

Bezpieczeństwo komputerowe - lista

3

Bartosz Biegalski

1.1Przechwytywanie maili

Ustawienia: port 110, bez szyfrowania, hasło jako metoda uwierzytelniania

Efekt: przechwycona wiadomość w plaintekscie, do tego nazwa pliku załączonego w mailu. Login i hasło także w plaintekście!!!

```
Content-Transfer-Encoding: quoted-printable\r\n\r\n+ Line-based test data: text/plain (36 lines)\r\nS=C5=82uchajcie, s=C5=82uchajcie, mieszka=C5=84cy Khorinis! Na rozkaz wielm=\r\no=C5=Bcego lorda\r\nHagena o=C5=82asza si=C4=99 co nast=C4=99puje. W zwl=C4=85zku z zaistnia=\r\n=C5=82=C4=85 sytuacji=C4=85 dla\r\nw=C5=82anego bezpiecze=C5=84stwa, obywatele powinni unika=C4=87 las=C3=Bw=\r\n1 bezdro=C5=Bcy dokoo=C5=82arln\r\nmiasto ci w=C5=82osiej zabrania si=C4=99 kontakt=C3=Bw ze zbuntowanymi wie=\r\n=C5=99niaki=. Od\r\nchwili obecnej lord Andre przejmuj wy=C5=82=C4=85cne dow=C3=B3dztwo nad n=\r\nasz=C4=85 straz=C5=84C=C4=85.rln\r\nWszyscy mieszk=C5=84cy kt=C3=B3rzy posiadaj=C4=85 jakiegokolwiek przestolen=\r\nie w zakresie\r\nwalki niech wt=C4=99puj=C4=85 w szeregi stra=C5=Bcy. Wszelkie =C5=9Brodki =r\nbeziepcze=C5=84stwarln\r\ndotycz=C4=85ce g=C3=B3rnego miasta zostan=C4=85 jeszcze bardziej zaostrozene=r\n.\r\nStra=C5=Bcnicy strzeg=C4=85cy bram nie b=C4=99d=C4=85 przepuszczaj=C4=87 nik=\r\nko kto nie posiada\r\nzewozlenia na wej=C5=9Bcie od miasta. We wszystkich miastach i regionach\r\n=C5=84stwla zostaje wprowadzony stan wojenny. S=C4=99dziwoleby cywilni zos=\r\ntaj=C4=85rln\r\npozbowieni swych praw a ich owbi=C4=85zki przejmuj kr=C3=B3lewscy paladyni=\r\n.. Ka=C5=Bcdyrln\r\nkto pope=C5=82ni=C5=82 przest=C4=99stwo lub sprzeciw si=C4=99 kr=C3=B3lew=r\nskiej straz=C5=84cy podlega\r\nsurowej krze. Egzekucj=C4=85 tego prawa zajmie si=C4=99 wielmo=C5=Bcny lord=D  
Andre. Ka=C5=Bcdyrln\r\nmieszkanie Khorinis, kt=C3=B3ry pope=C5=82ni=C5=82 jakiegokolwy wykrokzenie=r\nma obowi=C4=85tek\r\nzg=C5=82osi=C4=87 si=C4=99 do lorda Andre. W zwl=C4=85zku z atakiem zagra=C5=  
=C5=Bcaj=C4=85cym naszymu miasturln\r\nma obowi=C4=85stek przygotowa=C4=87 si=C4=99 do walki tak jak pozwala mu jeg=r  
o stawn\r\nmaj=C4=85tkowy, dotyczy do zaopatrzenia si=C4=99 w zbroj=C4=99 i or=C4=99n=\r\n=C5=BC, a tak=C5=Bce\r\nnatychmiastowo rozpocz=C4=99cie treningu bojowego.rln\r\nBoundary: ~~~~~00000000000009b7f40616b36c97~
```

```
6 39014 → 110 [ACK] Seq=1 Ack=17 Wi
2 C: CAPA
6 110 → 39014 [ACK] Seq=17 Ack=7 Wi
2 S: +OK Capability list follows
7 C: USER IngmarRabarbar
```

- ▼ Internet Message Format

```

- Unknown-Extension [truncated]: stan maj=C4=85tkowy, dotyczy to zaopat=\
  Type [truncated]: stan maj=C4=85tkowy, dotyczy to zaopat=\r\n\rzenia :
  Value: text/x-csharp; charset="US-ASCII"; name="main.cs"
- Unknown-Extension: Content-Disposition: attachment; filename="main.cs" (
  Type: Content-Disposition
  Value: attachment; filename="main.cs"

```

1.2 Bezpieczeństwo odnośnie SMTP i SSL/TLS

Protokół SMTP nie przewiduje szyfrowania wiadomości na poziomie maili. Na podanych ustawieniach, czyli z wyłączonym bezpieczeństwem połączenia jesteśmy całkowicie narażeni na przeczytanie zawartości naszych maili. Wybranie szyfrowania TLS/SSL sprawia, że klient ThunderBirda nie pozwoli na pobranie maili ze skrzynki, co sprawi że potencjalny podglądacz nic nie zobaczy. Jeśli chcemy więc zwiększyć bezpieczeństwo zawartości maili, powinniśmy wybierać szyfrowanie, dobrą metodę uwierzytelniania, no i najlepiej takich dostawców poczty, którzy nie pozwolą na wyłączenie najbardziej podstawowych zabezpieczeń.

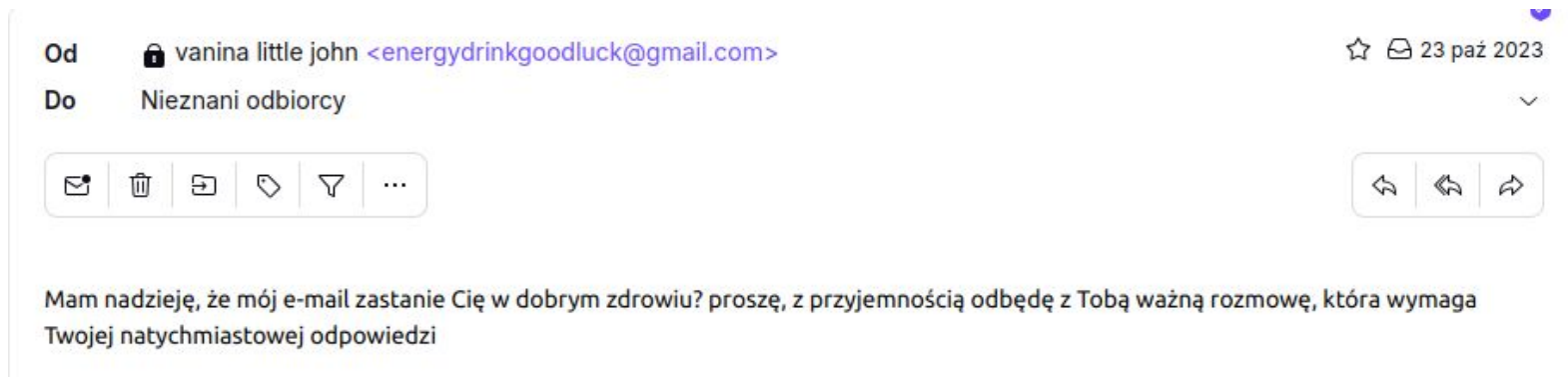
```
66 40660 → 110 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3554199171 TSecr=1529268040
583 C: \026\003\001\002\000\001\000\0010\003\00300P\016\03000\u070F)0\0350{000\03100T0t00\c
82 S: +OK POP3 ready
66 40660 → 110 [ACK] Seq=518 Ack=17 Win=64256 Len=0 TSval=3554199197 TSecr=1529274952
66 110 → 40660 [ACK] Seq=17 Ack=518 Win=64768 Len=0 TSval=1529277000 TSecr=3554199173
88 S: -ERR invalid command
66 40660 → 110 [ACK] Seq=518 Ack=39 Win=64256 Len=0 TSval=3554199228 TSecr=1529282632
66 110 → 46340 [RST, ACK] Seq=39 Ack=518 Win=64768 Len=0 TSval=1015637583 TSecr=3554160688
```

1.3 Protonmail - jego rozwiązania i zabezpieczenia

1. Szyfrowanie emaili end-to-end - tylko nadawca i odbiorca mają dostęp do treści maili, nawet Proton nie wie co się w nich znajduje
2. 2FA z kluczami, np z FIDO-2
3. Chowanie adresu IP, dzięki czemu reklamodawcy nie mogą namierzyć klienta i zbierać jego danych konsumenckich
4. Możliwość zakładania hasła na dany email oraz jego czasu ważności

2. Spam i adresy mailowe, które nie należą do domeny, za którą się podają

Niestety, jakiś czas temu czyściłem sobie wszystkie skrzynki pocztowe ze spamu i śmieciowych wiadomości. Udało mi się znaleźć jedną, podejrzaną wiadomość, która o dziwo przeszła przez zabezpieczenia ProtonMaila:



Przeanalizowałem jego nagłówki i wrzuciłem do programu dig:

Wynik zapytania dla programu dig

Dla tego konkretnego podejrzanego maila DMARC wskazuje na brak szczególnego zakwalifikowania jako niebezpieczny (spośród none, quarantine, ...)

```
bartek@bartek-Lenovo-Legion-5-15IMH05: $ dig _dmarc.gmail.com TXT
; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> _dmarc.gmail.com TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3993
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;_dmarc.gmail.com.                IN      TXT

;; ANSWER SECTION:
_dmarc.gmail.com.                350     IN      TXT      "v=DMARC1; p=none; sp=quarantine; rua=mailto:mailauth-reports@google.com"

;; Query time: 28 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Apr 22 22:16:20 CEST 2024
;; MSG SIZE rcvd: 129
```

Change Log

Nagłówek pokazał, że SPF, DMARC i DKIM przeszły. W tym wypadku narzędzia najprawdopodobniej nie wykryły żadnych zagrożeń w plain tekście. Również adres, z którego został wysłany mail znalazł się na liście dozwolonych serwerów.

Gdyby jednak mail zawierałby jakiś link, najprawdopodobniej trafiłby do spamu, a tak dostałem go w głównej skrzynce pocztowej.

```
Return-Path: <energydrinkgoodluck@gmail.com>
X-Original-To: bartoszbiegalski@protonmail.com
Delivered-To: bartoszbiegalski@protonmail.com
Authentication-Results: mailin032.protonmail.ch; dkim=pass (Good 2048
    bit rsa-sha256 signature) header.d=gmail.com header.a=rsa-sha256
Authentication-Results: mailin032.protonmail.ch; dmarc=pass (p=none dis=none)
    header.from=gmail.com
Authentication-Results: mailin032.protonmail.ch; spf=pass smtp.mailfrom=gmail.com
Authentication-Results: mailin032.protonmail.ch; arc=none smtp.remote-ip=209.85.216.42
Authentication-Results: mailin032.protonmail.ch; dkim=pass (2048-bit key)
    header.d=gmail.com header.i=@gmail.com header.b="R0wLd2oE"
Received: from mail-pj1-f42.google.com (mail-pj1-f42.google.com [209.85.216.42]) (using
    TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256 bits)
    key-exchange X25519 server-signature RSA-PSS (4096 bits) server-digest SHA256) (No
    client certificate requested) by mailin032.protonmail.ch (Postfix) with ESMTPS id
    4SDZGn6YtWz7QQ5P for <bartoszbiegalski@protonmail.com>; Mon, 23 Oct 2023 12:28:17 +0000
    (UTC)
Received: by mail-pj1-f42.google.com with SMTP id 98e67ed59e1d1-27d3c886671so2783423a91.3
    for <bartoszbiegalski@protonmail.com>; Mon, 23 Oct 2023 05:28:17 -0700 (PDT)
```

2. Uzupełnienie

Jeśli chodzi o przypadek, w którym wszystkie polityki zostaną uznane, a wiadomość zawiera złośliwy link, to jest to jak najbardziej możliwe w przypadku gdy adres mailowy podszywa się pod zaufane domeny (np gmail). Z drugiej strony, mi ProtonMail nie pozwala na wysyłanie pustych wiadomości z linkiem, więc po części zależy to też od skrzynki.