Zabezpieczanie poczty DMARC

Vladimir ‚vovcia' Mitiouchev

Spis treści

- Nagłówki
- Autoryzacja adresów IP
- Uwierzytelnianie podpisu DKIM
- Monitorowanie poczty
- Ochrona DMARC

Nagłówki

- From **YouTube** <noreply@youtube.com>
- Reply-to 
- Return-Path, czyli MAIL FROM w SMTP

```
Return-Path: <3E38qUqcLDCoTUXKVReeUaZaHK.IUSSUPQUSVaZKXiMSG
```

Adresy IP - SPF

- Kontroluje pole „Return-Path”
- Sprawdza wpis SPF (TXT) w domenie

```
bounce.r.com TXT „v=spf1 ip4:127.0.0.1/8 -all”
```

```
Return-Path: <3E38gUgcLDCoTUXKVReeUaZaHK.IUSSUPQUSVaZKXiMSG
Received-SPF: pass (google.com: domain of 3E38gUgcLDCoTUXKV
```

DKIM

- Uwierzytelnianie domeny
- Klucz publiczny w DNS
- Wybór klucza selektorem

```
20120806._domainkey.youtube.com. IN TXT
"k=rsa\; p=MIIBIjANBgkqhkiG9w0aWL5dsZ66MG4Y…
```

DKIM

- Podpisywanie nagłówków i treści wiadomości

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=youtube.com; s=20120806;
        h=mime-version:list-unsubscribe:message-id:date:subject:from:to
         :content-type;
        bh=ilqe1w8ASUKzoqoke70Px9YD0SoFZVYv6DBMZ7oyQfo=;
        b=kT92WUOOMLTjX26wQ1VIDUCk1+2fSz0ybTt/E0amdEIeSiQcp3omJGiA5XrjFHgseY
         LkJhLiywccyw/ol9MDD2aw2crxw0b/ArKcRVgf0H4OEuM+T0SKQbxTc2p6qKhNnvKWjw
         mGWuBrapCFGLipa+5ay9BqY+OZ6JUqKg5Nxew+IH2KgvjaAPLO92iKOfMkTXWCCg+3Eu
         r9b2h/iRAlwCd3P/ew1Lr2iIkFV1vsPtixIdjtGxGZoSfI9Ry9noeNaCwiLGZ78M9jDR
         qudb+NAAtLtbRCguxvc41PsP1rQgslsVWQXo5A50895mXhKOMvXgBvVYxV//zb/+oFj0
         ynlw==
```

DMARC

- Monitorowanie

126.com, 163.com, AOL, Comcast.net, google.com, linkedin.com, Mail.Ru, Microsoft Corp., Yahoo! Inc.

```
v=DMARC1; p=none; rua=mailto:reprts@exmpl.com;
```

DMARC

- Monitorowanie
- Testowanie

```
v=DMARC1; p=quarantine; pct=5;
```

DMARC

- Monitorowanie
- Testowanie
- Ochrona

```
v=DMARC1; p=reject;
```

DMARC

„dmarcian provides tools, support, and advocacy to continue growing DMARC within the email ecosystem.”