurnost opskrbnog lanca**
- ✓ Obveze provođenja testiranja i revizija/audita
- ✓ **Upravljanje imovinom** (*Asset Management*), **kategorizacija** i **upravljanje rizicima**
- ✓ Jače kontrole pristupa podacima i sustavima
- ✓ **Sigurnost ljudskih resursa**
- ✓ Kriptografske procedure i enkripcija
- ✓ Obveza provođenja treninga i edukacija

- ✓ **RA** (*Risk Assessment*)
- ✓ **BIA** (*Business Impact Analysis*)
- ✓ **BCP** (*Business Continuity Plans*)
- ✓ **DRP** (*Disaster Recovery Plans*)
- ✓ **TCP** (*Technology Contingency Plans*)
- ✓ **CMP** (*Crisis Management Plans*)
- ✓ **SLA** (*Service Level Agreements*)

- ✓ Do 17.10.2024. godine (bi članice morale) donijeti mjere i odmah obavijestiti EK
- ✓ Primjena mjera od 18.10.2024. godine

DORA

- ✓ **Akt o digitalnoj operativnoj otpornosti (DORA)** uspostavlja transformacijski regulatorni okvir kako bi se adresirali rizici informacijske i komunikacijske tehnologije (IKT) u financijskom sektoru EU-a
- ✓ Upravljanje rizicima informacijske sigurnosti i otpornosti s **RTS od ESA-e**
- ✓ **Uredba**! - *lex specialis* za financijske institucije, na snazi od 16.01.2023. godine i primjenjivat će se od 17.01.2025. godine

- ✓ **Važno za EES:**
  Upravljanje rizikom trećih strana (TPRM) – utjecaj na sigurnost i kontinuitet poslovanja obveznika DORA-e

CER Direktiva

- ✓ **Critical Entities Resilience Directive**
- ✓ Ojačavanje otpornosti kritične infrastrukture u kontekstu **upravljanja rizicima** s obzirom na **širi portfelj identificiranih prijetnji**
- ✓ *Uključuje*: prirodne nepogode, terorističke napade, prijetnje od unutarnjih faktora i sabotažu
- ✓ **11 sektora**: energetski, transport, bankarstvo, infrastruktura financijskog tržišta, zdravstvo, pitka voda, otpadne vode, digitalna infrastruktura, javni servisi, svemir i hrana

- ✓ Do 17.10.2024. godine (bi članice morale) donijeti mjere, isto kao NIS2

Informacijska sigurnost vs. IT sigurnost

- **IT sigurnost čini samo dio informacijske sigurnosti**
- **Informacijska sigurnost**, **uz IT sigurnost (s OT/IoT)**, **uključuje** još i fizičku sigurnost, upravljanje ljudskim resursima, pravne aspekte, organizaciju poslovanja, definiranje i dokumentiranje procesa, **cjelovito i ažurirano upravljanje rizicima**...

Sigurnost i otpornost

Osiguravanje kontinuiteta poslovanja

Minimum: *RA, BIA, BCP, DRP, TCP, CMP, testovi*

- ***MAD*** *Maximum Allowable Downtime,* ***MTD*** *Maximum Tolerable Downtime*
- ***MAO*** *(Maximum Acceptable Outage),* ***MTPD*** *(Maximum Tolerable Period of Disruption)*
- ***RTO*** *Recovery Time Objective*
- ***RPO*** *Recovery Point Objective (acceptable data loss)*

ORGANIZACIJSKE MJERE

- ✓ odnose se na **dokumentirano uređenje** te **organizacijsku kulturu, poslovnu praksu i procese** unutar organizacije na način da se internim aktima i ugovornim klauzulama uređuje područje zaštite podataka i osiguravanja kontinuiteta poslovanja te da se ono što je **propisano aktivno procesno provodi** sukladno dokumentiranoj informaciji, te organizacijske mjere koje organizacija **ugovorno regulira s trećim stranama,** a koje imaju utjecaj na njenu informacijsku sigurnost ili otpornost, uz uvjet da su **sve od navedenih strana** u mogućnosti i da je organizacija u mogućnosti **nedvojbeno to dokazati**

TEHNIČKE MJERE

- ✓ odnose se na **zaštitne mjere** koje se postavljaju na **fizička mjesta te IT/OT sustave ili proizvode** koji se koriste unutar organizacije ili u sklopu krajnjih proizvoda klijentima, a vezano uz ophođenje s podacima ili osiguravanje kontinuiteta poslovanja; ili tehničke mjere koje organizacija **ugovorno regulira s trećim stranama,** a koje imaju utjecaj na njenu informacijsku sigurnost ili otpornost, a da su **sve od navedenih strana** u mogućnosti **nedvojbeno to dokazati**

Rizik = učinak nesigurnosti na ciljeve

RIZIK = f (imovina, prijetnja, ranjivost)

Razina rizika = vjerojatnost x učinak

Prijetnja

- **Izvori prijetnji mogu biti:**

  prirodna događanja (klimatska, seizmička, vulkanska, meteorološka, poplave)

  fizička oštećenja (vatra, prašina, korozija, smrzavanje ...)

  kompromitiranost podataka (presretanje signala, špijunaža podataka, socijalni inženjering, nedovoljno obrisani mediji, krađa podataka, otkrivanje podataka, virusi, slučajne ili namjerne ljudske pogreške ...)

  kompromitiranost funkcija (zloupotreba prava, krivotvorenje prava, uskraćivanje radnji ...)

  tehnički kvarovi (kvar uređaja, zasićenje informacijskog sustava, softverske smetnje ...)

  neovlaštene aktivnosti (neovlašten pristup sustavima, neovlašteno korištenje opreme, oštećenje podataka, ilegalna obrada podataka ...)

Ranjivost

- **Slabost bilo kojeg dijela imovine** organizacije ili **pojedine zaštitne mjere** (preventivne ili korektivne)

- **Nedostatak ili slabost sustava** u aspektima zadanih procedura i politika vezanih uz informacijsku sigurnost i kontinuitet poslovanja, ili njihovoj provedbi

Strateški rizici
Operativni rizici

- Imovina vs procesi
- Inherentni rizik
- Analiza korijenskog uzroka (*root-cause analysis*)
- Vjerojatnost i učinak
- Rangiranje ili skaliranje rizika
- Prioritizacija rizika
- Rezidualni rizik
- Učenje iz posljedica *(lessons-learned)*

Najčešći faktori rizika

IT/OT

IoT

Hardver – mreža – softver

Digitalna transformacija

work@home, remotework, telework

Usluge trećih strana

Najčešća područja rizika informacijske sigurnosti i otpornosti

Organizacija informacijske sigurnosti (Uloge i odgovornosti, Segregacija dužnosti)

Mobilni uređaji i rad na daljinu (*Telework, Remotework*)

Sigurnost ljudskih resursa (Prije zapošljavanja: *screening*, ugovorni uvjeti, Tijekom zaposlenja: odgovornosti, *infosec* edukacija i trening, disciplinski proces, Prekid i promjena zaposlenja: obveze odgovornosti vezanih uz *infosec* nakon završetka ili promjene u radnom odnosu)

Upravljanje imovinom (Popis informacijske imovine, vlasništvo, upotreba i povrat)

Klasifikacija informacija (Klasifikacija tajnosti, Označavanje informacija, Rukovanje informacijama)

Rukovanje medijima (Upravljanje prenosivim medijima, prenošenje i sigurno uklanjanje)

Kontrola pristupa (Poslovni zahtjevi za kontrolu pristupa informacijama, aplikacijama i mrežama, Upravljanje korisničkim pristupom: registracija i de-registracija, Odgovornost korisnika, Kontrola pristupa IT sustavima i aplikacijama)

Fizička sigurnost i sigurnost povezana s okolinom

Oprema

Sigurnost operacija (Radne procedure i odgovornosti, Zaštita od zloćudnog softvera, Sigurnosne kopije, Kreiranje logova i nadzor, Kontrola operacijskog softvera, Upravljanje tehničkim ranjivostima)

Sigurnost komunikacija (Upravljanje sigurnošću mreže, Prijenos informacija...)

Nabava, razvoj i održavanje sustava (Sigurnosni zahtjevi informacijskih sustava, osiguranje aplikacijskih usluga na javnim mrežama, zaštita transakcija aplikacijskih usluga; Ograničenja promjena softverskih paketa; Procedure kod promjena; Praćenje sigurnosti kod razvoja ustupljenog podizvođačima)

Upravljanje opskrbnim lancem (Politika informacijske sigurnosti za odnose s dobavljačima; Obrada sigurnosti unutar ugovornih klauzula, SLA i kontinuitet pružanja usluge)

Upravljanje incidentima informacijske sigurnosti (Odgovornosti i procedure, Izvještavanje i odgovori na incidente, Učenje na incidentima, Prikupljanje dokaza)

Aspekti informacijske sigurnosti upravljanja neprekinutošću poslovanja

Redundancija

Usklađenost sa zakonskim i ugovornim zahtjevima u opsegu informacijske sigurnosti (Identificiran obvezujući zakonski okvir i zahtjevi za zaštitu podataka, Intelektualno vlasništvo, Obveze kod upravljanja osobnim podacima...)

Politike i priručnici informacijske sigurnosti, standardizacija

...

Izvedeno iz ISO/IEC 27001:2022

Sigurnost ljudskih resursa

Rizici ljudskih resursa

- potencijalne sigurnosne **prijetnje i slabosti** koje su izravno **povezane s upravljanjem zaposlenicima** unutar organizacije
- **nedostatak odgovarajućih kompetencija i treninga te korištenja pravnih alata** vezanih uz sigurnosne protokole, što može dovesti do nenamjernih grešaka kao što su slanje povjerljivih podataka na nesigurne destinacije ili slabljenje sigurnosnih mjera kroz neoprezno upravljanje lozinkama ili opstrukciju funkcionalnosti sustava
- **neadekvatno postupanje s promjenama u radnoj snazi**, kao što su odlasci ili otpuštanja zaposlenika, gdje pristupi informacijama možda nisu pravilno ukinuti ili se događa neispravno rukovanje povjerljivim podacima

Rizici od ljudskih resursa

- potencijalne **namjerne štetne radnje** koje zaposlenici mogu poduzeti
- *insider* prijetnje gdje zaposlenici koji **imaju pristup** osjetljivim informacijama i sustavima **mogu svjesno** zloupotrijebiti svoje ovlasti, što rezultira krađom podataka, sabotiranjem sustava ili drugim zlonamjernim aktivnostima
- posebno opasni rizici jer zaposlenici obično **znaju kako zaobići postojeće sigurnosne mjere**

Određivanje protumjera

scenariji upravljanja rizicima prema ISO/IEC 27005

Modifikacija rizika (*Risk modification*) - treba odabrati **odgovarajuće i opravdane kontrole** kako bi se ispunili zahtjevi utvrđeni procjenom rizika pri njihovom tretmanu. Ovaj odabir također treba uze**ti u obzir troškove i vremenski okvir** za provedbu kontrola ili tehničke, ekološke i kulturološke aspekte.

Zadržavanje rizika (*Risk retention*) - ako razina rizika zadovoljava kriterije **prihvatljivosti rizika**, nema potrebe za provođenjem dodatnih kontrola i rizik se može zadržati. Zadržani rizik se tada iskazuje se kao rezidualni rizik.

Izbjegavanje rizika (*Risk avoidance*) - kada se identificirani rizici smatraju previsokima ili **troškovi provedbe** drugih opcija njihove obrade **premašuju koristi**, može se donijeti odluka o potpunom izbjegavanju rizika povlačenjem iz planirane ili postojeće aktivnosti ili niza aktivnosti ili promjenom uvjeta pod kojim se obavlja rizična aktivnost.

Podjela rizika (*Risk sharing*) - uključuje odluku o podjeli određenih rizika s **vanjskim stranama**. Podjela rizika **može stvoriti nove rizike** ili modificirati postojeće, već identificirane rizike, te stoga može biti potrebna dodatna obrada afektiranih rizika.
SLA se može koristiti u svrhu podjele rizika, kao i različite police osiguranja.

ISO/IEC izdvojeni kvalitativni alati za usklađivanje sa zahtjevima NIS2, DORA-e i CER-a

- **Sadržaj EU i nacionalne regulative vezane uz informacijsku sigurnost i otpornost oslanja se na zahtjeve propisane u ISO/IEC 27001 i ISO 22301**
- **ISO/IEC 27001 i ISO 22301 imaju i prateće standarde upravljanja rizicima, nadzora i uputa postupanja, NIST standardi mogu poslužiti i kao dopuna po potrebi**
- **Sektorske specifičnosti NIS2 i CER često definiraju smjernice ENISA-e, koje su u skladu sa zahtjevima standarda**
- **DORA RTS usklađeni s ISO/IEC 27001 i ISO 22301**
- **Akreditirana certifikacija**

ISO 27001

Informacijska sigurnost, kibernetička sigurnost i zaštita privatnosti – Sustavi upravljanja informacijskom sigurnošću

- Utvrđuje **zahtjeve** za uspostavljanje, primjenu, održavanje i kontinuirano poboljšanje sustava upravljanja **informacijskom i kibernetičkom sigurnošću te zaštitom privatnosti** u cijelom opsegu djelokruga organizacije
- **Sadrži set konkretnih kontrola i zahtjeva za procjenu i postupanje s rizicima informacijske sigurnosti**
- Namijenjen primjeni na **sve organizacije**, bez obzira na vrstu, veličinu ili prirodu poslovanja/sektor djelovanja

ISO 22301

Sigurnost i otpornost – Sustavi upravljanja neprekinutošću poslovanja

- Utvrđuje zahtjeve za primjenu, održavanje i poboljšanje sustava upravljanja **kontinuitetom poslovanja** radi **zaštite od ugroza** te **smanjenja vjerojatnosti pojave ugroze, pripreme i odgovora te oporavka od ugroza**
- **Opseg primjene** zahtjeva ovisi o prirodi procesa, složenosti regulatornog okruženja, operativnom okruženju i složenosti same organizacije.
- Namijenjen primjeni na **sve organizacije**, bez obzira na vrstu, veličinu ili prirodu poslovanja/sektor djelovanja

IEC 62443

Industrial Cyber Security

- Definira zahtjeve za uspostavljanje, primjenu, održavanje i kontinuirano **unaprjeđenje sigurnosnih mjera za industrijske automatizacijske i kontrolne sisteme**
- Uključuje **specifičan set sigurnosnih kontrola i zahtjeva** za procjenu i upravljanje rizicima povezanim s industrijskim kontrolnim sistemima
- Primjenjiv na **sve vrste organizacija** koje se bave industrijskom automatizacijom, bez obzira na njihovu veličinu, vrstu ili sektor industrije
- **Obitelj standarda IEC 62443** osigurava da industrijski sistemi, **uključujući SCADA sisteme**, **distribuirane kontrolne sisteme (DCS) i druge vrste kontrolnih sistema**, budu zaštićeni od kibernetičkih prijetnji i mogućih sigurnosnih incidenata.

Zahvaljujem na pažnji :)

dr. sc. Natalija Parlov Una
Authorised IRCA Lead Tutor & Senior Lead Certification Auditor

direktni kontakt: una@apicura.hr
linkedin: natalijaparlovuna