Zlatý erb – kyberbezpečnost

Dominik Marek
Kraj Vysočina

Kraj Vysočina

Intro

- Ročník 2023 – do hodnocení vstupují i základní bezpečnostní mechanizmy
- Vznik myšlenky – Kraj Vysočina
- Spolupráce s CSIRT.CZ
  - Testování
  - Know-how
- Nejčastější nálezy při testování

Nejčastější nálezy

Absence DNSSEC

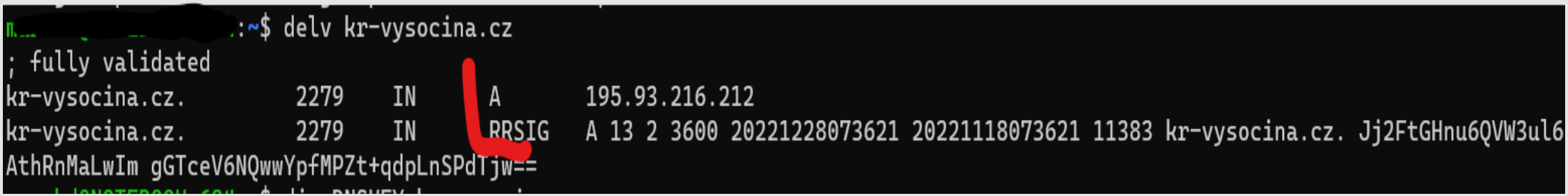
- DNSSEC
  - chrání před MITM, podvržením IP adresy
  - Pomáhá se zabezpečením SMTP (TLSA záznamy & DANE protokol)
- DNSSEC je digitální podpis kořenové zóny
- DNSSEC zavádí nové RR záznamy:
  - DNSKEY – veřejný klíč pro ověření digitálního podpisu
  - RRSIG – samotný digitální podpis RRSetu (nikoliv 1 RR)

```
[redacted]:~$ dig DNSKEY kr-vysocina.cz @8.8.8.8

; <<>> DiG 9.18.1-1-Debian <<>> DNSKEY kr-vysocina.cz @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36195
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;kr-vysocina.cz.                        IN      DNSKEY

;; ANSWER SECTION:
kr-vysocina.cz.         3600    IN      DNSKEY  256 3 13 5ofMYVQTGys1CNEbNdTU6QY7RrwR39iyvrwkLRsGWBxsmMpMw/9iXHyF 9NdlN8yp4LuFsTPcGslSSAoX85piPQ==
kr-vysocina.cz.         3600    IN      DNSKEY  257 3 13 rI7QYW2oaVomZJQ57AG021yLRoyHJu4E8qBsdvdevfg4O5R21JP6Af5D m7Ktm3xG8LUJd1n8Ge2/UvOTu0w4mw==

;; Query time: 41 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sun Nov 20 14:53:20 CET 2022
;; MSG SIZE  rcvd: 203
```

Nejčastější nálezy

Absence DNSSEC

- DNSSEC
  - chrání před MITM, podvržením IP adresy
  - Pomáhá se zabezpečením SMTP (TLSA záznamy & DANE protokol)
- DNSSEC je digitální podpis kořenové zóny
- DNSSEC zavádí nové RR záznamy:
  - DNSKEY – veřejný klíč pro ověření digitálního podpisu
  - RRSIG – samotný digitální podpis RRSetu (nikoliv 1 RR)



Absence DNSSEC

- Užitečné nástroje:
  - dig (bash)
  - delv (bash)
  - https://dnssec-analyzer.verisignlabs.com/
- Další informace:
  - https://www.dnssec.cz/
  - https://www.jakfungujedns.cz/

HTTP headers

- Chybějící bezpečnostní hlavičky
  - Strict-Transport-Security (HSTS)
    - Po stanovenou dobu komunikuj pouze přes HTTPS
    - Lepší než redirect (302)
  - Content-Security-Policy (CSP)
    - Definice odkud mohou být načítány které zdroje
    - Ochrana před XSS
  - X-Frame-Options (XFO)
    - Brání zneužití obsahu webu na cizím webu
  - X-Content-Type-Options
    - Říká prohlížeči, jak se má chovat k MIME typům
    - (ochrana např. před scripty v txt či img)
  - Set-Cookie - Nastavení flagů pro session cookies:
    - » Secure
    - » HttpOnly

HTTP headers

- Přebývající bezpečnostní hlavičky
  - Ty hlavičky, které odhalují citlivé informace
  - Server
    - Apache/2.4.38 (Debian)
    - Microsoft-IIS/7.5
  - X-Powered-by
    - ASP.NET
    - PHP/5.4.45

HTTP headers

- Další informace a nástroje:
  - www.securityheaders.com
  - https://securityheaders.cz/
  - https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers
  - Testssl (bash) - https://testssl.sh/

TLS (Transport Layer Security)

- Podpora zastaralých verzí TLS protokolu
- SSL2.0, SSL3.0, TLS1.0, TLS1.1 – zastaralé, zranitelné
- TLS1.2 a TLS1.3 – požadované, ale správně nakonfigurované
- Doporučené postupy:
  - Server prefered order
  - Upřednostňovat eliptické křivky (např. ECDHE vs DHE)
  - Výměna klíčů podporuje Perfect forward secrecy
    - Tzn. že šifrovací klíč je vyměněn mezi klientem a serverem tak, aby jej nebylo možné získat se znalostí privátního klíče serveru
    - Zajistí DHE nebo ECDHE
    - E>>ephemeral – pro každou session je generován nový set klíčů
  - AEAD
  - Délky klíčů – viz doporučení NÚKIB
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS (Transport Layer Security)

- Nástroje:
  - Online:
    - https://www.ssllabs.com/ssltest/index.html
    - https://observatory.mozilla.org/
  - testssl (bash)
    - https://testssl.sh/
- Další informace:
  - https://ciphersuite.info/
  - https://nukib.cz/cs/infoservis/doporuceni/1843-doporuceni-v-oblasti-kryptografickych-prostredku-verze-2-0
  - https://wiki.mozilla.org/Security/Server_Side_TLS
  - https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml

Kontakt

Děkuji za pozornost!

Dominik Marek

Bezpečnostní analytik

Krajský úřad Kraje Vysočina

marek.dominik@kr-vysocina.cz

tel: 564 602 325

gsm: 724 650 242