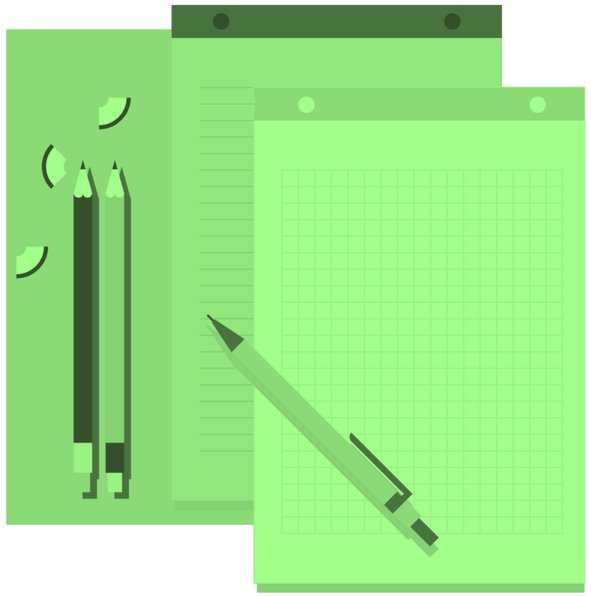
Informacijska i kibernetička sigurnost u poslovnom okruženju logistike i transporta

Vlatko Košturjak
Tehnički direktor

Agenda



- Uvod
- Incidenti i primjeri globalno
- Incidenti u Hrvatskoj
- Obrana
- Sustav upravljanja
- Pitanja i odgovori

IRAN'S RAIL SERVICE DELAYED WITH FAKE MESSAGES	07/02/2021	• Iran's railroad system	• Meteor • Hacker Attack	• Indra	OT IT	• Iran
RANSOMWARE HITS MA FERRY SERVICE	06/02/2021	• Woods Hole, Martha's Vineyard and Nantucket Steamship Authority	NO MALWARE IDENTIFIED	NO THREAT SOURCE IDENTIFIED		• United States
AIR INDIA: HACK LEAKED PASSENGERS' DATA	02/21/2021	• Air India	NO MALWARE IDENTIFIED	NO THREAT SOURCE IDENTIFIED		• India
FRENCH BOAT MAKER, BENETEAU, HIT BY CYBERATTACK	02/18/2021	• Beneteau	NO MALWARE IDENTIFIED	NO THREAT SOURCE IDENTIFIED	OT	• France
RANSOMWARE HITS VANCOUVER'S TRANSLINK	12/01/2020	• Translink	• Egregor	NO THREAT SOURCE IDENTIFIED		• Canada
GLOBAL TRANSPORTATION COMPANY HAS MULTIPLE SERVERS AND INTRANET TAKEN DOWN BY ATTACK	10/01/2020	• International Maritime Organization	NO MALWARE IDENTIFIED	NO THREAT SOURCE IDENTIFIED		• Global
CMA CGM SA SHUTDOWN AFTER ATTACK WITH RANSOMEWARE	09/28/2020	• CMA CGM	• Ragnar Locker	NO THREAT SOURCE IDENTIFIED		• Asia-Pacific
MAERSK RANSOMWARE ATTACK	09/27/2020	• Maersk	• NotPetya	• Russia	IT	• Global • United States
ATTACK AT NORTHERN TRAIN.	07/14/2021	• Northern Trains Limited	NO MALWARE IDENTIFIED	NO THREAT SOURCE IDENTIFIED	IT	• United Kingdom

Primjeri

Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks

Maersk was hit by a worm dubbed NotPetya, which locked access to systems that the company uses to operate shipping terminals all over the world. Above, containers at a terminal in Germany in 2010. (Patrik Stollarz / AFP/Getty Images)

PRO CYBER NEWS

Expeditors International Shuts Down Computer Systems After Cyberattack

The logistics giant hasn't said when it will fully restore operations.

Expeditors International, which is based near the Port of Seattle, pictured here, was hit by a cyberattack that could put more stress on already fragile global supply chains.
PHOTO: DAVID RYDER/BLOOMBERG NEWS

By *Nicolle Liu*
Feb. 22, 2022 4:47 pm ET

MOST POPULAR NEWS

1. Russia Targets Ukrainian Civilian Areas in Tactical Shift and Strikes Kyiv TV Tower
2. When Is Biden's State of the Union? What to Know
3. Cargo Ship Carrying Thousands of Luxury Cars Sinks in the Atlantic
4. Ukraine Crisis Kicks Off New Superpower Struggle Among U.S., Russia and China
5. Car Dealerships Don't Want Your Cash—They Want to Give You a Loan

MOST POPULAR OPINION

1. Opinion: Marjorie Taylor Greene Plays Dumb
2. Opinion: The Economic Price of Putin's Invasion

Susjedstvo

Rusija dodala i Hrvats
neprijateljskih zemalj

Piše 24sata, petak, 22.7.2022. u 10:48

Foto: SPUTNIK/REUTERS

Vlada je ažurirala popis stranih država uključenil
aktivnosti usmjerene protiv ruskih veleposlanstava i konzulata u
inozemstvu

securityweek.com/fbis-team-investigate-massive-cyberattack-montenegro

sometimes | jaj | images | security | js | misc

AP

FBI's Team to Investigate Massive Cyberattack in Montenegro

By Associated Press on August 31, 2022

Share Tweet RSS

A rapid deployment team of FBI cyber experts is heading to Montenegro to investigate a **massive and coordinated attack on the tiny Balkan nation's government** and its services, the country's Ministry of Internal Affairs announced Wednesday.

"This is another confirmation of the excellent cooperation between the United States of America and Montenegro and a proof that we can count on their support in any situation," the ministry said of the deployment of the Cyber Action Team.

Other Eastern European states deemed enemies of Russia have recently also sustained cyberattacks, mostly nuisance-level denial of service campaigns, in recent weeks. Targets have included networks in Moldova, Slovenia, Bulgaria and Albania.

https://www.securityweek.com/fbis-team-investigate-massive-cyberattack-montenegro

Incidenti

INCIDENT	DATE	VICTIM	MALWARE	THREAT SOURCE	IMPACTS	COUNTRY
INA GROUP CYBER ATTACK	02/14/2020	• INA Group	• CLOP	NO THREAT SOURCE IDENTIFIED		• Croatia

ina.hr/obavijest-o-kibernetickom-napadu/

news sometimes jaj images security js misc

INA O kompaniji Kup

INA, d.d. > Vijesti > Obavijest o kibernetičkom napadu

21.02.2020.

Poštovani,

INA Grupa u procesu je otklanjanja poteškoća u informatičkim sustavima na koje je utjecao kibernetički napad koji se dogodio krajem prošlog tjedna. Započeli smo s oporavkom sustava te radimo na ponovnoj uspostavi svih usluga koje povremeno nisu radile.

Kao što je ranije napomenuto, kibernetički napad prijavljen je mjerodavnim institucijama s kojima INA u potpunosti surađuje. Napad i mogući neovlašteni pristup podacima se istražuje. Kao i kod svakog kibernetičkog napada, u ovom trenutku ne možemo isključiti mogućnost da je došlo i do neovlaštenog pristupa osobnim podacima.

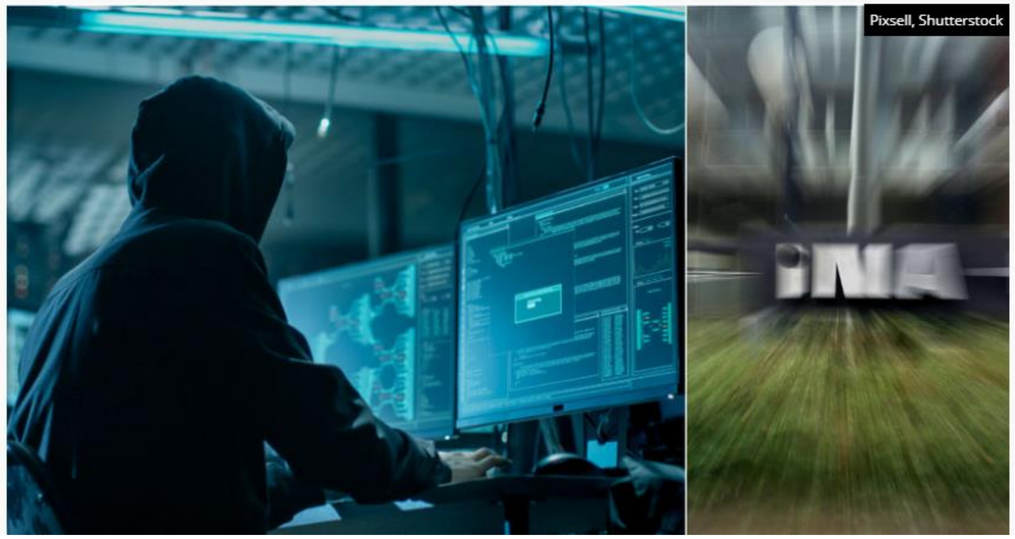
Napominjemo kako je opskrba tržišta sigurna, a prodaja goriva na našim maloprodajnim mjestima se nastavlja odvijati neometano. Također, provedba svih plaćanja je sigurna, neovisno o tome radi li se o gotovinskom plaćanju, INA kartici ili bankovnoj kartici.

Ispričavamo se našim kupcima i poslovnim partnerima za eventualne neugodnosti koje je ova situacija mogla prouzročiti. Cijenimo vašu kontinuiranu podršku i razumijevanje u ovoj situaciji.

SANIRANJE ŠTETE

Hakerski napad na Inu ostavio ozbiljne posljedice: 'Započeli smo s oporavkom sustava'

21.02.2020 13:46 Vijesti.hr



Diverto godišnji izvještaj

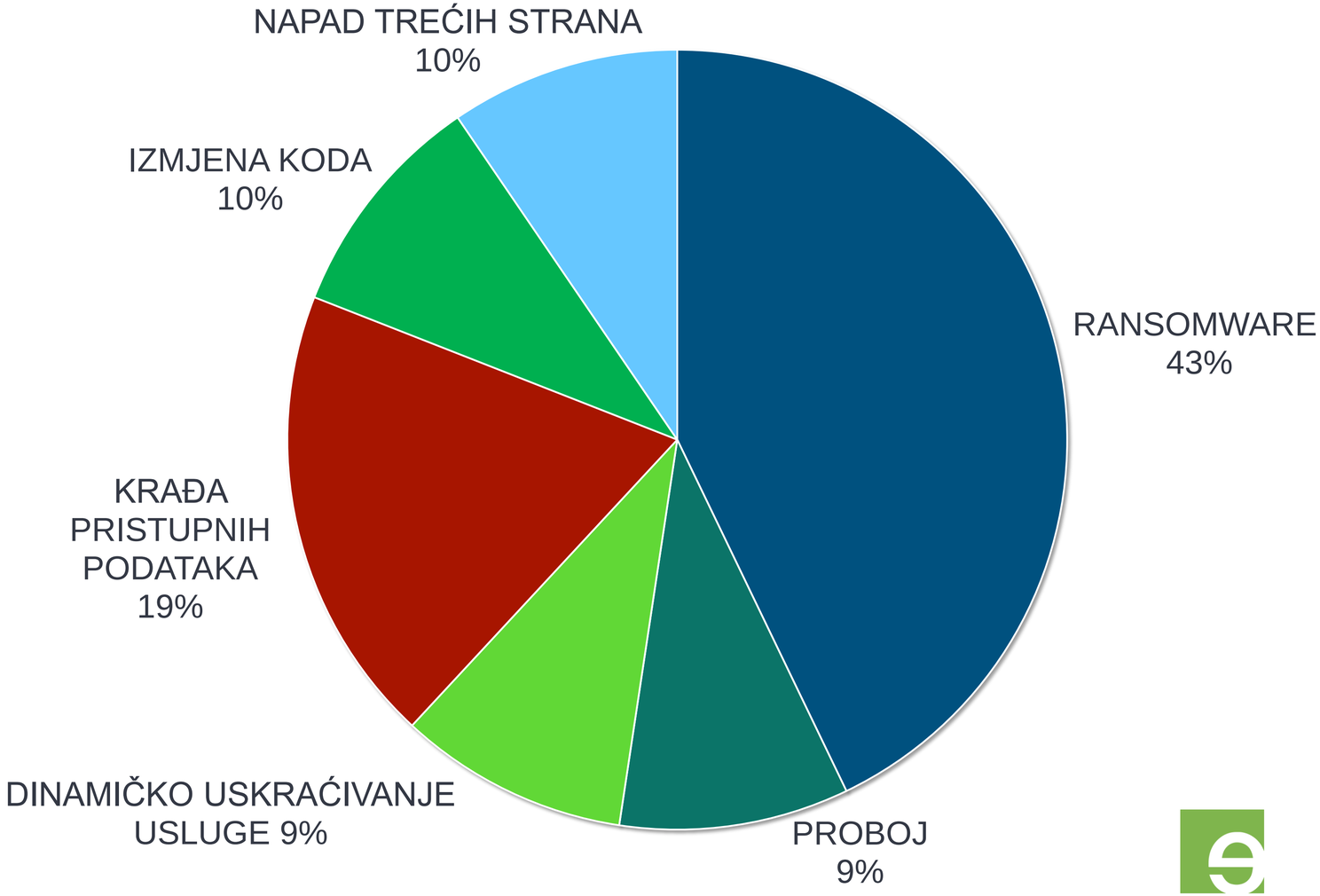
- Treće izdanje
- Fokus
  - Hrvatska
  - Pravne osobe
- Godine
  - 2021
  - 2020
- Izdavač
  - Diverto
  - Svibanj, 2022.

https://diverto.hr/documents/diverto_stanje_informacijske_sigurnosti_2021.pdf

Incidenti izvan SOC-a

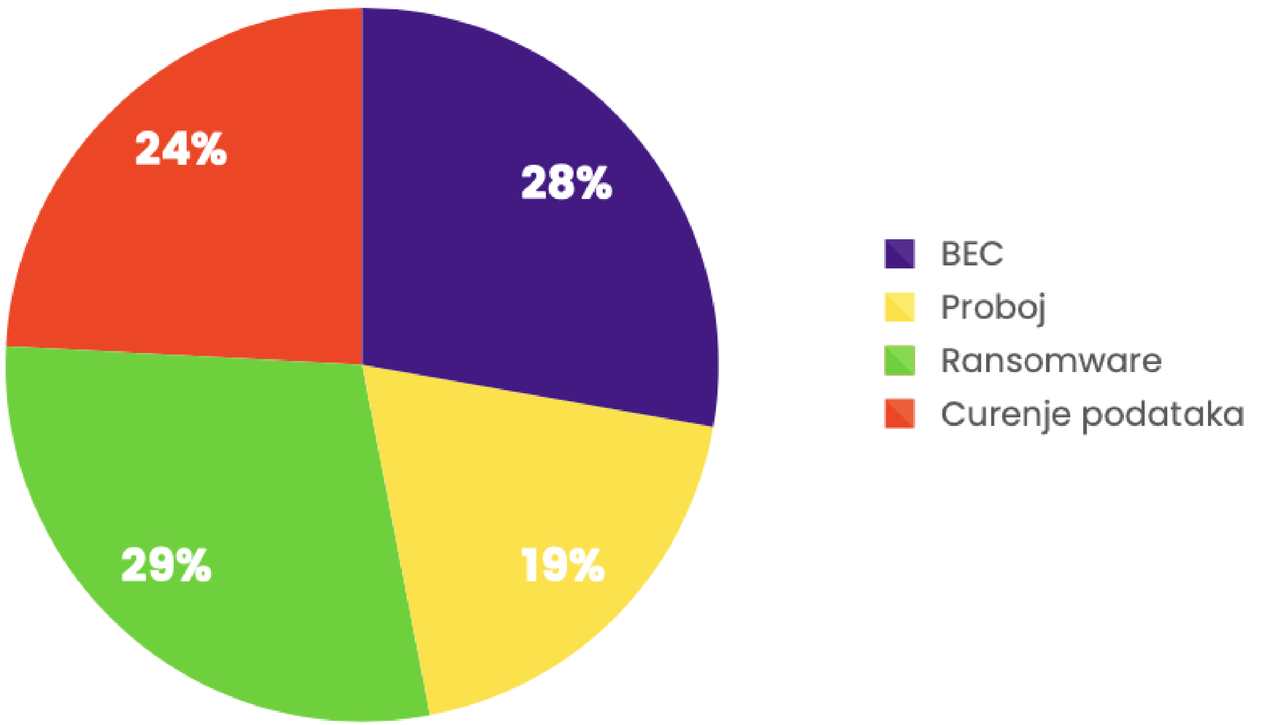
PORAST INCIDENATA

400%



Izvor: Diverto SOC

Diverto SOC – značajni incidenti

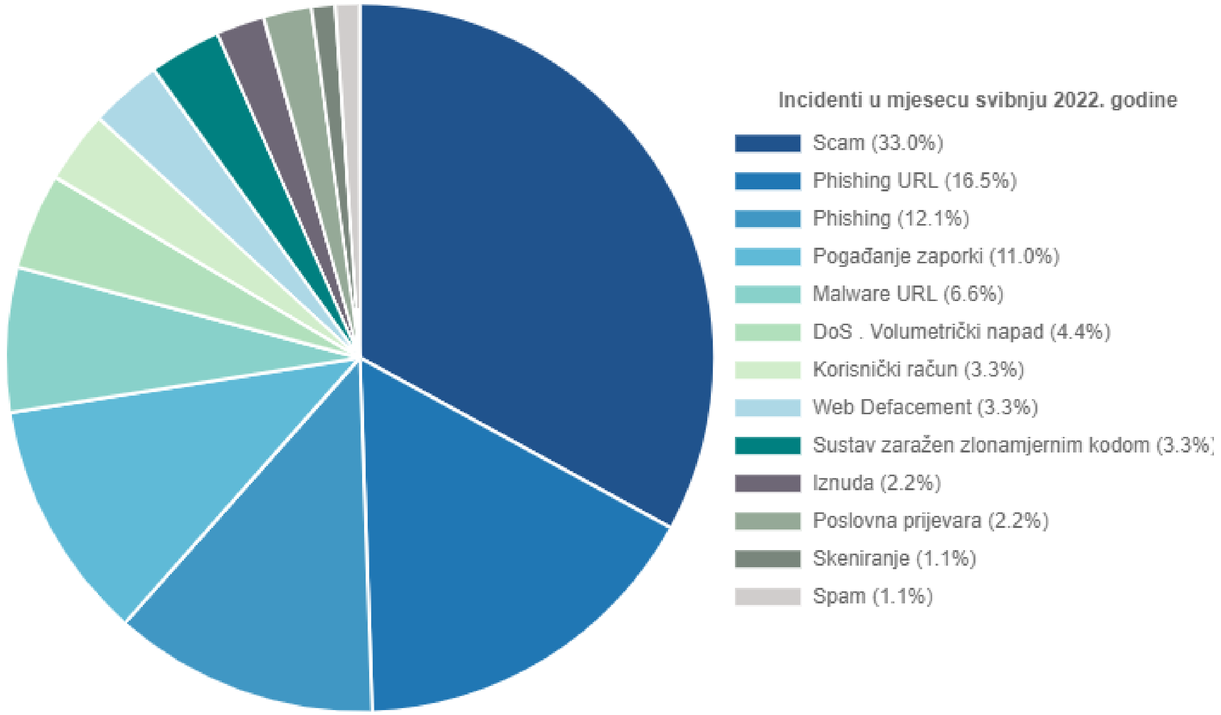


Izvor: Diverto SOC

Nacionalni CERT – phishing

TIP INCIDENTA	BROJ	TREND
PHISHING URL	353	–
PHISHING	166	–
MALWARE URL	139	▲
WEB DEFACEMENT	112	–
POGAĐANJE ZAPORKI	111	▼
SUSTAV ZARAŽEN ZLONAMJERNIM KODOM	96	▲
POKUŠAJ ISKORIŠTAVANJA RANJIVOSTI	57	▲
DOS - VOLUMETRIČKI NAPAD	39	▲
SCAM	25	–
KORISNIČKI RAČUN	20	▲
SPAM	20	▼
OSTALO	17	▲
PRIJEVARE	17	▲
HOAX	15	▼
DOS - NAPAD NA APLIKACIJSKOM SLOJU	11	▲
ISPAD USLUGE (ENG. OUTAGE)	6	▲
C&C	3	▼
SKENIRANJE	3	▼
PRIKUPLJANJE INFORMACIJA	1	▲
UKUPNO	**1211**	▼

Prikaz incidenata po tipu u 2021. godini



Izvor: CERT

Posljedice

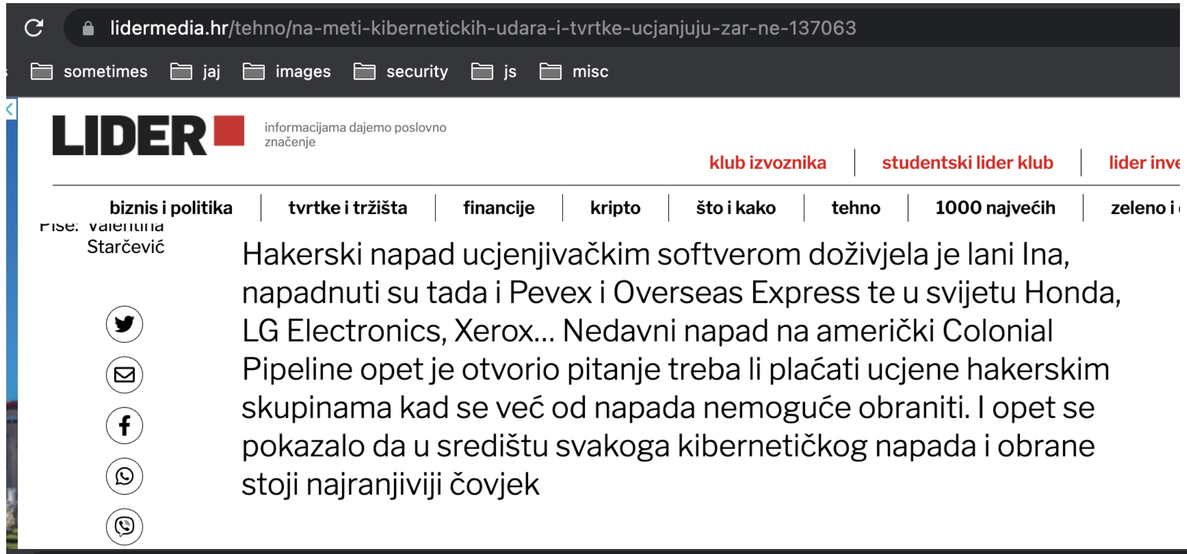
Broj kibernetičkih kaznenih djela u I-IX.2022. godini

Materijalna šteta

4.819.665 EUR

https://rep.hr/vijesti/tehno-i-it/raste-broj-phishing-i-ransomware-napada-u-eu/8762/

Incidenti u Hrvatskoj



Primjer inicijalnog pokušaja

From: <podrska@m- .com>
Sent: Monday, August 8, 2022 11:17 AM
To:
Subject: VAŽNO: Ažuriranje m aplikacije zbog uvođenja Eura

Poštovani,

U cilju ostvarenja visokog stupnja održive ekonomske konvergencije i uspješnog sudjelovanja u europodručju, Republika Hrvatska se obvezala na provedbu dodatnih mjera u reformskim područjima te je iskazala čvrstu namjeru da uvede euro kada kriteriji konvergencije budu ispunjeni.

Molimo da ažurirate novu verziju aplikacije m sukladno uputama koji se nalaze na linku ispod:

https://m- .com/Prijava/ERM-II-Azuriranje.php

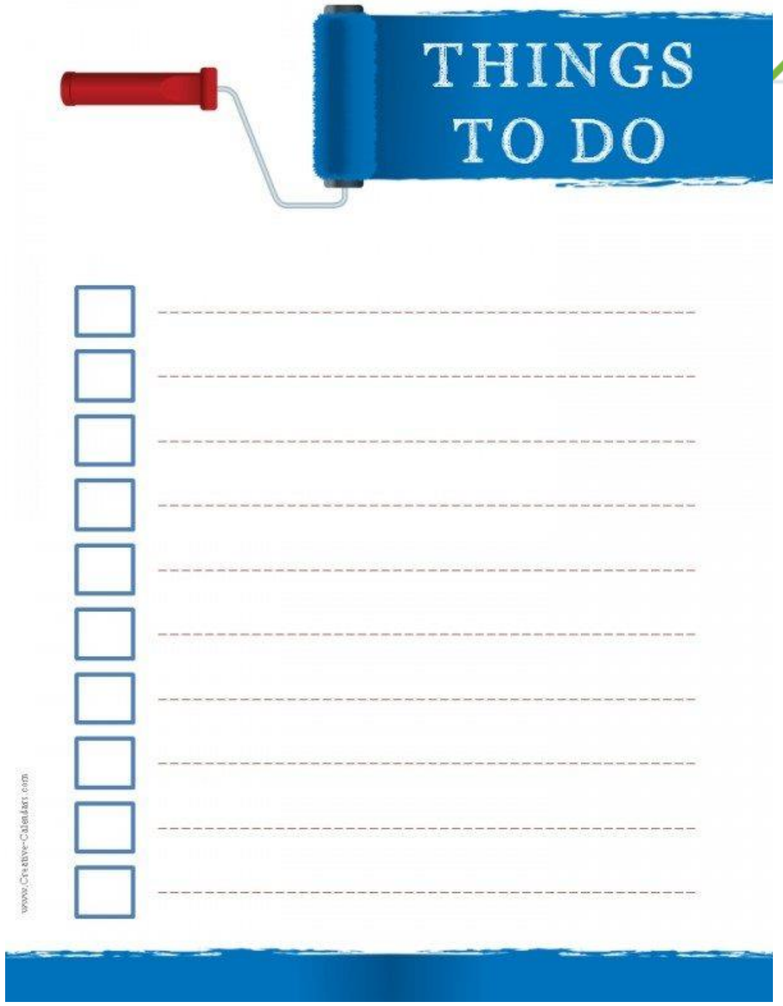
S tim ćete uspješno ažurirati neophodne korake za nesmetan rad m- mobilne aplikacije i prilagodit je ERM II tečajnom mehanizmu.

Kako se obraniti?

- **Edukacija**
- **Osvješćivanje**
- **Sustavni pristup**
- **Testiranje**
- **Kontinuirano poboljšanje**

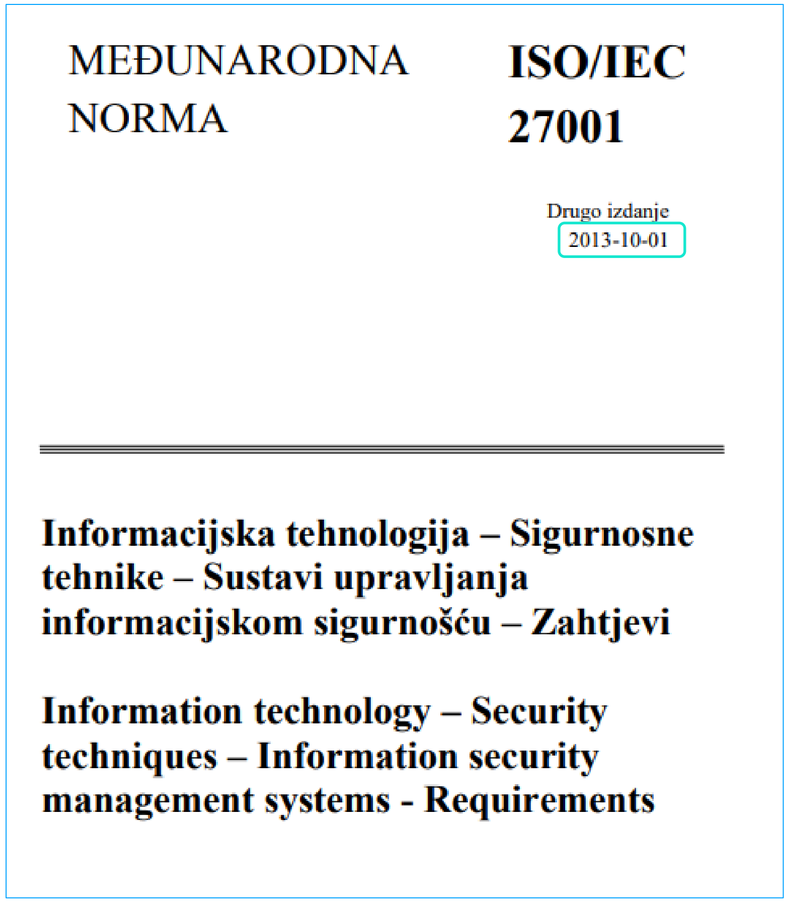
Kako se obraniti - detaljnije

- **Sustavni pristup**
  - **Uspostava upravljačkog okvira**
  - **Identifikacija informacijske imovine**
  - **Upravljanje rizikom**
  - **Implementacija sigurnosnih kontrola**
  - **Testiranje sigurnosnih kontrola**
  - **Kako možemo poboljšati?**
- **Kontinuirani proces**
  - **Kako možemo poboljšati?**
  - **Testiranje**
  - **Poboljšanja**



ISO IEC 27001 - ISMS

- međunarodni standard
- definira zahtjeve za uspostavljanje, primjenu, održavanje i poboljšanje sustava upravljanja sigurnošću podataka
- propisano na što sve treba paziti, počevši od fizičke sigurnosti, preko sigurnosnih procedura za zaposlenike do zaštite informacijskog sustava
- odnosi na sigurnost podataka pohranjenih ili transferiranih preko svih vrsta formata - tiskanih, elektroničkih, poštanskih, audiovizualnih i verbalnih



MEĐUNARODNA NORMA

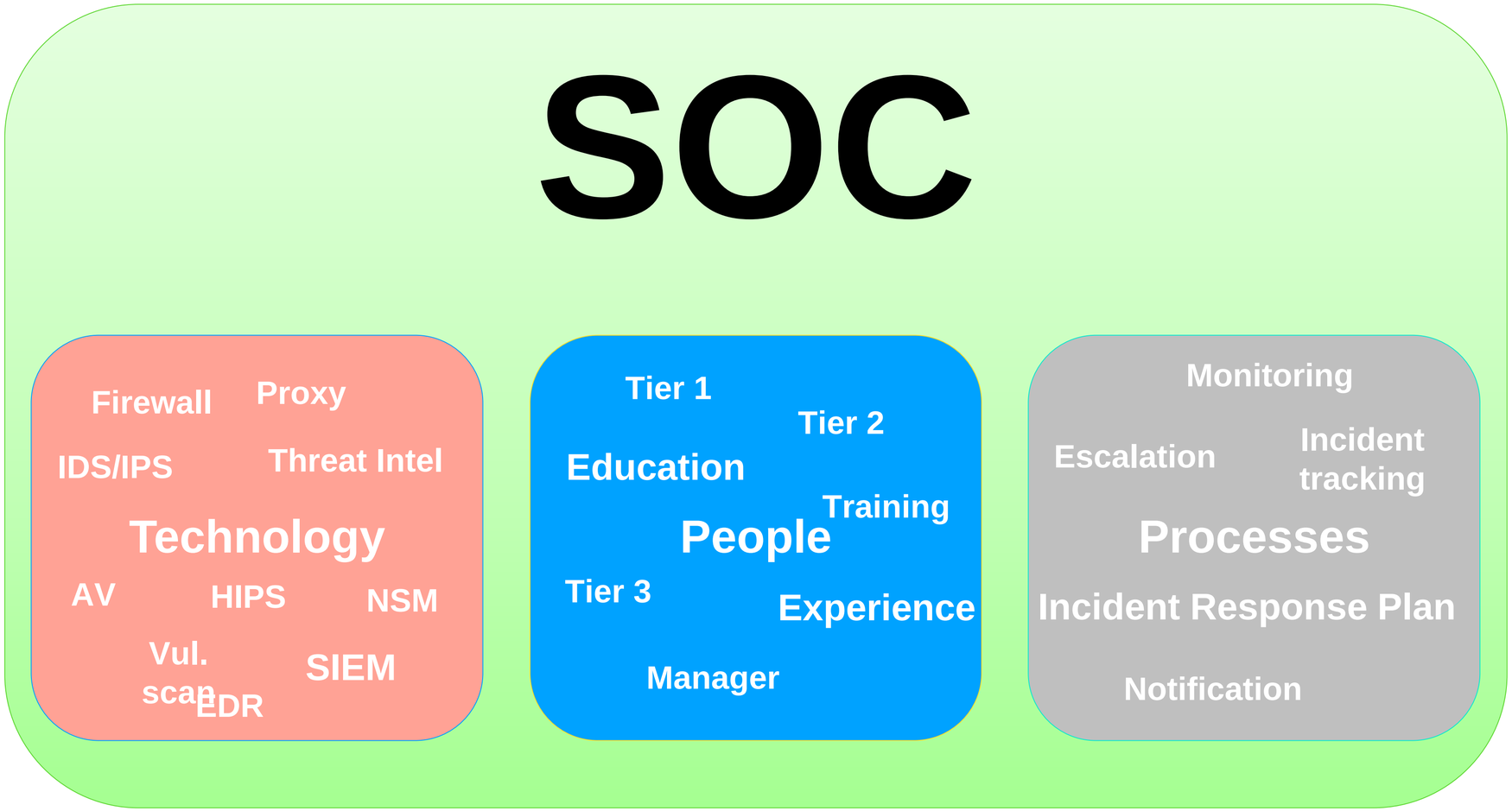
ISO/IEC 27001

Drugo izdanje
2013-10-01

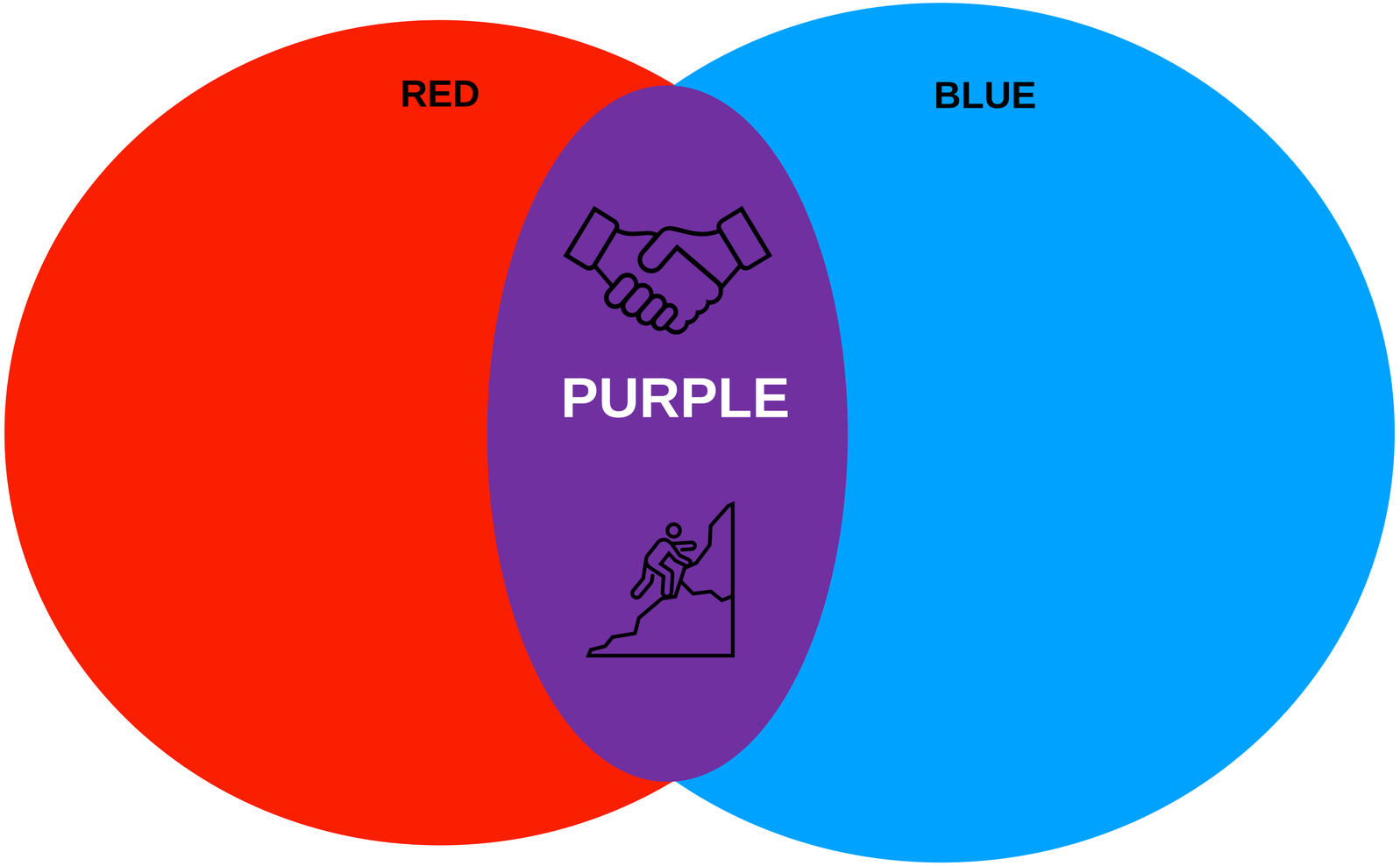
Informacijska tehnologija – Sigurnosne tehnike – Sustavi upravljanja informacijskom sigurnošću – Zahtjevi

Information technology – Security techniques – Information security management systems - Requirements

Sigurnosno-operativni centar (SOC)



Timovi



Testiranja

- **Tipovi**
  - **Tabletop**
  - **Proces**
  - **Tehnologija**
  - **Socijalni inžinjering**
  - **Simulacija određene napadačke skupine**
  - **Sveobuhvatna**
- **Tipični**
  - **Penetracijski test**
  - **Red Teaming**
  - **Purple Teaming**
  - **…**

Industrijski kontrolni sustavi i automatizacija

- **Podložni napadu**
- **Izolirani?**
  - **Vrlo često se pokažu da izolacija nije potpuna**
- **Ukoliko su spojeni na Ethernet mrežu**
  - **Računalno upravljivi**
- **Izazovi**
  - **Prekid operacija**
  - **Dugoročno planiranje**
  - **Dugoročne posljedice**

Sažetak

- **Sve više napada**
- **Žrtve napada**
  - **Ciljana organizacija**
  - **Kolateralna**
  - **Drive-by**
- **Obrana**
  - **Edukacija**
  - **Osvješćivanje**
  - **Sustavni pristup**
  - **Testiranje**
  - **Kontinuirano poboljšanje**

Hvala!

https://diverto.hr/documents/diverto_stanje_informacijske_sigurnosti_2021.pdf

diverto
information security

Pitanja?

@k0st
vlatko.kosturjak@diverto.hr