



# Analýza síťového provozu

Ve společnosti XXXXXXXXXXXX

## Vzorová zpráva

Tento dokument je interním dokumentem Linux Services, bez souhlasu autora nesmí být zveřejněn.

(Implementační scénáře a metodiky aktualizovány dle zákona o kybernetické bezpečnosti - NÚKIB a BSI - IT Grundschutz, Německo)

Ing. Michal Vymazal  
Ing. Jiří Richter

Duben 2019



## Obsah

Analýza síťového provozu.....	3
Externí měřicí bod, WAN.....	4
Topologické schema zapojení sondy.....	4
Sdílení síťových disků.....	4
Identifikované nálezy.....	4
Nešifrovaný přístup k poště, poštovní klient.....	4
Odesílání hesel v nešifrovaném tvaru, protokol HTTP.....	6
Pokus o odeslání dat na servery Cloudflare.....	8
Poštovní klient, imap na portu 143.....	10
Neidentifikovaný provoz, zřejmě externí WiFi router.....	12
Poznámka.....	13
Interní měřicí bod, vnitřní LAN.....	14
Topologické schema zapojení sondy.....	14
Identifikované nálezy.....	14
Odesílání hesel v nešifrovaném tvaru, protokol HTTP.....	14
Pokus o odeslání dat na servery Cloudflare.....	16
Tiskárna, odesílající data na internetový server.....	17
Počítače, odesílající data na internetový server.....	18
Doporučení jednotlivých opatření.....	19
Sdílené datové úložiště (sdílení souborů).....	19
Pevné vnitřní IPv4 adresy pro jednotlivé (nepřenosné) uživatelské stanice.....	19
Hardening www prohlížečů na uživatelských stanicích.....	19
Zákaz IPv6 provozu na všech zařízeních.....	19
Vypnutí ladících funkcí na všech zařízeních.....	20
Vystavení bezpečných (doporučených) parametrů pro šifrované tunely (IKE, IPSEC).....	20
Slovníček pojmů.....	21



## Analýza síťového provozu

Analýza síťového provozu slouží pro vyhodnocení síťového provozu v dané lokalitě. Sondy je možné připojit do jakékoliv LAN nebo WAN sítě. Na základě výstupu ze sondy je možné provést vyhodnocení veškerého síťového provozu v dané lokalitě a určit, zda některé zařízení není např. napadeno škodlivým kódem, optimalizovat provoz jednotlivých zařízení, vyhodnotit stávající bezpečnostní opatření apod.

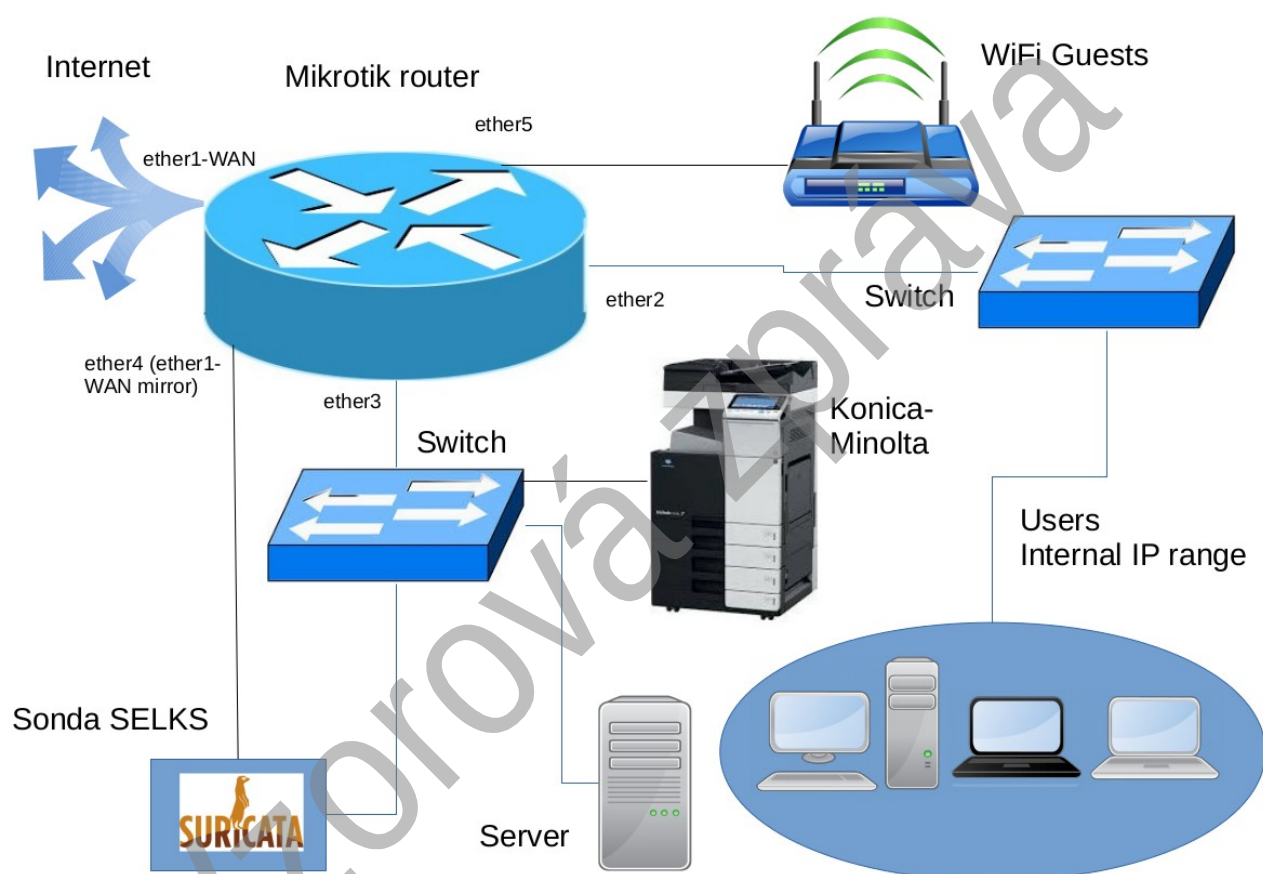
Veškerá analýza síťového provozu probíhá tzv. "pasivním odposlechem", kdy síťová sonda (Analyzátor síťového provozu na bázi programového vybavení Suricata) je připojena k Mirror portu zařízení (Switch, Router) na kterém měříme síťový provoz. Veškerý provoz je pak zaznamenán, analyzován a vyhodnocen. Nedochozí k ovlivňování provozu, prolamování šifer atp.

Tento dokument je interním dokumentem Linux Services, bez souhlasu autora nesmí být zveřejněn.

## Externí měřící bod, WAN

Sonda je připojena k WAN rozhraní externího routeru. Je zachycen veškerý síťový provoz směřující z routeru a interní LAN směrem do internetu a veškerý síťový provoz směřující směrem z internetu na WAN rozhraní routeru a dále veškerý síťový provoz směřující z internetu do vnitřní LAN sítě.

### Topologické schéma zapojení sondy



### Sdílení síťových disků

Na externím měřícím bodu nebyly zachyceny žádné pakety obsahující data z protokolů SMB, NFS nebo jiných nešifrovaných protokolů určených pro síťové sdílení diskových kapacit. Tento nálezní hodnotíme **kladně**.

### Identifikované nálezy

#### Nešifrovaný přístup k poště, poštovní klient

Vlastní komunikace mailového klienta s poštovním serverem není šifrovaná, je



možné sledovat celou komunikaci včetně uživatelského jména a přístupového hesla (user credentials)

## Riziko

Vysoké

## Možné dopady

Útočník může získat kopii mailové korespondence a tyto informace zneužít.

## Doporučení

Přejít na šifrovanou komunikaci mailového klienta s poštovním serverem. Doporučujeme TLSv1.2

**Nastavení serveru**

Typ serveru: Poštovní server (IMAP)

Adresa serveru:  Port: 993   Výchozí: 993

Uživatelské jméno:

**Nastavení zabezpečení**

Zabezpečení spojení: SSL/TLS

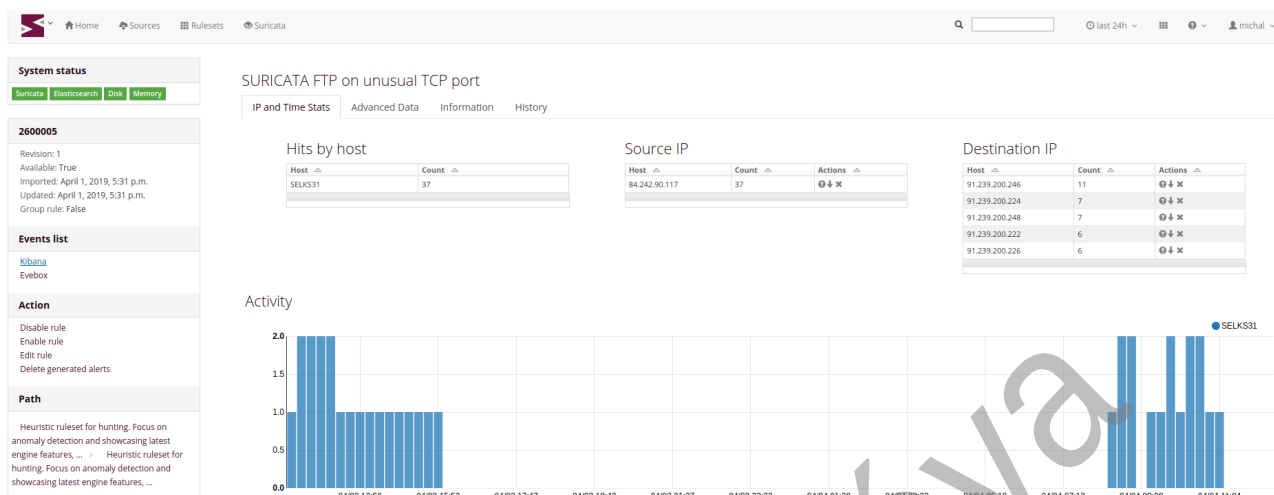
Způsob autentizace: Heslo, zabezpečený přenos

(Obrázek ve vzorové zprávě vynechán)

Ukázka analýzy spojení mailového klienta s poštovním serverem. Spojení není šifrované. Lze identifikovat uživatelský účet a heslo.



Četnost výskytu spojení mailového klienta s poštovním serverem. Spojení není šifrované.



## Odesílání hesel v nešifrovaném tvaru, protokol HTTP

Komunikace se serverem není šifrovaná. Analýzou spojení lze získat uživatelské jméno a heslo k účtu.

### Riziko

Vysoké

### Možné dopady

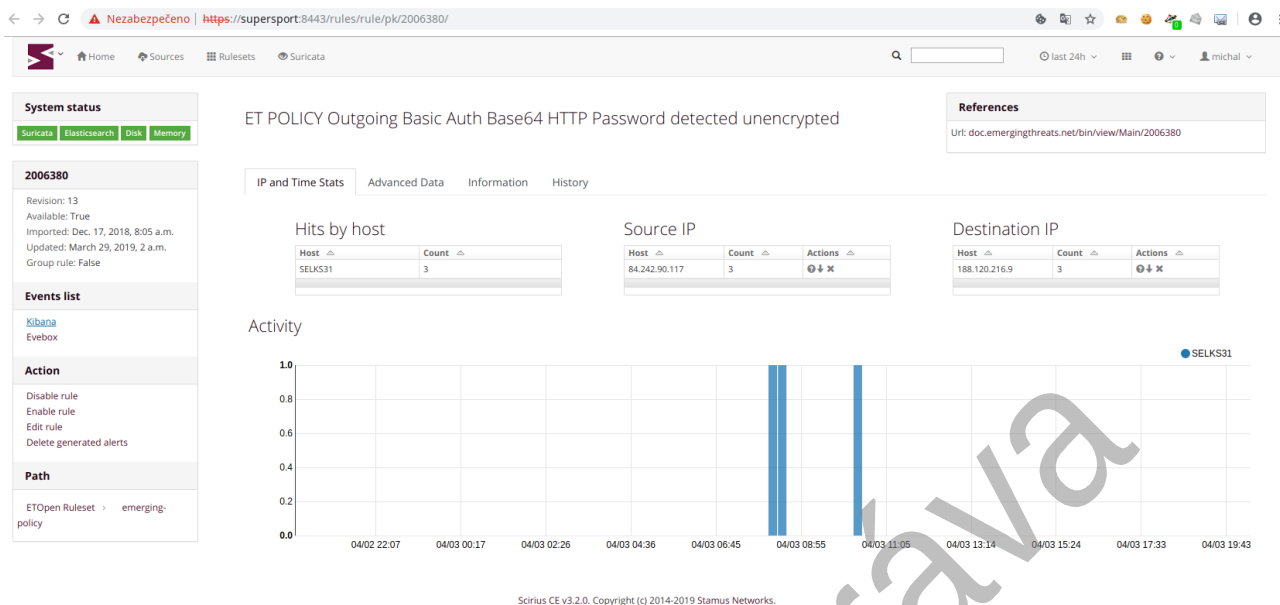
Útočník může získat přihlašovací údaje k serveru a tyto informace zneužít.

### Doporučení

Nalézt zařízení, ze kterého spojení probíhá (viz. následující měření z interního měřicího bodu) a identifikovat aplikaci, která spojení provádí. Určit význam komunikace s tímto serverem.



## Četnost výskytu nešifrovaného spojení na server xx.xx.xx.xx



Analýza spojení se serverem xx.xx.xx.xx. Je patrné uživatelské jméno.

Sessions SPIView SPIGraph Connections Files Stats History Settings Users

ip == 84.242.90.117 && port == 60906 && ip == 188.120.216.9 && port == 8085 && protocols == tcp

Last 24 hours    Start 2019/04/02 20:12:58    End 2019/04/03 20:12:58    Bounding LastPacket Interval Auto

50 per page    1    Showing 1 - 1 of 1 entries

Src IP/Port \* 84.242.90.117 : 60906 ( CZ ) [ AS6830 Liberty Global B.V. ] { RIPE }  
Dst IP/Port \* 188.120.216.9 : 8085 ( CZ ) [ AS49985 IP4ISP z.s.p.o ] { RIPE }  
Payload \* Src 474554202f6a6173 ( GET /jas )    Dst 485454502312e31 ( HTTP/1.1 )  
Tags \*  
TCP Flags \* SYN 1    SYN-ACK 1    ACK 66    PSH 17    RST 0    FIN 2    URG 0

HTTP

Method \* POST GET  
Status code \* 200  
Hosts \* 188.120.216.9:8085 188.120.216.9  
User Agents \* Mozilla/5.0  
Request Headers \* accept-encoding accept-language authorization connection content-length content-type cookie host user-agent x-remote-domain  
Client Versions \* 1.1  
Response Headers \* cache-control content-disposition content-length content-type date expires output-final p3p server set-cookie transfer-encoding  
Server Versions \* 1.1  
Body MD5s \* 9e7834093f23a03207b50236ae67269 a24cb0112e51902b6b3ed4606a7cd727 488cd65ae3a36004a6d32e9434340016 5ef1369708f6b5b9e9d55f84cd117656 dd02d09b61b0ce40d5bee467740b69f 7596b91f6ccea4048034c2cf005f96930  
QS Keys \* fileData userLocale  
Cookie Keys \* JSESSIONID  
User \* jasperadmin  
Auth Type \* basic  
libfile content type \* application/pdf text/plain text/xml

Suricata

Signature \* ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted SURICATA HTTP on unusual port ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted  
Category \* <empty> Potential Corporate Privacy Violation  
Flow Id \* 1178854414945901



## Pokus o odeslání dat na servery Cloudflare

Dochází k neúspěšnému pokusu o odeslání dat na servery Cloudflare

### Riziko

Střední

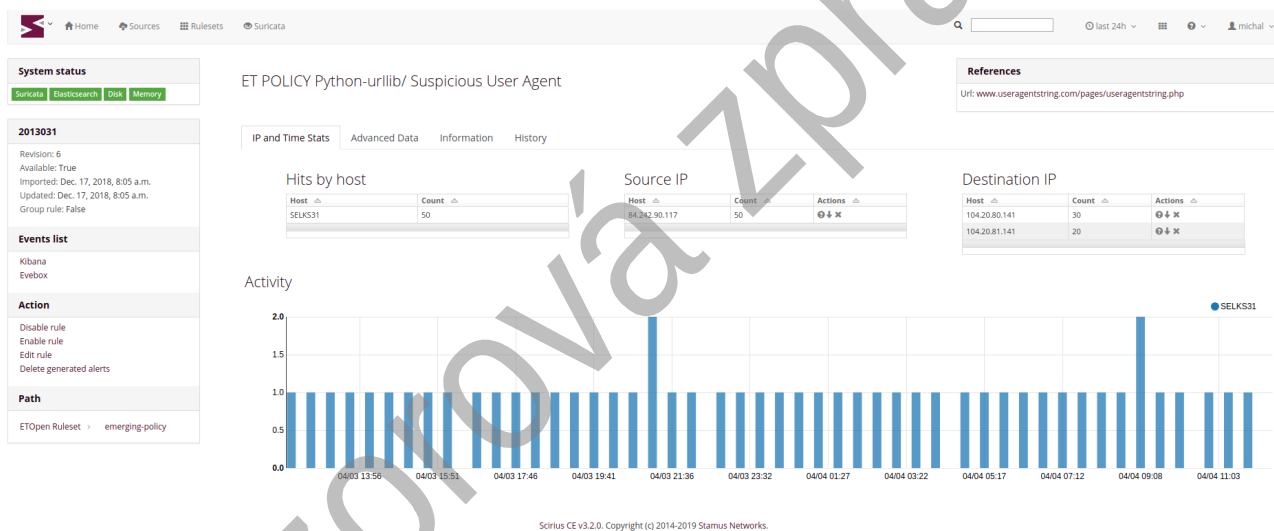
### Možné dopady

Útočník může získat data z interní sítě.

### Doporučení

Nalézt zařízení, ze kterého spojení probíhá (viz. následující měření z interního měřicího bodu) a identifikovat aplikaci, která spojení provádí. Určit význam komunikace s tímto serverem.


Četnost výskytu komunikace se servery Cloudflare








## Identifikace serveru Cloudflare

Home Blog Documentation Pricing Sign-In

---



### 104.20.80.141

Reverse Unknown

---

#### Geoloc \*

Country	US
City	Unknown
Organization	<a href="#">Cloudflare, Inc.</a>
ASN	AS13335
Subnet	104.16.0.0/13

#### Inetnum

Country	US
Netname	Undisclosed
Subnet	Undisclosed
Information	Undisclosed

---

#### Pastries

Nothing known (yet)

#### Resolver

- Forward - [raptr.com](#) (2019-04-04)
- Forward - [raptr.com](#) (2019-04-03)
- Forward - [raptr.com](#) (2019-03-31)
- Forward - [raptr.com](#) (2019-03-26)

---

#### Synscan

- 80/tcp - [Linux](#) (2019-03-29) - <http://104.20.80.141/>
- 443/tcp - [Linux](#) (2019-03-26) - <https://104.20.80.141/>
- 8080/tcp - [Linux](#) (2019-03-21)

#### Datascan

- 443/tcp - [http](#) (2019-04-03) - <https://104.20.80.141/>
- Product - Cloudflare Cloudflare (version: N/A)

```
HTTP/1.1 403 Forbidden
Server: cloudflare
Date: Wed, 03 Apr 2019 17:26:01 GMT
```



## Poštovní klient, imap na portu 143

Poštovní klient "obsluhuje" poštu na poštovním serveru pomocí zastaralých šifrovacích mechanismů. Samotné šifrování na protokolu imap nemusí být příliš "odolné".

### Riziko

Střední

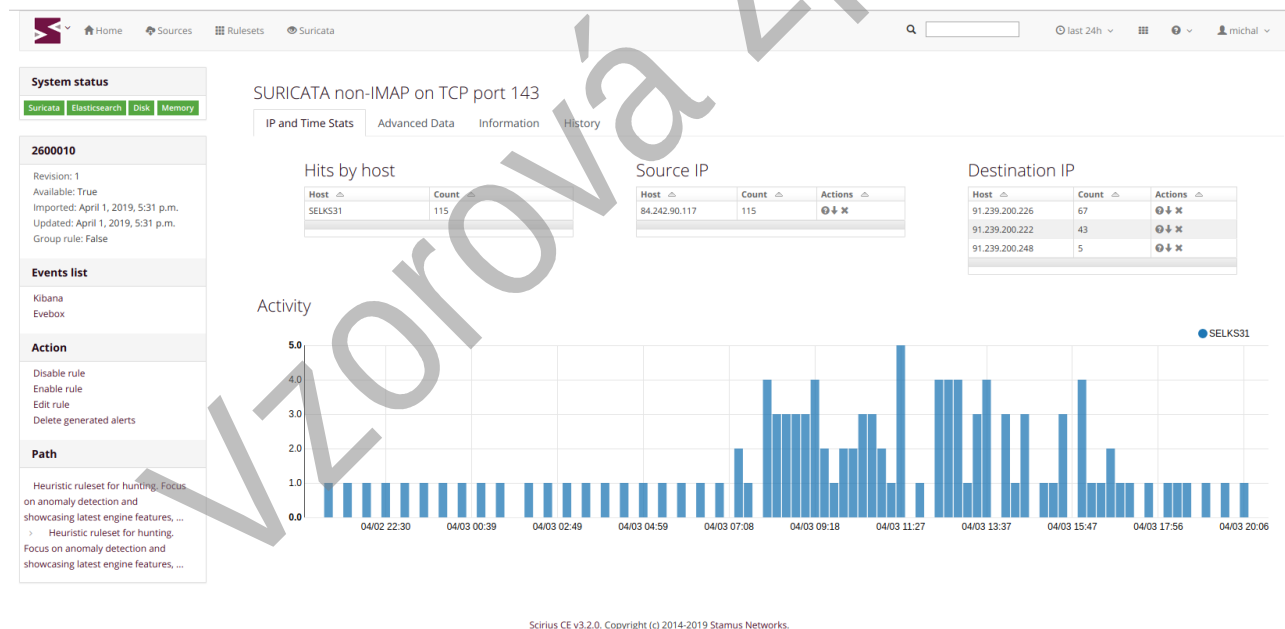
### Možné dopady

Útočník může získat kopii mailové korespondence a tyto informace zneužít.

### Doporučení

Přejít na šifrovanou komunikaci mailového klienta s poštovním serverem. Doporučujeme TLSv1.2. Viz. doporučení z kapitoly "Nešifrovaný přístup k poště, poštovní klient".

### Četnost výskytu spojení





## Analýza spojení poštovního klienta se serverem

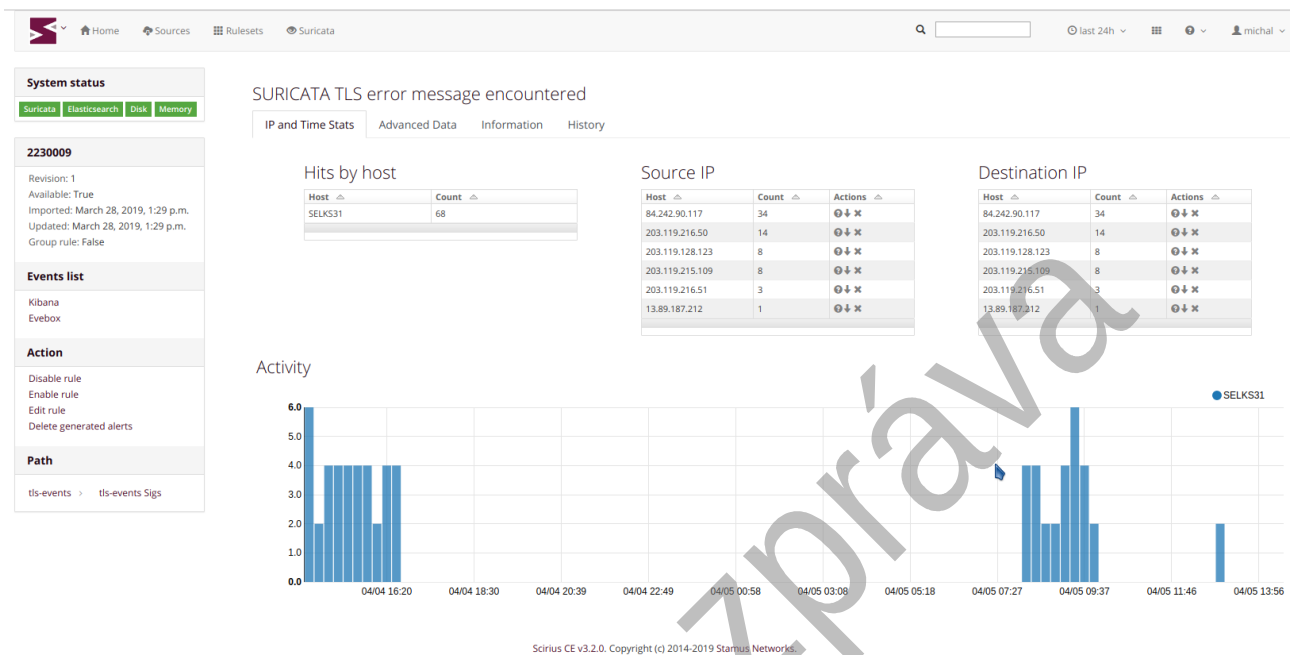
The screenshot displays the Suricata interface with the following details:

- Search Query:** `ip == 84.242.90.117 && port == 54232 && ip == 91.239.200.222 && port == 143 && protocols == tcp`
- Time Range:** Start: 2019/04/02 20:36:28, End: 2019/04/03 20:36:28
- Packet Details:**
  - Time:** 2019/04/03 14:33:52 - 2019/04/03 14:34:23
  - Node:** SELKS31
  - Protocols:** imap, tcp
  - IP Protocol:** tcp
    - Src:** Packets 121, Bytes 120,387, Databytes 113,805
    - Dst:** Packets 79, Bytes 13,896, Databytes 9,330
  - Ethernet:** Src Mac: cc:2d:e0:38:16:3d (OUI: Routerboard.com), Dst Mac: 00:01:5c:69:d6:46 (OUI: Cadant Inc.)
  - Src IP/Port:** 84.242.90.117 : 54232 (CZ) [AS6830 Liberty Global B.V.] [RIPE]
  - Dst IP/Port:** 91.239.200.222 : 143 (CZ) [AS43541 VSHosting s.r.o.] [RIPE]
  - Payloads:** Src: 3367737820434150 (3gxx CAP), Dst: 2a2044b205b4341 (\* OK [CA])
  - Tags:** [C]
  - TCP Flags:** SYN 1, SYN-ACK 1, ACK 113, PSH 82, RST 2, FIN 2, URG 0
- Suricata Signature:**
  - Signature:** GPL login SURICATA non-IMAP on TCP port 143
  - Category:** <empty> An Attempted Login Using a Suspicious Username was Detected
  - Flow id:** 1312218409902641
  - Action:** allowed
  - Gid:** 1
  - Severity:** 2 3
  - Signature id:** 2,600,010 500,720
- Source:** 3gxx CAPABILITY, xs8o STARTTLS
- Destination:** \* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot ready, \* CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS AUTH=PLAIN AUTH=LOGIN, 3gxx OK Pre-login capabilities listed, post-login capabilities have more, xs8o OK Begin TLS negotiation now

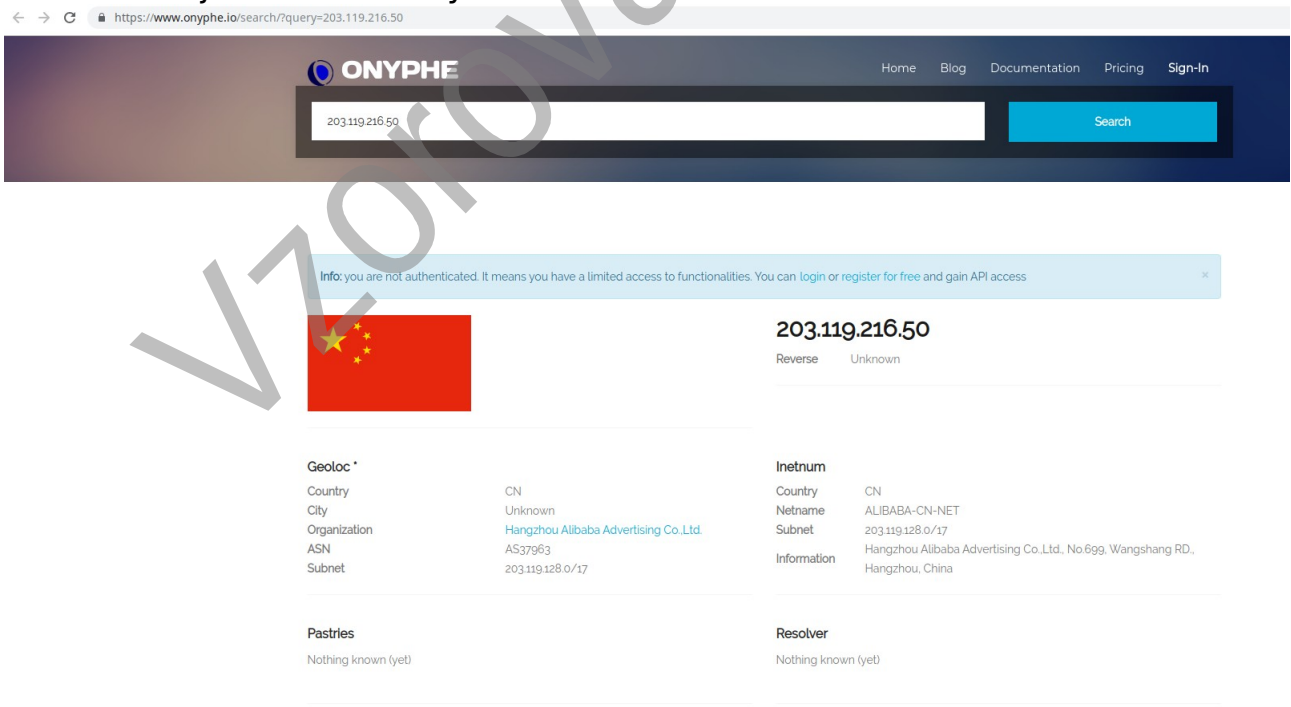


## Neidentifikovaný provoz, zřejmě externí WiFi router

Byl nalezen neidentifikovaný datový provoz. Zařízení se pokoušelo odesílat data na čínské servery



## Identifikace jednoho z čínských serverů





## Ukázka datového toku na čínský server

2019-04-03 10:13:53 6 days ago	ALERT	S: 203.119.216.50 D: 84.242.90.117	SURICATA TLS error message encountered
2019-04-03 10:06:56 6 days ago	ALERT	S: 203.119.216.50 D: 84.242.90.117	SURICATA TLS error message encountered
2019-04-03 08:05:18 6 days ago	FLOW	S: 203.119.216.50 D: 84.242.90.117	TCP 203.119.216.50:443 -> 84.242.90.117:38014; Age: 0; Bytes: 60; Packets: 1
2019-04-03 08:05:18 6 days ago	FLOW	S: 203.119.216.50 D: 84.242.90.117	TCP 203.119.216.50:443 -> 84.242.90.117:38014; Age: 0; Bytes: 60; Packets: 1
2019-04-03 08:03:47 6 days ago	FLOW	S: 203.119.216.50 D: 84.242.90.117	TCP 203.119.216.50:443 -> 84.242.90.117:38014; Age: 18; Bytes: 658; Packets: 7
2019-04-03 08:03:47 6 days ago	FLOW	S: 203.119.216.50 D: 84.242.90.117	TCP 203.119.216.50:443 -> 84.242.90.117:38014; Age: 18; Bytes: 658; Packets: 7
2019-04-03 08:01:09 6 days ago	ALERT	S: 203.119.216.50 D: 84.242.90.117	SURICATA TLS error message encountered
2019-04-02 16:24:04 7 days ago	ALERT	S: 203.119.216.50 D: 84.242.90.117	SURICATA TLS error message encountered

Vylučovací metodou jsme dospěli k zařízení TP-LINK WIFI router. Po dohodě s provozovatelem routeru byl tento router odpojen. Při tomto kroku vyšel najevo fakt, že do „podezřelého“ routeru byla připojena zabezpečovací ústředna Jablotron. Vlastní zabezpečovací ústředna byla přepojena do přepínače (switch) ve vnitřní síti.

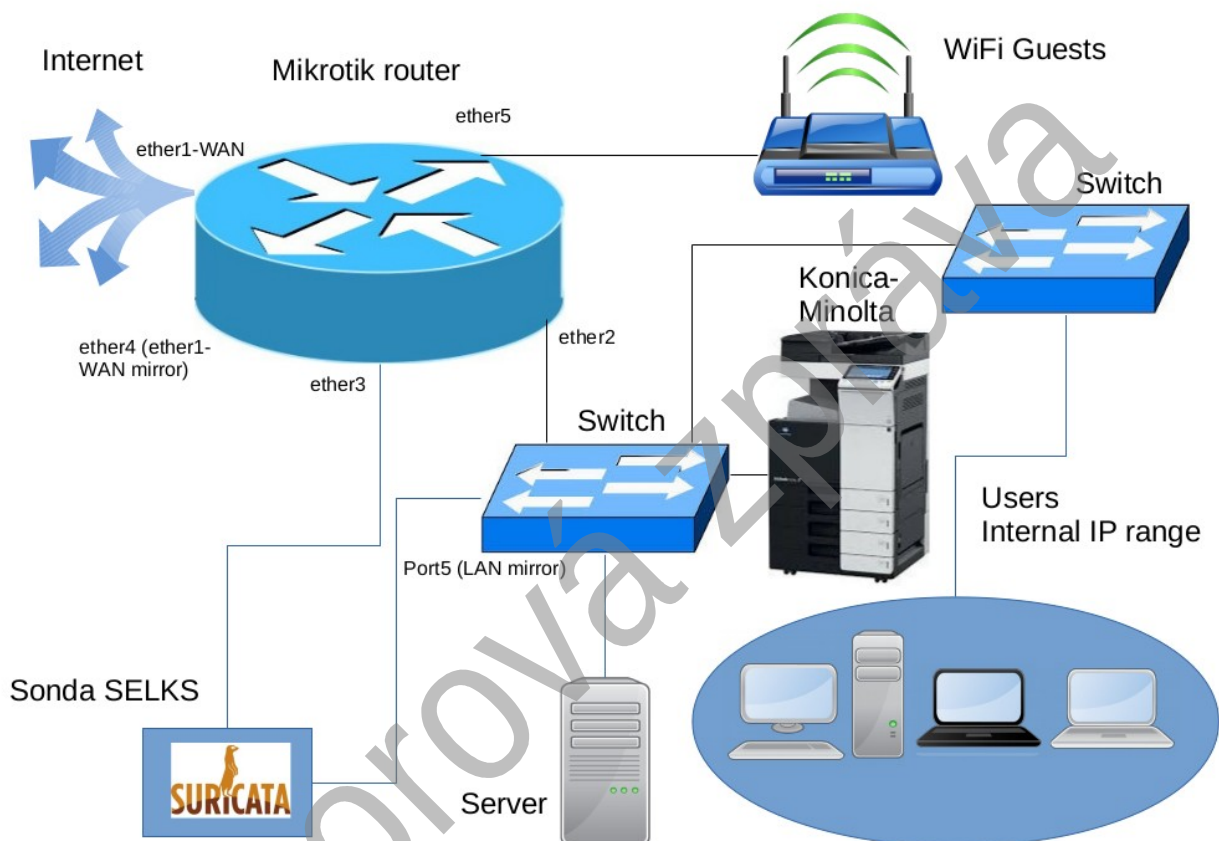
## Poznámka

Toto zjištění hodnotíme jako velmi závažné, zabezpečovací ústředny (resp. jejich datový kanál) by nikdy neměly být připojeny k zařízením podobného typu. Do budoucna doporučujeme konzultovat připojení datového kanálu ústředny s výrobcem zabezpečovací ústředny.

## Interní měřicí bod, vnitřní LAN

Sonda je připojena k LAN rozhraní interního přepínače. Je zachycen veškerý síťový provoz v interní LAN a dále veškerý síťový provoz směřující z interní LAN do internetu a veškerý síťový provoz směřující z internetu do interní LAN.

### Topologické schema zapojení sondy



### Identifikované nálezy

#### Odesílání hesel v nešifrovaném tvaru, protokol HTTP

Komunikace se serverem není šifrovaná. Analýzou spojení lze získat uživatelské jméno a heslo k účtu.

#### Riziko

Vysoké

#### Možné dopady

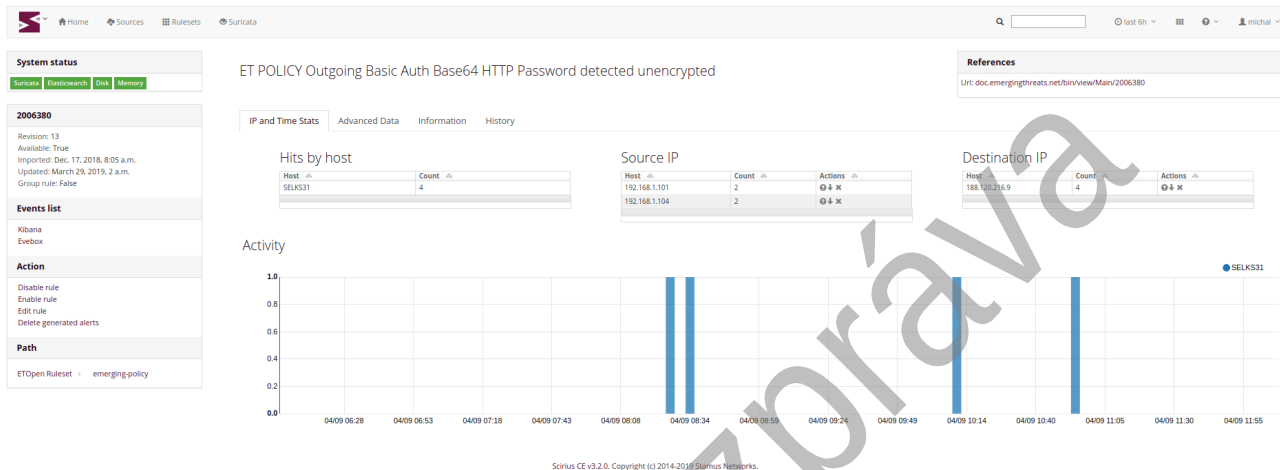
Útočník může získat přihlašovací údaje k serveru a tyto informace zneužít.



## Doporučení

Jedná se o stroje 192.168.1.101 a 192.168.1.104. Na straně serveru je pravděpodobně hotelový rezervační systém. Spojení není šifrováno, na straně serveru je možné identifikovat položky jako "Pokladna".

## Spojení se serverem xx.xx.xx.xx





## Pokus o odeslání dat na servery Cloudflare

Dochází k neúspěšnému pokusu o odeslání dat na servery Cloudflare

### Riziko

### Střední

### Možné dopady

Útočník může získat data z interní sítě.

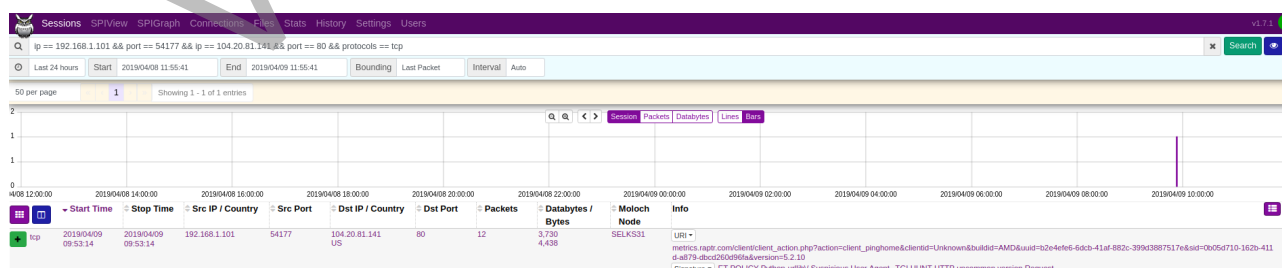
### Doporučení

Jedná se o zařízení s IPv4 interní adresou 192.168.1.101. Je třeba určit význam komunikace s tímto serverem.

## Četnost výskytu komunikace se servery Cloudflare



## Analýza spojení se serverem Cloudflare







## Tiskárna, odesílající data na internetový server

Tiskárna Konica Minolta (IPv4 192.168.1.13) odesílá data na server 195.234.183.240, tato IPv4 adresa je registrována na Konica Minolta Business Solutions Europe GmbH. Data jsou šifrována v rámci protokolu TLSv1.0. Nelze vyloučit, že v rámci odesílaných dat jsou zahrnuty i dokumenty na této tiskárně vytištěné nebo skenované.

### Riziko

Střední

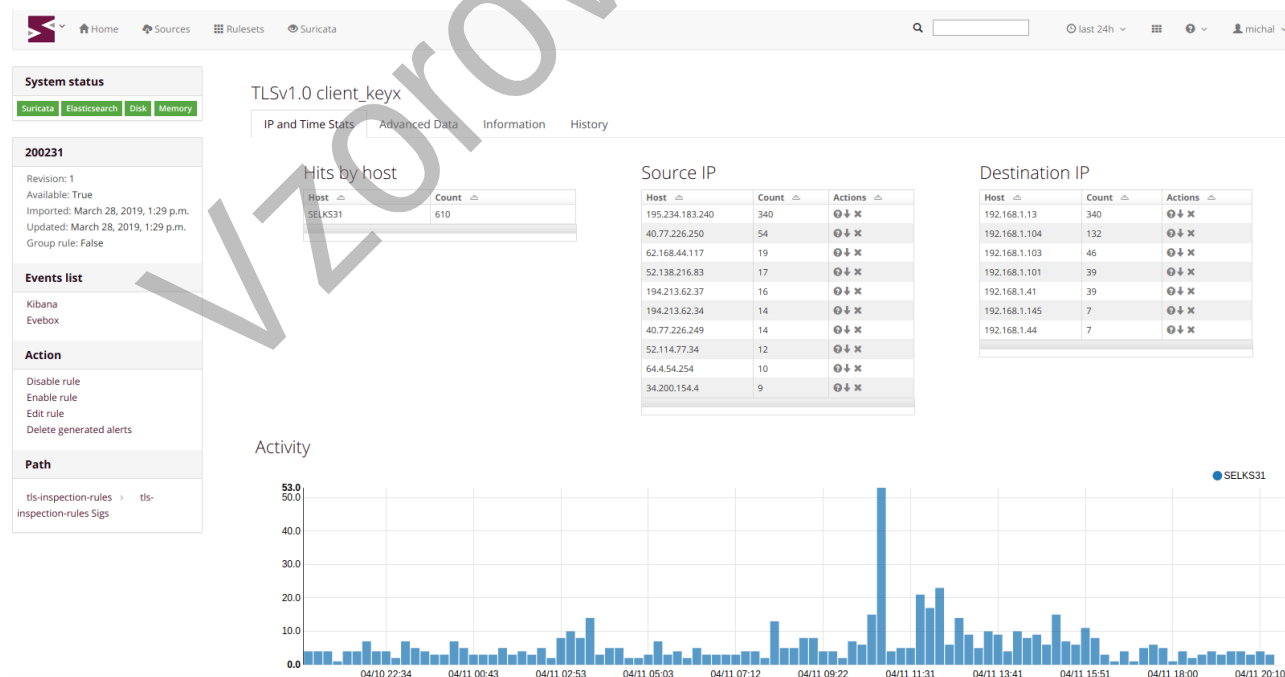
### Možné dopady

Útočník může získat data z interní sítě.

### Doporučení

Doporučujeme zvážit využití multifunkčního zařízení (tiskárna, scanner), které bude autonomní a nebude vysílat data z interní sítě na servery v internetu.

Tiskárna Konica Minolta (IPv4 192.168.1.13) odesílá data na server 195.234.183.240, zbylé public IPv4 adresy patří společnosti Microsoft nebo Google.





## Počítače, odesílající data na internetový server

Některé uživatelské stanice odesílají data na internetové servery společnosti Microsoft nebo Google (obrázek viz. Předchozí obrázek). Data jsou šifrována v rámci protokolu TLSv1.0. Nelze vyloučit, že v rámci odesílaných dat jsou zahrnuta i data nad rámec běžné telemetrie.

### Riziko

Střední

### Možné dopady

Útočník může získat data z interní sítě.

### Doporučení

Doporučujeme vypnout na všech stanicích odesílání telemetrických dat na servery technologických společností (Google, Microsoft aj.)



## Doporučení jednotlivých opatření

### Sdílené datové úložiště (sdílení souborů)

Doporučujeme sdílet datové soubory prostřednictvím privátního datového úložiště. Vhodná je například technologie Nextcloud (<https://nextcloud.com/about>, <https://www.linuxservices.cz/owncloud>). Vlastní přenos dat mezi klientem a serverem je vždy šifrován, data mezi klientem a serverem jsou synchronizována automaticky).

Stávající Samba server doporučujeme vyřadit a již dále nepoužívat. Samba server používá pro komunikaci s jednotlivými stanicemi nešifrovaný protokol, rovněž je problematické ověřování a vystavování přístupových práv k jednotlivým souborům na serveru. **Dále doporučujeme vyřadit služby pro sdílení pevných disků na pracovních stanicích.**

Data ze samba serveru lze zmigrovat na nextcloud server. Tento převod je bezztrátový.

### Pevné vnitřní IPv4 adresy pro jednotlivé (nepřenosné) uživatelské stanice

V současnosti uživatelské stanice dostávají přiděleny vnitřní IPv4 adresy od DHCP serveru. Tato praxe způsobuje, že stejnou IPv4 adresu může postupně získat více uživatelských stanic. V případě jakékoliv anomálie je pak obtížné identifikovat stanici dle IPv4 adresy. Doporučujeme každé uživatelské stanici (jedná se o nepřenosné stroje) přidělit pevnou IPv4 vnitřní adresu a tyto adresy zanést do provozního deníku spolu s popisem (názvem) jednotlivých stanic. Přenosná zařízení budou nadále dostávat IPv4 vnitřní adresy prostřednictvím DHCP serveru.

### Hardening www prohlížečů na uživatelských stanicích

Doporučujeme provést hardening www prohlížečů na uživatelských stanicích. Viz. <https://www.linuxservices.cz/hardening>

### Zákaz IPv6 provozu na všech zařízeních

Některá zařízení mají povolen IPv6 provoz. Doporučujeme vypnout podporu pro IPv6 na všech zařízeních. Na řadě zařízení není v současné době podpora IPv6



dobře implementována a povolení IPv6 tak může představovat bezpečnostní hrozbu.

## Vypnutí ladících funkcí na všech zařízeních

Některá zařízení (patrně přenosné telefony a tablety) mají evidentně povoleny ladící funkce. V případě šifrovacích knihoven toto znamená i povolení TLS režimu

Cipher Suite: TLS\_EMPTY\_RENEGOTIATION\_INFO\_SCSV (0x00ff)

Pokud bude mít tento režim zároveň povolený i server, pak může v rámci vyjednávání parametrů pro šifrované spojení na bázi TLS dojít k tomu, že přenos dat mezi zařízením a serverem nebude šifrován.

## Vystavení bezpečných (doporučených) parametrů pro šifrované tunely (IKE, IPSEC)

Analýzou šifrovaného spojení na bázi IKEv1, IPSEC bylo zjištěno, že některé kanály mají jako alternativu povoleny i parametry 1024 modp group (Diffie Hellmann) a 3DES symetrický šifrovací algoritmus. Oba tyto parametry již dnes nejsou považovány za bezpečné a jsou zakázány. Doporučujeme každému IKE, IPSEC kanálu vystavit samostatný předpis s doporučenými parametry (IPSEC tunnel mode) dle těchto dokumentů

### IKEv1

NÚKIB - Doporučení v oblasti kryptografických prostředků

<https://www.govcert.cz/cs/doporuceni-v-oblasti-kryptografickyh-prostredku/>

### IKEv2

BSI TR-02102-3 "Cryptographic Mechanisms: Recommendations and Key Lengths - Use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2)" Version: 2019-1

<https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-3.pdf>



## Slovníček pojmů

Zkratka	Vysvětlení zkratky
<b>Audit IS</b>	Vlastním auditem informačního systému rozumíme proces jehož výstupem je zdokumentování informačního systému, popis jeho vazeb na okolní informační systémy a prostředí. Metodika BSI pro audit informačního systému <a href="https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/ISRevision/guideline-isrevision_pdf.pdf?__blob=publicationFile">https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/ISRevision/guideline-isrevision_pdf.pdf?__blob=publicationFile</a>
<b>Analýza rizik</b>	Metodika sloužící k rozpoznání, předpovězení a vyhodnocení jednotlivých hrozeb a jejich dopadů na daný informační systém. Analýza rizik navazuje na vlastní bezpečnostní proces a představuje zpětnou vazbu pro daný informační systém a oblasti tímto informačním systémem dotčené. Výstupní dokument je třeba periodicky aktualizovat <a href="https://www.bsi.bund.de/EN/Publications/BSIStandards/standards.html">https://www.bsi.bund.de/EN/Publications/BSIStandards/standards.html</a>
<b>BIA</b>	Business Impact Analysis Analýza dopadů (BIA) je základem celého procesu řízení kontinuity činností organizace (Business Continuity Plan, BCP). <a href="http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf">http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf</a> <a href="https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.html">https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.html</a>
<b>BSI</b>	<i>Bundesamt für Sicherheit in der Informationstechnik</i> Německá národní bezpečnostní autorita (obdoba českého NÚKIB). <a href="http://www.bsi.bund.de">www.bsi.bund.de</a>
<b>DRP</b>	Disaster Recovery Plan Jedná se o metodiky a postupy sloužící k obnově funkčnosti informačního systému po živelných pohromách a jiných zásadních událostech.
<b>ISO</b>	International Organization for Standardization Označení mezinárodní normy <a href="http://www.iso.org/iso/home.html">http://www.iso.org/iso/home.html</a>
<b>NÚKIB</b>	Národní úřad pro kybernetickou a informační bezpečnost <a href="http://www.nukib.cz">www.nukib.cz</a>
<b>NIST</b>	National Institute of Standards and Technology, USA <a href="http://www.nist.gov/">http://www.nist.gov/</a>
<b>Penetrační testy</b>	Cílem penetračních testů je odhalení zranitelností cílového informačního systému, stanovení způsobu jejich možného využití a doporučení vedoucí k jejich nápravě. <a href="http://www.linuxservices.cz/penetracni-testy">http://www.linuxservices.cz/penetracni-testy</a>