Emailové správy, emailové hlavičky a ich analýza

Email management, email headers and their analysis

JANA ZACHAR KUCHTOVÁ[1], PAVOL HORVÁT[2]

Abstrakt

Príspevok rozoberá problematiku elektronickej komunikácie, konkrétne prostredníctvom emailov. V súčasnosti ide o rozšírenú formu komunikácie, ktorá je zneužívaná na páchanie rôznych foriem kriminality. Vzhľadom na to, je cieľom príspevku poukázať na vybrané riziká, ktoré súvisia s používaním elektronickej pošty a zároveň popísať postup pri zaisťovaní emailov za účelom ich správneho uchovania pre ďalšie skúmanie.

Kľúčové slová

email, elektronická pošta, elektronické zaisťovanie, hlavička emailu, IP adresa

Abstract

The article discusses the issue of electronic communication, specifically through emails. Currently, it is a form of communication that is abused to commit various forms of crime. In view of this, the aim of the paper is to point out selected risks related to the use of electronic mail and at the same time to describe the procedure for securing emails in order to learn them correctly for further investigation.

Key words

Email, Electronic Security, Email Header, IP Address

DOI

http://dx.doi.org/10.37355/fvpk-2023/2-14

[1] *npor. JUDr. Jana Zachar Kuchtová, Akadémia Policajného zboru v Bratislave, Katedra Informatiky a manažmentu*

[2] *mjr. JUDr. Pavol Horvát, odbor počítačovej kriminality, Národná centrála osobitných druhov kriminality Prezídia Policajného zboru*

Úvod

Emailová komunikácia sa stáva vecou v zmysle § 130 ods. 2 Tr. zák. (vrátane všetkých súborov ktoré prenášala), až keď sa uloží do mobilného telefónu, počítača alebo iného zariadenia.[3] Jednou z výziev je zhromažďovanie a vytváranie emailových dôkazov tak, aby boli vhodné na použitie v trestných alebo občianskych súdnych sporoch. Preto je veľmi dôležité, aby sa emailové dôkazy zhromažďovali a archivovali zákonným, opakovateľným a obhájiteľným spôsobom. Potreba správneho zaisťovania emailov sa stáva kvôli množstvu nebezpečných emailových správ nevyhnutnou súčasťou nie len práce kompetentných orgánov ale aj samotných používateľov.

Dôvody zaisťovania emailov

Komunikácia v digitálnom priestore je dnes už bežnou súčasťou života. Okrem okamžitej výmeny informácií ponúka možnosť zdieľania akéhokoľvek obsahu. Jedným zo spôsobov je využívanie emailov alebo webmailov. Rozdiel spočíva v tom, odkiaľ sa k emailu pristupuje. V prípade webmailu sa pristupuje prostredníctvom webového prehliadača, nie prostredníctvom aplikácie emailového klienta. Aj napriek pozitívnemu prínosu elektronickej komunikácie tá so sebou prináša aj mnoho hrozieb a rizík[4]. Môže ísť napríklad o šírenie malware prostredníctvom prílohy alebo linku, medzi ktorý patrí ransomware, vírusy, spamy, sociálne inžinierstvo, phishing a iné. Pre zákonodarcu znamená enormná dynamika činnosti v online priestore náročnú výzvu.[5]

Malware je pojem zahrňujúci akýkoľvek škodlivý program, ktorý bol použitý za účelom hacknutia, narušenia alebo poškodenia zariadenia. Patria sem ransomware, vírusy, trojské kone, cryptojacking, rootkity, spamy, červy, adware, spyware.

Ransomware je typ malvéru, ktorý zabraňuje používateľom v prístupe k ich systémovým alebo osobným súborom. Na opätovné získanie prístupu vyžaduje útočník zaplatenie výkupného, aby mohli používatelia znova získať prístup. Ide o inú formu škodlivého softvéru ako je vírus. V súčasnosti je rozšírený spôsob požadovania výkupného prostredníctvom kryptomeny.

Vírus je program alebo kód, ktorý sa šíri v zariadení bez toho aby o tom používatelia vedeli. Existuje viacero typov vírusov, napríklad:

---

[3] *Burda, E. a kol.: Trestný zákon. Všeobecná časť. Komentár. I. diel. 1. Vydanie. Praha: C.H.Beck, 2010, s. 957 a nasl.*

[4] *Bližšie pozri: Ivančík, R. 2022. Dezinformácie ako hybridná hrozba. In Dezinformácie a právo (úlohy a postavenie bezpečnostných zložiek) : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou. Bratislava : Akadémia Policajného zboru, 2020, s. 54-65; Ivančík, R. 2022. Falošné správy – hrozba pre súčasnú spoločnosť. In Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou. Bratislava : Akadémia Policajného zboru, 2022, s. 86-97.*

[5] *Hajdúková, T. 2022. Zneužívanie elektronických služieb na sexuálne zneužívanie detí. In Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou. Bratislava : Akadémia Policajného zboru, 2022, s. 71-85.*

Makrovírus je typ vírusu, ktorý je zabudovaný v softvérových aplikáciách, najčastejšie textových alebo tabuľkových procesoroch.

Polymorfné a metamorfné vírusy pri každej svojej kópii alebo po infikovaní sa do nového zariadenia zmenia svoj zdrojový kód. Polymorfný vírus sa šifruje sám prostredníctvom variabilného šifrovacieho kľúča, metamorfný vírus prepisuje svoj kód sám, bez použitia šifrovacieho kľúča.

Okrem vyššie uvedeného, vzniká potreba zaisťovania emailov aj v prípadoch, kedy dochádza k spáchaniu niektorých trestných činov podľa Trestného zákona č. 300/2005 Z.z., napríklad vyhrážaniu, obťažovaniu, šíreniu poplašných správ alebo vydieraniu.

Nebezpečné vyhrážanie § 360

„Kto sa inému vyhráža smrťou, ťažkou ujmou na zdraví alebo inou ťažkou ujmou takým spôsobom, že to môže vzbudiť dôvodnú obavu.“

Nebezpečné elektronické obťažovanie § 360b

„Kto úmyselne prostredníctvom elektronickej komunikačnej služby, počítačového systému alebo počítačovej siete podstatným spôsobom zhorší kvalitu života iného tým, že ho dlhodobo ponižuje, zastrašuje, neoprávnene koná v jeho mene alebo dlhodobo inak obťažuje.“

Šírenie poplašnej správy § 361

„Kto úmyselne spôsobí nebezpečenstvo vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta tým, že rozširuje poplašnú správu, ktorá je nepravdivá, alebo sa dopustí iného obdobného konania spôsobilého vyvolať také nebezpečenstvo.“[6]

Vydieranie § 189

„Kto iného násilím, hrozbou násilia alebo hrozbou inej ťažkej ujmy núti, aby niečo konal, opomenul alebo trpel.“[7]

Emailové správy

Elektronická pošta je založená na princípe využívania elektronických schránok. Po tom, čo dôjde k odoslaniu emailu je správa smerovaná zo servera na server, to znamená na emailový server príjemcu. Správa je odoslaná na poštový server, ktorý má za úlohu prenášať emaily Mail Transport Agent (ďalej len *„MTA“*) do MTA príjemcu. Komunikácia medzi MTA prebieha pomocou protokolu SMTP, ktoré sa volajú servery SMTP[8]. MTA príjemcu potom doručí email na server prichádzajúcej pošty Mail Delivery Agent (ďalej len *„MDA“*), ktorý ukladá email,

[6] *Trestný zákon č. 300/2005 Z.z., §360 - §361*
[7] *Trestný zákon č. 300/2055 Z.z. §189*
[8] *Niekedy nazývané aj ako servery odchádzajúcej pošty.*

zatiaľ čo čaká, kým ho používateľ prijme. Na získavanie emailov na MDA sa používajú dva hlavné protokoly:

Post Office Protocol (ďalej len *„POP3“*), starší z týchto dvoch protokolov, ktorý sa používa na získavanie emailov[9] a Internet Message Access Protocol (ďalej len *„IMAP“*), ktorý koordinuje stav emailov ako prečítané, odstránené alebo presunuté vo viacerých emailových klientoch. S protokolom IMAP sa kópia každej správy ukladá na server, takže je možné dokončiť úlohu synchronizácie.

MTA fungujú ako pošta, konkrétne triediaca oblasť a poštový doručovateľ, ktorá sa stará o prepravu správ, zatiaľ čo MDA fungujú ako poštové schránky, v ktorých sa uchovávajú správy. MDA je chránený užívateľským menom (loginom) a heslom. Z uvedeného vyplýva, že nato aby bol príjemcovi doručený email nemusí byť nijak spojený s odosielateľom.

Preberanie pošty sa vykonáva pomocou softvérového programu nazývaného Mail User Agent (ďalej len *„MUA“*). Ako je uvedené v časti Dôvody zaisťovania emailov, v prípade, že je MUA nainštalovaný v systéme používateľa, nazýva sa emailový klient (napríklad Microsoft Outlook). Ak ide o webové rozhranie používané na interakciu so serverom prichádzajúcej pošty, nazýva sa webmail.[10]

Otvorené relé

V predvolenom nastavení nie je potrebné autentifikovať sa na odoslanie emailu, takže je veľmi jednoduché sfalšovať svoju adresu. Otvorené relé nerobia nič na to, aby identifikovali pôvodného odosielateľa emailových správ, čím sa stávajú veľmi zraniteľnými voči spoofingu adries[11], čo je technika, ktorá mení hlavičky emailov tak, aby vyzerali, akoby pochádzali z iného zdroja, než je ten skutočný. Hoci takto bol email pôvodne nastavený, tento typ systému často zneužívajú spameri.[12] Keďže otvorený prenos je známy ako otvorený prenosový server, resp. nezabezpečený prenos, takmer všetci poskytovatelia internetových služieb blokujú svoje SMTP servery, aby ich mohli používať iba ich predplatitelia, ktorých IP adresa patrí do domény ISP.

Mnohí poskytovatelia internetových služieb vedú zoznam otvorených prenosov, aby zabránili predplatiteľom prijímať správy z takýchto serverov a tie končili automaticky v spame.[13]

---

[9] *V niektorých prípadoch sa používa na ponechanie ich kópie na serveri.*

[10] *ElenaKM. How email works: step-by-step, diagram. [online] [cit.15.11.2022]. Dostupné na internete: https://ccm.net/apps-sites/email/9999-how-email-works-mta-mda-mua/*

[11] *Typ útoku, pri ktorom osoba alebo program maskuje svoju totožnosť a tvári sa ako druhá osoba.*

[12] *Open Relay. [online] [cit.15.11.2022]. Dostupné na internete: https://www.techopedia.com/definition/1699/open-relay*

[13] *ElenaKM. How email works: step-by-step, diagram. [online] [cit.15.11.2022]. Dostupné na internete: https://ccm.net/apps-sites/email/9999-how-email-works-mta-mda-mua/*

Formát emailovej správy

Všetky internetové správy pozostávajú z obálky, určitého počtu hlavičkových súborov, prázdneho riadku a z tela správy. To je definované v protokolovom štandarde RFC 5322.

Telo správy

Každá správa obsahuje hlavičku. Pole sa skladá z názvu poľa a hodnoty poľa oddelených dvojbodkou. Pole môže obsahovať iba znaky American Standard Code for Information Interchange (ďalej len „*ASCII*") znakovej sady. Obsahuje latinskú abecedu, číslice, netlačiteľné znaky, iné špeciálne znaky a riadiace kódy slúžiace k riadeniu dátového prenosu. Multipurpose Internet Mail Extensions (ďalej len „*MIME*") je rozšírenie internetového emailu, ktoré bolo vyvinuté ako štandard na identifikáciu správy tela emailu. Používa sa pre iné znaky ako ASCII.

Email bol pôvodne navrhnutý pre 7-bitové ASCII. Aby sa toto obmedzenie obišlo, zaviedlo sa rozšírenie v podobe štandardu MIME (Multipurpose Internet Mail Extensions). MIME definuje mechanizmy prenosu aj iných informácií ako sú texty v iných jazykoch než anglickom (podpora iného než ASCII kódovania) a 8-bitový binárny obsah ako sú zvukové, obrazové alebo video súbory.[14]

Hlavička správy

Hlavička emailu je útržok kódu v HTML formáte, ktorý obsahuje informácie o odosielateľovi, príjemcovi, ceste emailu do doručenej pošty a ďalšie detaily podľa emailového klienta.

Každá správa obsahuje jednu hlavičku, ktorá je rozdelená na polia. Každý riadok hlavičky, ktorý začína viditeľným znakom, značí samostatné pole. Pokiaľ je pole dlhšie ako jeden riadok, na začiatok nového riadka je vložená medzera alebo tabulátor. Pole sa skladá z názvu pola a hodnoty pola oddelených dvojbodkou. Pole môže obsahovať iba ASCII znaky (pre ne-ASCII znaky sa používa rozšírenie MIME).[15]

Hlavička obsahuje informácie o prenose – adresa odosielateľa, adresa príjemcu, čas doručenia, názov emailového servera, IP adresa emailového servera a iné. Za účelom analýzy hlavičky je preto nevyhnutné zálohovať správu z emailovej schránky príjemcu. Korektne zálohovaná správa tak obsahuje informácie o prenose z adresy A (typicky páchateľ) na adresu B (typicky poškodený).[16]

---

[14] *AWATI, R. MIME (Multipurpose Internet Mail Extensions). [online] [cit.18.11.2022]. Dostupné na internete: https://www.techtarget.com/whatis/definition/MIME-Multi-Purpose-Internet-Mail-Extensions*

[15] *Zálohovanie emailových správ z webmailových služieb. Dostupné na: https://info.minv.sk/pz/ppz-ncodk/ppz-ncodk-opk/Metodiky/Forms/AllItems.aspx*

[16] *Zálohovanie emailových správ z webmailových služieb. Dostupné na: https://info.minv.sk/pz/ppz-ncodk/ppz-ncodk-opk/Metodiky/Forms/AllItems.aspx*

Ukladanie správ

Ukladanie emailových správ sa do lokálnej schránky realizuje prostredníctvom MDA. Najbežnejšie sú tieto formáty ukladania správ:

MBOX – ukladá všetky správy do jedného súboru,

Maildir – je väčšia adresárová štruktúra, v ktorej je každá správa uložená v samostatnom súbore.

Základný rozdiel spočíva v tom, že MBOX umiestňuje všetky správy do rovnakého súboru na serveri, zatiaľ čo Maildir ukladá správy do jednotlivých súborov s jedinečnými názvami.

MBOX[17] vyjadruje súvisiace formáty súborov, ktoré sa používajú na ukladanie zbierok správ elektronickej pošty. Ukladané sú pritom všetky správy z priečinka. Z toho dôvodu vznikne databázový súbor, do ktorého sa nové správy ukladajú na koniec súboru. Správy oddeľuje čiara a ukončené sú prázdnym riadkom. Pred prvou správou sa bude nachádzať oddeľovací riadok, každá ďalšia správa bude začínať dvomi sekvenciami konca riadku, kde jedna bude na konci samotnej správy a druhá na označenie konca správy v rámci toku databázového súboru MBOX. Novú správu symbolizuje oddeľovací riadok a za koniec databázového súboru sa považuje, keď sa už v databázovom súbore MBOX nenachádzajú žiadne ďalšie údaje správy a ani oddeľovacie riadky.

Formát správy:

- začína riadkom „Od“[18], čo znamená akýkoľvek riadok v správe alebo hlavičke, ktorý začína piatimi znakmi „F“, „r“, „o“, „m“ a medzerou.
- Odosielateľ[19] (napr. jozef@gmail.com) je jedno slovo bez medzier alebo tabulátorov.
- Dátum[20] obsahuje 24 znakov v štandardnom formáte a označuje dátum doručenia správy.
- Riadok „viac informácií“[21] je voliteľný, môže obsahovať ľubovoľné informácie.

Za riadkom „Od“ nasleduje správa vo formáte RFC 5322, pričom posledný riadok je prázdny, bez medzier a tabulátorov.

Varianty MBOX:

- MBOXO,
- MBOXRD,
- MBOXCL a
- MBOXCL2.

[17] *Niekedy známy ako formát Berkeley.*
[18] *V preklade „from“.*
[19] *V preklade „sender“.*
[20] *V preklade „date“.*
[21] *V preklade „moreinfo“*

Tieto verzie sa od seba odlišujú najmä zmenami v riadku „Od“ a použitím poľa „Dĺžka obsahu:“ v hlavičke správy. Ak sú v správe prítomné prílohy, súbory MBOX ich obsahujú v pôvodnom formáte MIME.[22]

Formát Maildir funguje na princípe, že každý priečinok poštovej schránky je adresár a každá správa súbor. Vďaka tomu je možné jednotlivé emaily upravovať, odstraňovať a pridávať bez toho, aby bola ovplyvnená poštová schránka alebo iné emaily. Maildir má index pre každý priečinok, ktorý umožňuje kontrolovať duplikáty, časy exspirácie a fulltextové vyhľadávanie. Vzhľadom na štruktúru formátu Maildir je možný rýchlejší prístup k emailom, čo je významné pri forenznej analýze dátového súboru a pri odhaľovaní možnej počítačovej kriminality.[23]

Elektronické zaisťovanie

Z praxe vyplýva, že poškodení, ktorí chcú nahlásiť podozrenie zo spáchania trestného činu prostredníctvom emailovej správy, nedokážu správnym spôsobom poskytnúť potrebné dáta kompetentným orgánom pre ďalšie vyšetrovanie.[24] Problém spočíva najmä v tom, že ak poškodený prepošle email, ten stráca pôvodnú hlavičku. Takáto preposlaná správa bude v hlavičke emailu obsahovať dáta poškodeného a obsah pôvodnej správy od potenciálneho páchateľa. Preto je dôležité aby poškodený, resp. osoba zaisťujúca email, pracovala s hlavičkou podozrivého emailu. Medzi najpopulárnejších emailových klientov patrí v súčasnosti Apple, Gmail a Outlook.[25]

Zobrazenie hlavičky emailu vybraných emailových klientov

Apple

V aplikácii Mail na stránke iCloud.com je po prihlásení sa do emailov potrebný výber správy.

Kliknutím na tlačidlo  sa zobrazí možnosť zobrazenia všetkých hlavičiek.

Gmail

Po prihlásení sa do Gmailu a zobrazení zvoleného emailu je potrebné kliknúť na tlačidlo  a zvoliť možnosť „Zobraziť pôvodnú správu“.

[22] *MBOX Email Format. [online] [cit.19.11.2022]. Dostupné na internete: https://www.loc.gov/preservation/digital/formats/fdd/fdd000383.shtml*

[23] *Maildir File Format. [online] [cit.19.11.2022]. Dostupné na internete: https://www.systoolsgroup.com/maildir/*

[24] *Bacigál, I., Hajdúková, T., Hlavička, L 2016. Bezpečnosť elektronickej komunikácie a ochrana dát, Bratislava : Akadémia Policajného zboru, 2016, 175 s.*

[25] *Email Client Market Share in June 2022. [online] [cit.20.11.2022]. Dostupné na internete: https://www.litmus.com/blog/email-client-market-share-june-2022/*

Outlook

Po prihlásení sa do Outlooku a otvorení zvoleného emailu je potrebné kliknúť na tlačidlo ▪▪▪ Z ponuky je potrebné vybrať možnosť „Zobraziť“, v ktorej sa nachádza „Zobraziť podrobnosti o správe“.

Kopírovanie a exportovanie hlavičky emailu

Potom, čo je hlavička emailu zobrazená, je možné ju skopírovať označením myšou a klávesovej skratky Ctrl + C, prípadne kliknutím pravým tlačidlom myši a zvolením možnosti kopírovať. Najjednoduchší spôsob je skopírovanú hlavičku vložiť do nástroja na spracovanie textu s názvom „Poznámkový blok“. Po jeho otvorení je potrebná klávesová skratka Ctrl + V alebo kliknutie pravým tlačidlom myši a zvolením možnosti prilepiť. Pokiaľ je text zobrazovaný len v jednom riadku, na karte Zobraziť je možnosť zvoliť Zalomenie textu.

Takto vložený textový dokument je následne potrebné uložiť do zariadenia s príponou *.txt a ten je následne možné poslať ako prílohu emailu alebo ho uložiť na prenosné úložisko a odovzdať na ďalšie skúmanie.

Príklad analýzy hlavičky podvodného emailu

Do emailového klienta Outlook bola doručená správa s nasledujúcim obsahom:

Obrázok 1: Príklad podvodného emailu

Od slečny Rose Richard.

Od slečny Rose Richard.
Abidjan, Pobrežie Slonoviny.

V dôvere sa musím predstaviť, som slečna Rose Richard, 22 rokov, som jedinou dcérou zosnulého pána a pani Wilfred Richard. Kontaktoval som vás po niekoľkých dňoch mojej modlitby za čestného a zodpovedného človeka, ktorý sa dobre postará o mňa a moje dedičstvo, ktoré som legálne zdedil po svojom zosnulom otcovi tu v mojej krajine, prosím, preboha, nevnímajte moju poštu ako rozpaky, pretože sa predtým nepoznáme.

Chcel by som vás požiadať o pomoc v mojom úsilí o zabezpečenie prevodu mojich zdedených peňazí na investičné podniky podľa vašej starostlivosti a smernice, zatiaľ čo tam budem pokračovať vo vzdelávaní vo vašej krajine. Zdedil som tu v mojom mene štyri milióny, päťstotisíc dolárov (4 500 000,00 dolárov) s jednou z hlavných bánk v mojej krajine a budem potrebovať vašu pomoc pri prijímaní prevodu môjho dedičského fondu na váš miestny účet na investičné účely, pretože je mojím želaním prísť do vašej krajiny, aby som pokračoval v mojom vzdelávaní, zatiaľ čo sa budete starať o investovanie peňazí.

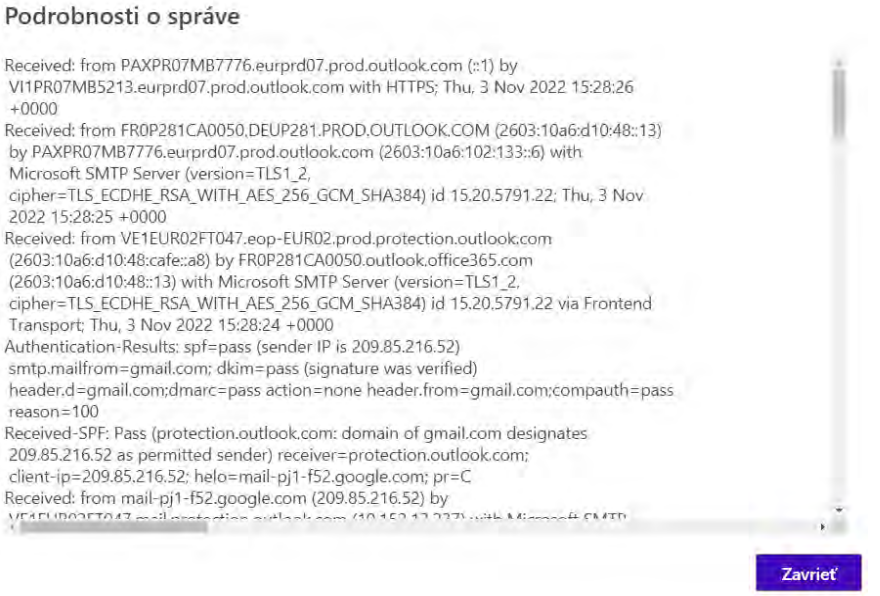
Prosím, som sirota a potrebujem vašu pomoc pri prevode môjho dedičského fondu do vašej krajiny a tiež vašu pomoc pri zabezpečení peknej školy pre mňa vo vašej krajine, kde budem pokračovať vo vzdelávaní. Prosím, osloboďte svoje srdce a pomôžte mi, všetko je legálne, pretože mám v sebe certifikáty týkajúce sa vkladu.

Ďakujem a prajem vám dobrý deň.
Dúfam, že sa vám ozvete.
Váš úprimný.
Slečna Rose Richard.

Po kliknutí na ▪ ▪ ▪ a zvolení možnosti Zobraziť – Zobraziť podrobnosti o správe sa zobrazí hlavička tohto emailu.

Po skopírovaní hlavičky tohto emailu do Poznámkového bloku je možné textový súbor odoslať kompetentným orgánom na skúmanie v podobe *txt.

Obrázok 2: Hlavička podvodného emailu



Zdroj: www.outlook.com

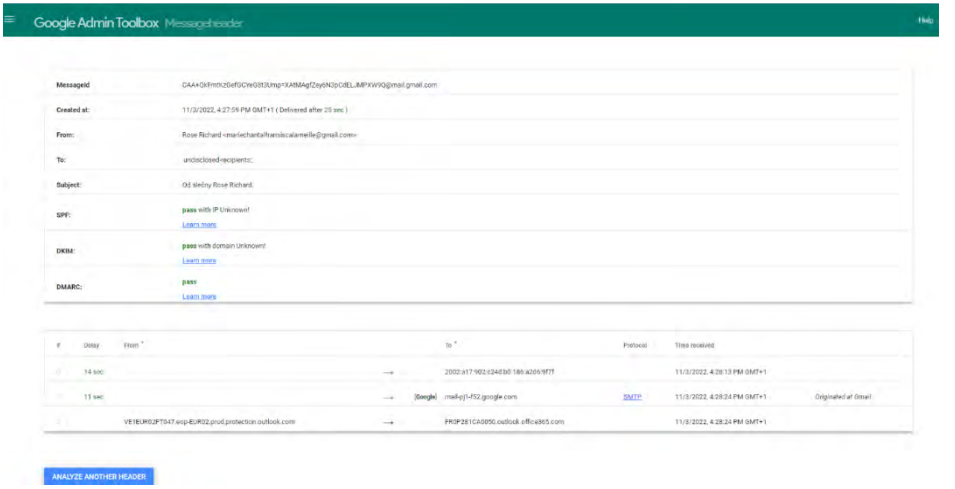
Skúmanie hlavičky podvodného emailu

Prvým krokom k analýze hlavičky emailu je poznanie podstatných náležitostí. Podstatná je identifikácia odosielateľa a príjemcu. Na analýzu emailovej hlavičky je možné využiť rôzne automatické nástroje, tzv. OSINT nástroje. V tomto prípade bol použitý Google Admin Toolbox Messageheader[26] a Gaijin[27].

Ďalšie nástroje na overovanie IP adresy alebo hlavičky emailu:
https://www.ip2location.com/free/email-tracer
https://mha.azurewebsites.net/
https://gaijin.at/en/tools/email-header-analyze

[26] *Dostupné na https://toolbox.googleapps.com/apps/messageheader/analyzeheader*
[27] *Dostupné na https://gaijin.at/en/tools/email-header-analyze*

Obrázok 3: Online nástroj na analýzu hlavičky emailu



Zdroj: https://toolbox.googleapps.com/apps/messageheader/analyzeheader

Z uvedeného je možné zistiť:

Tabuľka 1: Základné údaje z emailovej hlavičky

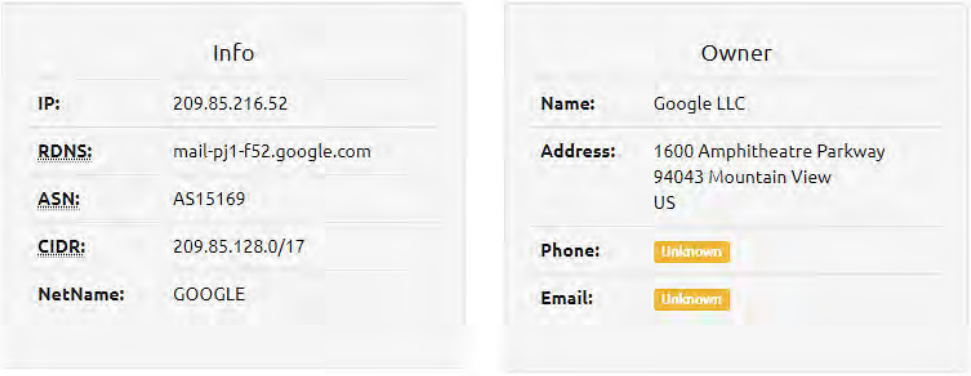
Názov súboru	hlavička.txt
Odosielateľ [From]	**Rose Richard <mariechantalfransiscalameille@gmail.com>**
Príjemca [To]	undisclosed-recipients[28]
Kópia [CC]	jana.kuchtova@akademiapz.sk
Dátum odoslania správy [Date]	Thu, 3 Nov 2022 15:27:59 +0000
Predmet správy [Subject]	Od slečny Rose Richard.
Identifikátor správy [Message-ID]	<CAA+QkFmtKzGefGCYeG8t3Ump=XAtMAgfZey6N3pCdELJMPXW9Q@mail.gmail.com>
Adresa pre vrátenie nedoručiteľného emailu [Return-Path]	mariechantalfransiscalameille@gmail.com
Reply-To:	roserichardd@outlook.com
Emailový server odosielateľa [Received: by]	**mail-pj1-f52.google.com**
IP adresa odosielateľa	**209.85.216.52 (Google LLC)**

Zdroj: vlastné spracovanie

[28] *An undisclosed recipient is an email recipient whose email address is only visible to the sender of the email. In other words, no other recipients - primary or copied (CC or BCC) - will be able to see another recipient's details.*

Analýzou emailovej hlavičky bolo zistené, že IP adresa 209.85.216.52 (https://www.ipalyzer.com/209.85.216.52), ktorá sa nachádza v hlavičke emailovej správy je v správe spoločnosti Google LLC.

Obrázok 4: Informácie k IP adrese



Zdroj: https://www.opalyzer.com

Od spoločnosti Google LLC, so sídlom na adrese Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA, 94043, USA, je v trestnom konaní možné žiadať, cestou medzinárodnej právnej pomoci, informácie k emailovému kontu „Rose Richard <mariechantalfransiscalameille@gmail.com>" a k emailovej správe s nasledovným Message ID:

<CAA+QkFmtKzGefGCYeG8t3Ump=XAtMAgfZey6N3pCdELJMPXW9Q@mail.gmail.com>

Požadované informácie:

- basic subscriber information – základné registračné údaje (meno a priezvisko, registračná IP adresa, email, telefónne číslo a pod.),
- recovery email,
- recovery SMS,
- IP logy,
- logy prihlásení,
- aké účty sú prepojené s príslušným emailovým kontom, tel. číslom, IP adresou,
- iné údaje, ktorými disponujú k danému používateľskému kontu.

Záver

V zmysle uvedeného v úvode tohto príspevku, je v súčasnej dobe komunikácia prostredníctvom internetu považovaná za bežnú súčasť života. Elektronická komunikácia na jednej strane uľahčuje získavanie, výmenu, zber a ukladanie informácií, ale na strane druhej prináša riziká, ktorým nevenujú používatelia vždy dostatočnú pozornosť. To sa v prípade emailovej

komunikácie, súkromnej alebo profesionálnej, odráža v množstve pokusov o spam, vydieranie, šírenie škodlivých vírusov a mnoho iného. Preto je nevyhnutné, aby v prípade, ak dôjde k podozreniu, že v rámci emailovej komunikácie došlo k nezákonnému konaniu, je dôležitým faktorom ďalší postup používateľa a následne kompetentného orgánu. Vzhľadom na formát každej emailovej správy je možné určité údaje získavať z otvorených, t.j. OSINT zdrojov. Aj napriek tomu je však odhalenie identity odosielateľa podozrivého emailu na kompetentných orgánoch, čo znamená, že pre bežného používateľa je zásadné správne zaistenie podozrivého emailu, ktoré sa realizuje prostredníctvom zobrazenia, následného uloženia a distribúcie hlavičky emailu kompetentným orgánom. Správne realizovaný postup prispieva k zefektívneniu vyšetrenia skutku, aj keď stále ide o vysoko latentnú trestnú činnosť.

Literatúra

AWATI, R. MIME (Multipurpose Internet Mail Extensions). [online] [cit.18.11.2022]. Dostupné na internete: https://www.techtarget.com/whatis/definition/MIME-Multi-Purpose-Internet-Mail-Extensions

Bacigál, I., Hajdúková, T., Hlavička, L. 2016. Bezpečnosť elektronickej komunikácie a ochrana dát, Bratislava : Akadémia Policajného zboru, 2016, 175 s. ISBN 978-80-8054-690-8.

Burda, E. a kol. Trestný zákon. Všeobecná časť. Komentár. I. diel. 1. Vydanie. Praha: C.H.Beck, 2010, s. 957 a nasl.

Elena KM. How email works: step-by-step, diagram. [online] [cit.15.11.2022]. Dostupné na internete: https://ccm.net/apps-sites/email/9999-how-email-works-mta-mda-mua/

Email Client Market Share in June 2022. [online] [cit.20.11.2022]. Dostupné na internete: https://www.litmus.com/blog/email-client-market-share-june-2022/

Hajdúková, T. 2022. Zneužívanie elektronických služieb na sexuálne zneužívanie detí. In Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou. Bratislava : Akadémia Policajného zboru, 2022, s. 71-85. ISBN 978-80-8054-965-7.

IVANČÍK, R. 2022. Dezinformácie ako hybridná hrozba. In *Dezinformácie a právo (úlohy a postavenie bezpečnostných zložiek) : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou.* Bratislava : Akadémia Policajného zboru, 2020, s. 54-65. ISBN 978-80-8054-965-7.

IVANČÍK, R. 2022. Falošné správy – hrozba pre súčasnú spoločnosť. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou.* Bratislava : Akadémia Policajného zboru, 2022, s. 86-97. ISBN 978-80-8054-968-8.

Maildir File Format. [online] [cit.19.11.2022]. Dostupné na internete: https://www.systoolsgroup.com/maildir/

MBOX Email Format. [online] [cit.19.11.2022]. Dostupné na internete: https://www.loc.gov/preservation/digital/formats/fdd/fdd000383.shtml

Open Relay. [online] [cit.15.11.2022]. Dostupné na internete: https://www.techopedia.com/definition/1699/open-relay

Trestný zákon č. 300/ 2005 Z.z.