Analysera e-post – Outlook.

Reviderat 2019-12-25

Ju mer man försöker lära sig om hur och varför e-post **klassas som SPAM**, eller varför de **ibland hamnar i skräpkorgen och ibland i inkorgen**, eller varför de **inte kommer fram till mottagaren,** desto tydligare blir det att det inte går att sätta upp en enkel instruktion för hur man skall gå tillväga för att **analysera specifik e-post**. Märkning kan ske både i avsändarens och i mottagarens system samt i alla de servrar som meddelandet passerar genom. Det innebär att många system och därmed aktörer/leverantörer är inblandade. Så att söka orsak till ett problem bara inom Microsoft känns som att man avgränsar sig för mycket. Informationen (internethuvudet) som slutligen bestämmer hur meddelandet skall hanteras har uppdaterats av flera av de servrar som passerats. Det är viktigt att ha i åtanke då det kommer till analysfasen. Se därför det här som ett sätt att beskriva hur man tekniskt kommer åt den information om meddelandet som är intressant för att sedan överlåta åt betraktaren att dra egna slutsatser därifrån.

Analysmetoden kan till exempel användas

- för att **avgöra om ett mejl är skickat från din egen adress** då man kan misstänka att kontot kapats.
- för att ta reda på om **formatet på avsändaren** är sådant att det **inte går att spärra/blockera**.
- för att avgöra **om mejlet är Spam** och därför hamnar i Skräpkorgen.
- för att avgöra om avsändarens **domän är ”förfalskad”,** d.v.s. använder någon annan adress än sin egen som avsändaradress. Detta kan leda till att meddelandet flaggas som spam eller inte når mottagaren.
- för att helt allmänt **kontrollera uppgifter** om avsändaren och annat kring försändelsen.
- för att avgöra om mejlet **producerats av spammare**, vilket gör det svårare att åtgärda. Vanliga funktioner för spärr fungerar då inte utan man måste ta till användning av regler. Inte sällan ingår tecken i avsändaren som inte är ASCII, t.ex. ❄

Anm. Ett meddelande som flaggats som spam behöver de facto inte vara ett. T.ex. kan ett automatiskt frånvaro besked som inte skickas från en användares domän orsaka spam.

Ursprungligen var denna analysmetod i första hand till för att med **rimlig träffsäkerhet** försöka avgöra om ett konto hackats eller om det ”bara” är ett SPAM.

> Vill du slippa mejl från dig själv i inkorgen kan du lägga upp din egen mejladress i listan över spärrade avsändare.
>
> Om mejlet verkligen kommer från dig själv är kontot troligtvis hackat. Har man tur (”otur”) kan uppgiften finnas kvar i din Sänd mapp. Då känns det som ett hack av kontot. Finns det inte i sänd korgen kan den ha blivit rensad. Då får man ta till nästa knep med att analysera varifrån det kommer.

Det borde vara möjligt att med rimlig träffsäkerhet avgöra om ett mejl verkligen kommer från dig själv**, baserat på IP adress**. Detta kan åstadkomma genom att du skickar ett mejl till dig själv och jämför avsändarens information i det mejlet med det mejl du vill undersöka.

Information om vad som finns i mejlhuvudet kan hämtas på mer än ett sätt. Metoder för detta finns beskrivet nedan: Analysera basinformation i e-post

Vill du ta reda på om mejlet kommer från dig själv.

- Skicka ett mejl till dig själv.
- Gör samma analys för båda mejlen.
- Leta reda på IP adress i de båda mejlen. Om dessa är någorlunda lika (nivå 1 o 2 identiska) är det troligt att det kommer från ditt konto.

Vill du kolla formatet på avsändaren.

- Leta reda på Avsändaren

Vill du kolla om mejlet markerats som spam under resans gång, eller förhindrats att levereras p.g.a. felaktig avsändare. (För utförligare beskrivning se avsnitt ”3/ Analysera innehållet on-line”)

- Leta reda på Antispam
- Leta reda på SCL
- Leta reda på SPF

Vill du helt allmänt undersöka meddelandet.

- Leta reda på de sökord du är intresserad av

Analysera basinformation i e-post.

1a/ Behandla e-post som finns i Outlook-Desktop.

Dubbelklicka på e-post så att det öppnas i ett eget fönster.
Välj den lilla pil som finns i nedre högra hörnet i gruppen Taggar.
Markera den text som visas i Internethuvud.
Markera allt (Ctrl + A), kopiera (Ctrl + C) det och klistra in (Ctrl + V) i analysverktyget on-line.

Fortsätt till avsnitt 3/.

1b/ Behandla e-post som finns i eM klient.

Om man inte har installerat Outlook-Desktop finns det en gratisversion av eM klient att hämta från MS Store och den fungerar snarlikt Outlook.

Klicka på e-post i mellersta panelen som skall undersökas.

Välj den lilla pil som finns längst ut till höger i den högra panelen.
Välj alternativ Visa e-post sidhuvud …
Markera den text som visas i nytt fönster.
Markera allt (Ctrl + A), kopiera (Ctrl + C) det och klistra in (Ctrl + V) i analysverktyget on-line.

Fortsätt till avsnitt 3/.

2a/ Behandla e-post som finns på webmail (outlook.com).

Markera meddelandet
Välj ••• uppe till höger i meddelandet och sedan **Visa meddelandekällan**.

Markera texten i **Meddelandekällan**
Kopiera (högerklick)
Klistra in (Ctrl + V) i analysverktyget on-line.

Fortsätt till avsnitt 3/.

2b/ Behandla e-post som finns på webmail (outlook.com) - ett andra alternativ.

För att göra den e-post som bara finns på webben tillgänglig på datorn begärs en första export av Postlådan och lagras på datorn som .pst fil.

Gå till webmail: https://outlook.live.com/mail/inbox
Välj Inställningar (kugghjulet) uppe till höger.
Välj Visa alla inställningar nere till höger.
Skriv Exportera i Sökfönstret.
Välj Exportera Postlåda och följ anvisningarna.
Efter ca 4 dagar kommer en länk till den fil som begärts.
Öppna länken och ”Spara filen som” på lämplig plats med lämpligt namn.

Fortsätt till avsnitt 2d/

2c/ Behandla lokal e-post baserat på .pst fil

Öppna Outlook - Desktop
Kopiera Inkorgen till en .pst fil på lämpligt ställe (skrivbordet).
Välj Arkiv>Öppna o Exportera>Importera och Exportera>Exportera till en fil>Outlook datafil.

Markera Inkorg>Ange filnamn

2d/ Analysera .pst fil

Detta kräver någon form av analys verktyg. Ett sådant är Kernel Outlook Pst Viewer som är gratis och kan hämtas och installeras från https://www.nucleustechnologies.com/pst-viewer.html

Kör analys programmet genom att trycka på Ikonen som dykt upp vid installation

Sök önskad .pst fil via Bläddra.
Välj Nästa
Välj Slutför
Markera Inkorgen
Tryck Sök
Markera Inkorgen
Bocka i lämpligt datum (före i morgon)
Tryck Sök nu
Dubbelklicka på den fil du vill undersöka
Markera Textinnehållet
Markera allt (Ctrl + A), kopiera (Ctrl + C) det och klistra in (Ctrl + V) i analysverktyget on-line.

3/ Analysera innehållet on-line

Använd med fördel detta verktyg där du klistrar in texten för att få informationen läsbar:

https://mha.azurewebsites.net/

För att underlätta analysarbetet kopierar du in resultatet från on-line verktyget i Excel där det går att söka i materialet.

Markera innehållet i alla kolumner och rader i avsnittet Other headers
Kopiera (Ctrl + C)
Klistra in (Ctrl + V)
Formatera celler utan radbrytning
Utöka kolumnbredderna
Formatera celler med radbrytning

Om du hellre vill analysera genom att klistra in i ett Word dokument, i stället för i on-line verktyget, går det också bra. Det kan rent av vara att föredra om du analyserar data från webmail enligt punkt 2b.

Genomför analysen efter din egen modell. Exempel på några intressanta element

X-Sender-IP: Avsändarens IP
From: Avsändaren e-postadress
To: Mottagarens e-postadress

X-Microsoft-Antispam: (länken tar dig till förklaring av koden)
X-Microsoft-Antispam-Message-Info:
X-MS-Exchange-Organization-SCL:
Intressanta sökord är SCL, SPF, DKIM, DMARC, ARC

SCL: (Spam Confidense Level)

Hitta förklaring här: https://docs.microsoft.com/sv-se/microsoft-365/security/office-365-security/spam-confidence-levels

SPF: (Sender Policy Framework)

En SPF-post är ett ramverk. Det används för att indikera för e-postutbyten vilka värdar som har behörighet att skicka e-post för en domän. Det definieras i RFC 4408 och klargörs av RFC 7208.

Sender Policy Framework, eller Sender Permitted From som var det ursprungliga namnet, är en metod för att förhindra att e-post skickas med förfalskade domännamn i avsändaradressen. Med förfalskad menas här att domänen visserligen existerar men att avsändaren använder någon annan adress än sin egen som avsändaradress.

DKIM:

Det är en process för att validera skicka domännamn som är kopplade till e-postmeddelanden via kryptografisk autentisering. Det åstadkommer detta genom att infoga en digital signatur i meddelandeshuvudet som senare verifieras av den mottagande värden för att validera sändningsdomänens äkthet.

DMARC:

Det står för domänbaserad meddelandeautentisering, rapportering och överensstämmelse, är en DNS TXT-post som kan publiceras för en domän för att kontrollera vad som händer om ett meddelande misslyckas med autentisering (dvs. mottagarservern kan inte verifiera att meddelandets avsändare är vem de säger att de är)

ARC: http://arc-spec.org/