Varnostni testi aplikaciji, zakaj in kako?

Mag. Damijan Marinšek, MDP/DDI/SIV

9. 5. 2023

Ministrstvo za digitalno preobrazbo

Ministrstvo za digitalno preobrazbo spremlja in analizira stanje digitalne preobrazbe in informacijske družbe na državni ravni. Pristojno je za delovno področje informacijske družbe, elektronskih komunikacij, digitalne vključenosti, digitalnih kompetenc, podatkovne ekonomije, **upravljanja z informacijsko-komunikacijskimi sistemi in zagotavljanja elektronskih storitev javne uprave**. V sodelovanju s pristojnimi ministrstvi in vladnimi službami pripravlja, usklajuje in izvaja državne ukrepe in projekte na področju informacijske družbe in digitalne preobrazbe gospodarstva, javne uprave, zdravstva, pravosodja, kmetijstva in izobraževanja ter drugih področjih.

https://www.gov.si/drzavni-organi/ministrstva/ministrstvo-za-digitalno-preobrazbo/o-ministrstvu-za-digitalno-preobrazbo/

V okviru Direktorata za digitalno infrastrukturo je Sektor za informacijsko varnost:

- izvajamo naloge varnostno-operativnega centra (ang. SOC);
- kot so pregled in ugotavljanje ranljivosti spletnih aplikacij in informacijskih sistemov na vseh stopnjah razvoja in delovanja
- odzivni center za obravnavo incidentov s področja informacijske varnosti v informacijskih sistemih v upravljanju ministrstva.

Št.	Področje SOC
0	Preverjanje PZI
1	Preverjanje izvorne kode (ang. Source Code Review),
2	Izvajanje testov vdorov testov (ang. Penetration testing),
3	Upravljanje ranljivosti v informacijskih sistemih (ang. Vulnerability Management),
4	Upravljanje in odzivanje na incidente v informacijskih sistemih (ang. Incident Hunting and Incident Response),
5	Analiza incidentov v informacijskih sistemih (ang. Incident Analyze),
6	Upravljanje z informacijsko varnostjo (ang. Information Security Management and Security Baselining),
7	Upravljanje s sistemom vab (ang. Honeypot),
8	Ozaveščanje in usposabljanje uporabnikov in skrbnikov informacijskih sistemov (ang. Information Security Awareness and Training).

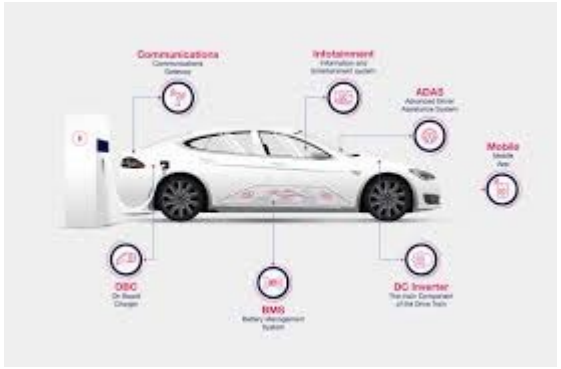
Varnostni testi aplikacij in sistemov. Zakaj? 1.

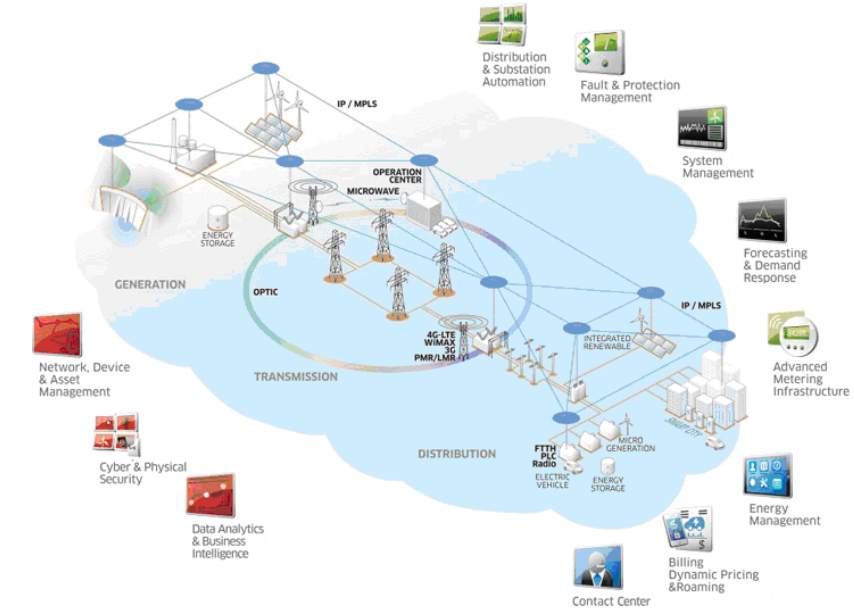
- Pisalo se je daljno leto 2012, ko pojem informacijska ali kibernetska varnost še ni bil »in« in v vsakdanji rabi. Poskusno smo izvedli varnostni pregled informacijskega sistema. Ta je pokazal predvsem odsotnost ustreznih kontrol na aplikativnem nivoju, ter nekaj neustrezno nastavljenih strežnikov, s tem pa povečano možnost vdora v sistem. Akcije smo nato periodično ponavljali, dodali vdorne (ang. pen) teste, preverjali izvorno kodo aplikacij. Napredek je bil viden, a »ad hoc« akcije niso predstavljale sistemske rešitve.

- Povod za storitev SOC št. 1 – Varnostno preverjanje izvorne kode in SOC št. 2 - Pen testi so bile slabe aplikacije brez ustreznih kontrol.
- Ker aplikacije gostujejo na skupni infrastrukturi.
- Zgodnejše odkrivanje napak v kodi znižuje stroške popravkov ali morebitno sanacijo škode po vdoru.
- Statična analiza ni nujno 100% zanesljiva. Zato je potrebna še dinamična analiza (Penetracijski testi).
- Temu sledi stalno spremljanje in upravljanje ranljivosti Informacijskih sistemov.
- S ciljem nič ali čim manj vdorov v sisteme - incidentov informacijske varnosti.

Varnostni testi aplikacij in sistemov. Zakaj? 2.

- Tudi tekst preverjamo z orodji s črkovalniki in slovnico, slovarji.
- Ker je programska koda vključena v naprave (IoT, vozila), kjer napake lahko povzročijo tudi smrt, katastrofo…
- Iskanje ranljivosti v kodi, stranska vrata za vdor, vohunjenje.
- Pregled kode, tudi tiste dele, ki se bolj redko uporablja.
- Ranljivosti SCADA sistemov.
- Zgodnejše odkrivanje napak v kodi, vpliva na proces razvoja in znižuje stroške popravkov ali sanacije škode po vdoru.



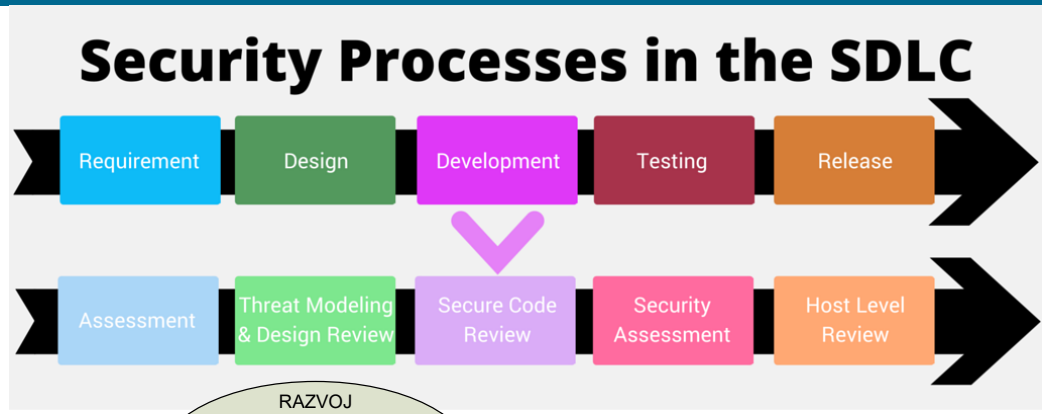


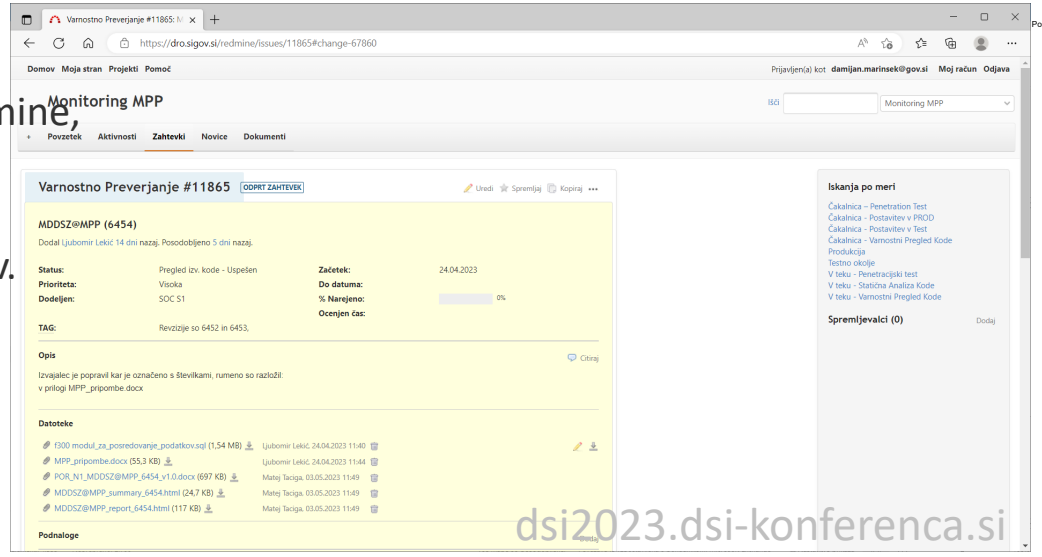
Varnostni testi aplikacij in sistemov. Zakaj? 3.

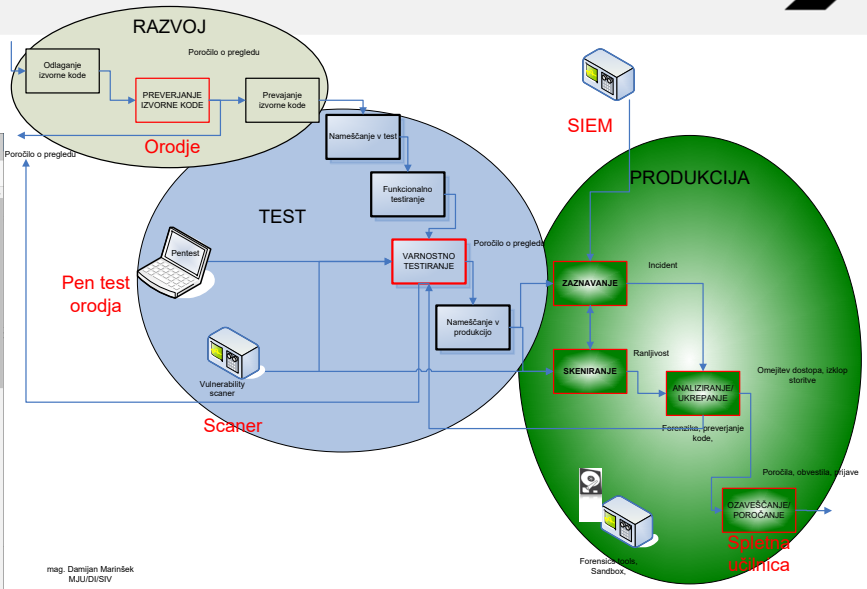
- Varnostni testi aplikaciji so ključni korak pri zagotavljanju varnosti programske opreme. Aplikacije, ki niso varne, so lahko tarča zlonamernih napadov, kar lahko povzroči škodo tako za uporabnike kot za podjetje ali organizacijo, ki stoji za aplikacijo. Zato je nujno, da se varnostne teste izvede pred izdajo – produkcijo aplikacije.
- Varnostni testi aplikacije se izvajajo z namenom odkriti morebitne ranljivosti in pomanjkljivosti v aplikaciji, ki bi lahko ogrozile varnost uporabnikov.
- Da bi zagotovili učinkovite varnostne teste, je priporočljivo, da jih izvajajo strokovnjaki za varnostne teste. Ti lahko najdejo ranljivosti, ki jih drugi morda ne bi našli. Po izvedbi testov mora podjetje ali organizacija takoj odpraviti najdene ranljivosti in izboljšati varnost aplikacije.
- Izvajanje varnostnih testov aplikacij je ključno za zagotavljanje, da so aplikacije varne pred morebitnimi napadi in zlonamernimi dejanji. Varnostni testi pomagajo odkriti morebitne ranljivosti aplikacij in omogočajo razvijalcem, da jih odpravijo preden jih izkoristijo napadalci.
- Poleg tega varnostni testi zagotavljajo, da aplikacije izpolnjujejo varnostne standarde in predpise, kot so GDPR, HIPAA in PCI.
- **Na splošno so varnostni testi aplikacij ključni za zagotavljanje varnosti in zasebnosti uporabnikov ter preprečevanje finančne škode in reputacijskih tveganj za podjetja ali celo za preprečevanje poškodb/smrti.**

Proces gostovanja na infrastrukturi DRO in ISO27.001

- Poleg tehničnih pogojev, ki jih mora izpopolnjevati sistem iz GTZ https://nio.gov.si/nio/asset/dokument+genericne+tehnoloske+zahteve+gtz-743
- Smo vzpostavili proces gostovanja na DRO,
- kjer smo v proces vgradili **varnostna preverjanja** v celotnem ciklu informacijskega sistema.
- Pridobili certifikat ISO 27.001.
- Proces podprli z informacijskim sistemom Redmine, preko katerega se vodijo zahtevki posameznih projektov.

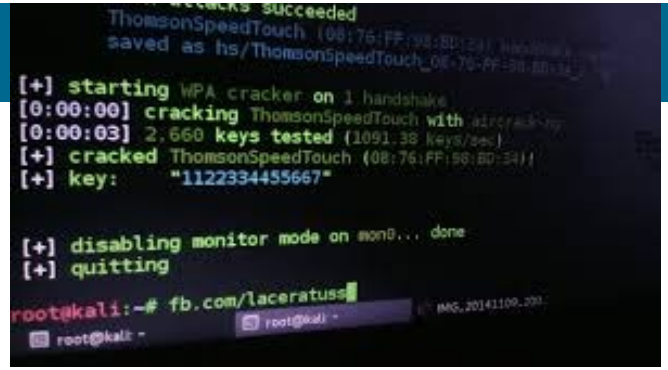


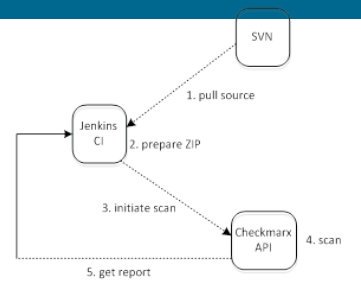




SOC 1 - Preverjanje Izvorne kode

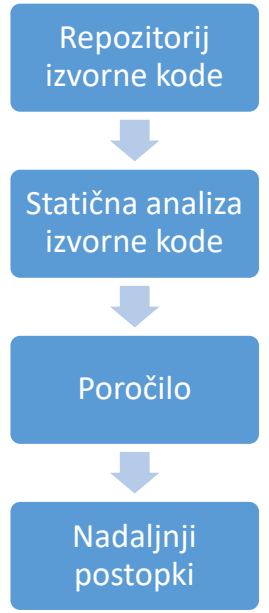
S preverjanjem izvorne kode poskušamo preprečiti namestitev programske opreme, ki vsebuje resne varnostne ranljivosti.





vir: dokument „pregled izvorne kode SVN-CheckMarx delovni tok.pdf"

- Začetne ročne postopke so zamenjali avtomatizirani procesi, ki se izvedejo ob uspešni namestitvi kode na repozitorij izvorne kode z ustrezno manifest datoteko. (test se izvede v roku 24h).
- Aplikacija ne sme vsebovati ranljivosti s stopnjo „**visoko**" ali „**srednje**".
  - *Ta faza se lahko avtomatsko ponavlja dokler niso izpolnjene zahteve.*
  - *V primeru, da se razvijalec z ugotovitvami ne strinja, lahko ta poda zahtevek za ročno preverjanje rezultatov in svoje mnenje na poročilo. SOC ekipa skupaj z razvijalcem ugotovitve potrdi ali zavrže.*
- Obveščanje odgovornih oseb po končanem preverjanju.
- Ko aplikacija zadosti zahtevanim pogojem, je primerna za nadaljnje postopke.
- V prvi iteraciji noben projekt ni OK.
- Vsaka sprememba mora skozi isti proces!
- Testi vplivajo na časovnico projektov!



Opis	Primernost za nadaljnje postopke
Spletna aplikacija **NI** primerna za nadaljnje postopke. Pred nadaljevanjem je potrebno odpraviti vse visoko ali srednje kritične pomanjkljivosti.	☒
Spletna aplikacija **JE** primerna za nadaljnje postopke pod pogojem, da se v dogovorjenem časovnem okviru odpravijo preostale najdene pomanjkljivosti.	☐
Spletna aplikacija **JE** primerna za nadaljnje postopke.	☐

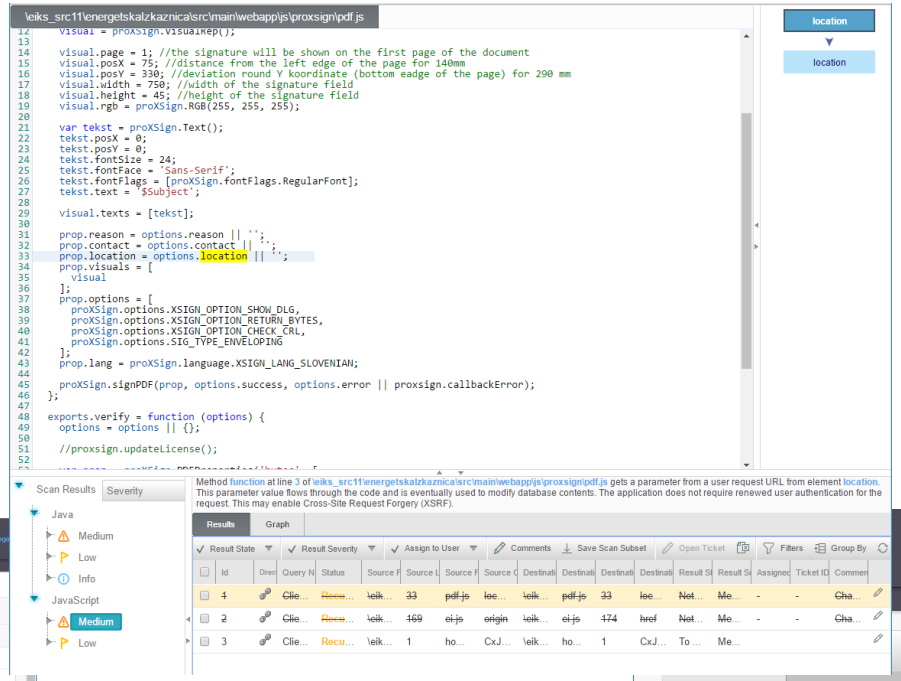
SOC 1 - Preverjanje Izvorne kode – poročila, orodja

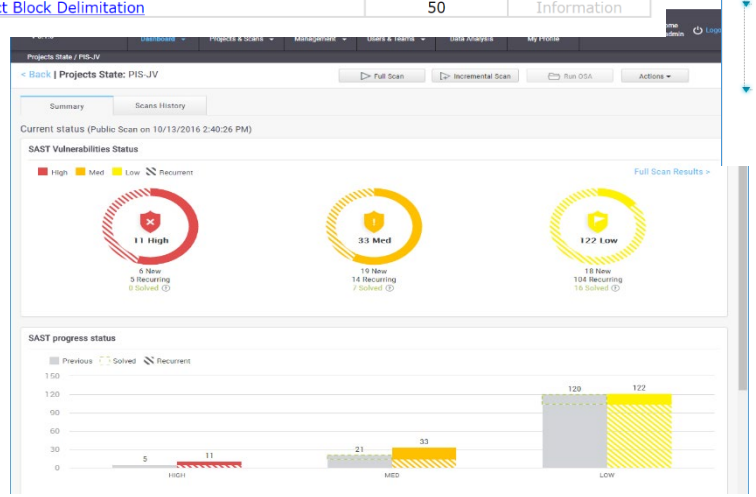
Results Distribution By State

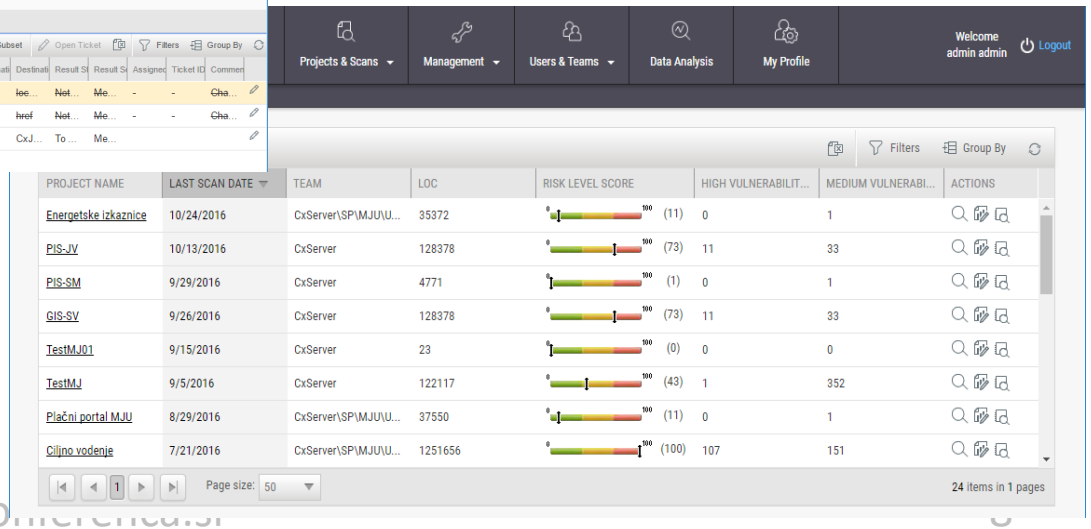
	High	Medium	Low	Information	Total
To Verify	4	32	0	726	762
Not Exploitable	0	0	0	0	0
Confirmed	0	0	0	0	0
Urgent	2	0	0	0	2
Total	6	32	0	726	764

Result Summary

Vulnerability Type	Occurrences	Severity
Stored XSS	4	High
Improper Restriction of XXE Ref	7	Medium
Unnormalize Input String	7	Medium
Stored LDAP Injection	6	Medium
XSRF	5	Medium
Client DOM XSRF	2	Medium
Heap Inspection	2	Medium
Client Cross Frame Scripting Attack	1	Medium
Cross Site History Manipulation	1	Medium
Unchecked Input for Loop Condition	1	Medium
Declaration Of Catch For Generic Exception	50	Information
ESAPI Banned API	50	Information
Exposure of Resource to Wrong Sphere	50	Information
Incorrect Block Delimitation	50	Information



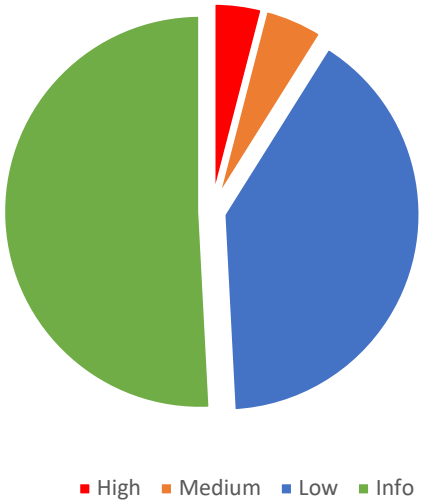




PROJECT NAME	LAST SCAN DATE	TEAM	LOC	RISK LEVEL SCORE	HIGH VULNERABILIT...	MEDIUM VULNERABI...	ACTIONS
Energetske izkaznice	10/24/2016	CxServer\SP\MJU\U...	35372	(11)	0	1	
PIS-JV	10/13/2016	CxServer	128378	(73)	11	33	
PIS-SM	9/29/2016	CxServer	4771	(1)	0	1	
GIS-SV	9/26/2016	CxServer	128378	(73)	11	33	
TestMJ01	9/15/2016	CxServer	23	(0)	0	0	
TestMJ	9/5/2016	CxServer	122117	(43)	1	352	
Plačni portal MJU	8/29/2016	CxServer\SP\MJU\U...	37550	(11)	0	1	
Ciljno vodenje	7/21/2016	CxServer\SP\MJU\U...	1251656	(100)	107	151	

Page size: 50
24 items in 1 pages

SOC 1 - Preverjanje Izvorne kode – Statistka leto 2022 - 294



Odkrite pomanjkljivosti

4630 visoko kritičnih

5620 srednje kritičnih

46259 nizko kritičnih

58425 informativnih odkritij

Visoko kritične – S1:

- XSS
- Vrivanje stavkov SQL
- Poljubno izvajanje kode
- Poljubno branje datotek
- Deserializacija podatkov iz nezaupljivih virov
- Reference na zunanje datoteke (skripte)

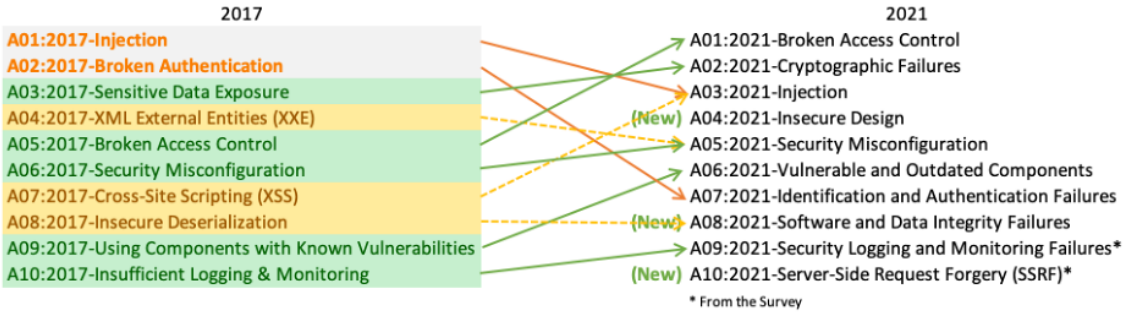
- **Nizko kritične – S1**
- Uporaba šibkih šifrirnih algoritmov
- Neustrezna implementacija šifrirnih algoritmov (sicer varnih)
- Neustrezna avtorizacija
- Neomejeno nalaganje datotek
- Manjkajoč Content Security Policy
- Izdajanje informacij o sistemu pri izpisu napak
- Prirejanje dnevniških zapisov
- Gesla zapisana v pomnilniku

Srednje kritične – S1:

- Manipulacija parametrov
- Neomejeno izvajanje zank
- Šibki generatorji naključnih vrednosti (pri šifriranju)
- Omogočeno nalaganje DTD entitet
- Odtekanje zaupnih informacij (dnevnik, zunanje sisteme)
- SSRF
- Masovno dodeljevanje vrednosti
- Statično zapisani šifrirni ključi
- Statično zapisana gesla do zunanjih sistemov
- Omogočeno sprehajanje po direktorijih

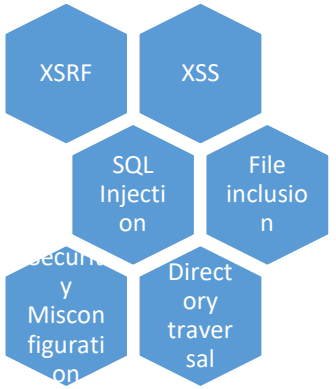
SOC 2 - Penetracijski testi

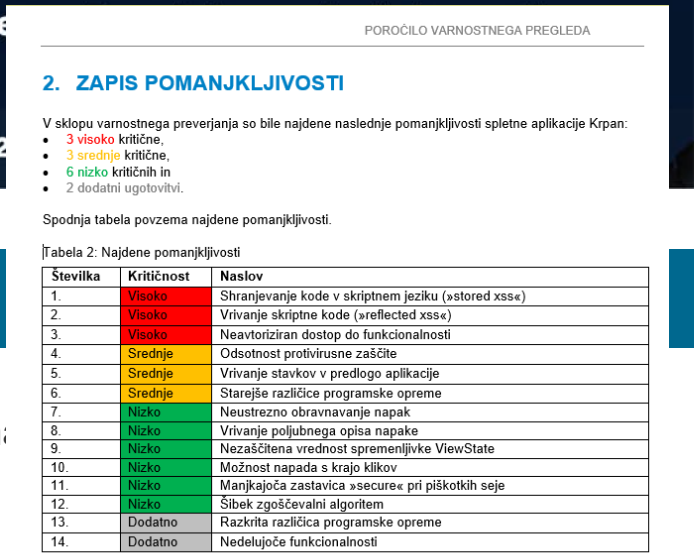
- S penetracijskimi testi izvedemo varnostno testiranje aplikacij – preveri se na ranljivosti po OWASP TOP 10 metodologiji.
- Izvede se avtomatično ter ročno preverjanje ranljivosti.
- V primeru, da aplikacija vsebuje ranljivosti stopnje „**visoko**“ ali „**srednje**“ morajo razvijalci te ranljivosti odpraviti. Po odpravi ranljivosti se postopek preverjanja ponovi.
- Obveščanje odgovornih oseb po končanem preverjanju.



Pogoji za izvedbo testa:

- Opis aplikacije
- Uporabniška navodila
- Poročilo o opravljenem funkcionalnem testiranju
- Delujoče testno okolje
- Pripravljeni testni računi, certifikati
- Urejen mora biti dostop iz okolja SOC
- Test traja v povprečju 5 dni





POROČILO VARNOSTNEGA PREGLEDA

2. ZAPIS POMANJKLJIVOSTI

V sklopu varnostnega preverjanja so bile najdene naslednje pomanjkljivosti spletne aplikacije Krpan:

- 3 visoko kritične,
- 3 srednje kritične,
- 6 nizko kritičnih in
- 2 dodatni ugotovitvi.

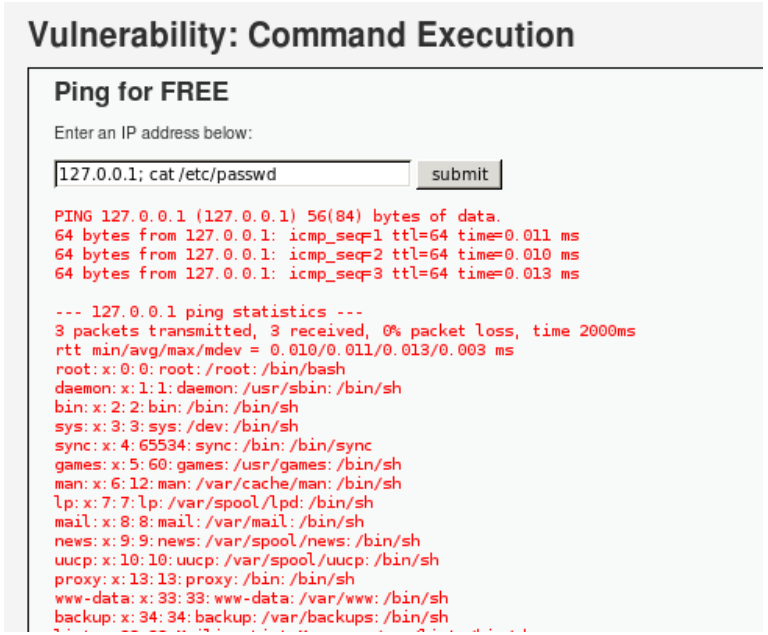
Spodnja tabela povzema najdene pomanjkljivosti.

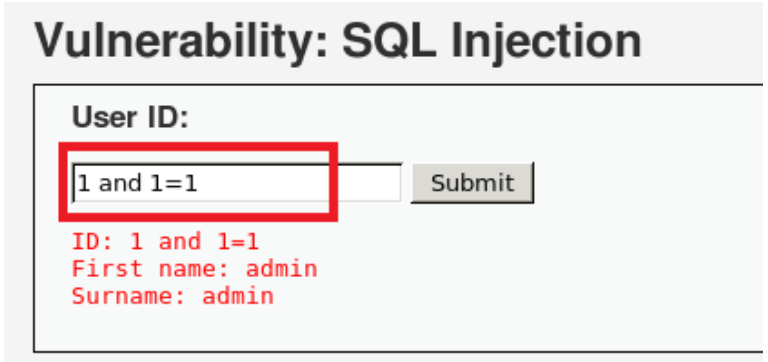
Tabela 2: Najdene pomanjkljivosti

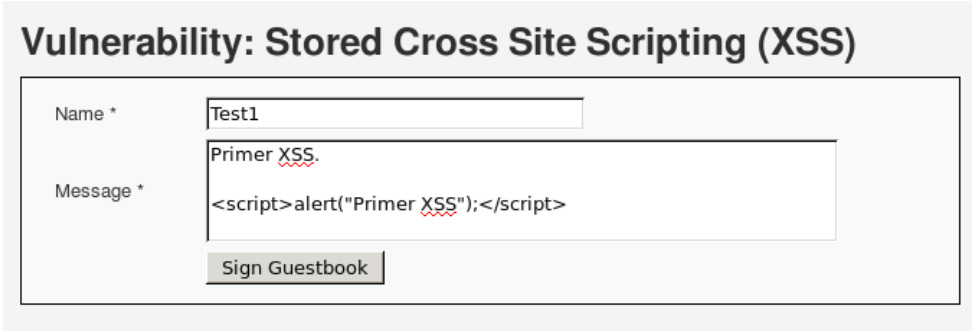
Številka	Kritičnost	Naslov
1.	Visoko	Shranjevanje kode v skriptnem jeziku (»stored xss«)
2.	Visoko	Vrivanje skriptne kode (»reflected xss«)
3.	Visoko	Neavtoriziran dostop do funkcionalnosti
4.	Srednje	Odsotnost protivirusne zaščite
5.	Srednje	Vrivanje stavkov v predlogo aplikacije
6.	Srednje	Starejše različice programske opreme
7.	Nizko	Neustrezno obravnavanje napak
8.	Nizko	Vrivanje poljubnega opisa napake
9.	Nizko	Nezaščitena vrednost spremenljivke ViewState
10.	Nizko	Možnost napada s krajo klikov
11.	Nizko	Manjkajoča zastavica »secure« pri piškotkih seje
12.	Nizko	Šibek zgoščevalni algoritem
13.	Dodatno	Razkrita različica programske opreme
14.	Dodatno	Nedelujoče funkcionalnosti

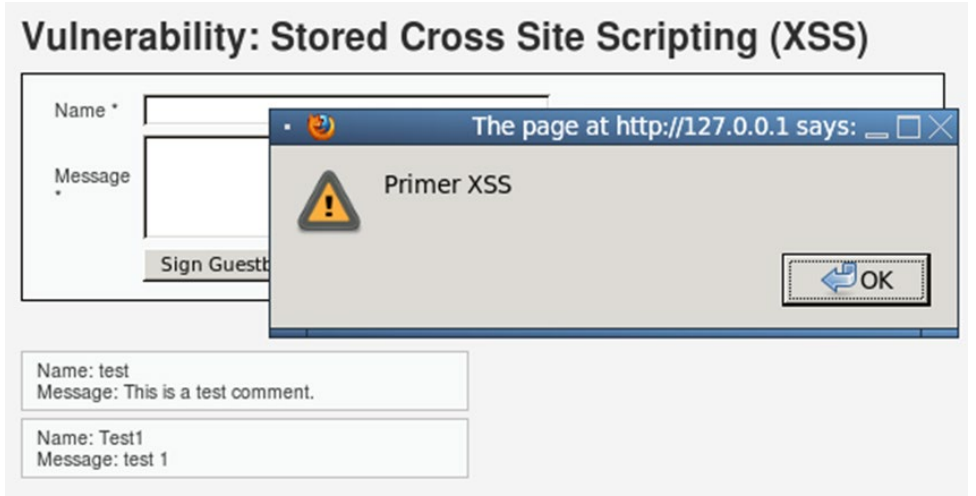
Opis	Primernost za nadaljnje postopke
Spletna aplikacija **NI** primerna za nadaljnje postopke. Pred nadaljevanjem je potrebno odpraviti vse visoko ali srednje kritične pomanjkljivosti.	☒
Spletna aplikacija **JE** primerna za nadaljnje postopke pod pogojem, da se v dogovorjenem časovnem okviru odpravijo preostale najdene pomanjkljivosti.	☐
Spletna aplikacija **JE** primerna za nadaljnje postopke.	☐

SOC 2 - Penetracijski testi- primeri

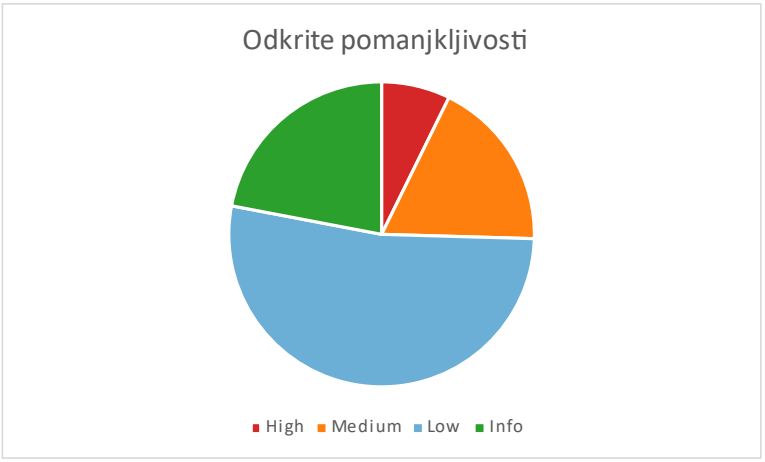








SOC 2 - Penetracijski testi- Statistika zadnjih 90 projektov



Odkrite pomanjkljivosti

- 40 visoko kritičnih
- 100 srednje kritičnih
- 289 nizko kritičnih
- 121 informativnih odkritij

Visoko kritične

- Kontrola dostopa
- Možnost spreminjanja vloge
- Neustrezna validacija JWT žetonov
- Poljubno branje sistemskih datotek
- Poljubno izvajanje kode
- Poljuben prenos datotek
- Vrivanje stavkov SQL

Srednje kritične

- Izpis mape na datotečnem sistemu
- Izpostavljena prijava v skrbniški del sistema
- Možnost brisanja revizijske sledi
- Nepravilna odjava
- Neustrezna politika gesel
- Spletni strežnik z vlogo visoko privilegiranega uporabnika
- XSS (DOM, Reflected, Stored)
- Zgoščena vrednost gesla vrnjena v odgovoru strežnika

Nizko kritične

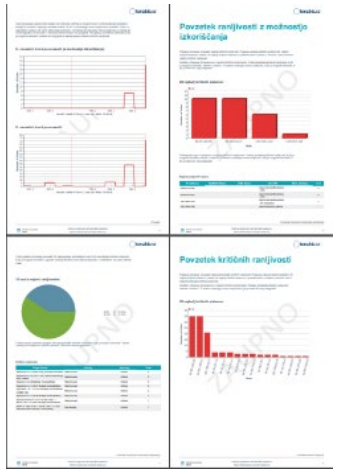
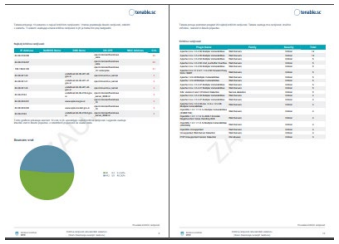
- Daljše trajanja prijavne seje
- Enumeracija map na spletnem strežniku
- Izdajanje izvorne kode
- Manjkajoče zastavice pri piškotkih seje (»HttpOnly«, »Secure« in »SameSite«)
- Možnost onemogočanja storitev z iskalnikom
- Možnost zabrisovanja revizijske sledi
- Poljubno nalaganje datotek
- Uporaba zastarelih knjižnic

Primerjava

- Večja podjetja proti manjšim
  - Že poznajo naročnike, proces so osvojili,
  - Boljše sodelovanje,
  - Hitrejša odprava,
  - Boljše razumevanje odkritih pomanjkljivosti,
  - Uporabljajo bolj standardne in preverjene knjižnice,
  - testiranje pred samimi vdornimi testi,
  - Boljša dokumentacija,
  - Večja proizvedejo boljše aplikacije.

SOC 3 – Upravljanje ranljivosti

- Na področju izvajanja »Storitev 3 – Upravljanje ranljivosti« izvajamo skeniranje računalniških sistemov z namenom odkrivanja in odprave zaznanih ranljivosti.
- Delo poteka v treh sklopih in sicer:
  - Stalno skeniranje kritične infrastrukture
  - Periodično skeniranje državnih organov
  - Ad hoc skeniranje

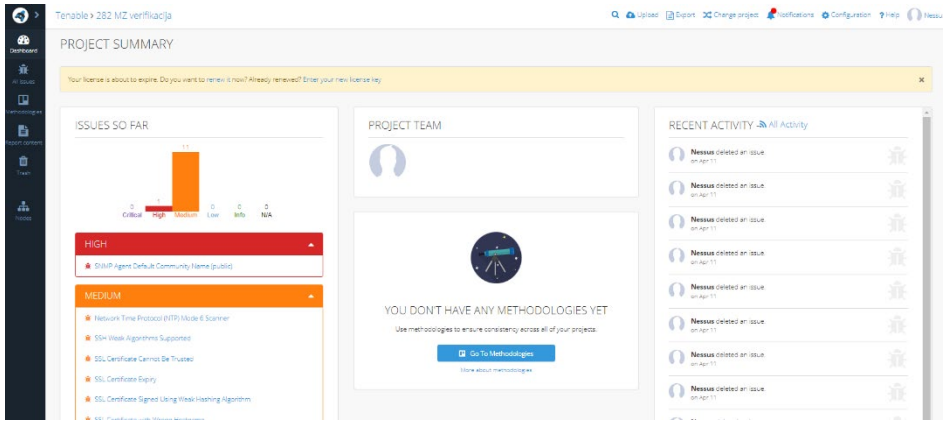




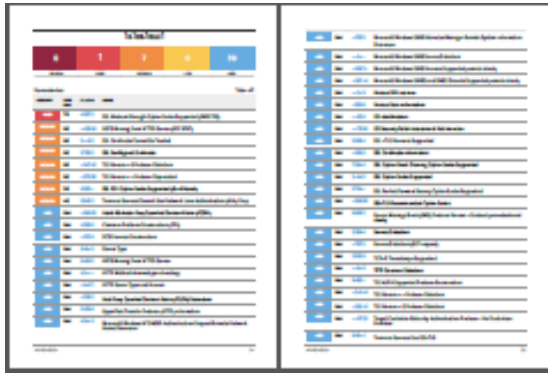
- Stalno skeniranje kritične infrastrukture:

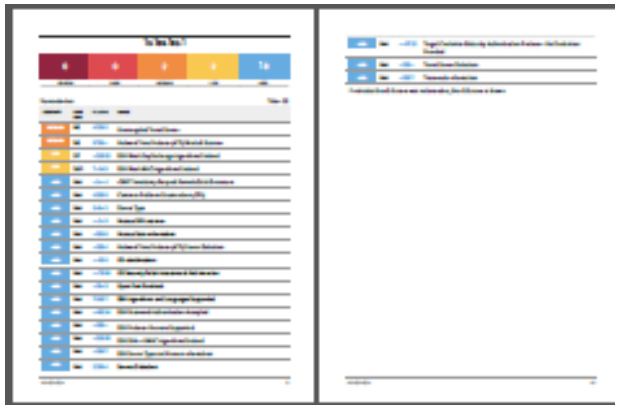
Stalno skeniranje kritične infrastrukture izvajamo s pomočjo orodja Tenable.sc, ki omogoča avtomatsko skeniranje s katerim zaznavamo ranljivosti računalniških sistemov. Rezultati se hranijo v lokalni bazi. Na sistemu je konfiguriran sistem izdelave poročil, ki generira okoli 20 poročil mesečno. Stalno skeniranje je razdeljeno v 6 sklopov, izvaja se avtomatsko z razmakom od enega tedna do enega meseca.

SOC 3 – Upravljanje ranljivosti

- Periodično skeniranje državnih organov:
- V letu 2022 smo varnostno pregledali, izvedli skeniranja omrežij in izdelali poročila o najdenih ranljivostih za 38 državnih organov, v letu 2023 pa smo do konca aprila varnostno preverili 14 državnih organov. Pregledi se izvajajo s pomočjo orodja, rezulatati se uvozijo v poročilni sistem, kjer se podatki obdelajo, nato pa se izdela poročilo v katerem so zaznane ranljivosti razvrščene po kritičnosti, po omrežjih in združene po napravah, kjer so bile zaznane.



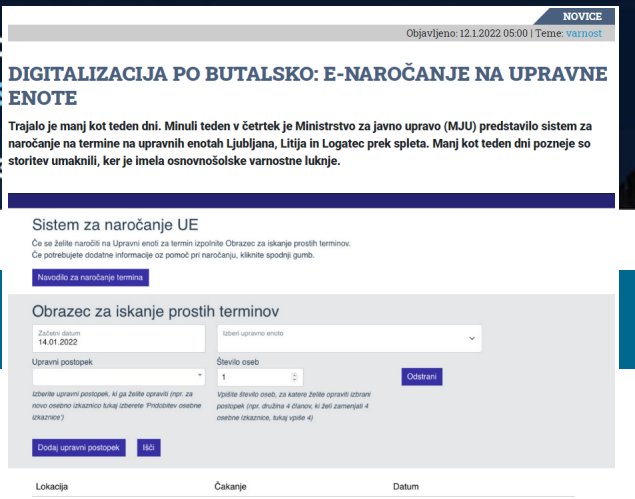




SOC 3 – Upravljanje ranljivosti

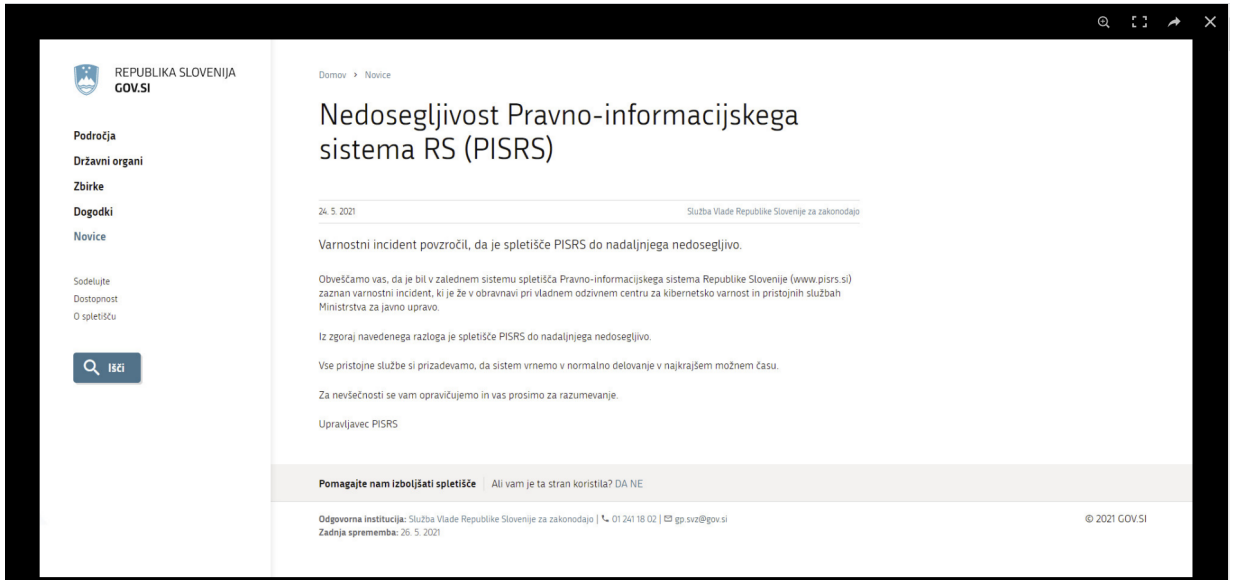
- Ad hoc skeniranje za potrebe SOC:

- V varnostno operativnem centru (SOC) analitiki neprestano nadzorujejo povezave in komunikacija med napravami, spremljajo se komunikacije uporabnikov in se izvajajo druge aktivnosti z namenom čim hitrejšega odkrivanja možnosti kibernetskega napada na računalniško infrastrukturo.
- Pri zaznavi sumljivih komunikacij se na zahtevo analitika izvede skeniranje posameznih naprav z namenom odkrivanja ranljivosti preko katerih bi bilo možno izvesti kibernetski napad. Za skeniranje uporabljamo orodje, preko katerega izdelamo podrobno poročilo ranljivosti za vsako napravo posebej.



V kolikor tega ne bi delali

- Od zunaj bi najverjetneje prišli do občutljivih datotek
- Navadni uporabniki bi si nastavili višje privilegirane vloge
- Razkrivali bi notranje tehnologije
- Napadalci imeli bistveno več podatkov o aplikacijah in sistemih




```
01110010111001111010111
10001100101010010101011
10101101101010110110111
11101011HACKED11110110
00010101001000010111111
10010101010101010100100
11111001111110110010000
```

Cilji in želje

- Da se naročniki zavedajo pomena tega procesa.
- Da preskakovanje faz ni opcija.
- Da se naročniki zavedajo, da mora vsaka verzija skozi isti proces.
- Da to stane in terja svoj čas.
- Da je to najboljša preventiva proti kibernetskim napadom.

- Da smo zgled in bo proces še kje kdo posvojil.

DIGITRAJNO Z VGRAJENO VARNOSTJO PODATKOV.