50 let e-mailu

… a stále s ním neumíme pracovat

Srpen 2024

Jan Dušátko (jan.dusatko@cryptosession.cz)
Jan Kopřiva (jan.kopriva@untrustednetwork.net)

https://cryptosession.cz/download/LinuxDays2024.pdf

SPAM nebo E-MAIL

E-MAIL nebo SPAM

Stav využívání technologií v roce 2023

- Odhadovaná zátěž $3{,}473 \cdot 10^{11}$ e-mailů denně, tedy $1{,}268 \cdot 10^{14}$ e-mailů ročně
- Meziroční nárůst počtu e-mailů 4, 3 %
- 85 % e-mailů je označeno jako spam a 49 % e-mailů je prokazatelně spam
- 14,3 % běžné e-mail komunikace je chybně zachyceno spam filtry
- Přibližně 4.3 miliardy uživatelů vlastní asi 7.9 miliard poštovních účtů
- Meziroční nárůst počtu poštovních účtů je 2,7 %
- Průměrná velikost e-mailu bez obrázků je 50KB, s obrázky 2,5MB
- Přečtení průměrného e-mailu zabere 10s

Denně lidstvo stráví čas zhruba 15 000 člověkoroků pouze čtením přijatých e-mailů.
Denně se v e-mailech přenese téměř 700 EB dat. Pravděpodobně téměř polovinu tohoto objemu tvoří spam a malware.

Zdroj: https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/

Nevyžádaná pošta (SPAM)

Základní fakta

- Nevyžádaná pošta je subjektivní hodnocení, proto objektivní filtry nikdy nemohou být dokonalé
- Organizace vyžadují objektivní hodnocení
- Konsenzuální dohoda na akceptované formě cenzury (odmítání, mazání, editaci komunikace)
- Účel ochrany
  - primárně za účelem ochrany před maligním obsahem
  - sekundárně za účelem ochrany před uživatelem nevyžádanou (nezajímavou, nepodstatnou nebo neužitečnou) komunikací, zatěžující pozornost a zabírající čas
- Pravidla určuje vlastník nebo provozovatel systému
- Nedodržování pravidel může vést k odmítnutí komunikace (dodržování norem, společensky přijatelného chování nebo legislativních pravidel)

Nevyžádaná pošta (SPAM) a technologie

Současné technologie dovolují

- Odesílateli nabízet metody k jeho ověření
  (poskytnutí nástrojů pro zvýšení důvěryhodnosti a ochranu značky)
- Příjemci využít metody k ověření odesílatele
- Na základě pravidel příjemce a dokonce i odesílatele zamítnout poštu, která neprošla ověřením
- Tyto technologie pouze **NABÍZÍ** možnost ověření, příjemce by je **MĚL** ve vlastním zájmu využívat
- Příjemcova svobodná vůle určuje, zda tyto možnosti využije

Závěr:

Příjemce nelze nutit ke kontrole ověřitelnosti e-mailů, ale příjemce nemůže využít chybějících mechanismů.

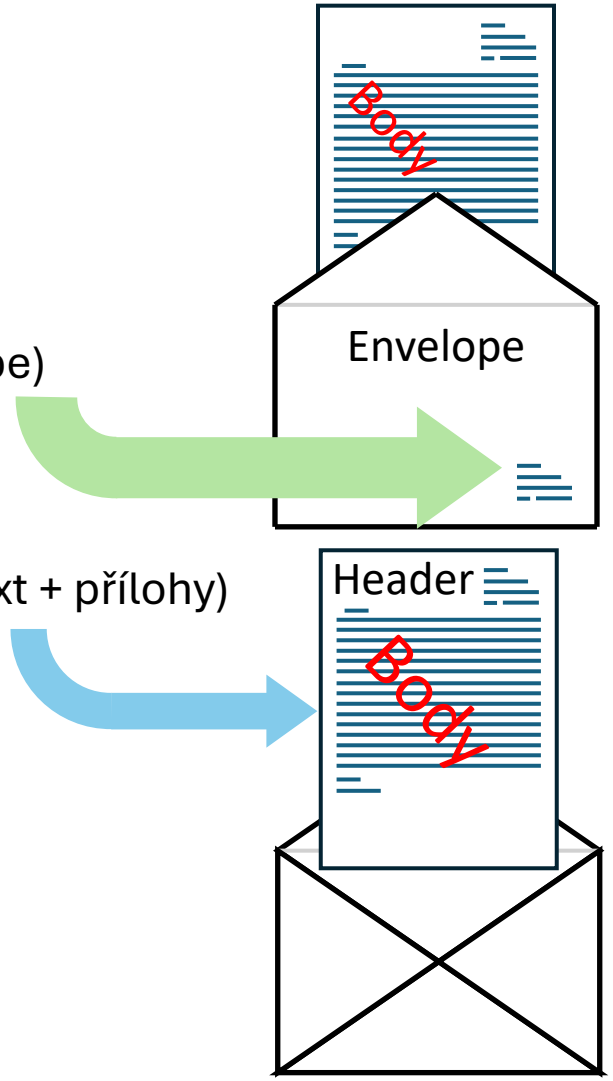
Poskytování těchto mechanismů lze považovat za formu slušného chování (etiky).

Nikdo vás nemůže nutit bavit se s neslušnými. Protože vady v chování mohou mít i finanční podobu.

Struktura e-mailu

SMTP protokol poskytuje informace o obálce (envelope)

SMTP protokol v rámci dat přenáší hlavičku a body (text + přílohy)



RFC:
- 5321
- 5322

Mangling – přepis hlaviček dovoluje upravit hlavičkové záznamy.

Munging – maskování e-mail adres jako ochrana před jejich sběrem (zpravidla na web stránkách).

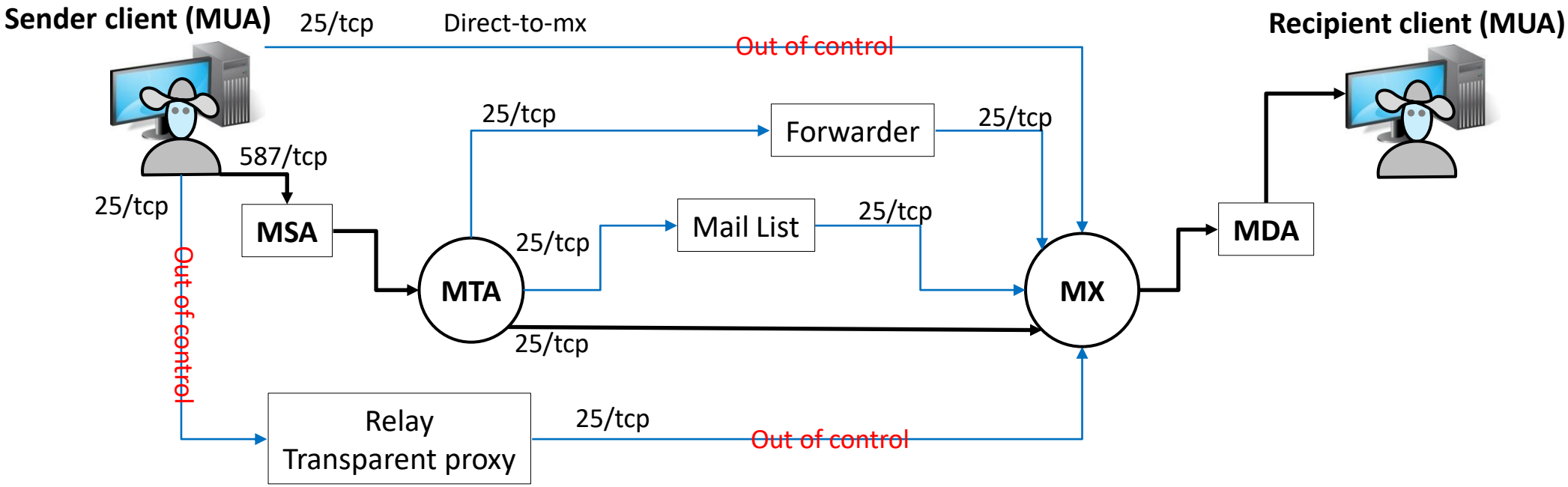
Struktura SMTP komunikace

SMTP protokol dovoluje ochranu proti výpadku komunikace (dostupnosti)

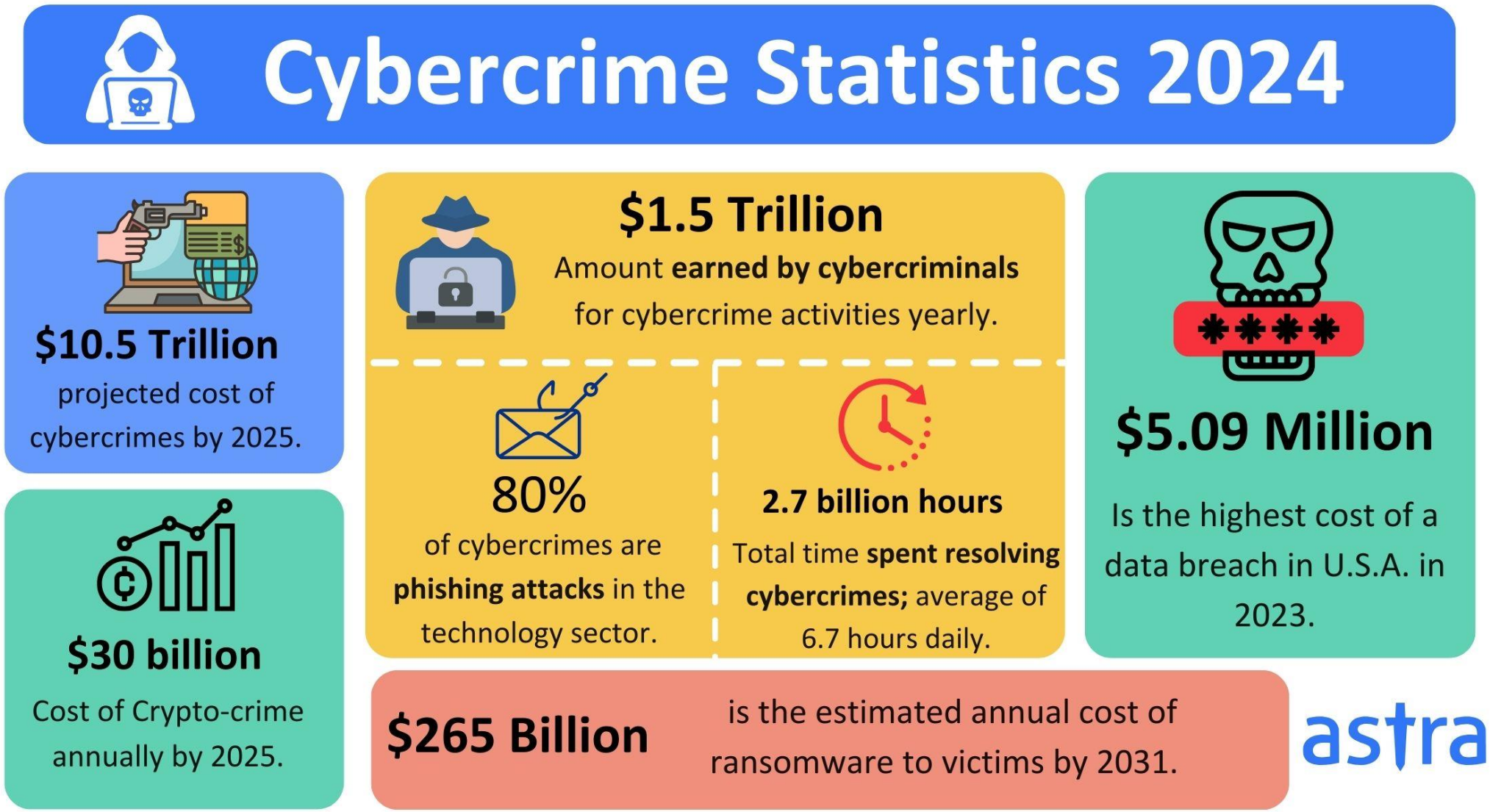
SMTP protokol NEZAJIŠŤUJE doručení koncovému uživateli (Silent Drop na MX) nebo přečtení zprávy uživatelem

Zajištění ochrany jména odesílatele vyžaduje striktní kontrolu nad poskytnutými komunikačními kanály

Mimo portu 25/tcp (zpravidla STARTTLS) se používají 587/tcp (zpravidla TLS nebo STARTTLS) a 465/tcp (zpravidla TLS)



Výhled na rok 2024



HDP 2022

Svět
$101{,}3.10^{12}$ USD

USA
$25{,}44.10^{12}$ USD

Čechy
$0{,}209.10^{12}$ USD

Slovensko
$0{,}115.10^{12}$ USD

https://www.getastra.com/blog/security-audit/cyber-crime-statistics/


FASCINATING
TELL ME ALL ABOUT YOUR BEST PRACTICES
makeameme.org

IETF (Internet Engineering Task Force)

Jedná se o mezinárodní neziskovou oborovou organizaci

- Zastupuje akademickou sféru i výrobce software/hardware
- Poskytují standardy (RFC), kterými se řídí provoz internetu
- Poskytují doporučení (BCP)
- Odklon od těchto standardů může zapříčinit výrazný nárůst obtížnosti komunikace

https://www.rfc-editor.org/retrieve/

Zájmové organizace M³AAWG a APWG

M³AAWG je mezinárodní nezisková organizace, sdružující subjekty poskytující nebo využívající služby elektronické pošty (The Messaging, Malware and Mobile Anti Abuse Working Group)

Říjen 2023: Google a Yahoo oznámili pravidla, ke kterým se postupně připojují Apple, Meta, Microsoft a další ...

- Validní forward a reverse DNS záznamy poštovních serverů
- **Nutnost** používat alespoň technologie SPF+DKIM+DMARC
- Pro marketingovou komunikaci jsou vyžadované hlavičky Precedence, List-Unsubscribe-Post, List-Unsubscribe
- Objem reportované nevyžádané pošty pod 0,3%

M³AAWG | Messaging Malware Mobile Anti-Abuse Working Group

https://www.m3aawg.org/

APWG je mezinárodní nezisková organizace s cílem zvýšit ochranu před kyberzločinem (Anti Phishing Working Group)

APWG

https://apwg.org/

Řešení na území České republiky

NUKIB (CZ) 11. října 2021 vydal ochranné opatření vydané na základě § 14 zákona č. 181/2014 Sb., o kybernetické bezpečnosti (číslo jednací: 8477/2021-NÚKIB-E/350):

- Orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti … které jsou zároveň orgány veřejné moci zapojenými do předsednictví České republiky v Radě EU … podílejících se na přípravách a výkonu předsednictví v roce 2022, musí splnit body … nejpozději do 1. července 2022.

- Ostatní orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti, musí splnit body 1.1. až 1.8. nejpozději do 1. ledna 2023.

Požadavky na splnění:
- Podpora DNSSEC a DANE TLSA
- Implementace SPF, DKIM, DMARC
- MTA-STS a TLS 1.2+, validní certifikáty

Další změny budou pravděpodobně vycházet z implementace NIS2

Řešení na území Slovenské republiky

CSIRT (SK) vydal:

- "Odporúčané nasadenie overovacích a autorizačných systémov pre e-mailové servery" dne 21.05.2021

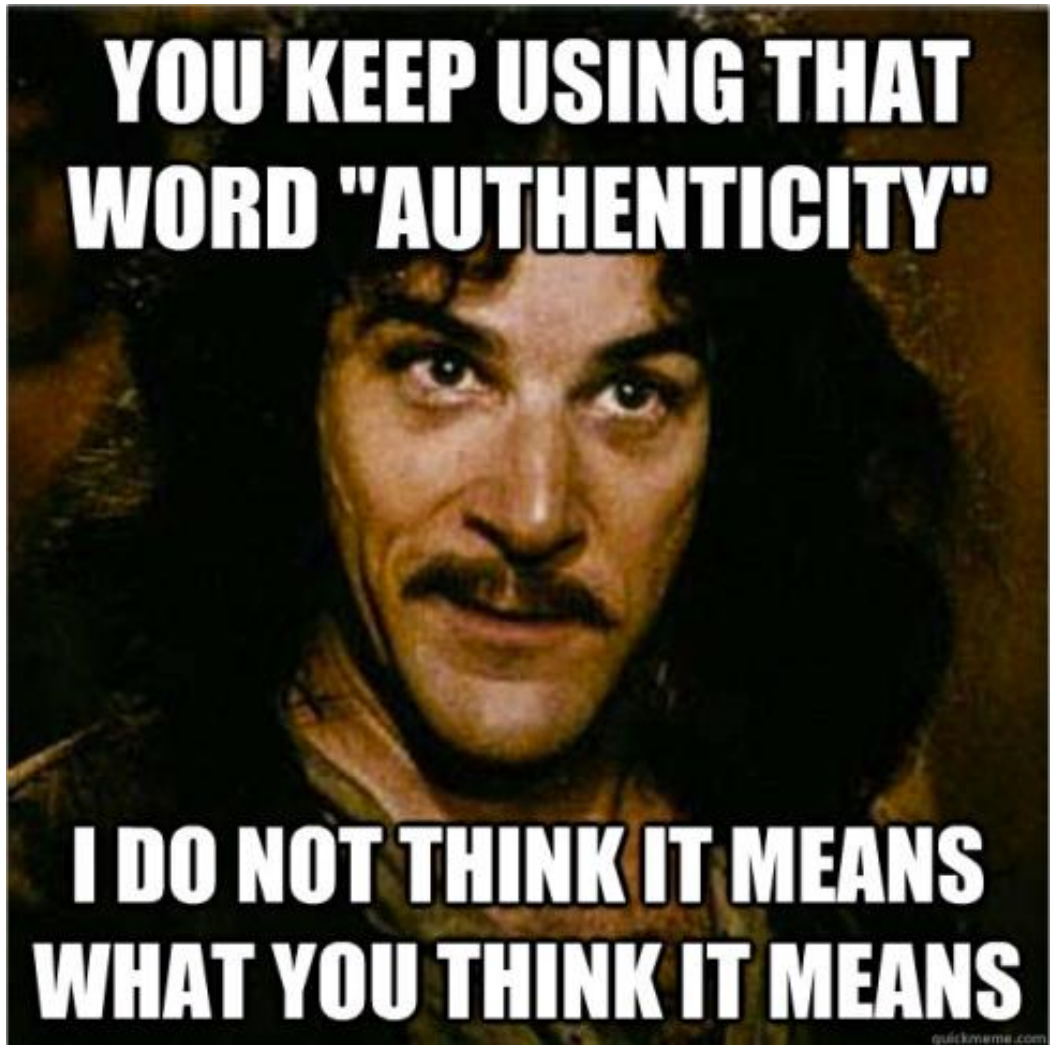
- "Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti" 28.02.2024

Doporučení na splnění:
- SPF, DKIM, DMARC

Další změny budou pravděpodobně vycházet z implementace NIS2

Přehled technologií: Autenticita zdroje původu

- Forward lookup / Reverse lookup / Forward confirmed reverse lookup
- SPF
- SenderID (zastaralé)
- Domainkey (zastaralé)
- DKIM
- ADSP (zastaralé)
- ATPS
- DMARC
- ARC
- BIMI



Reverzní záznamy a odpovědnost

Použití dopředných a zpětných záznamů je vyžadováno v RFC 5321 , RFC 1912 a RFC 2821

- Doména má definovaného vlastníka
- IP adresy mají zase svého vlastníka (zpravidla jsou součástí autonomních systémů a pronajaté dále)
- Neexistuje vlastnický vztah mezi IP a DNS
- Adresní záznam může vytvořit vlastník domény v DNS (**Forward lookup**)
- Reverzní záznam zřizuje vlastník IP adres tj. rDNS (**Reverse lookup**)
- Potvrzení souladu DNS názvů FCrDNS (**Forward Confirmed Reverse Lookup**)

Tedy dopředné a reverzní záznamy tvoří ucelený vztah a zároveň jistou úroveň slabé autentizace

RFC:
- 5321

U domén další úrovně poskytnutých vlastníkem třetí straně je problém s určením odpovědnosti.
Návrh řešení: DBOUND TXT record - https://datatracker.ietf.org/doc/html/draft-levine-dbound-dns

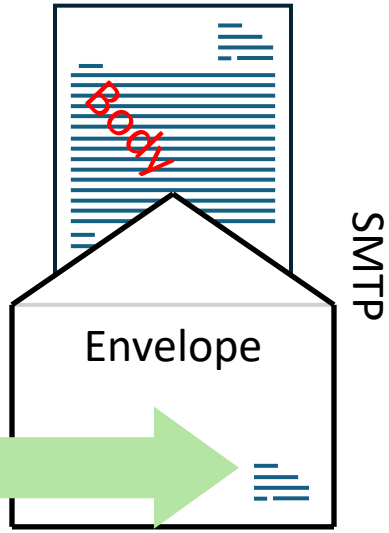
```
_bound.domain.tld IN TXT "bound=1 NOBOUND . domain.tld"
```

SPF – Sender Policy Framework

Locator: @ domain.tld

Header after MTA …

```
Received-SPF: pass (mailfrom) identity=mailfrom; client-ip=123.45.67.89;
helo=server.sender.tld; envelope-from=noreply@sender.com;
receiver=<UNKNOWN>
```




```
220 server.targetdomain.tld ready
EHLO server.sourcedomain.tld
250-server.domain.tld
.......
MAILFROM sender@sourcedomain.tld
250 2.1.0 Sender OK
RCPT-TO recipient@targetdomain.tld
250 2.1.5 Recipient OK
DATA
354 Start mail input
From: sender@sourcedomain.tld
To: recipient@targetdomain.tld
Subject: Important message
--- content ---
.
QUIT
```

RFC:
- 7208

Service:
- DNS

Protocol:
- SMTP
- DNS

SPF → DMARC

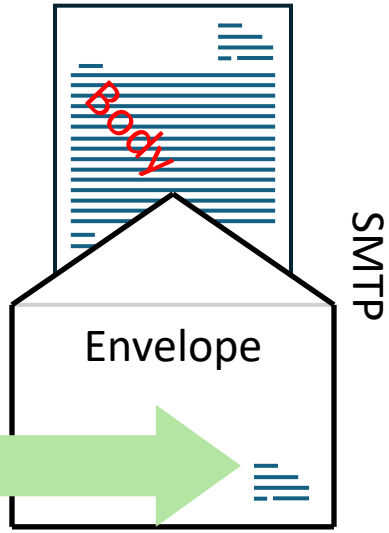
ARC

DKIM

BIMI

SenderID

Locator: @ domain.tld




```
220 server.targetdomain.tld ready
EHLO server.sourcedomain.tld
250-server.domain.tld
.......
MAILFROM sender@sourcedomain.tld
250 2.1.0 Sender OK
RCPT-TO recipient@targetdomain.tld
250 2.1.5 Recipient OK
DATA
354 Start mail input
From: sender@sourcedomain.tld
To: recipient@targetdomain.tld
Subject: Important message
--- content ---
.
QUIT
```

RFC:
- 4406

Service:
- DNS

Protocol:
- SMTP
- DNS

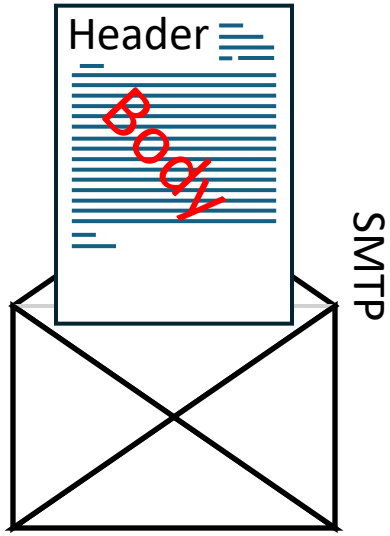
SPF ARC DMARC DKIM BIMI

DK (DomainKey)

Locator: *selector*._domainkey.domain.tld

Headers after MTA …

DomainKey-Signature: a=rsa-sha1; s=selector1; d=domain.tld; c=simple; q=dns; b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZVoG4ZHRNiYzR;



RFC:
- 4870

Service:
- DNS

Protocol:
- SMTP
- DNS

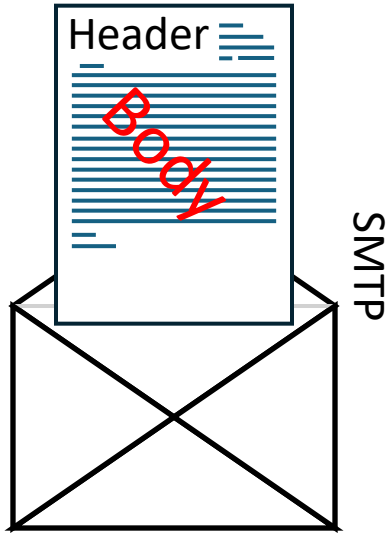
SPF ARC DMARC DKIM BIMI

DKIM – Domain Key Identified Mail

Locator: *selector*._domainkey.domain.tld

Headers after MTA …

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; q=dns/txt; d=sender.tld; i=marketing@sender.tld; s=dkimselector; h=Message-Id:Date:From:To:Subject:CC:Sender:Reply-To:MIME-Version:Content-Type:List-ID:List-Unsubscribe:List-Unsubscribe-Post:Feedback-ID:Precedence; bh=[*digital signature in Base64*]



RFC:
- 4871
- 5672
- 6376
- 8301
- 8463
- 8553
- 8616

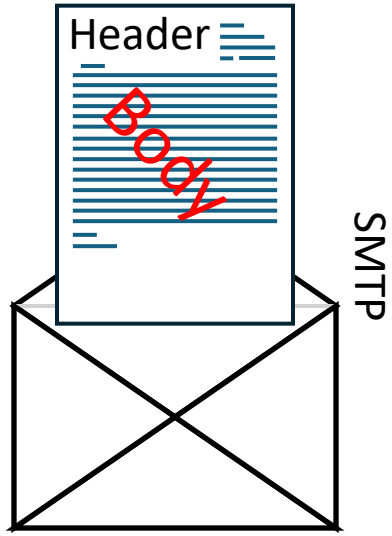
Service:
- DNS

Protocol:
- SMTP
- DNS

SPF ARC DMARC **DKIM** BIMI

ADSP – Author Domain Signing Practice

Locator: `_adsp.domain.tld`



RFC:
- 5617

Service:
- DNS

Protocol:
- SMTP
- DNS

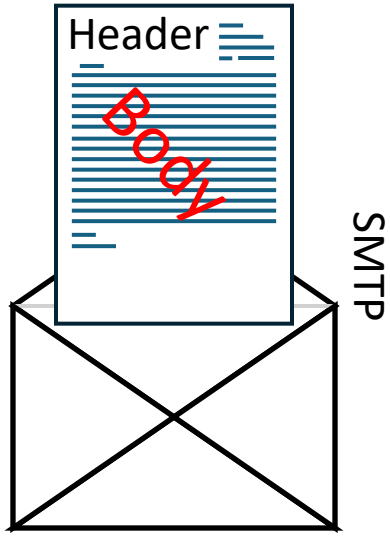
SPF ARC DMARC **DKIM** BIMI

ATPS – Authorized Third Party Signature

Locator: `domain.tld._atps.3rdparty.tld`
`[`*hash_názvu_domény*`]._atps.3rdparty.tld`

Headers after MTA …

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; q=dns/txt; d=sender.tld; i=marketing@sender.tld; s=dkimselector; h=Message-Id:Date:From:To:Subject:CC:Sender:Reply-To:MIME-Version:Content-Type:List-ID:List-Unsubscribe:List-Unsubscribe-Post:Feedback-ID:Precedence; bh=[*digital signature in Base64*]; **atps=3party.tld; atpsh=none**



RFC:
- 6541

Service:
- DNS

Protocol:
- SMTP
- DNS

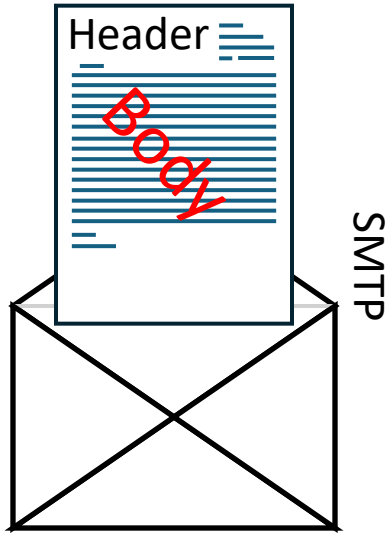
SPF ARC DMARC **DKIM** BIMI **ATPS**

DMARC – Domain-based Message Authentication, Reporting and Conformance

Locator: `_dmarc.domain.tld`

Headers after MTA …

Authentication-Results: server.targetdomain.tld; dkim=pass (2048-bit key; unprotected) header.d=sourcedomain.tld header.i=@sourcedomain.tld header.a=rsa-sha256 header.s=selector header.b=aabbccdd; dkim-atps=neutral



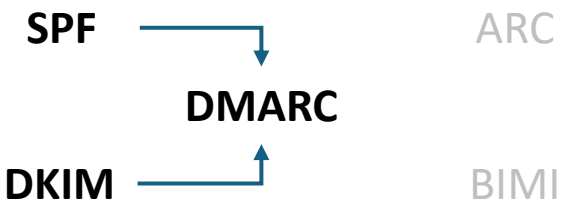
RFC:
- 7489
- 7601
- 8601
- 8616
- 9091

Service:
- DNS
- SPF

or

- DKIM

Protocol:
- SMTP
- DNS



ARC – Authenticated Receive Chain

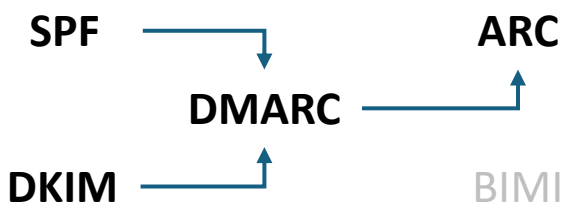
Locator: *selector*._domainkey.domain.tld

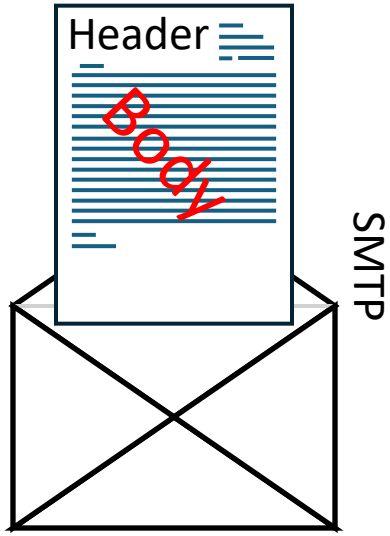
Headers after MTA …

ARC-Seal: i=1; a=rsa-sha256; s=arcselector; d=trusted.1$_{st}$1hop.tld; cv=none; b=[*digital signature in Base64*]

ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=sourcedomain.tld; s=arcselector; h=Message-Id:Date:From:To:Subject:CC:Sender:Reply-To:MIME-Version:Content-Type:List-ID:List-Unsubscribe:List-Unsubscribe-Post:Feedback-ID:Precedence; bh=[*digital signature in Base64*]

ARC-Authentication-Results: i=1; trusted.1$_{st}$1hop.tld 1; spf=pass smtp.mailfrom=sourcedomain.tld; dmarc=pass action=none header.from=sourcedomain.tld; dkim=pass header.d=sourcedomain.tld; arc=none





RFC:
- 8617

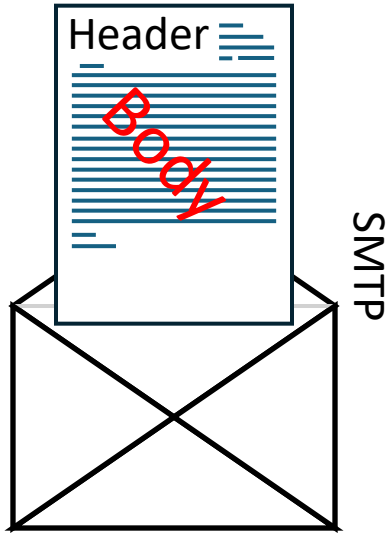
Service:
- DMARC
- DNS

Protocol:
- SMTP
- DNS

BIMI – Brand Message Mail Identification

Locator: *selector*._bimi.domain.tld
Default: default._bimi.domain.tld

Headers before MTA …
`BIMI-selector: v=BIMI1;s=selector`

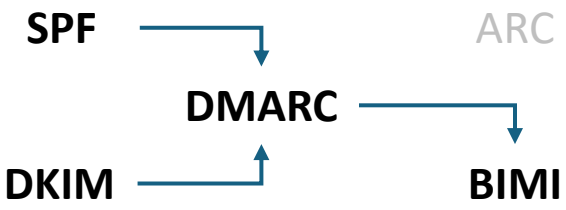


RFC:
- 3709
- 5280
- 6110
- 6170
- 6962
- 9399
- draft

Service:
- DMARC
- DNS
- HTTPs
- X.509

Protocol:
- SMTP
- DNS
- HTTPs

RFC 3709: GIF, JPEG, MP3
RFC 6170: GIF, JPEG, PDF, PNG, SVG
RFC 9399: GIF, JPEG, PDF, PNG, SVG, SVG+GZIP



Přehled technologií: Ochrana bounce adres

- BATV
- VERP
- SRS

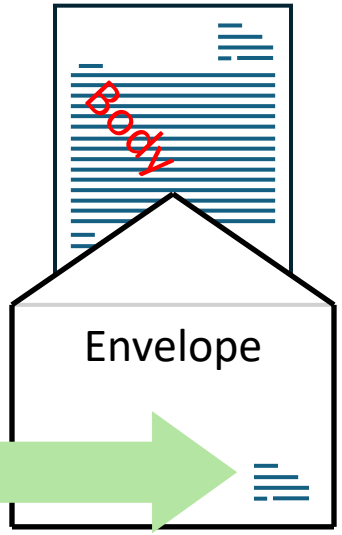
Bounce address protection - BATV

Locator:

Header after MTA …

```
Received-SPF: pass (mailfrom) identity=mailfrom; client-ip=123.45.67.89;
helo=server.sender.tld; envelope-from=prvs=sender/1123ABCDEF@domain.tld;
receiver=<UNKNOWN>
```

```
220 server.targetdomain.tld ready
EHLO server.sourcedomain.tld
250-server.domain.tld
.......
MAILFROM prvs=sender/1123ABCDEF@domain.tld
250 2.1.0 Sender OK
RCPT-TO recipient@targetdomain.tld
250 2.1.5 Recipient OK
DATA
354 Start mail input
From: sender@sourcedomain.tld
To: recipient@targetdomain.tld
Subject: Important message
--- content ---
.
QUIT
```



RFC:
- draft

Service:

Protocol:
- SMTP

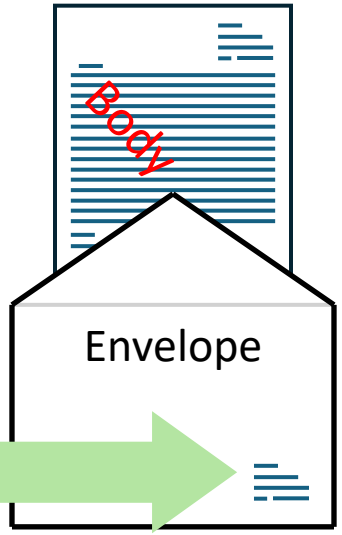
Variable Envelope Return Path - VERP

Locator:

Header after MTA …

```
Received-SPF: pass (mailfrom) identity=mailfrom; client-ip=123.45.67.89;
helo=server.sender.tld; envelope-from=
sender+recipient=targetdomain.tld@sourcedomain.tld; receiver=<UNKNOWN>
```

```
220 server.targetdomain.tld ready
EHLO server.sourcedomain.tld
250-server.domain.tld
.......
MAILFROM sender+recipient=targetdomain.tld@sourcedomain.tld
250 2.1.0 Sender OK
RCPT-TO recipient@targetdomain.tld
250 2.1.5 Recipient OK
DATA
354 Start mail input
From: sender@sourcedomain.tld
To: recipient@targetdomain.tld
Subject: Important message
--- content ---
.
QUIT
```



RFC:
- 3464

Service:

Protocol:
- SMTP

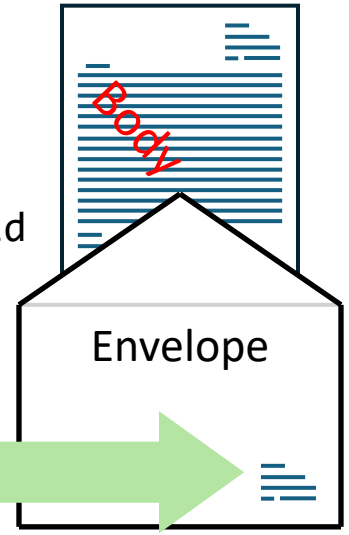
Sender Rewriting Scheme - SRS

Locator:

Header after MTA …

```
Received-SPF: pass (mailfrom) identity=mailfrom; client-ip=123.45.67.89;
helo=server.sender.tld; envelope-from=SRS0=01..ef=01..89=sourcedomain.tld
=sender@recipientdomain.tld; receiver=<UNKNOWN>
```

```
220 server.targetdomain.tld ready
EHLO server.sourcedomain.tld
250-server.domain.tld
.......
MAILFROM SRS0=01..ef=01..89=sourcedomain.tld=sender@recipientdomain.tld
250 2.1.0 Sender OK
RCPT-TO recipient@targetdomain.tld
250 2.1.5 Recipient OK
DATA
354 Start mail input
From: sender@sourcedomain.tld
To: recipient@targetdomain.tld
Subject: Important message
--- content ---
.
QUIT
```



RFC:
- draft

Service:

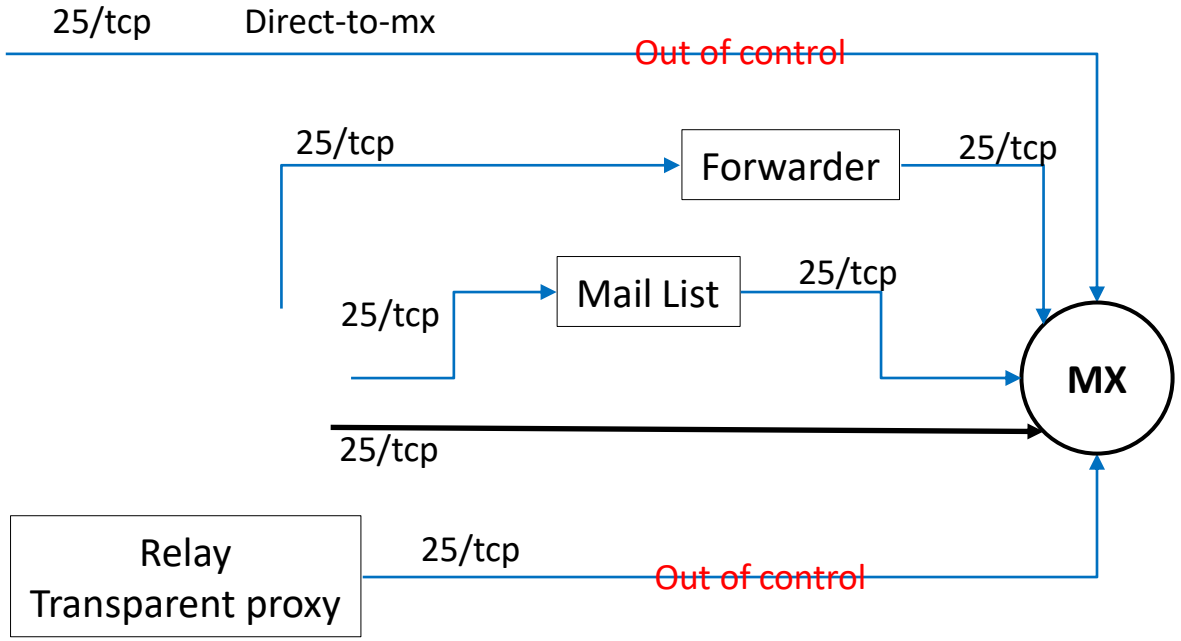
Protocol:
- SMTP

Přehled technologií: Zajištění transportní bezpečnosti

- MTA-STS
- DANE TLSA

MTA-STS

Locator: `_mta-sts.domain.tld.  TXT  "v=STSv1; id=20201231;"`
`mta-sts.domain.tld.  A  IP.AD.DR.ES`
`https://mta-sts.domain.tld/.well-known/mta-sts.txt`



MTA-STS web:

About SMTP supported:

- Plaintext only
- **Support TLS**
- **Enforce TLS**

RFC:
- 8640
- 8641

Service:
- SMTP
- DNS
- HTTPs
- X.509
- TLS

Protocol:
- SMTP
- DNS
- HTTPs

DANE TLSA

Locator: **`_587._tcp.mail.domain.tld IN TLSA 3 0 1`**
`5494492464623acb8155a1b1949000ef334c968dd1d5351a3e3baae737c0c1ab`

RFC:
- 8640
- 8641

Certificate SKI/AKI
Trusted 1st party

Certificate Authority
Trusted 3rd party

DNSSEC + DANE TLSA
Trusted 4th party

Communication partner
Trusted 2nd party

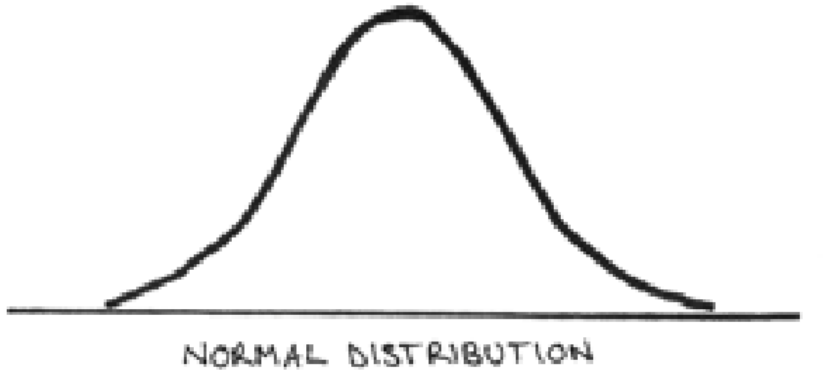
Service:
- DNS
- X.509
- TLS

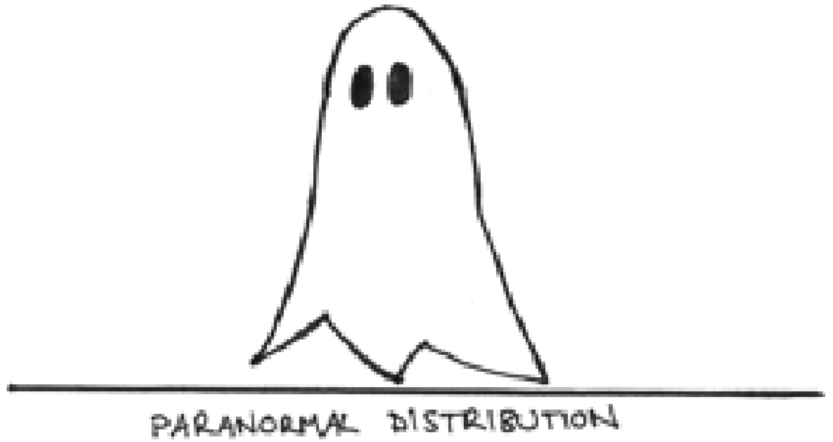
Protocol:
- DNS

Bez DNSSEC je nasazení TLSA nesmysl!

Přehled technologií použitelných pro získávání zpětné vazby

- Bounces
- DMARC report
- TLS report
- DKIM report
- ADSP report





Bounces

Důležitou informací jsou vlastní chybové zprávy, kde by měly být vyhodnocovány kódy či případně rozšířené chybové kódy poskytované poštovním serverem. Některé ze zpráv jsou bohužel zasílány pouze v textovém stavu.

220	Successfully delivered
421	Service not available, closing transmission channel
422	The recipient’s mailbox is over quota
431	The recipient’s server is temporarily unavailable
432	The recipient’s server is not accepting messages at this time
450	Requested action not taken; mailbox unavailable
451	Temporary server error; try again later
452	Insufficient system storage
453	No mail
454	Temporary authentication failure
550	Non-existent email address or domain
551	User not local; please try forwarding
552	Mailbox full; exceeded storage allocation
553	Invalid recipient address format
554	Transaction failed; message refused
555	Syntax error in parameters or arguments
556	Domain does not exist (DNS)
557	Recipient's mailbox is full
558	Mail server requires authentication

2.X.X	Successful delivery
4.1.X	Temporary delivery - addressing issues
4.2.X	Temporary delivery - mailbox issues
4.3.X	Temporary delivery - mail system issues
5.1.X	Permanent delivery - addressing issues
5.2.X	Permanent delivery - mailbox issues
5.3.X	Permanent delivery - mail system issues

Reporting

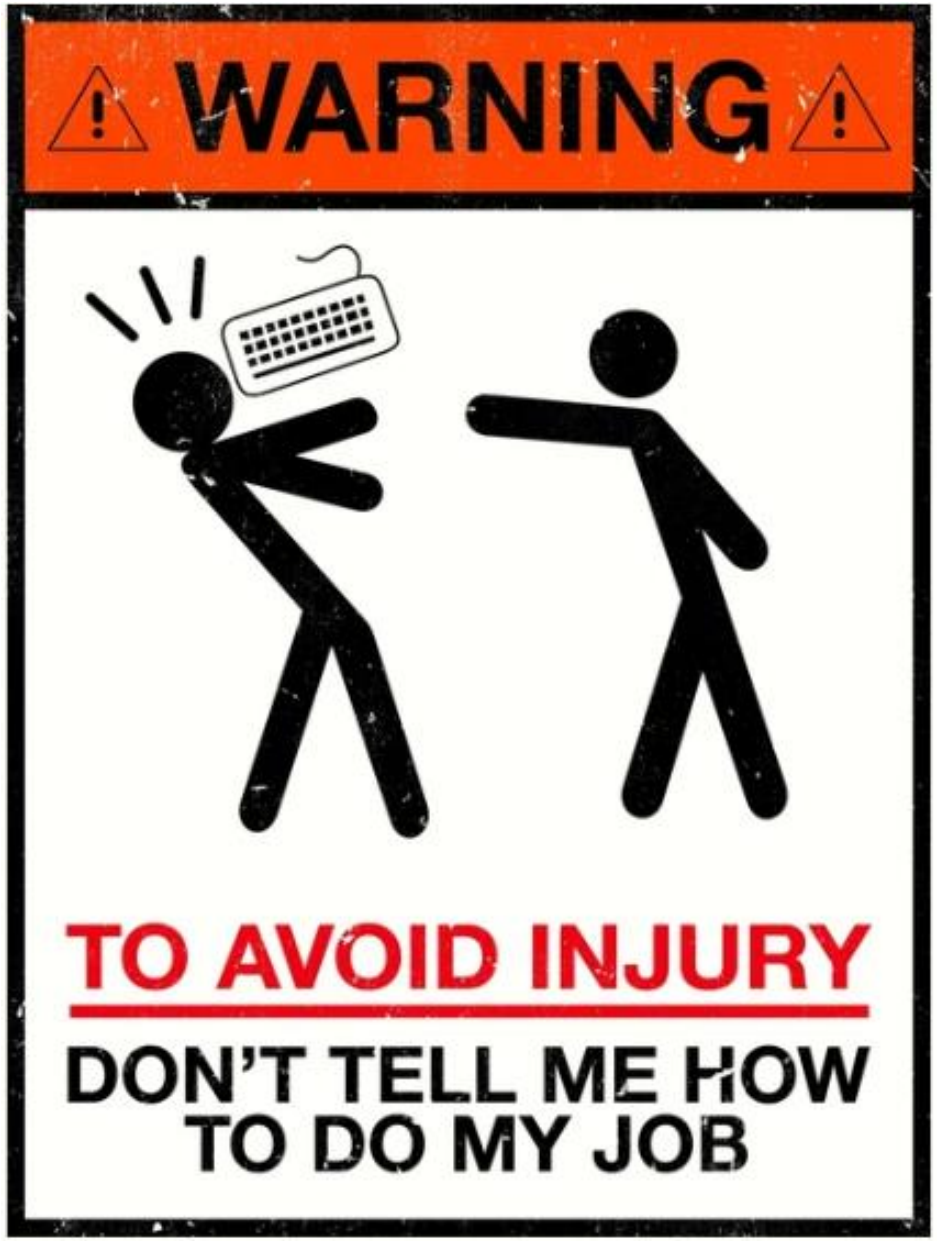
- **DMARC** (RFC 7489)
  - Součástí nastavení DMARC
  - Analytické (rua), vytváří přehledové reporty za období
  - Forenzní (ruf), možnost vytvářet report ke každému chybnému vyhodnocení
  - `"v=DMARC1;...;rua=mailto:postmaster@domain.tld;ruf=mailto:postmaster@domain.tld„`

- **TLS** (RFC 8460, RFC 8461)
  - Vztaženo k MTA-STS, report problémů při navazování zabezpečeného spojení
  - `_smtp._tls.domain.tld.  IN  TXT  "v=TLSRPTv1;rua=mailto:postmaster@domain.tld„`

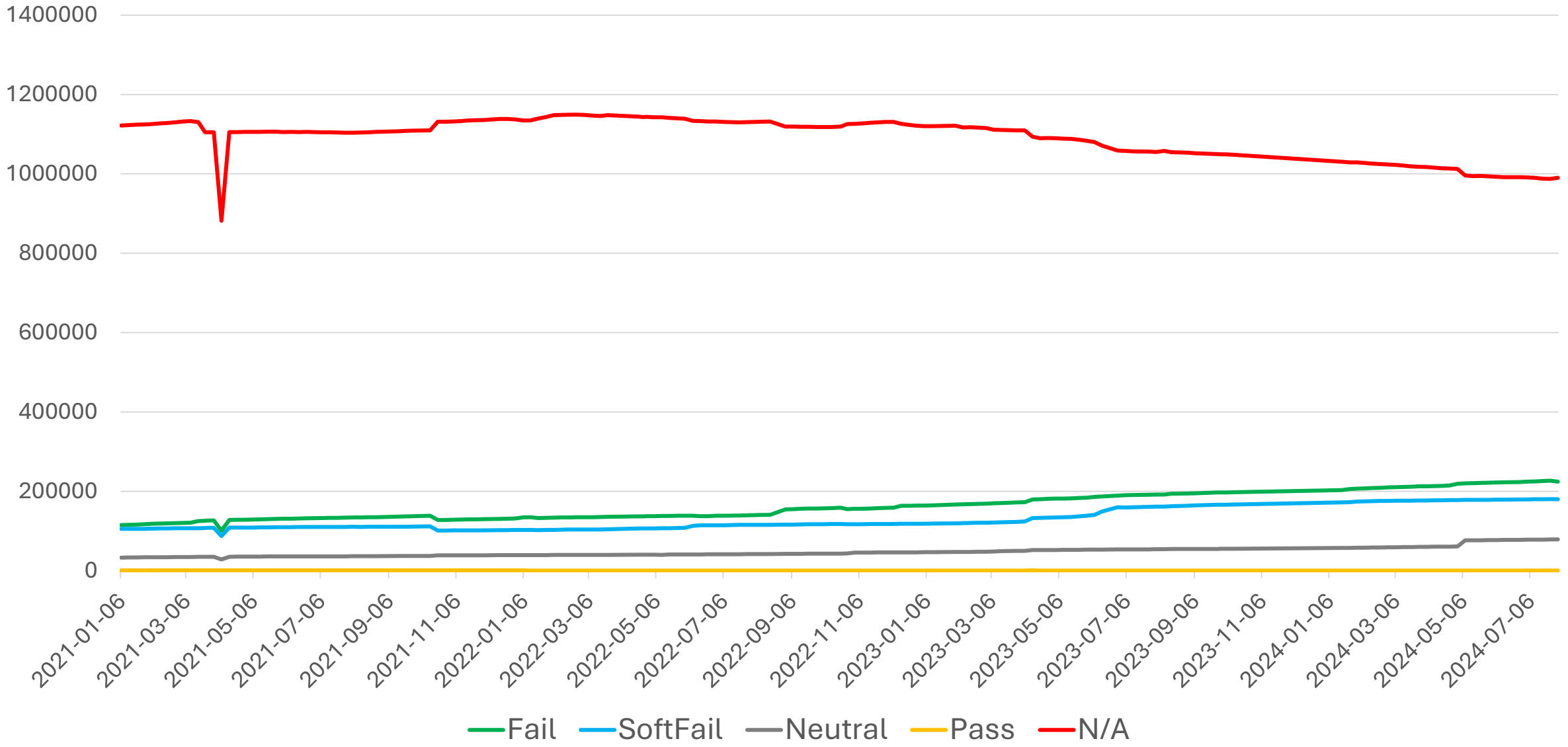
- **DKIM** (RFC 6651)
  - Vztaženo k DKIM, reportuje problémy při ověření podpisů konkrétnímu uživateli reportované domény
  - `_report._domainkey.domain.tld.  3600  IN  TXT "ra=dkim-report;„`

- **ADSP** (zastaralé, RFC 6651)
  - Vztaženo k DKIM a ADSP, reportuje problémy při ověření podpisů konkrétnímu uživateli této domény
  - `_adsp._domainkey.domain.tld.  3600  IN  TXT "dkim=all;ra=adsp-report;"`

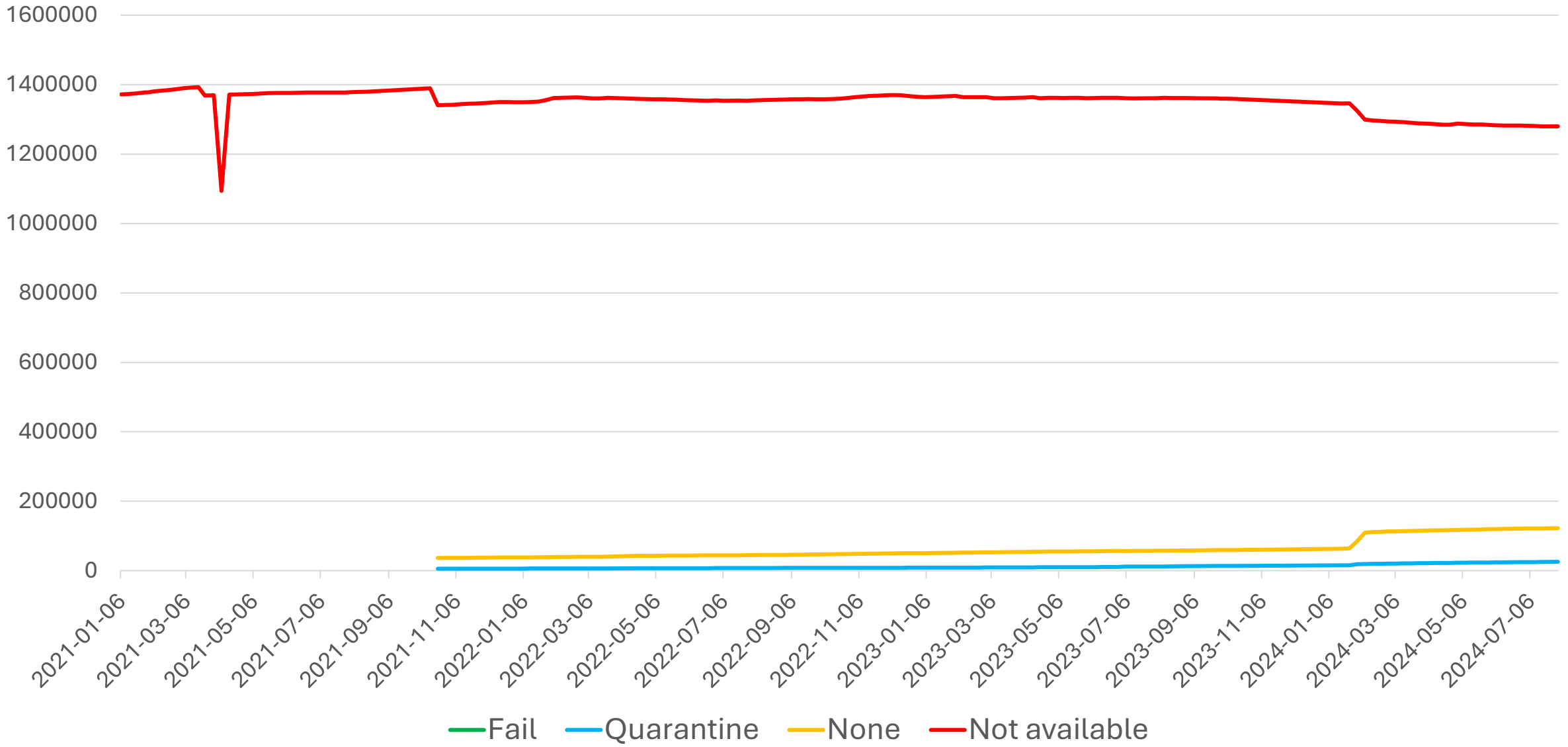
Realita?



Něco málo statistik z ČR: změna počtu a typu SPF s časem

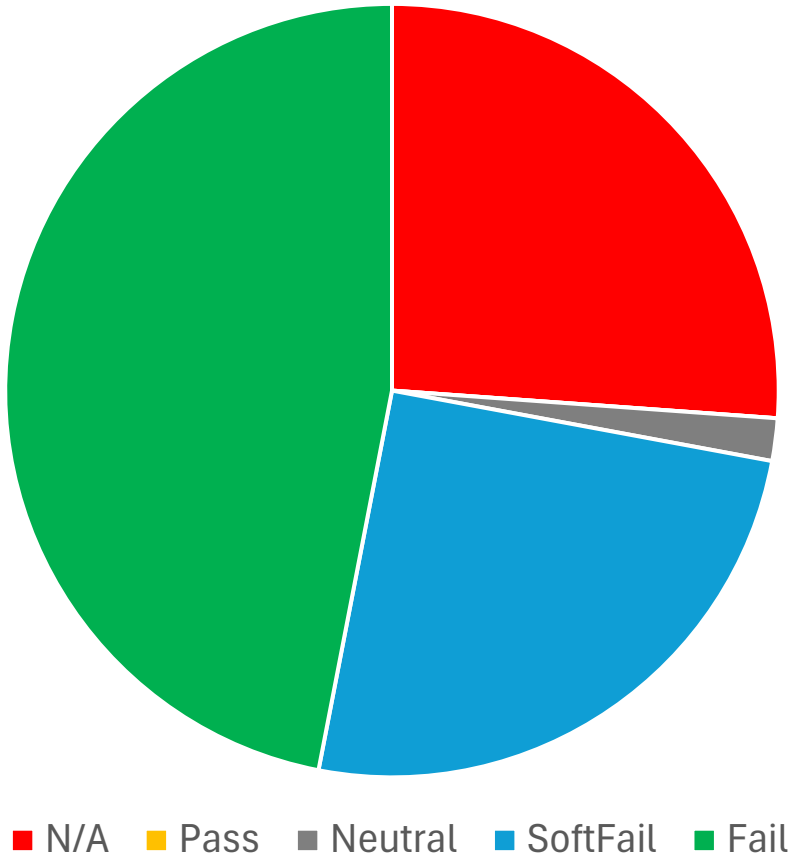


Něco málo statistik z ČR: změna počtu a typu DMARC s časem



Něco málo statistik z ČR: SPF

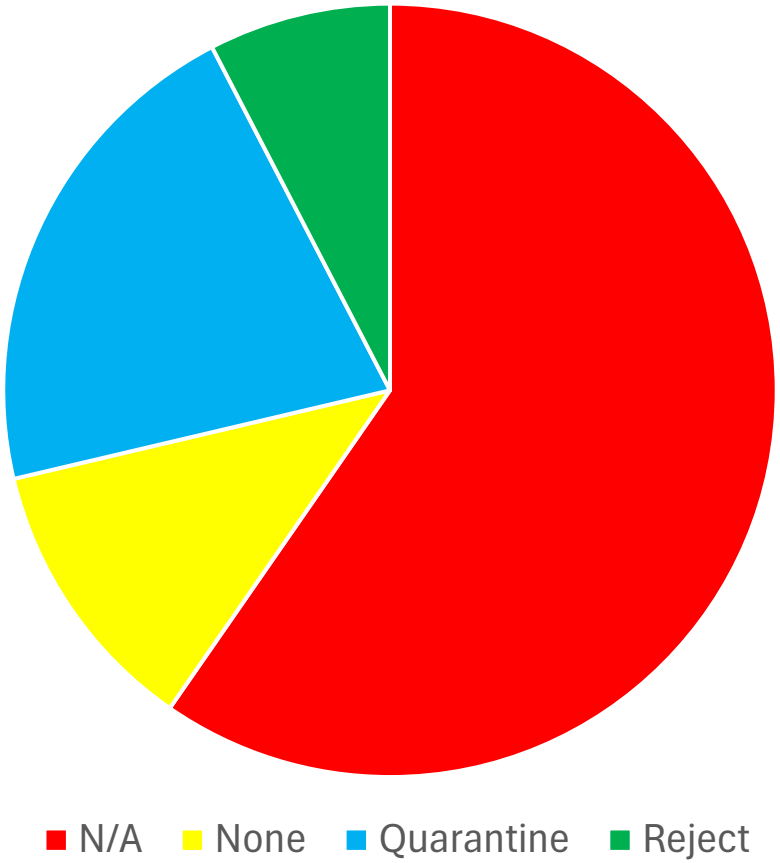
SPF záznamy původních státních domén (v současnosti probíhá migrace na gov.cz)
Počet testovaných domén a subdomén: 436



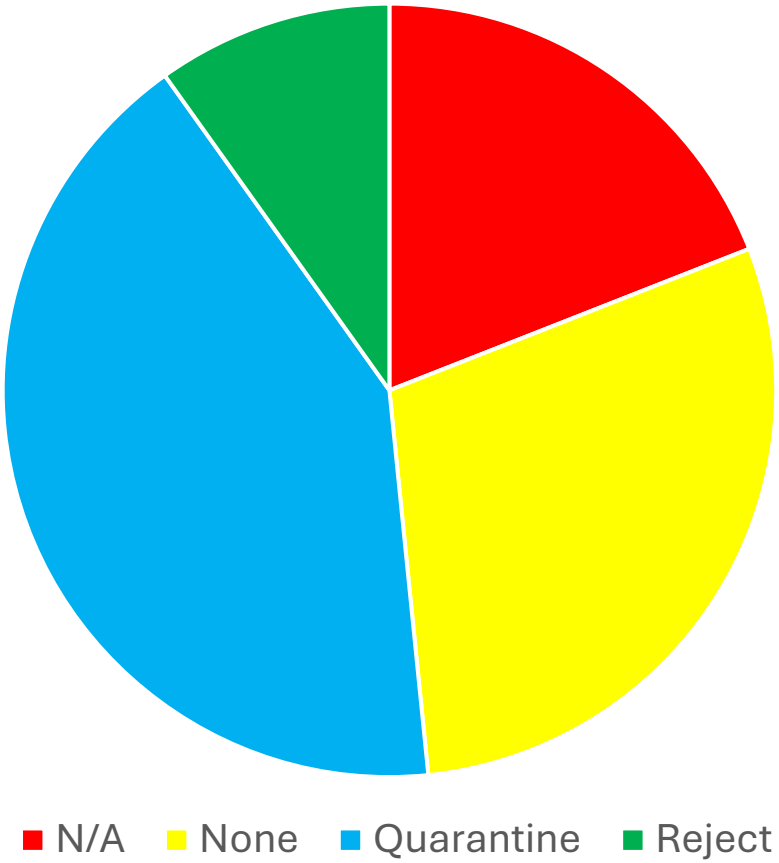
Něco málo statistik z ČR: DMARC

DMARC záznamy původních státních domén (v současnosti probíhá migrace na gov.cz)
Počet testovaných domén a subdomén: 436

Politiky pouze v doméně/subdoméně

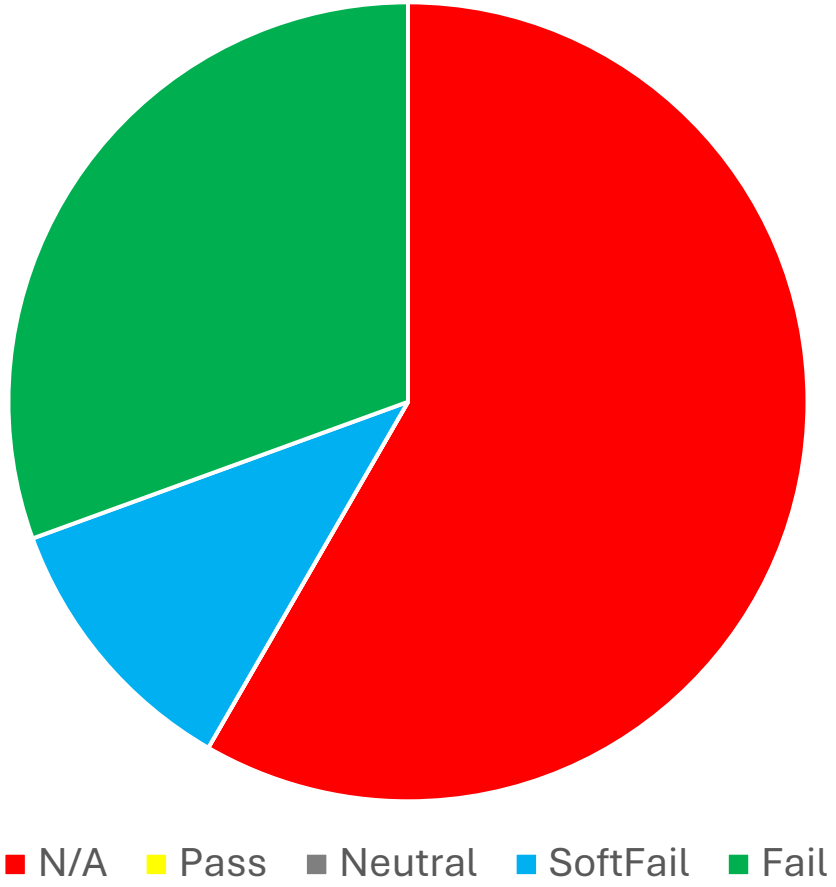


Politiky v doménové struktuře



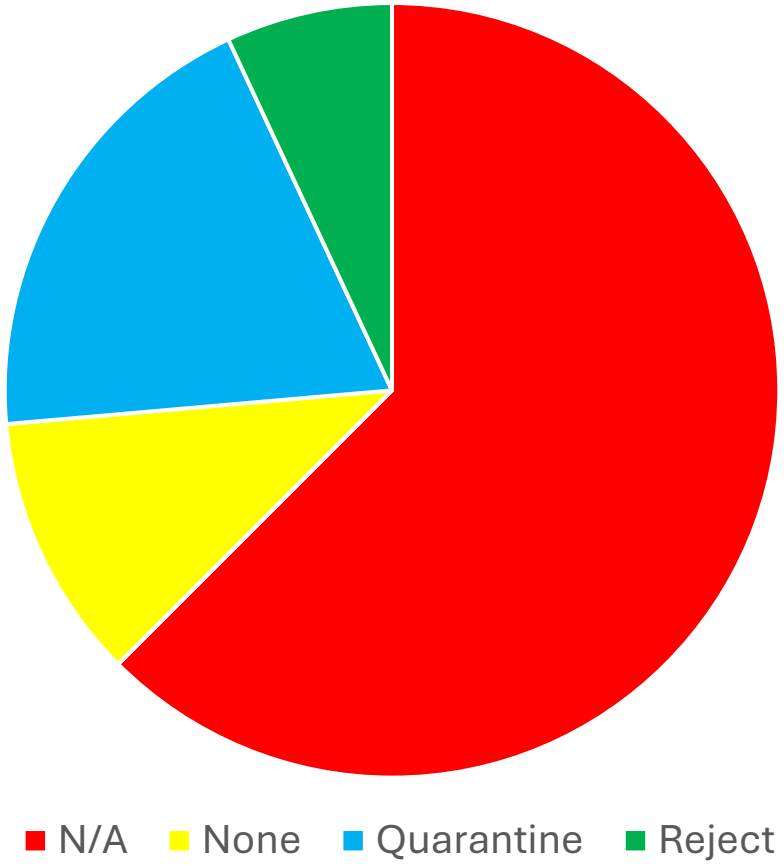
Něco málo statistik z ČR: SPF

SPF záznamy známých státních domén v rámci gov.cz
Počet testovaných domén a subdomén: 72
Migrace stále ještě probíhá, může se jednat o dočasnou situaci



Něco málo statistik z ČR: DMARC

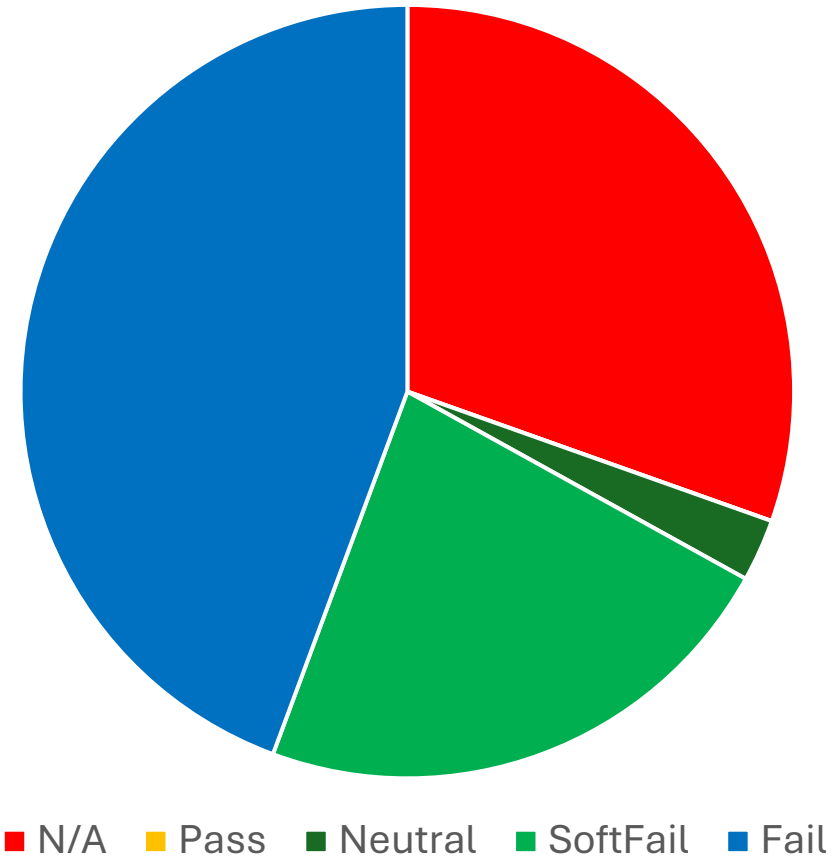
DMARC záznamy známých státních domén v rámci gov.cz
Počet testovaných domén a subdomén: 72
Migrace stále ještě probíhá, může se jednat o dočasnou situaci
Doména gov.cz NEMÁ nastaven DMARC



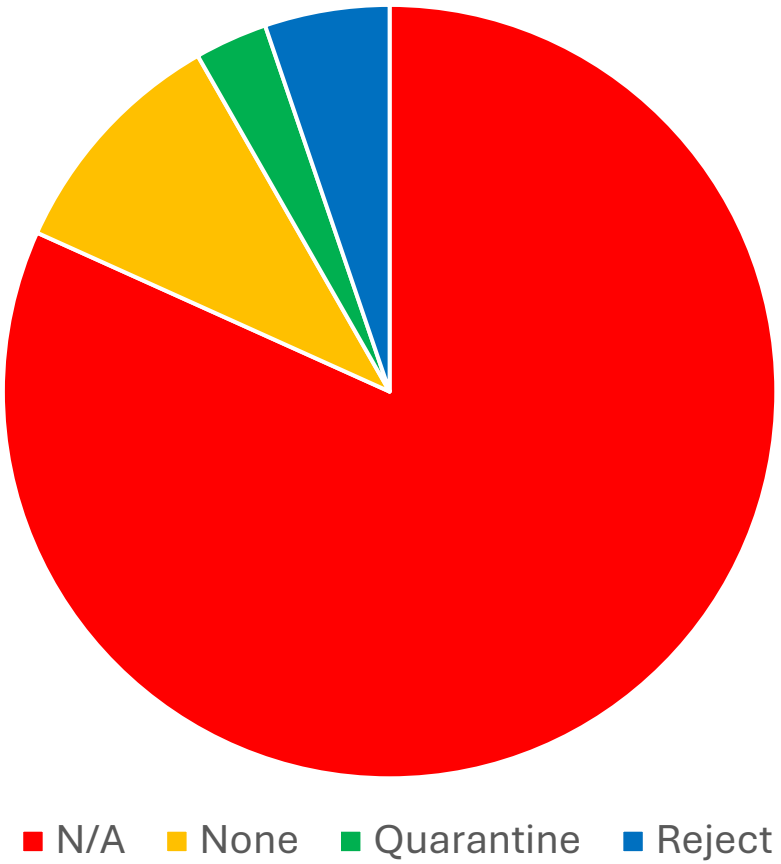
Něco málo statistik z ČR – průmysl a služby

SPF a DMARC záznamy seznamu citlivých subjektů MPO
Počet testovaných domén a subdomén: 247

SPF



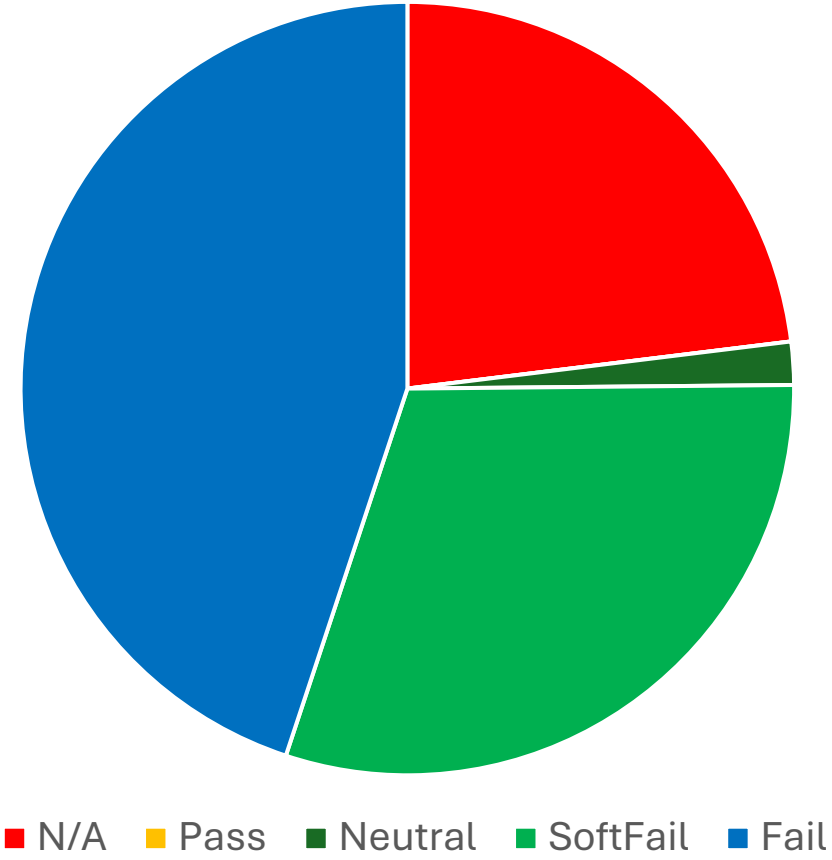
DMARC



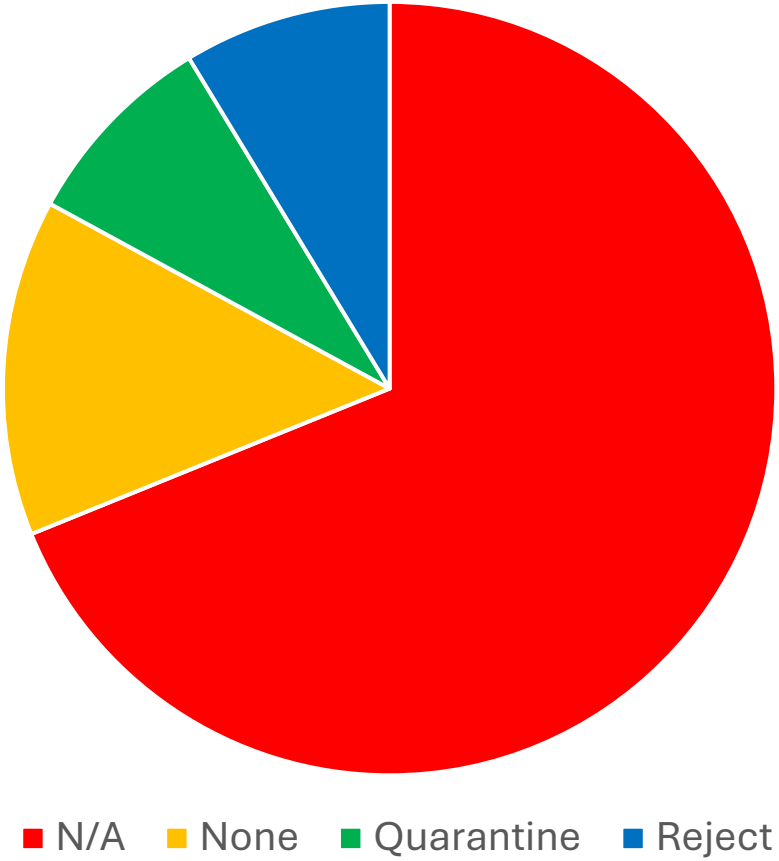
Něco málo statistik z ČR – průmysl a služby

SPF a DMARC záznamy dalšího seznamu citlivých subjektů MPO
Počet testovaných domén a subdomén: 360

SPF

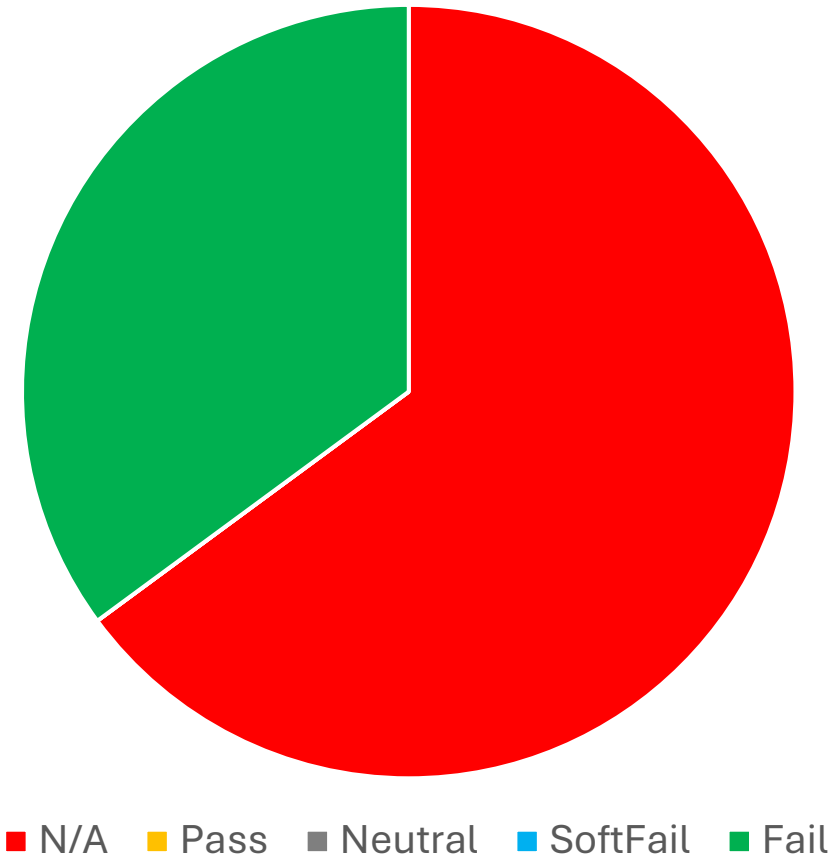


DMARC



Něco málo statistik ze SR: SPF

SPF záznamy známých státních domén v rámci gov.sk
Počet testovaných domén a subdomén: 208



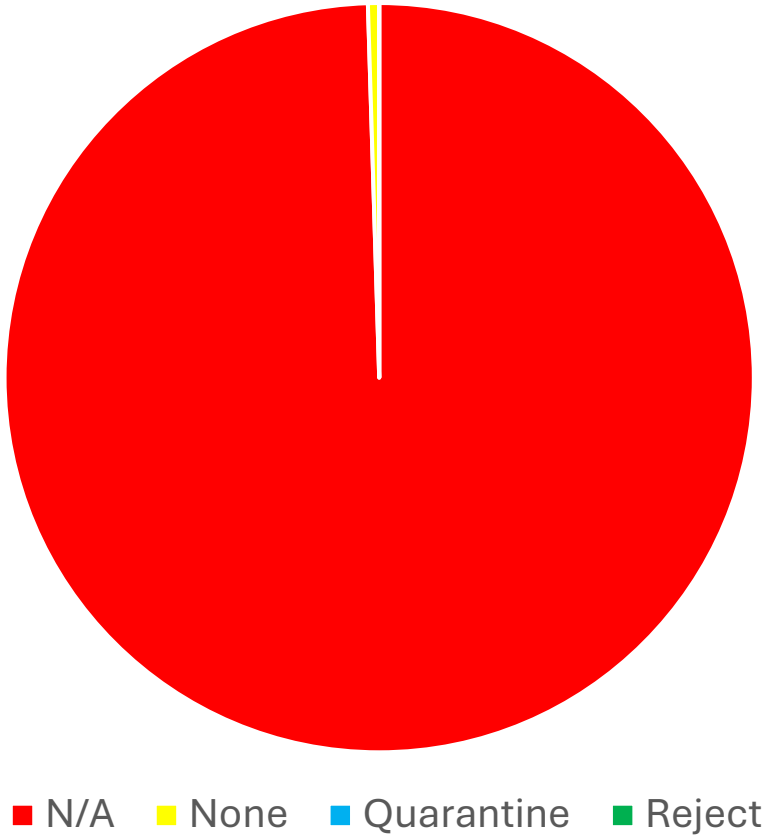
Něco málo statistik ze SR: DMARC

DMARC záznamy známých státních domén v rámci gov.sk

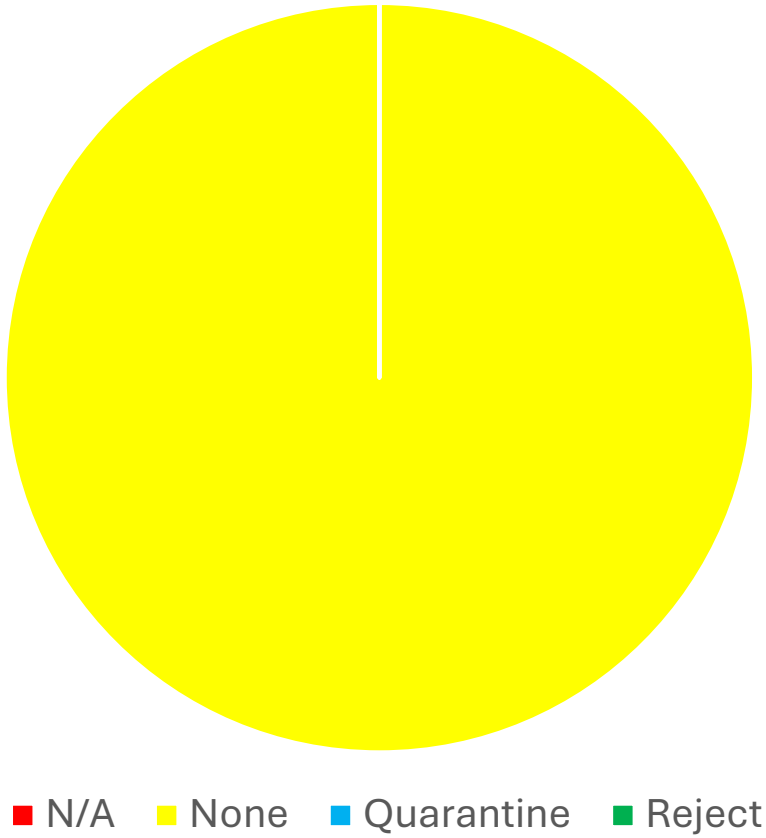
Počet testovaných domén a subdomén: 208

Doména gov.sk má nastaven DMARC, ale domény dalšího řádu DMARC nastaveny nemají

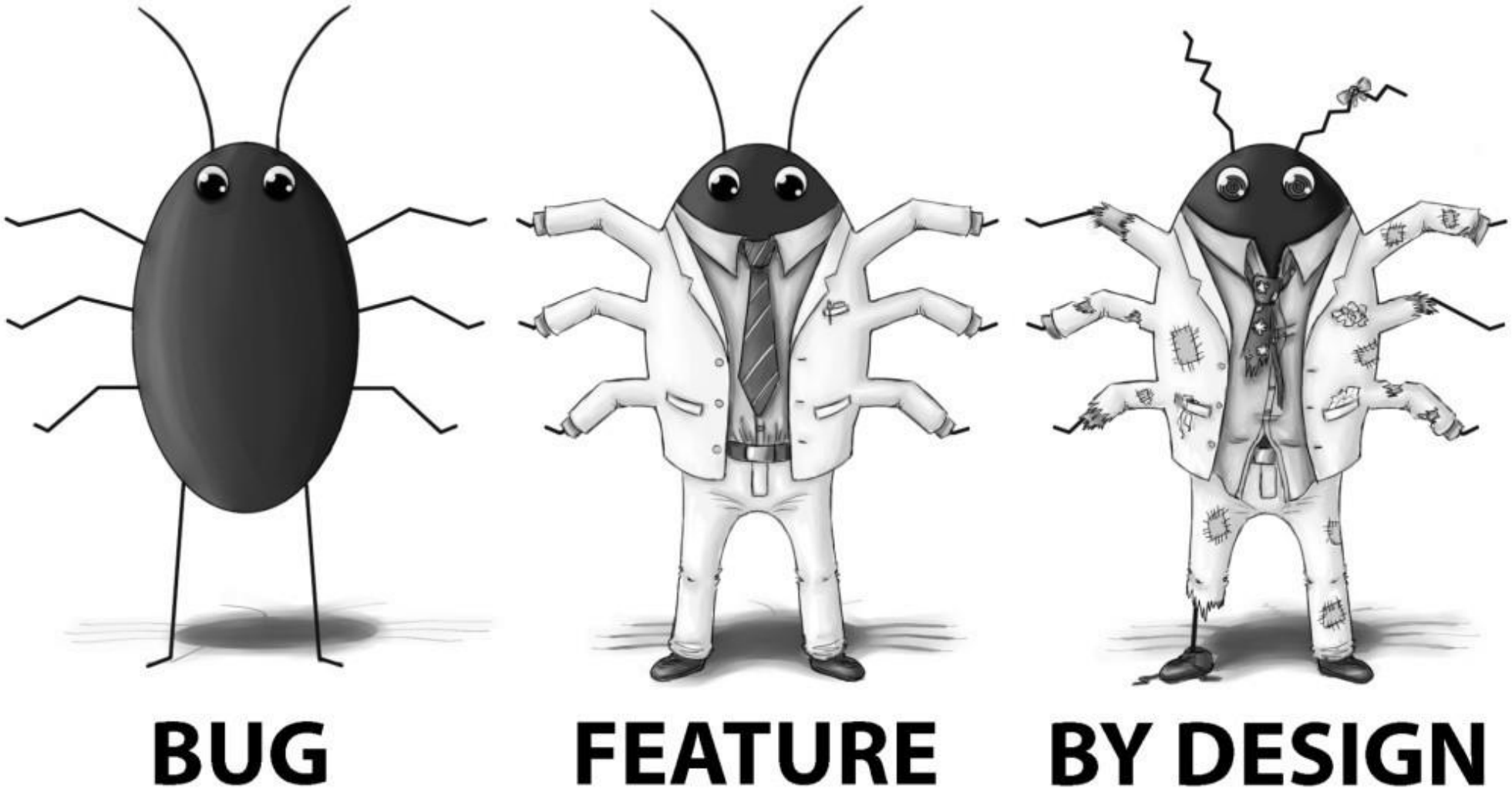
Politiky pouze v doméně/subdoméně



Politiky v doménové struktuře



Problémy technologií

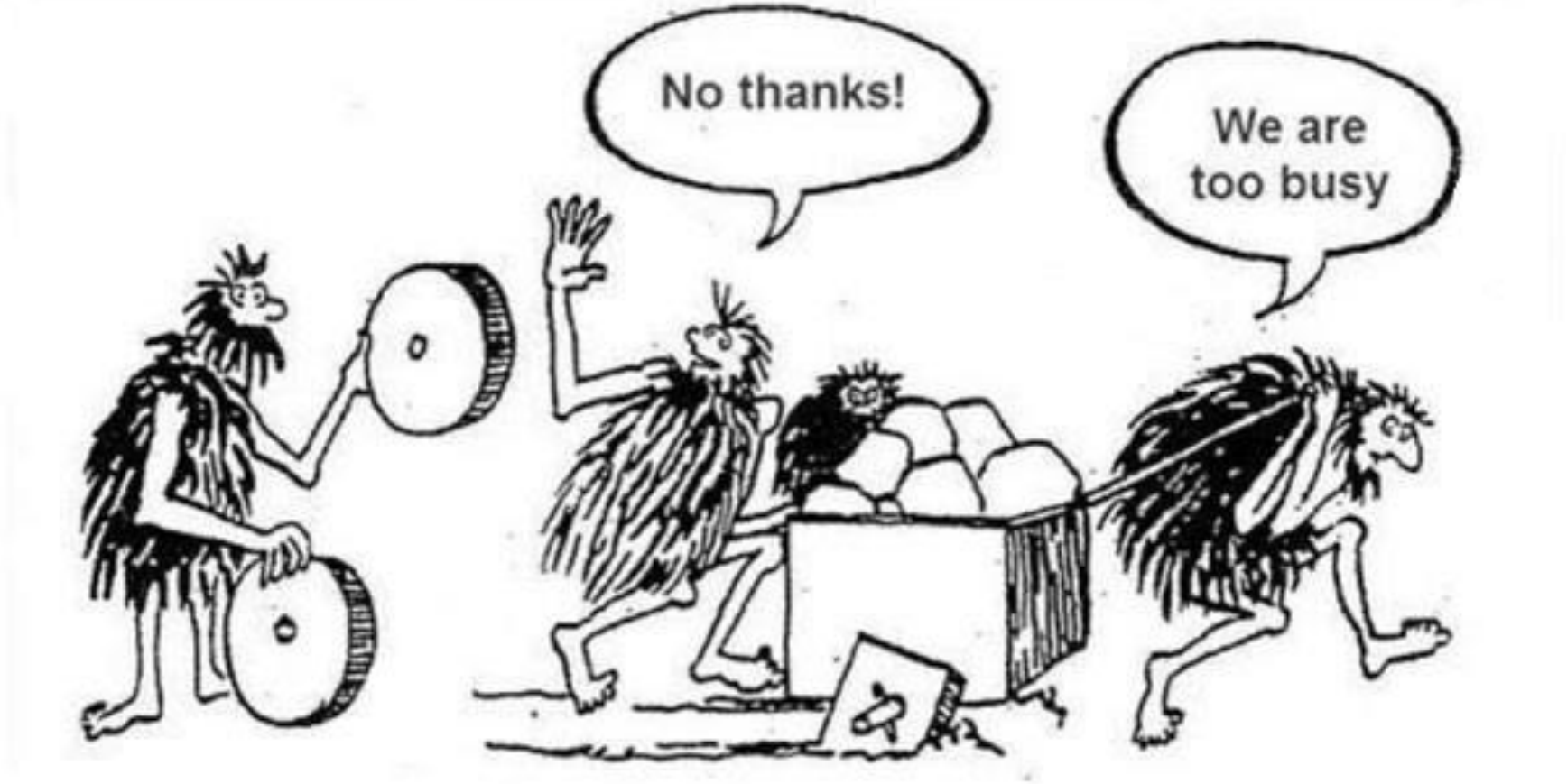


Odklon od standardů definovaných IETF

vysoké riziko

Opravdu je nutné vyvíjet vlastní kolo a spálit všechny síly na rozjezd nestandardní služby?

- Služba nedokáže zajistit potřebnou doručitelnost poštovních zpráv, příčinou je vlastní návrh architektury



Použití a zneužití vyhrazených účtů

střední riziko

RFC 2142 (květen 1997) definuje standardní systémové účty:

- **`postmaster`** – správa poštovního serveru
- **`hostmaster`** – správa DNS serveru
- `www`, **`webmaster`** – správa HTTP serveru
- **`abuse`**, `trouble` – zneužití systému, hlášení o problémech
- *`news`, `usenet`* – NNTP protokol (news), dnes již málo využívaný
- `list` – správa poštovních konferencí

Další doporučené adresy jsou např. `info`, `sales`, `support`, `marketing`, `NOC`, `security`, jejich použití ale závisí na požadavcích provozu.

- Standardní účty, měla by existovat alespoň základní sada `postmaster`, `hostmaster`, `webmaster` a `abuse`
- Slouží k informování o technickém stavu systému, chybách, výpadcích a podobně
- Odesílání jiné než operační komunikace (např. marketing) z těchto účtů je porušením zavedených zvyklostí

Publikace a vyvozování odpovědnosti za domény

střední riziko

Organizace si mohou nechat zajišťovat část služeb třetí stranou. Přesto není z hlediska např. DMARC reportů a DNSBL listů rozdíl mezi službou třetí strany (i špatně nakonfigurovanou) a službou provozovanou na doméně. Tak může dojít k situaci, kdy poštovní služba třetí strany způsobí zařazení na DNSBL pro celou doménu.

- Odpovědnost poskytovaná v rámci domén různých úrovní není zcela průhledná
- Nedostatečná publikace odpovědnosti (zatím pouze draft pro DBOUND – Domain Boundary)

Částečným řešením provozních potíží je použití principu Zero Trust, kdy žádná aplikace s jinou nesdílí oblasti odpovědnosti a konfigurační údaje. Případný výpadek jedné aplikace tak neovlivní další. Přesto ani Zero Trust nevyřeší problémy s odpovědností.

- Sdílená odpovědnost je zlo
- Hrozbou se může stát jak třetí strana (a její případné zneužití), tak některá z aplikací využívající sdílený záznam

Relay a OpenRelay

vysoké riziko

Předávání pošty byla metoda ochrany pro zajištění doručitelnosti. Relay je používán autentizovanými uživateli, OpenRelay může být použit všemi uživateli internetu.

- Možnost použít různé metody formátování adresy a zástupných znaků nebo ohraničení adresy
- Historické formy adresace, využívající UUCP, News a FTP (vzájemné přenosy dat s těmito protokoly)
- Možnost použití "%" hacku

Testování je omezeno počtem požadavků v rámci jednoho spojení, zpravidla 8 nebo 20
Nejznámější testery:

- Anonymous Relay Test http://www.aupads.org/test-relay.html
- AppRiver Open Relay Test https://tools.appriver.com/OpenRelay.aspx
- MXToolBox https://mxtoolbox.com/diagnostic.aspx

Je možné použít i NMAP, nebo přímo Telnet na port 25

- Předávání bývá snadno zneužíváno útočníky
- Jedná se patrně o nejsnadnější způsob zneužití systému

Struktura SPF politiky

vysoké riziko

Časté chyby

- Překročení počtu 10 DNS dotazů (10 NS lookups)
- Nekonečné rekurze (include z jedné domény obsahuje include druhé domény, ta však obsahuje include na první doménu)
- Chybné použití operátorů

Příklady:

-	Strict – vyhodnocení platí/neplatí
~	Softfail – pokud neplatí, informace je uvedena pro další zpracování (původně pro testovací účely)
?	Neutral – je jedno, zda platí či neplatí
+	Pass – platí, defaultní parametr povolující platnost i když není uveden (+all = all, +mx = mx atd)

- Neporozumění nastavení SPF politik a odpovídajících operátorů může vést k dopadům na zabezpečení domény
- Klauzule **`all`** znamená **`+all`**, tedy možnost příjmu ze všech ostatních systémů
- Klauzule **a** akceptuje všechny adresní záznamy v doméně

SPF a rozsáhlé seznamy IP adres

vysoké riziko

Příliš široké IP rozsahy v cloudu mohou útočníci využít. Libovolný poštovní server v tomto rozsahu dovolí odesílat zprávy, autorizované pomocí SPF.

Příklady:

`_spf.google.com`

IPv4: 328 918
IPv6: 412 316 860 404

`spf.protection.outlook.com`

IPv4: 491 512
IPv6: 9 851 624 184 872 950

- Útočník může vytvořit vlastní server v cloudu pokrytého rozsahem a odesílat data dle svých požadavků
- Tyto problémy stojí za množstvím útoků

SPF a (ne)podporovaná makra

nízké riziko

Přesto, že jsou makra v SPF záležitostí starou a standardizovanou již v roce 2006 (RFC 4408), stále ještě ne všechny systémy makra podporují.

- Od roku 2019 se začínají makra masivně používat pro zploštění SPF záznamů

- Protože jsou makra subdoménové záznamy, bez jejich názvů má útočníka ztíženou práci
- Dovolují značně dynamičtější a komplexnější strukturu, bez nutnosti překročit počet SPF záznamů

Porovnání DomainKey a DKIM algoritmů

nízké riziko

	DomainKey	DKIM
v=DKIM1	No	Should
key algorithm	RSA	RSA, Ed25519
hash algorithm	No	SHA1, SHA2-256
Signature algorithms	RSA-SHA1 (<2048b)	RSA-SHA1 <4096b RSA-SHA2-256 <4096b Ed25519-SHA2-256
Self-sign the signature header field	No	Yes
Multiple signatures	No	Yes
Canonization	Data	Headers, Body
Signing	Data	Headers, Body
Timestamping	No	Yes
Expiration	No	Yes
Groups	No	Deprecated
Length of data	No	Deprecated
Policying	Yes	ADSP (deprecated)
Reporting	No	ADSP (deprecated), DKIM reporting (experimental)

- Použití zastaralé technologie DomainKey může vytvářet ohrožení pro bezpečnost a dávat útočníkovi šanci obejít nastavené mechanismy

Důležité DomainKey, DKIM a ARC tagy podpisu

střední riziko

Jak pro hlavičkové tagy DomainKey (**`DomainKey-Signature:`**), tak pro novější DKIM (**`DKIM-Signature:`**) a ARC (**`ARC-Message-Signature:`**) je možné definovat hlavičky počítané do obsahu podpisu. Neexistující hlavičky jsou ignorovány (nahrazeny prázdnou množinou).

Seznam podepisovaných hlaviček (**h=***headers list*)

• `From, To, CC, Sender, Reply-To`	Seznam příjemců, odesílatelů a adres odpovědí
• `Subject`	Název předmětu
• `Message-Id, In-Reply-To, References`	Identifikační číslo zprávy a odkazy na toto číslo
• `Date`	Datum odeslání
• `MIME-Version`	Verze MIME
• `Content-Type, Content-ID, Content-Description`	Typ přílohy, identifikace přílohy a popis přílohy
• `Content-Disposition, Content-Encoding`	Použití přílohy, kódování přílohy
• `Precedence`	Identifikace typu e-mailu (bulk, list atd.)
• `List-Unsubscribe, List-Unsubscribe-POST`	Definice a URL pro single-click unsubscribe

- Útočník může změnit nebo rozšířit přílohy, seznam příjemců, nebo změnit URL pro single-click unsubscribe na adresu poskytující maligní obsah

Důležité DKIM a ARC tagy podpisu

střední riziko

Jak pro DKIM (DKIM-Signature:) tak pro ARC (ARC-Message-Signature:) je možné definovat časové značky pro určení počátku a konce platnosti podpisu. Pro ARC není zmíněno ve standardu, ale odkazuje se na DKIM. V případě ARC proto doporučuji hlavně u konce platnosti podpisu prozatím vlastní experimentování, některé systémy uvedení tohoto příznaku označují za chybu. Ve všech případech by doba expirace měla být delší než je doba doručení e-mailů ("Maximum Deliveriability Time"), tedy přibližně 5 dní. Praktické nastavení limitu by měl být násobek této hodnoty (např. 15 dní).

Časové značky

• Timestamp (**t=***timestamp*)	Časová značka pro vytvoření podpisu
• Expirace (**x=***timestamp*)	Časová značka konce platnosti podpisu

- Pokud není SPF, útočník s přístupem k e-mailům bez časových značek může využít těchto zpráv k vytvoření DoS útoku na cílový server (spojení, diskový prostor)

(Ne)důležitý DKIM a ARC tag podpisu

vysoké riziko

Jak pro DKIM (**`DKIM-Signature:`**) tak pro ARC (**`ARC-Message-Signature:`**) je možné definovat délku podepisované části. Označuje délku důvěryhodné části e-mailu, pokud se zbytek zprávy změní, je zpráva stále důvěryhodná!!! Protože není vazba na délku zprávy a délku e-mailu, je správné použití bez definice délky. V jiném případě kryptografická ochrana poskytuje falešný pocit bezpečí a celkovou bezpečnost snižuje !!!

Length (**l=***délka*) Délka důvěryhodné podepsané části !!! Nepoužívat !!!

- Útočníkovi dovoluje snadno padělat komunikaci (přiložení malware, rozšíření textu)
- Pokud neexistují další ochrany (hlavičky, expirace), může využívat uvedeného podpisu dle svého

DomainKey, DKIM, ARC a útoky na algoritmy podpisu nízké riziko

Domainkey (**`DomainKey-Signature:`**), DKIM (**`DKIM-Signature:`**) a ARC (**`ARC-Message-Signature:`**) podporují pro digitální podpis algoritmus RSA ve formátu PKCS#1 v1.5.:

- Bleichenbacherův útok vyžaduje existenci orákula, kontrolující dotaz pomocí privátního klíče (1998)
- Útok pomocí malých exponentů (3, 17, 65537 … tj. „malá“ Fermatova prvočísla)
- Håstad/Coppersmiths útok vyžaduje rozeslání zprávy se stejným podpisem a exponentem, ale jiným privátním klíčem (není problémem při podpisech)
- Multiplikativní a deterministické vlastnosti (problematické hlavně při šifrování, nikoliv při podpisu)

DKIM (**`DKIM-Signature:`**) a ARC (**`ARC-Message-Signature:`**) podporují algoritmus Ed25519:

- Digitální podpis není vázán na náhodnou nonce jako u NIST křivek
- Nonce je generována hash podpisového klíče a otevřeného textu
- Nemůže být využita možná kolize dvou nonce, která by vedla k získání privátního klíče

Doporučení:

- Z preventivních důvodů nepoužívat podpisy pro bounce zprávy
- Dovolit odesílání zpráv pouze autentizovaným uživatelům (přes MSA) a blokovat jakýkoliv relay
- Používat doporučený bezpečnostní ekvivalent 128b (RSA3072 a Ed25519, přinejhorším alespoň RSA2048+)

Veřejný klíč podpisu a specifikace algoritmu

nízké riziko

DKIM (**`DKIM-Signature:`**) a ARC (**`ARC-Message-Signature:`**) dovolují specifikovat algoritmy použité v průběhu podpisu. Vlastní klíč je uveden v DER formátů a překódován do Base64, tedy asymetrický algoritmus je definován i zde a navíc i v hlavičce podpisu. Hash algoritmus je ale uveden pouze v hlavičce podpisu. Proto je vhodné zajistit ochranu před zneužitím.

- Útočník má možnost změnit hash algoritmus (na základě současných znalostí by to nemělo stačit pro útok)
- Pro padělání podpisu musí (na základě současných znalostí) znát privátní klíč

DMARC záznamy na doméně další úrovně

nízké riziko

Záznamy jsou vyhodnocované jak na doméně odesílatele, tak v nadřízené, až pokud není nalezen odlišný SOA.

- Vyhodnocování nejprve v dané doméně na základě názvu domény v hlavičce odesílatele (From:, Mailfrom:)
- Následuje vyhodnocení na nadřazená doméně (maximálně 5 kroků)
- Implementace vyhodnocování nadřazených domén není vždy korektní (Walking Tree Problem)

DMARC s politikou none a quarantine

střední riziko

DMARC s politikou **none** dovoluje pouze reportování problémů a nenastavuje žádná pravidla pro odmítání pošty. Měl by sloužit pouze pro testovací účely. Použití BIMI vyžaduje alespoň politiku **`quarantine`**. Některé společnosti tuto politiku při překročení určitých hranic odmítají.

DMARC s politikou **`quarantine`** je implementačně závislý. Některé implementace přesouvají SPAM do systémové karantény, jiné do uživatelských karantén, jiné obsah mažou. Z důvodu nepředvídatelnosti chování na cílových systémech je tato politika nešťastná. Pro předvídatelnější chování je vhodná politika **`reject`**.

- Politiku **none** může útočník použít, správce odesílajícího systému se informaci o zneužití dozví z pravidelných reportů (pokud je zpracovává)
- Z praktického hlediska vhodná pouze pro testovací účely

DMARC forenzní reporty a GDPR

střední riziko

Forenzní reporty slouží pro odeslání detailní analýzy problémů při příjmu zpráv. Přijímající server odesílá zpět informace o celém obsahu e-mailů, proto je některými organizacemi blokován. Report může obsahovat soukromé informace.

- Z hlediska GDPR je forenzní analýza problematická může mít právní dopady
- Je nutné zvážit, zda je nutné forenzní analýzu podporovat

ARC a (ne)důvěryhodný první hop

vysoké riziko

Použití ARC technologie dovoluje podepsat celou cestu, kterou e-mail urazil. Vyžaduje, aby první krok cesty zajistil důvěryhodnost zbytku trasy. Proto musí být první krok důvěryhodný a musí mít kvalitní reputaci.

- Pokud první krok cesty podepíše řetěz důvěry a má kvalitní reputaci, je cesta důvěryhodná
- Pokud první krok cesty nepodepíše řetěz důvěry, u cesty po první podpis důvěryhodného serveru je problematické určení její důvěryhodnosti
- Reputace podepisujících serverů není nikde uváděna

BIMI a důvěra v logo odesílatele

střední riziko

BIMI dovoluje zobrazit logo odesílatele klientem, ale co se zobrazuje?

- Logo se zobrazí pokud je validní vyhodnocení pomocí DMARC
- Problém s podporou VMC (Verifier Mark Certificate – odkazuje na seznam evidovaných certifikátů)
- Neexistuje ochrana před zkopírováním obrazových dat

Částečná nebo plná podpora: Apple, AT Mail, British Telecom, Cloudmark, Comcast, GMX, Google Gmail, Fastmail, Microsoft Dynamics 365 Customer Insights – Journeys, Mozilla Thunderbird s rozšířením DKIM Verifier, Qualitia, Seznam, Yahoo, Zone, Zoner ...

DANE TLSA

nízké riziko

DNS zajišťuje další zdroj důvěry, toto poskytování důvěry závisí na DNSSEC

- DANE TLSA vyžaduje automatizaci obnovy informací pomocí bezpečného API, často se jedná pouze o ignorované požadavky zákazníků
- Nestandardní implementace „podporující DNS“ ohrožují důvěryhodnost TLSA
- Použití Self-Sign certifikátů je možné, ale nesprávné
- Pokud na doméně není DNSSEC, je implementace TLSA nesmysl

DNSBL (Blacklisty)

vysoké riziko

Poskytovatel blacklistu na DNS dotaz (reverse IP.DNSBL) vrací hodnotu určující, zda je daná IP adresa součástí černé listiny a případně i kvůli jakému problému. Tyto seznamy by měli splňovat RFC 5782, hodnoty ale nejsou standardizované. Proto je nutné znát implementační detaily a citlivě volit DNSBL služby. Mezi nejznámější nástroje pro testování patří:

Blacklist Scan https://blacklistscan.com/
DNSBL Info https://www.dnsbl.info/
IP Blacklist Check https://www.ipvoid.com/ip-blacklist-check/

- Automatické blacklisty kontrolují svoje seznamy a případně odstraňují evidované adresy
- Semiautomatické blacklisty vyžadují aktivitu uživatele pro provedení testů za účelem odstranění
- Manuální blacklisty vyžadují kontaktovat provozovatele:
  - kontaktování provozovatele bývá problematické
  - odstranění probíhá dle systému zdarma či za úplatu

Reputační skóre a ověření stavu

vysoké riziko

Reputační skóre vyjadřuje míru důvěryhodnosti odesílajícího serveru nebo systému. Existují reputační schémata na IP adresu a na doménu. Mezi nejznámější reputační systémy patří:

Baracuda Central	https://www.barracudacentral.org/lookups
CISCO TALOS	https://talosintelligence.com/
SenderScore	https://senderscore.org/
SpamHaus	https://www.spamhaus.org/domain-reputation/
	https://www.spamhaus.org/ip-reputation/
VirusTotal	https://www.virustotal.com/gui/home/url

- Reputace odesílajícího serveru je ovlivněna jeho vyhodnocováním příjemci
- Nízké skóre ukazuje na obtížnou ověřitelnost a časté porušování pravidel
- Příliš volná pravidla dovolují útočníkovi odesílat neakceptovatelnou komunikaci a snižovat reputaci domény

Zahřívání domén

vysoké riziko

V případě problémů s reputací a v případě nových domén je nutné před použitím domény „zahřát“. Cílem je napravit reputační hodnocení, nebo ho přesunout z hodnocení Neutral na hodnotu Trusted. V případě nových domén je nutné zajistit jejich „dozrání“ po dobu několika týdnů. Nové domény jako odesílatelé jsou po vytvoření nedůvěryhodné.

- Tvorba reputačního skóre je časově náročná, je snadné o přijít o kvalitní skóre kvůli hloupým chybám

Přibližní doba bezpečného zahřívání domén (orientační doba, může se lišit dle dalších podmínek):

Dní	E-mailů/den
2	10
5	25
8	50
13	100
28	250
50	500
91	1000
193	2500
358	5000
667	10000

FBL (Feedback Loop) a ARF (Automatic Reporting Format)

nízké riziko

ARF (RFC 3462) standardizuje formát automatických odpovědí a dovoluje systémovým nástrojům zaslat uživatelem reportovaný spam (Feedback Loop, RFC 6449, RFC 6591, RFC 6692 a RFC 9477) na adresu domény odesílatele (uživateli abuse nebo postmaster). Na straně odesílatele by mělo docházet k pravidelnému vyhodnocování.

- Útočník pro plně automatický mód může zneužít Feedback loop pro zablokování některého z účtů
- Velcí provideři (např. Google) FBL nepoužívají, přestože se právě jejich účty často používají pro rozesílání SPAMu

Měření doručitelnosti a analýza logů

vysoké riziko

Služby elektronické pošty umožňují vnitřní komunikaci společnosti a zároveň komunikaci se zákazníky. Přesto, že se jedná o důležitou součást provozu, na rozdíl od klasické komunikace zpravidla není vyhodnocována účinnost (doručitelnost). Na rozdíl od doporučených dopisů, komunikace datovou schránkou, trasování balíkových zásilek a vyhodnocování spokojenosti uživatelů těchto služeb tak dochází k podceňování této služby.

- Největší hrozbou se pro dostupnost služby poštovního systému stává jeho správce, který komunikaci nevyhodnocuje

Technický Report	Popis	Priorita
Systémové logy	Technické zprávy informující o provozu daného systému. Jejich sběr a analýza dokáže identifikovat, co se se zprávou dělo v průběhu a po přijetí, nebo před a v průběhu odeslání.	Vysoká
Bounces	Technické zprávy informující o nedoručitelnosti. Bounces je nutné sbírat na straně poštovního serveru pomocí služeb poštovního serveru, rozšíření nebo vlastních nástrojů.	Vysoká
DMARC Report	Zprávy o výsledcích kontrol souladu SPF/DKIM, definováno pomocí DMARC.	Střední
TLS Report	Zprávy o problémech s navazováním TLS spojení, definováno pomocí TLSRPT.	Nízká
DKIM Report	Zprávy o problémech s DKIM klíči, definovatelné pomocí DKIM extensions.	Nízká

Vlastnosti nastavení SMTP serveru

střední riziko

SMTP server podporuje v rámci ESMTP (po výzvě EHLO) několik rozšířených vlastností, které mohou být rizikem samy o sobě. Za riziko se považuje již přístup k informacím nad rámec nezbytně nutných. Jedněmi z těchto příkladů jsou informace poskytované serverem, které je nutné odpovídajícím způsobem „pročistit“.

VRFY

- Ověření existence jména uživatele nebo skupiny
- Útočníkovi dovolí ověřit existenci uživatele

EXPN

- Expanze (rozpad) skupiny na uživatelská jména
- Útočníkovi dovolí získat seznam jmen v dané skupině

AUTH

- Seznam autentizačních mechanismů
- Použití na portu 25/tcp je diskutabilní, mělo by být součástí definice architektury
- Tento seznam slouží pouze pro klientský software a přihlášení uživatelů
- Útočníkovi dovolí získat seznam algoritmů, na které lze útočit

https://cryptosession.cz/download/LinuxDays2024.pdf