KONTROLA
ZRAČNEGA
PROMETA
SLOVENIJE

OPERATIVNO ZAGOTAVLJANJE SKLADNOSTI Z ZAHTEVAMI PART IS

KONTROLA ZRAČNEGA PROMETA SLOVENIJE

ID 220

IS.I.OR.220 Informacijsko-varnostni incidenti – zaznavanje, odzivanje in sanacija

- A)
- Organizacija na podlagi rezultata ocene tveganja, izvedene v skladu s točko IS.I.OR.205, in rezultata obravnave tveganja, izvedene v skladu s točko IS.I.OR.210,

izvaja ukrepe za zaznavanje incidentov in ranljivosti, ki kažejo morebitno uresničitev nesprejemljivih tveganj

- in ki bi lahko vplivali na varnost v letalstvu.
- Navedeni ukrepi za zaznavanje organizaciji omogočajo, da: (1) opredeli odstopanja od vnaprej določenih izhodišč za funkcionalno učinkovitost; (2) sproži opozorila za aktiviranje ustreznih odzivnih ukrepov v primeru kakršnega koli odstopanja.

KONTROLA ZRAČNEGA PROMETA SLOVENIJE

ID 220

IS.I.OR.220 Informacijsko-varnostni incidenti – zaznavanje, odzivanje in sanacija

- B)
- Organizacija izvaja **ukrepe za odziv** na kakršne koli dogodke, opredeljene v skladu s točko (a),

- **ki so prerasli v informacijskovarnostni incident ali bi vanj lahko prerasli.**

Navedeni ukrepi za odzivanje organizaciji omogočajo, da: (1) sproži odziv na opozorila iz točke (a)(2) z aktiviranjem vnaprej določenih virov in potekov ukrepov; (2) zajezi širjenje napada in prepreči, da bi se scenarij grožnje v celoti uresničil; (3) nadzira vrsto okvare prizadetih elementov, opredeljenih v točki IS.I.OR.205(a).

KONTROLA ZRAČNEGA PROMETA SLOVENIJE

POJMI

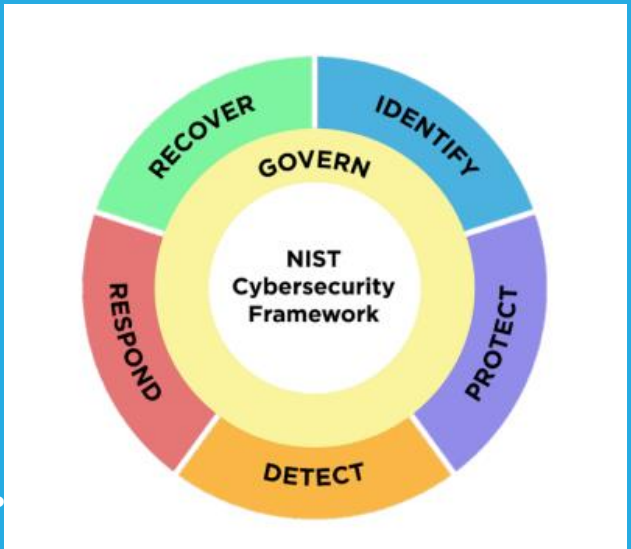
- **„informacijsko-varnostni dogodek**“ pomeni ugotovljen dogodek stanja sistema, storitve ali omrežja, **ki kaže na morebitno kršitev politike informacijske varnosti** ali neuspeh pri kontrolah informacijske varnosti ali na predhodno neznane razmere, ki so lahko pomembne za informacijsko varnost

- **„incident“** pomeni vsak dogodek, ki **dejansko negativno vpliva** na varnost omrežij in informacijskih sistemov, kot so opredeljeni v členu 4(7) Direktive (EU) 2016/1148

- **grožnja“** pomeni morebitno kršitev informacijske varnosti, ki nastane zaradi subjekta, okoliščine, dejanja ali dogodka, ki bi lahko povzročil škodo;

NIST - CSF 2.0

- Vir; [The NIST Cybersecurity Framework (CSF) 2.0]



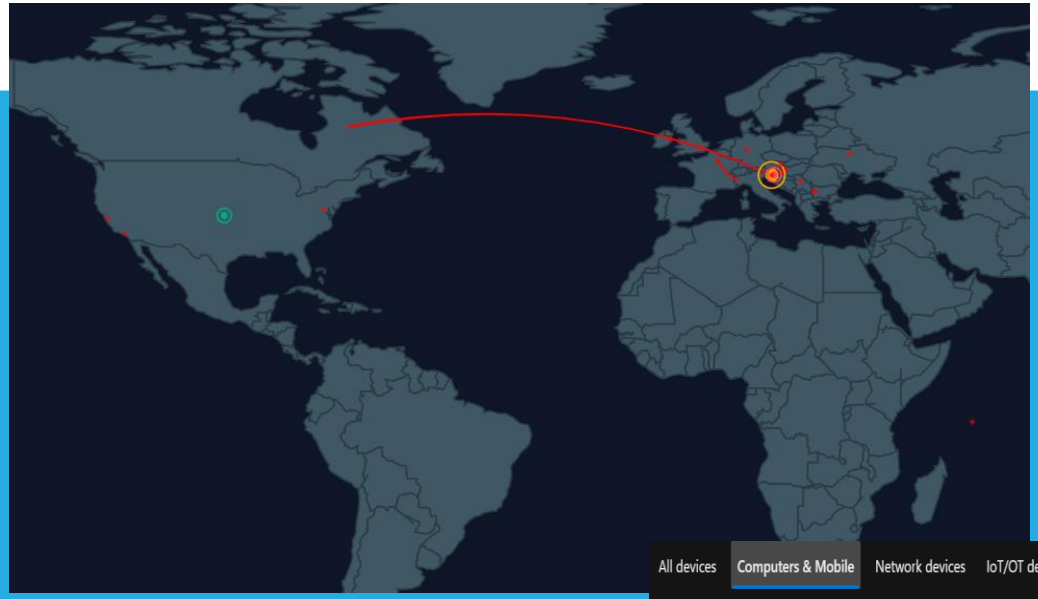
in EASA AMC in GM to Part IS.OR ISSUE 1

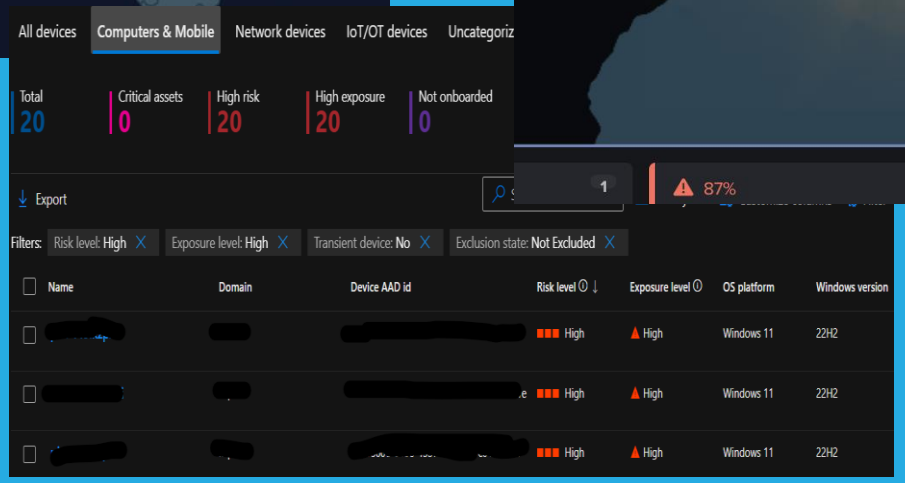
ISO/IEC 27001		
Paragraph Clause	Annex A Control	
	:2013	:2022
	A11.1.2	A7.2
	A12.4.1	A8.8
	A12.6.1	A8.15
	A16.1.1	A8.16
	A16.1.2	A5.24
	A16.1.3	A5.25
	A16.1.4	A5.26
	A16.1.5	A6.8

A 8.8: Man. of tech. vul,
A8.15 Logging

KONTROLA ZRAČNEGA PROMETA SLOVENIJE

DETEKCIJA / ODKRIVANJE





SIEM, SOC, EDR, XDR, NDR

KONTROLA ZRAČNEGA PROMETA SLOVENIJE

RANLJIVOSTI

- Brez poseganja v obveznosti iz Uredbe (EU) št. 376/2014 organizacija zagotovi, da se o vsakem informacijskovarnostnem incidentu **ali ranljivosti, ki lahko pomeni znatno tveganje za varnost v letalstvu**, poroča njenemu pristojnemu organu.

- Poleg tega: (1) kadar tak incident ali ranljivost vpliva na zrakoplov ali z njim povezan sistem ali komponento, organizacija o tem poroča tudi nosilcu odobritve projekta; (2) kadar tak incident ali ranljivost vpliva na sistem ali komponento, ki jo uporablja organizacija, organizacija o tem poroča organizaciji, odgovorni za projektiranje sistema ali komponente

KONTROLA ZRAČNEGA PROMETA SLOVENIJE

UPRAVLJANJE RANLJIVOSTI

- **ranljivost“** pomeni hibo ali pomanjkljivost v sredstvu ali sistemu, postopkih, zasnovi, izvajanju ali ukrepih za informacijsko varnost, ki bi jih bilo mogoče izkoristiti in katerih posledica je kršitev politike informacijske varnosti

- Kršitev CIA / ZCR triade

KONTROLA ZRAČNEGA PROMETA SLOVENIJE

SPREMLJANJE / OBVALDOVANJE TEHNIČNIH RANLJIVOSTI

- Spremljanje / obvladovanje tehničnih ranljivosti;
  - ISO / IEC 27002:2022 - 8.8 Management of technical vulnerabilities
  - ISO / IEC 27002:2022 - 5.9 Inventory of information and other associated assets
- Zagotavljati varnost pri pridobivanju, razvoju in vzdrževanju omrežnih in informacijskih sistemov, vključno z obravnavanjem in razkrivanjem ranljivosti
- SPREMLJANJE NAPADALNE POVRŠINE / ATTACK SURFFACE MANAGEMENT

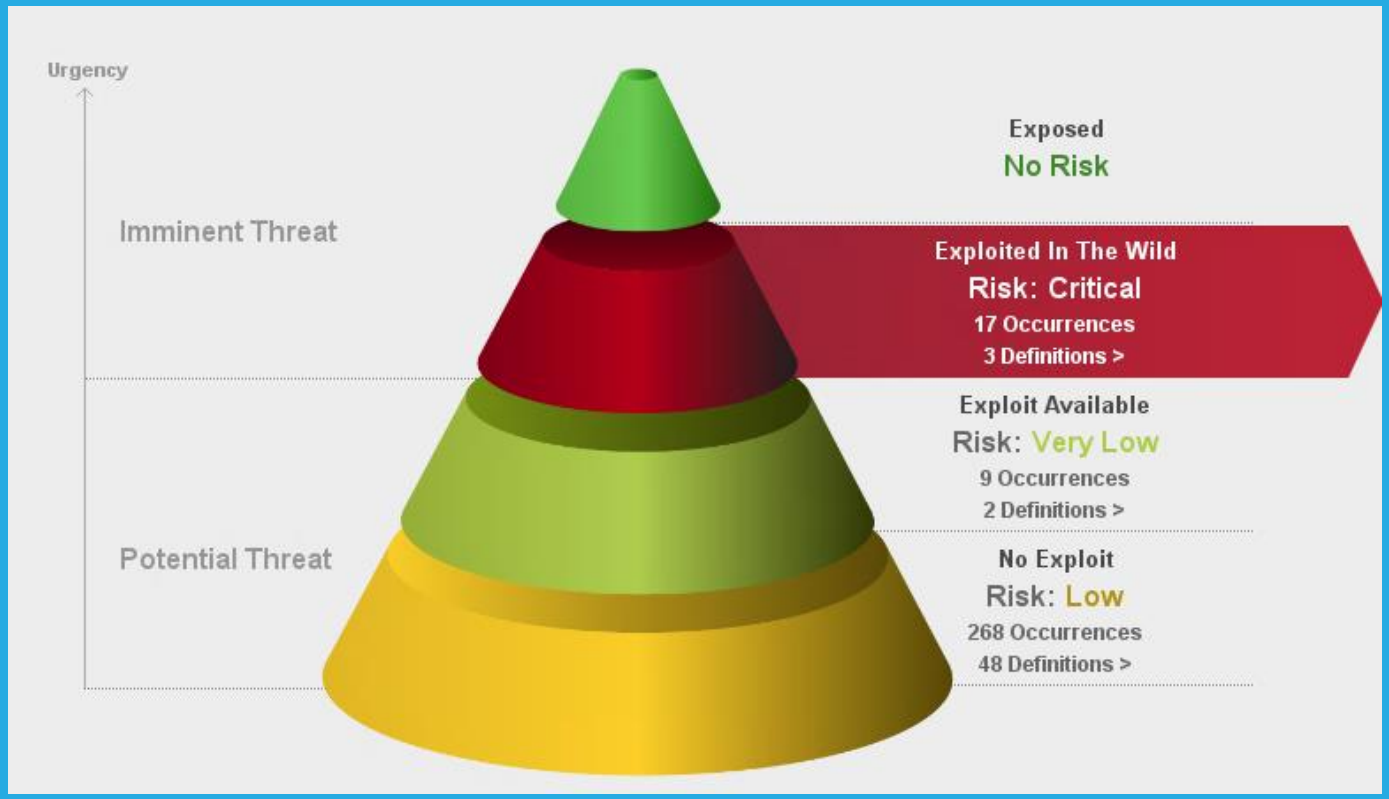
KONTROLA ZRAČNEGA PROMETA SLOVENIJE

RANLJIVOSTI IT / OT SISTEMOV

ID	RISK	VULNERABILITY	RISK RATING
R1	Exploitation of unpatched system vulnerabilities	Security patches are not installed	High
R3	TLS communication decryption	Vulnerable versions of TLS and/or weak encryption algorithms within TLS are supported.	Medium

KONTROLA ZRAČNEGA PROMETA SLOVENIJE

SISTEM ZA UPRAVLJANJE RANLJIVOSTI



KONTROLA ZRAČNEGA PROMETA SLOVENIJE

- Vprašanja?