3. lab - Analiza ustroja organizacije HOPS - Maltego & Shodan

Treća laboratorijska vježba iz predmeta Sigurnosne prijetnje na internetu.

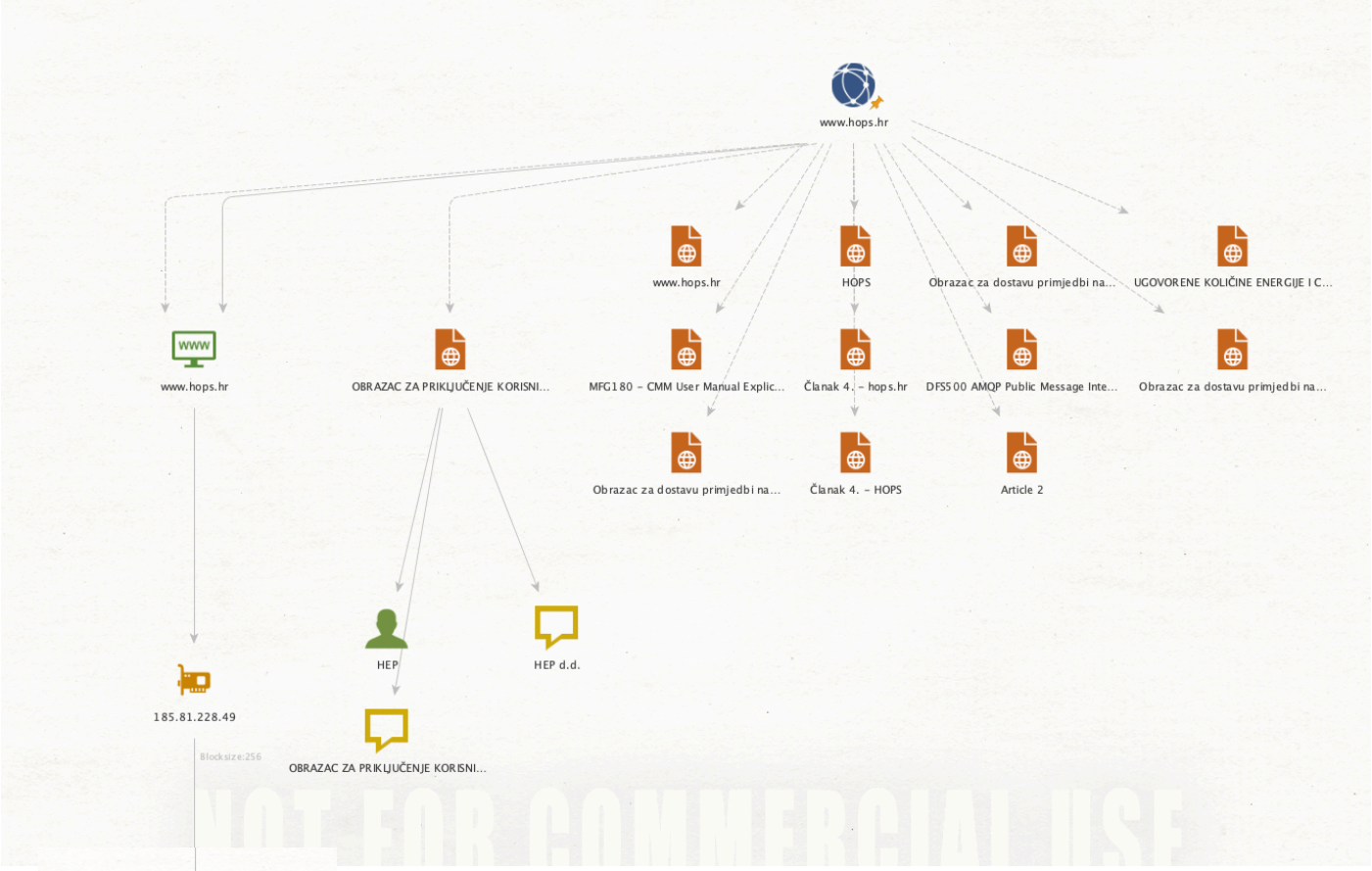
Alati

Alati korišteni u analizi: Maltego. Maltego je open source alat za grafičku analizu veza i inteligencija (OSINT) koji se koristi u cilju prikupljanja i povezivanja informacija vezanih za istražne zadatke. Shodan je tražilica koja korisnicima omogućuje pretraživanje različitih vrsta poslužitelja povezanih na internet pomoću različitih filtera.

Organizacija - HOPS

Primjer organizacije nad kojom se provodi analiza ustroja je HOPS. Hrvatski operator prijenosnog sustava (HOPS) je institucija koja svoje mjesto na tržištu električne energije pronalazi od 2013. godine. HOPS d.o.o. jedini operator elektroenergetskog prijenosnog sustava u RH, a uz to obavlja i djelatnosti prijenosa električne energije kao regulirane javne usluge. Cjelokupna hrvatska prijenosna mreža je u vlasništvu upravo HOPS-a.

Maltego grafovi & Shodan rezultati



SHODAN | Explore | Downloads | Pricing | @hops.hr org:"Hrvatski operator prijenosnog sustava d.o.o." org:"Hrvatsk | Account

TOTAL RESULTS

2

View Report | View on Map

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

185.81.228.73

2022-01-10T23:56:44.538942

mail01.hops.hr

Hrvatski operator prijenosnog sustava d.o.o.

Croatia, Zagreb

```
554-mail01.hops.hr
554 Your access to this mail system has been rejected due to the sending MTA's poor reputation. If you believe
```

185.81.228.74

2021-12-29T05:25:30.515870

mail02.hops.hr

Hrvatski operator prijenosnog sustava d.o.o.

Croatia, Zagreb

```
554-mail02.hops.hr
554 Your access to this mail system has been rejected due to the sending MTA's poor reputation. If you believe
```

// LAST UPDATE: 2022-01-10

General Information

Hostnames	**mail01.hops.hr**
Domains	HOPS.HR
Country	**Croatia**
City	**Zagreb**
Organization	**Hrvatski operator prijenosnog sustava d.o.o.**
ISP	**Hrvatski operator prijenosnog sustava d.o.o.**
ASN	**AS200990**

Open Ports

25

// 25 / TCP

-1683705502 | 2022-01-10T23:56:44.538942

```
554-mail01.hops.hr
554 Your access to this mail system has been rejected due to the sending MTA's poor
reputation. If you believe that this failure is in error, please contact the intend
ed recipient via alternate means.
```

hops.hr

Domain Records

	A	**185.81.228.49** 80 443
	MX	mail01.hops.hr
	MX	mail02.hops.hr
	SOA	dns1.hops.hr
	TXT	MS=ms30434184
	TXT	ciscocidomainverification=fccfd69ace84060ab4eec80289db1ccc55d1d5d2a20b13500ed840482cf5d47
	TXT	v=spf1 mx a ip4:185.81.228.71 ip4:185.81.228.72 ~all
isohops	A	**185.81.228.20** 80 443
isohopsproba	A	**185.81.228.27**
webmail	A	**185.81.228.26** 80 443
www	A	**185.81.228.49** 80 443

SHODAN | Explore | Downloads | Pricing | org:"Hrvatski operator prijenosnog sustava d.o.o."

HOPS e-PASIS projekt

2022-01-11T12:33:25.554826

185.81.228.64
Hrvatski operator prijenosnog sustava d.o.o.
Croatia, Zagreb

SSL Certificate

Issued By:
|- Common Name:
R3
|- Organization:
Let's Encrypt

Issued To:
|- Common Name:
e-pasis.eu

Supported SSL Versions:
TLSv1.2

Diffie-Hellman Fingerprint:
RFC3526/Oakley Group 14

```
HTTP/1.1 200 OK
Date: Tue, 11 Jan 2022 12:29:13 GMT
Server: Apache
Last-Modified: Wed, 16 Sep 2020 05:53:38 GMT
ETag: "2c78-5af67e3915c80"
Accept-Ranges: bytes
Content-Length: 11384
Content-Type: text/html; charset=UTF-8
```

HOPS

2022-01-11T04:38:31.501120

185.81.228.49
hops.hr
www.hops.hr
demo.hops.hr
Hrvatski operator prijenosnog sustava d.o.o.
Croatia, Zagreb

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Set-Cookie: .AspNetCore.Antiforgery.GnAe5BJT8T8=CfDJ8GU7nJppnpNJhg24_PlWsMevXWRzznRGRE0xX_gGkcdG_lQp3IMjlxxd3
```

185.81.228.64

Regular View | Raw Data | History

General Information

Country	**Croatia**
City	**Zagreb**
Organization	**Hrvatski operator prijenosnog sustava d.o.o.**
ISP	**Hrvatski operator prijenosnog sustava d.o.o.**
ASN	**AS200990**

Web Technologies

BOOTSTRAP | GOOGLE FONT API | JQUERY

Open Ports

80 | 443

// 80 / TCP

-2071303498 | 2022-01-11T21:35:59.565733

Apache httpd

```
HTTP/1.1 301 Moved Permanently
Date: Tue, 11 Jan 2022 21:31:47 GMT
Server: Apache
Location: https://www.e-pasis.eu
Content-Length: 230
Content-Type: text/html; charset=iso-8859-1
```

Apache httpd

```
HTTP/1.1 200 OK
Date: Tue, 11 Jan 2022 23:12:47 GMT
Server: Apache
Last-Modified: Wed, 16 Sep 2020 05:53:38 GMT
ETag: "2c78-5af67e3915c80"
Accept-Ranges: bytes
Content-Length: 11384
Content-Type: text/html; charset=UTF-8
```

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:ec:c5:9f:50:f5:a5:cd:8e:6f:a1:38:4a:bc:48:d0:59:1c
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Let's Encrypt, CN=R3
        Validity
            Not Before: Dec 30 10:58:54 2021 GMT
            Not After : Mar 30 10:58:53 2022 GMT
        Subject: CN=e-pasis.eu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:c5:34:c3:4c:c6:b8:a0:4c:f0:33:8a:ff:4f:7f:
                    9c:90:8b:45:fd:eb:a8:5f:fd:3e:89:c5:31:92:f1:
                    4b:3d:e4:41:16:b8:d8:7b:de:d0:c9:2d:41:33:3b:
                    a9:e9:be:72:8f:53:8c:21:91:e8:ac:ac:1d:e8:3a:
                    bc:9e:3a:3b:d2:99:55:f7:55:fd:21:d1:26:e5:ff:
                    4b:97:b4:06:7c:cd:bc:13:b3:95:7a:79:34:0f:64:
                    09:8c:6b:42:39:f4:76:9f:12:71:33:10:cf:13:ac:
                    10:07:b5:d6:11:ee:56:56:f5:99:87:49:7f:30:ed:
                    66:06:57:24:a0:51:b0:a4:18:ea:57:f8:22:b8:c2:
                    ae:35:cf:fc:aa:cb:18:00:e0:41:de:23:30:0d:a6:
```

```
            Modulus:
                00:c5:34:c3:4c:c6:b8:a0:4c:f0:33:8a:ff:4f:7f:
                9c:90:8b:45:fd:eb:a8:5f:fd:3e:89:c5:31:92:f1:
                4b:3d:e4:41:16:b8:d8:7b:de:d0:c9:2d:41:33:3b:
                a9:e9:be:72:8f:53:8c:21:91:e8:ac:ac:1d:e8:3a:
                bc:9e:3a:3b:d2:99:55:f7:55:fd:21:d1:26:e5:ff:
                4b:97:b4:06:7c:cd:bc:13:b3:95:7a:79:34:0f:64:
                09:8c:6b:42:39:f4:76:9f:12:71:33:10:cf:13:ac:
                10:07:b5:d6:11:ee:56:56:f5:99:87:49:7f:30:ed:
                66:06:57:24:a0:51:b0:a4:18:ea:57:f8:22:b8:c2:
                ae:35:cf:fc:aa:cb:18:00:e0:41:de:23:30:0d:a6:
                32:4b:6a:29:63:a6:0e:c3:1d:dc:eb:1f:1e:29:c5:
                eb:28:64:5a:fa:e6:62:52:7a:62:d8:ea:df:ca:13:
                c2:91:f8:c2:4a:b6:ac:6b:7c:f9:a6:b5:8c:ac:a9:
                96:7c:67:98:b3:e1:ab:55:d8:31:0c:94:41:81:88:
                3e:bb:51:00:37:f5:29:db:d6:23:97:b1:24:a6:0e:
                c0:1b:ea:49:df:6e:bb:85:a4:7d:82:58:59:83:56:
                2c:62:ed:09:9d:be:6c:4c:be:a0:b9:b1:48:47:b1:
                4b:ed
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Key Usage: critical
            Digital Signature, Key Encipherment
        X509v3 Extended Key Usage:
            TLS Web Server Authentication, TLS Web Client Authentication
        X509v3 Basic Constraints: critical
            CA:FALSE
        X509v3 Subject Key Identifier:
            31:09:DE:B8:05:C8:7F:B4:A8:4A:6E:1E:31:91:DC:6E:AE:09:72:CD
        X509v3 Authority Key Identifier:
            keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6

        Authority Information Access:
            OCSP - URI:http://r3.o.lencr.org
            CA Issuers - URI:http://r3.i.lencr.org/

        X509v3 Subject Alternative Name:
            DNS:e-pasis.eu
        X509v3 Certificate Policies:
            Policy: 2.23.140.1.2.1
            Policy: 1.3.6.1.4.1.44947.1.1.1
```

```
    Signed Certificate Timestamp:
        Version   : v1 (0x0)
        Log ID    : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
                    4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
        Timestamp : Dec 30 11:58:54.598 2021 GMT
        Extensions: none
        Signature : ecdsa-with-SHA256
                    30:44:02:20:25:BA:1A:9C:CF:C2:B4:AD:A7:66:42:51:
                    A1:B5:07:67:76:1D:D2:E4:F9:48:18:0C:6D:A2:51:19:
                    24:34:83:52:02:20:73:25:FB:DF:7C:BE:C6:29:5E:34:
                    20:8C:29:E5:40:EC:DA:52:F9:84:15:E5:E3:6E:41:C4:
                    0B:BB:71:F7:E0:A2
    Signed Certificate Timestamp:
        Version   : v1 (0x0)
        Log ID    : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:
                    11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47
        Timestamp : Dec 30 11:58:54.625 2021 GMT
        Extensions: none
        Signature : ecdsa-with-SHA256
                    30:44:02:20:39:D0:1E:E9:64:D3:C7:42:89:B5:D0:6F:
                    9A:78:62:58:18:DF:79:D9:EF:53:29:1E:D4:F0:2D:A2:
                    A0:93:4D:E3:02:20:32:FD:F9:4F:C9:40:2A:A9:44:58:
                    44:DB:B8:85:A4:6E:A5:9C:C4:49:55:C6:C6:0F:CE:0B:
                    76:02:F9:56:F2:57
Signature Algorithm: sha256WithRSAEncryption
     55:2a:e0:0e:f7:9d:02:b4:8c:d1:94:3e:3c:3c:04:3f:98:c7:
     1c:18:d8:be:ce:48:db:98:74:d8:e7:c5:0c:cc:b3:41:a9:79:
     6b:9e:dd:43:07:36:75:61:cf:c8:48:3e:fb:07:8b:a1:b3:7f:
     dd:06:58:ce:3d:3c:9f:19:26:74:13:37:18:48:b6:a5:5c:45:
     31:3b:e8:af:c8:f8:11:b1:19:9b:c6:2e:4a:f4:23:86:a0:34:
     2a:db:98:55:bc:18:4a:ef:b8:ee:23:95:d5:1c:54:a0:31:61:
     3f:06:32:03:0e:8b:ea:31:3d:77:b5:7c:6d:51:ea:1c:6c:f2:
     73:49:93:d0:57:c6:bb:78:f8:32:c1:54:84:6f:f9:48:e1:6b:
     ae:b5:e0:b0:d8:4b:ac:90:0b:87:c4:70:57:7c:e7:d8:91:db:
     37:91:35:64:f0:9d:08:38:ca:3c:ec:ea:7f:bc:44:e4:b7:dc:
     31:83:61:55:7d:6f:ac:f8:8e:db:1f:02:e2:92:52:26:56:0a:
     fe:f9:55:3d:4e:25:03:21:80:b0:ab:ba:96:fe:d3:32:f4:e3:
     7a:e5:75:8e:64:58:13:5c:54:e5:ad:32:3c:82:a6:4c:cb:5a:
     30:b0:14:08:ca:7c:2c:a4:b3:89:1f:53:c2:d0:1d:ae:92:3f:
     02:1e:03:22
```

// LAST UPDATE: 2022-01-13

General Information

Hostnames	**hops.hr, www.hops.hr, demo.hops.hr**
Domains	HOPS.HR
Country	**Croatia**
City	**Zagreb**
Organization	**Hrvatski operator prijenosnog sustava d.o.o.**
ISP	**Hrvatski operator prijenosnog sustava d.o.o.**
ASN	**AS200990**

Open Ports

80 443

// **80** / TCP -397401213 | 2022-01-13T07:10:23.482946

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Connection: close
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Content-Length: 247
P3P: CP="{}"
Set-Cookie: TS5f5842a5027=088189bcadab2000d0c9a98a3eab13632d9b19946814868781c2c6a0d
6c30be62709229689ba08a208d8c6d1081130007183265 3ff625f671e6c4db96398e9d39a6394637c91
cba8b5382765b826df94895fb24514fa944408a7edab5bebdbfb;Path=/
```

// **443** / TCP 2021357281 | 2022-01-09T09:44:56.557517

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Connection: close
Content-Type: text/html; charset=utf-8
Pragma: no-cache
```

Informacije o infrastrukturi i ustroju organizacije

Unosom domene email adrese pronađene na stranici HOPS-a (https://www.hops.hr/vijesti/obavijest-poslovnim-partnerima-i-suradnicima-hops-a) u alat Shodan, uz navedeno puno ime organizacije, dolazimo do mail01 i mail02 mail adresa i pripadajućih IP adresa. Daljnim promatranjem prve IP adrese vezane uz mail01, dolazimo do podataka kao što su ISP, ASN i povezana domena hops.hr. Odlasom na domenu hops.hr pronalazimo ostale informacije usko vezane uz navedenu domenu kao što su SOA DNS koji označava početak autoriteta servera, odnosno tko je zadužen za navedenu domenu.

Pretraživanjem same organizacije u alatu Shodan pronalazimo dvije IP adrese sa sadržajem koji ćemo dalje promotriti - 185.81.228.64 i 185.81.228.49. Prva IP adresa i povezana stranica odnosi se na interne stranice HOPS-a i nekog od projekata. Pokušajem pristupa navedenoj stranici dobivamo sigurnosno upozorenje o isteku certifikata. Također, možemo vidjeti razne pojedinosti SSL certifikata koji se koristi kao što su koja organizacija je izdala ssl, ime i Diffie Hellman fingerprint. Isto tako detektirane su tehnologije koje se koriste - Bootstrap, Google Font Api i jQuery. Pregledom daljnjih informacija primjećujemo otvorena dva porta 80 i 443, kao i pojedinosti što se na portovima nalazi. Primjećujemo da se nude i pojedinosti vezane za httpd na tcp portu 80 te koja vrste enkripcije (sha256) je korišten za potpise. Druga IP adresa, također ima dva porta na kojima se mogu vidjeti pojedinosti cookie-ja, te hostnames ostalih računala povezanih na mrežu: hops.hr, www.hops.hr, demo.hops.hr.

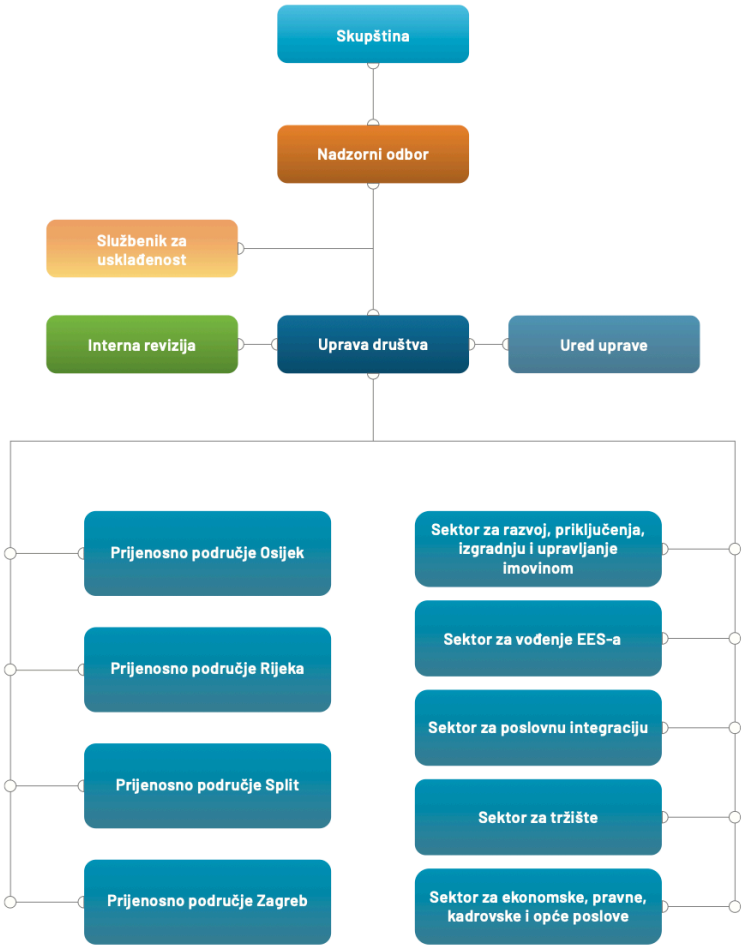
Iz alata Maltego, upisom službene stranice, vidimo da se pojavljuje IP adresa već spomenuta i pronađena preko alata shodan 185.81.228.49.

Informacije o insfrastrukturi kao što je ustroj organizacije vidljive su na javno dostupnim stranicama HOPS-a - https://www.hops.hr/page-file/WAVZXYJGgaU0agrr0C3XF0/godisnji-izvjestaji/HOPS%20GI%202020%20-%2029-7-2020.pdf (str. 20 i 21, screenshot dolje), isto kao i upravljačka struktura sa imenima i prezimena članova. Također, u navedenom dokumentu se nalaze vrlo detaljne statitstike zaposlenih, a vidljivi su i ostali dokumenti poput javne nabave, godišnjih izvještaja i ostalih internih dokumenata.

Suradničke firme HOPSA-a mogu se vidjeti u javno objavljenom članku na službenim stranicama https://www.hops.hr/vijesti/uprava-hops-a-sa-suradnicima-obisla-gradiliste-novog-110-kv-rasklopng-postrojenja-na-lokaciji-el-to-zagreb - to su Končar, Siemens.

Iz računa javne nabave, koji su javno objavljeni do 2017 godine, https://www.hops.hr/page-file/NrzfI9vgWwP3eygW03Q78F/registar/Pregled_sklopljenih_ugovora_2017.pdf dostupnog također na stranicama HOPS-a vidljive su iznosi sklopljenih ugovora.

Organizacijski ustroj



Značaj sakupljenih informacija

Analizom informacija iz oba alata, zaključujemo kako je veliki broj osjetljivih podataka HOPS-a dostupan na internetu - od infrastrukture do imena i prezimena zaposlenika i njihove pozicije. Ovakav pristup dijeljenju povjerljivih i/ili osjetljvih informacija može olakšati put potencijalnim napadačima, što dovodi u pitanje sigurnost ove organizacije.