TREĆA NACIONALNA KONFERENCIJA NKS-a

KIBERNETIČKA SIGURNOST

ČOVJEK U SREDIŠTU

NKS NACIONALNO KOORDINACIJSKO SREDIŠTE

CARNET

NCSC HR

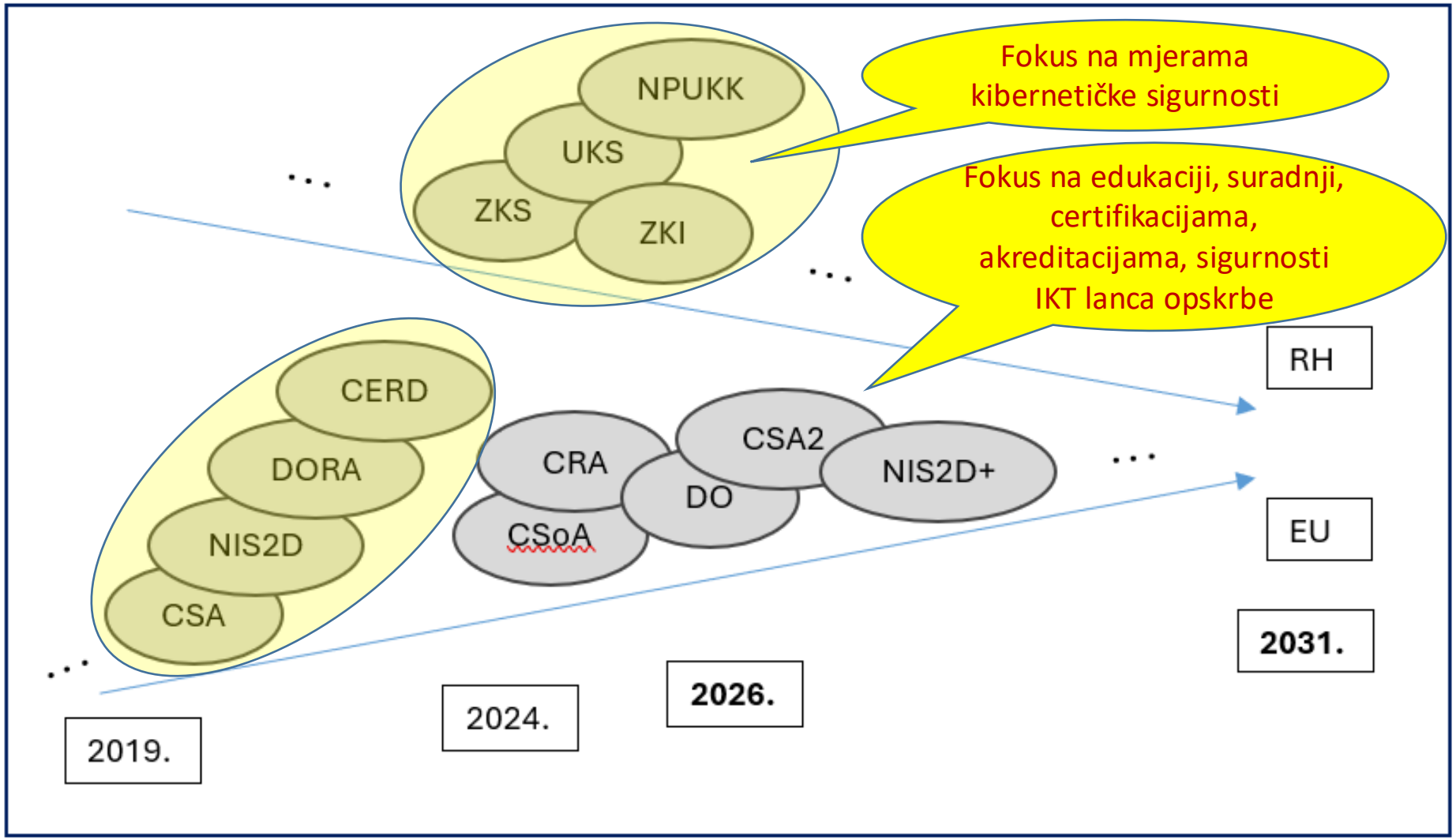
Zakonodavni okvir kao temelj kibernetičke otpornosti

dr. sc. Aleksandar Klaić, dipl. ing.

Nacionalni centar za kibernetičku sigurnost

Okvir Zakona o kibernetičkoj sigurnosti (ZKS):

Ilustracija zakonodavnog eko sustava kibernetičke sigurnosti u RH i EU



RH:
ZKS = Zakon o kibernetičkoj sigurnosti,
UKS = Uredba o kibernetičkoj sigurnosti,
NPUKK = Nacionalni program upravljanja kibernetičkim krizama,
ZKI = Zakon o kritičnoj infrastrukturi,

EU:
CSA = Cyber Security Act,
NIS2D = Network and Information Security Directive,
DORA = Digital Operational Resilience Act,
Critical Entities Resilience Directive,
CSoA = Cyber Solidarity Act,
CRA = Cyber Resilience Act,
DO = Digital Omnibus,
CSA2 = Cyber Security Act 2,
NIS2D+ = Ammandements to Network and Information Security Directive.

Mrežna stranica NCSC-HR - www.ncsc.hr

NCSC HR Nacionalni centar za kibernetičku sigurnost

Republika Hrvatska
Sigurnosno–obavještajna agencija

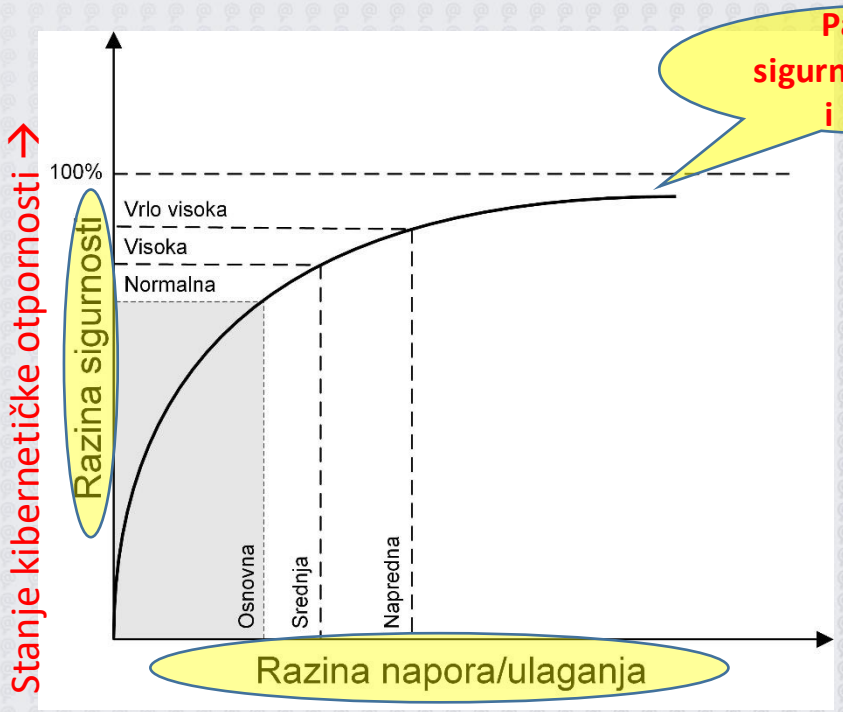
Naslovnica | Novosti | Sigurnosna upozorenja | SK@UT | Dokumenti | Česta pitanja | O nama | Kontakt | EN

Nacionalni centar za kibernetičku sigurnost

Nacionalni centar za kibernetičku sigurnost (NCSC-HR) ustrojen je u okviru Sigurnosno-obavještajne agencije (SOA) s ciljem zaštite nacionalnog kibernetičkog prostora te obavljanje zadaća središnjeg državnog tijela za kibernetičku sigurnost, nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti, CSIRT-a, tijela odgovornog za upravljanje kibernetičkim krizama i jedinstvene kontaktne točke prema Zakonu o kibernetičkoj sigurnosti.

Saznajte više

Kibernetička sigurnost i kibernetička otpornost



Paradoks sigurnosnih mjera i politika

Države u kojima će postojati pravne osobe „poslovni pobjednici" u novom desetljeću:
- Kibernetička sigurnost dio nacionalne sigurnosti i otpornosti društva u cjelini

Pravne osobe „poslovni pobjednici" u novom desetljeću:
- Kibernetička sigurnost integrirana u poslovanje
- Upravljaju lancem opskrbe
- Kontinuirano procjenjuju rizike

2015

- Najbolje prakse kibernetičke sigurnosti
- Strategije kibernetičke sigurnosti

2025

- Zakonski okvir kibernetičke sigurnosti
- Organizacija i upravljanje
- Procjene rizika

2030

- Akreditacije / certifikacije
- Proizvodi s digitalnim elementima (PDE)
- IKT lanac opskrbe

Čovjek u središtu kibernetičke sigurnosti - edukacija

- Čovjek provodi proces kibernetičke sigurnosti
  - Koristi rezultate tog procesa - kibernetičku otpornost
- Čovjek i kibernetički prostor

Osjetila čovjeka prilagođena su fizičkom prostoru i neposrednoj komunikaciji s ljudima

- Uloge čovjeka u politikama kibernetičke sigurnosti:
  - Odgovorne osobe
  - Operativni nositelji
  - Ostali
    - IT osoblje
    - Osoblje u poslovnim djelatnostima

Sigurnosna svijest
Znanje
Procjena rizika

- Nužnost različitih pristupa edukaciji osoblja prema njihovim ulogama

Edukacija kibernetičke sigurnosti

- Pravna edukacija – **procedura i zahtjevi**
  - „čitanje članaka” ZKS-a
  - Sažetak zakonskih obaveza – obavijest o kategorizaciji po ZKS-u
  - UKS s prilozima, upute i smjernice
- **Razvoj sigurnosne svijesti**
  - Periodični tečajevi – interni ili vanjski
  - Prate stanje kibernetičke sigurnosti i razvoj tehnologije
  - Profilirani za uloge osoblja
- **Norme i najbolje prakse, tehnički certifikati - znanje**
  - ISO 27001, 27005, NIST CSF, . . .
  - CISSP, ISACA, globalne kompanije, . . .
- **Modeli i okviri – razumijevanje**
  - Cyber Kill Chain, Diamond Model, MITRE ATT&CK, . . .

ZAHTJEVI ZKS i RAZRADA UKS – prilog II.

Mjere kibernetičke sigurnosti

ZKS, članak 30.

– korištenje višefaktorske provjere autentičnosti ili rješenja kontinuirane provjere autentičnosti, zaštićene glasovne, video i tekstualne komunikacije te sigurnih komunikacijskih sustava u hitnim slučajevima unutar subjekta, prema potrebi.

PRILOG II

MJERE UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA

1. Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima
2. Upravljanje programskom i sklopovskom imovinom
3. Upravljanje rizicima
4. Sigurnost ljudskih potencijala i digitalnih identiteta
5. Osnovne prakse kibernetičke higijene

5.3. uz provedbu politike korištenja lozinki, implementirati višefaktorsku autentifikaciju (MFA) za kritične mrežne i informacijske sustave koji su više izloženi potencijalnim kibernetičkim napadima. Primjena MFA je potrebna na VPN pristupu, SaaS alatima dostupnim s Interneta itd. Potrebno je osigurati da se korisnička imena i lozinke korištene na servisima s dvofaktorskom autentifikacijom ne koriste na drugim servisima bez dvofaktorske autentifikacije. Snaga provjere autentičnosti mora biti usklađena s procjenom rizika i izloženosti mrežnog i informacijskog sustava. Potrebno je uzeti u obzir višefaktorsku provjeru autentičnosti prilikom pristupanja kritičnim mrežnim i informacijskim sustavima s udaljene lokacije, sustavima za administriranje korisnika i mrežnih i informacijskih sustava, kritičnim podacima subjekta itd. Višefaktorska provjera autentičnosti se može kombinirati s drugim tehnikama kako bi se zahtijevali dodatni faktori u specifičnim okolnostima, temeljeno na unaprijed definiranim pravilima i obrascima, poput pristupa s neuobičajene lokacije, s neuobičajenog uređaja ili u neuobičajeno vrijeme.

Smjernice s mapiranjem normi i najboljih praksi na mjere iz Uredbe, www.ncsc.hr - lipanj 2025.

ISO/CIS/ETSI/NIST . . .

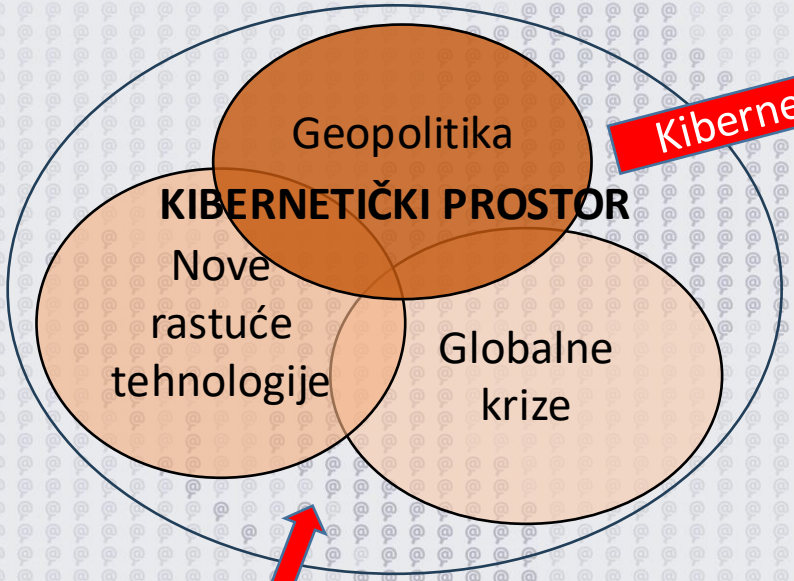
Korišteno ili odabrano tehničko rješenje

SIGURNOSNA SVIJEST i procjena rizika na nacionalnoj razini:

Smjernice i kalkulator na www.ncsc.hr

Kibernetički napadači

- Državno sponzorirane APT grupe
- Teroristi
- Kibernetički kriminalne grupe
- Haktivističke grupe
- Poslovni konkurenti



Kibernetički ciljevi

Obilježja kibernetičkih ciljeva

Vrste entiteta:
- Državna tijela
- Kritična infrastruktura
- Pravne osobe
- Građanstvo

Obilježja entiteta:
- Veličina
- Sektor
- Utjecaj poremećaja

Razina	Podskupovi mjere								
	2.1.	2.2.	2.3.	2.4.	2.5.	2.6.	2.7.	2.8.	2.9.
osnovna	A	A	A	A	A	C	C	C	C
srednja	A	A	A	A	A	A	A	C	C
napredna	A	A	A	A	A	A	A	A	A

Tri razine mjera kibernetičke sigurnosti:

1. Osnovna
2. Srednja
3. Napredna

Kibernetički napadi

- Poremećaj poslovanja/Sabotaža
- Krađa podataka/špijuniranje
- Kibernetički kriminal (RW, financijske prijevare)
- Vandalizam sadržaja i dostupnosti na Internetu
- Politički utjecaj i dezinformacije

Nacionalna procjena kibernetičkih sigurnosnih rizika

Prepoznavanje različitih:
- Profila rizika (sektori)
- Utjecaja (napadi)
- Razina rizika (subjekti)

NORME - informacijska i kibernetička sigurnost

SUBJEKT ZKS-a

INFORMACIJSKA SIGURNOST

Zaštita podataka u fizičkom i elektroničkom obliku

IT SIGURNOST

Zaštita mrežnih i informacijskih sustava

KIBERNETIČKA SIGURNOST

Zaštita IT imovine i korisnika od kibernetičkih ugroza

Government Security Policy

Ljudi, procesi, tehnologija

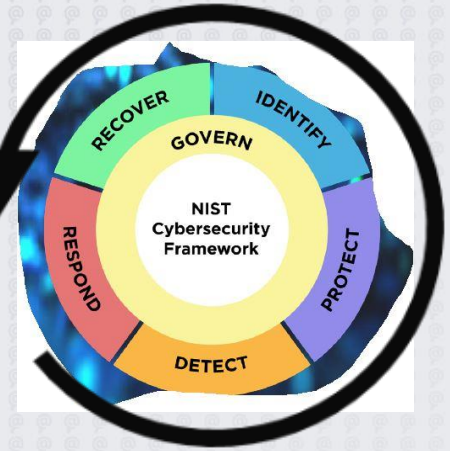
Plan, Do, Check , Act

ISO/IEC 27001:2022 + 27110, ...

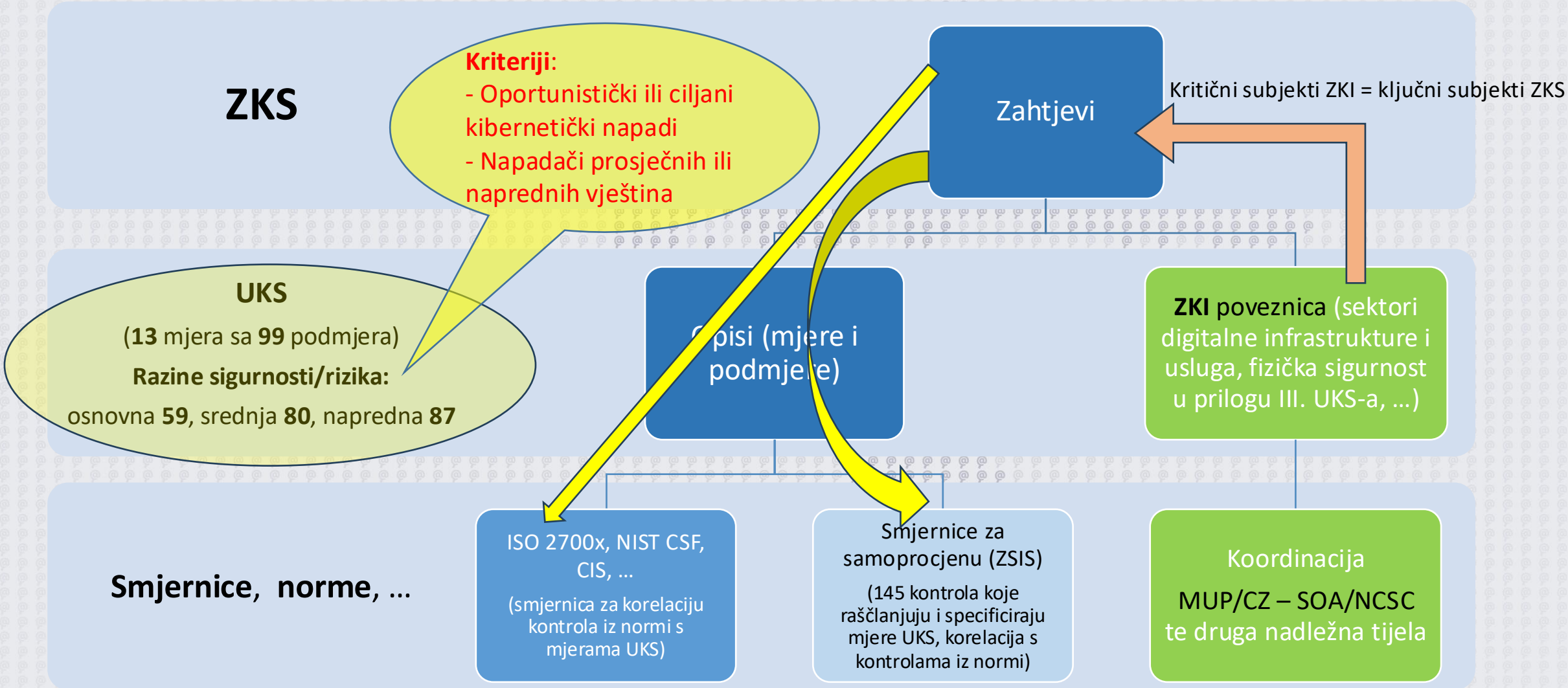
- People (8 controls),
- Organizational (37 controls),
- Technological (34 controls),
- Physical (14 controls).

- ETSI TR 103 305-1 Critical Security Controls for Cyber Defence (09/2018)
- CIS Controls
- ISA/IEC 62443 / NIST SP 800-82 Rev. 3

US NIST CSF 2.0



NAČIN PROVEDBE MJERA iz ZKS/UKS i poveznica sa ZKI



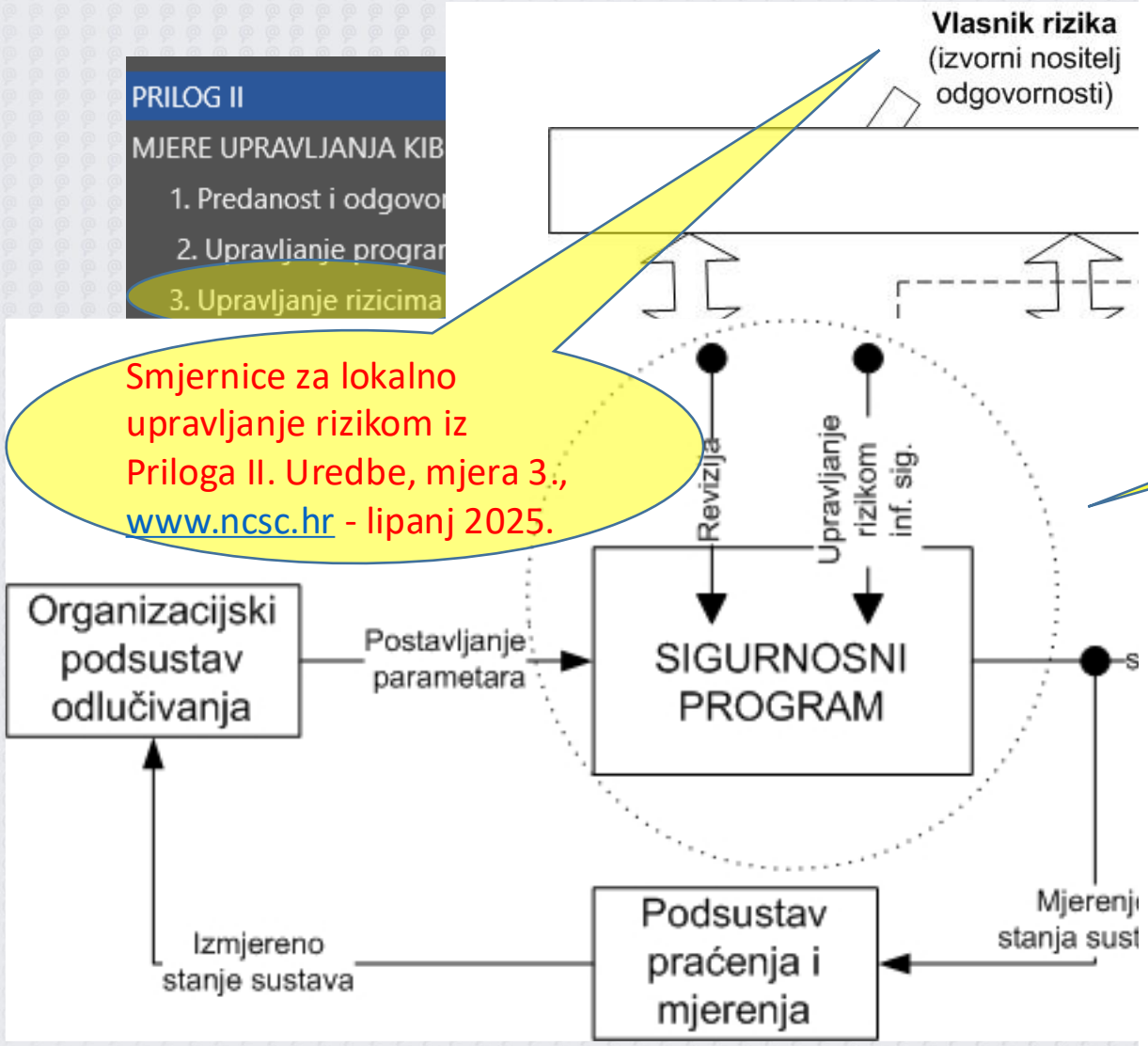
PROCJENA RIZIKA - Uredba o kibernetičkoj sigurnosti i lokalno upravljanje rizicima koje provode subjekti (All-Hazards-Approach)

PRILOG II

MJERE UPRAVLJANJA KIB

1. Predanost i odgovor
2. Upravljanje prograr
3. Upravljanje rizicima

Smjernice za lokalno upravljanje rizikom iz Priloga II. Uredbe, mjera 3., www.ncsc.hr - lipanj 2025.



Tablica 1. – Primjeri tipičnih prijetnji:

R.br.	Kategor
1.	Fizičke p
2.	
3.	
4.	
5.	
6.	
7.	Prirodne
8.	
9.	
10.	
11.	Kvarovi i
12.	
13.	
14.	
15.	
16.	
17.	Ljudske
18.	
19.	

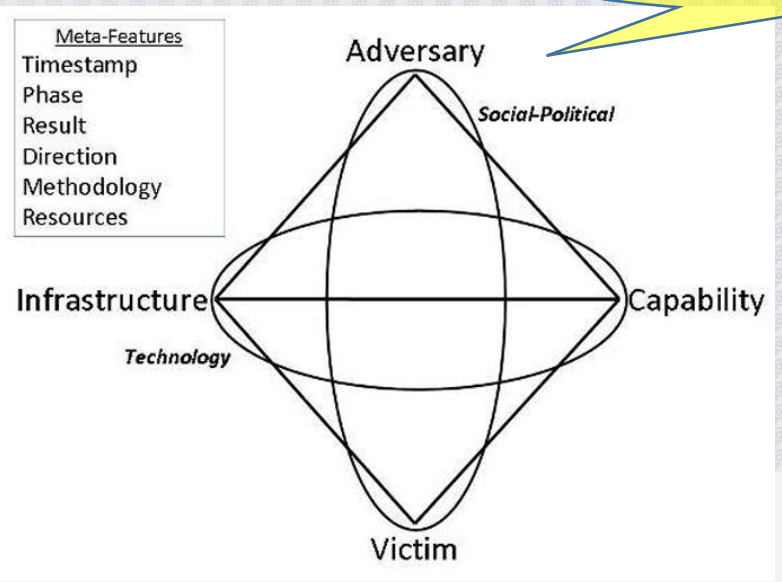
Tablica 2. – Primjeri tipičnih ranjivosti:

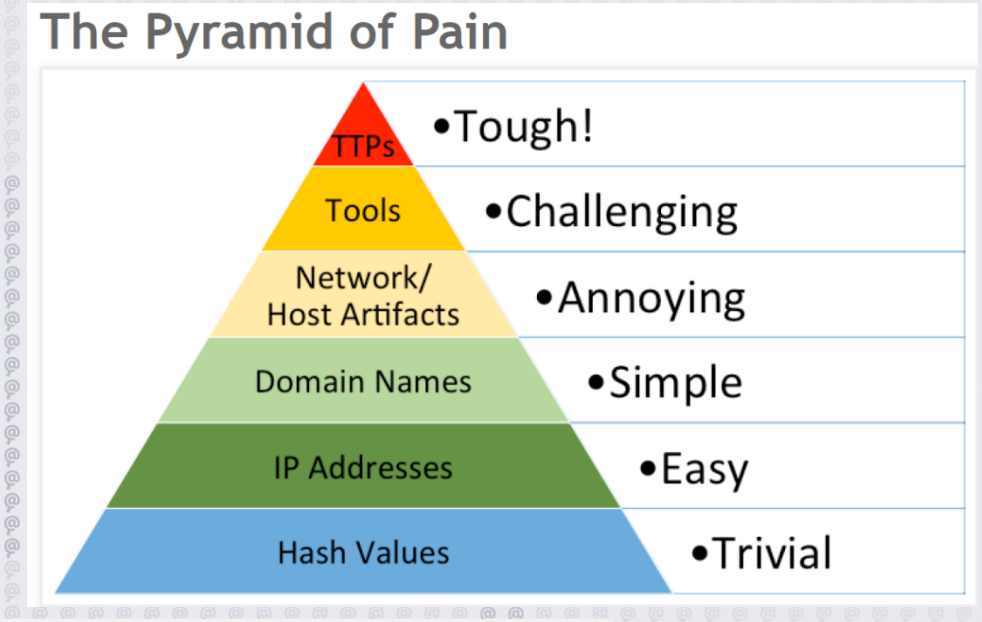
R.br.	Kategorija	Ranjivost
1.	Sklopovske ranjivosti	Nedovoljno održavanje/neispravna instalacija medija za pohranu
2.		Nedovoljne sheme za periodičnu zamjenu opreme
3.		Osjetljivost na vlagu, prašinu, prljavštinu
4.		Osjetljivost na elektromagnetsko zračenje
5.		Nedovoljna kontrola promjena konfiguracije
6.		Osjetljivost na naponske promjene
7.		Osjetljivost na temperaturne promjene
8.		Nezaštićena pohrana
9.		Nekontrolirano bacanje dotrajalih uređaja
10.	Programske ranjivosti	Nedostatno ili nepostojeće testiranje programske podrške
11.		Dobro poznati nedostaci u softveru
12.		Neodjavljivanje prilikom napuštanja radne stanice
13.		Bacanje ili ponovno korištenje podatkovnih medija bez prikladne procedure brisanja
14.		Nedovoljna konfiguracija dnevničkih zapisa potrebnih za praćenje ispravnosti rada mrežnog i informacijskog sustava
15.		Pogrešna dodjela prava pristupa
16.		Korištenje aplikativnih programskih rješenja s visokim privilegijama za pristup podacima u nepredviđenim vremenskim okvirima
17.		Složeno korisničko sučelje

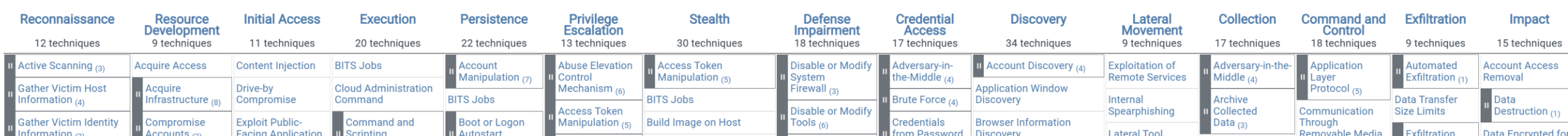
NIST IR 8286r1 (12/2025)
Integrating Cybersecurity and Enterprise Risk Management (ERM)

MODELI I OKVIRI kibernetičke sigurnosti - razumijevanje problematike

- Cyber Kill Chain
- Diamond Model
- MITRE ATT&CK



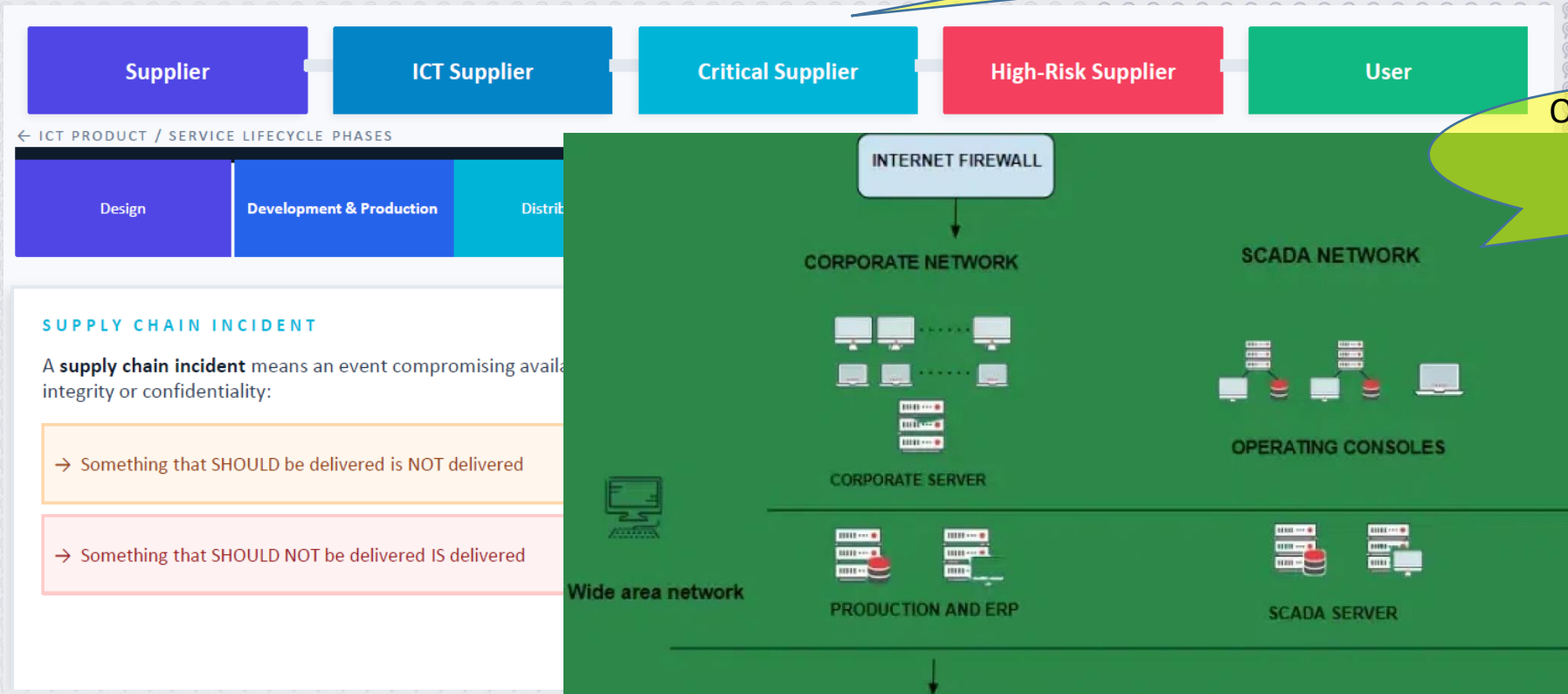




Teme od užeg interesa aktualnih kibernetičkih sigurnosnih politika

- IKT lanac nabave (UKS, Prilog II., mjera 8.)
- Sigurnost operativne tehnologije (OT)

- Usvojen paket mjera za sigurnost lanca opskrbe IKT usluga | NCSC-HR (EU, 02/2026.)
- Prijedlog **CSA2** Komisije iz 01/2026



Operativna tehnologija (OT)

- ISA/IEC 62443
- NIST SP 800-82 Rev. 3

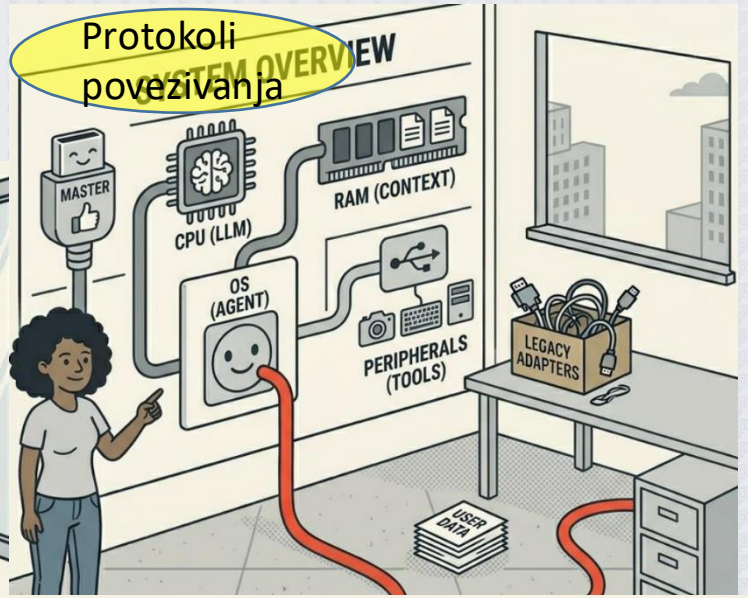
Nove tehnologije i kibernetička sigurnost

- Velike tehnološke promjene i kibernetička sigurnost:
  - Internet -> Mobilna tehnologija -> Umjetna inteligencija
    - Povećanje opsega korištenja (masovnost)
    - Rast izloženosti korisnika napadima (dijeljena tehnologija)
    - Ubrzani razvoj tehnologije (ranjivosti)
- Kibernetički napadi
  - Slične tehnike -> Različita izloženost korisnika -> Profiliranost napada
- Negativna psihologija ljudi:
  - „Zašto učiti danas nešto što već sutra neće vrijediti?”
- Činjenica:
  - ISO 27001 primjenjiv je **2026.g.**, a nastao je iz BS 7799 davne **1995.g.**

Nove tehnologije i kibernetička sigurnost

- Velike tehnološke p
  - Internet -> Mobilna
    - Povećan
    - Rast izlo
- Kib

Protokoli povezivanja



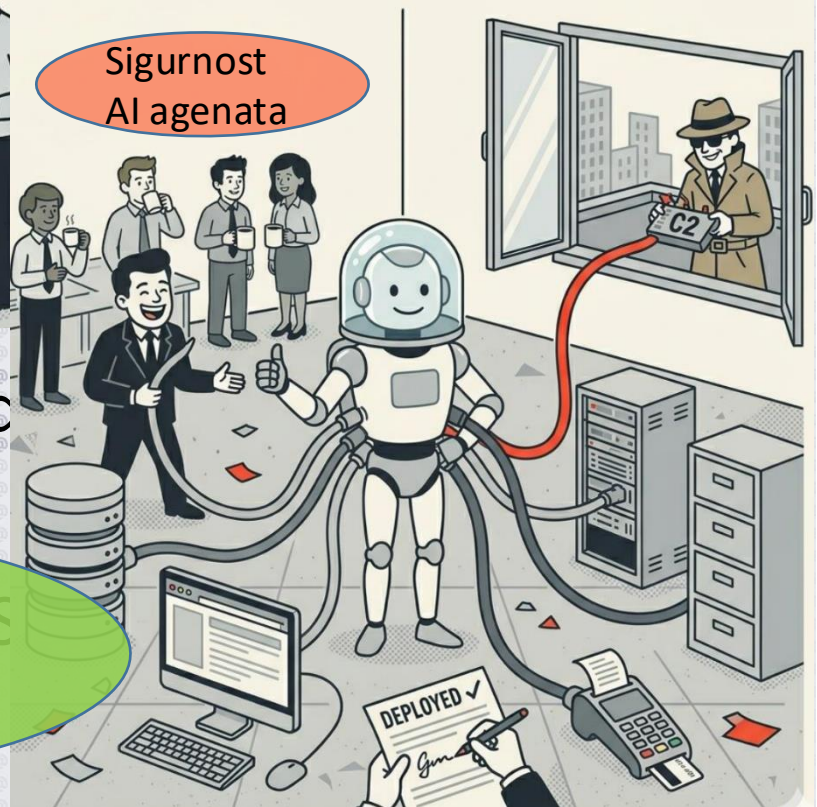
Povjerljivi podatci

Socijalni inženjering

Ugroze infrastrukture

Manipulacija podacima

Sigurnost AI agenata



MITRE ATLAS™
Adversarial **T**hreat **L**andscape for **A**rtificial-**I**ntelligence **S**ystems

Hvala na pažnji.

info@ncsc.hr