Az. P6200/282; P6510-1/2

## Analyse: Verknüpfung IMAP-Konto mit Microsoft Outlook App Android / iOS

**Vermerk**

Im Rahmen einer Analyse wurde das Datensendeverhalten der Outlook-Smartphone-App von Microsoft für Android und iOS analysiert. Diese App kann nicht nur mit Microsoft 365 (ehemals Office 365) genutzt werden, sondern auch mit beliebigen E-Mail-Diensten oder selbst betriebenen Servern über die weit verbreiteten Protokolle IMAP[1] (zum Empfangen und verwalten von auf Servern gespeicherter E-Mails) sowie SMTP[2] (zum Versand von E-Mails). Ebenso ist eine Nutzung mit (eigenen) Exchange-Servern möglich. Dabei ist aufgefallen, dass die App bei Nutzung eines beliebigen IMAP-Mail-Accounts sich nicht direkt mit dem entsprechenden Server sondern mit Microsoft-Servern verbindet. Dieses Verhalten wurde im Folgenden genauer untersucht.

**Zusammenfassung:**

Bei der Nutzung der mobilen Outlook App (iOS, Android) speichert Microsoft die Zugangsdaten zu dem E-Mail-Konto (einschließlich des Passworts) auf eigenen Servern, verarbeitet alle ein- und ausgehenden E-Mails auf eigenen Servern und hat damit vollen Einblick sowohl in Inhalts- als auch in alle Metadaten. Microsoft erhält damit sensible Einblicke in das Kommunikationsverhalten der betroffenen Personen.

Den Nutzern wird dieses Verhalten nicht transparent dargestellt, eine Rechtsgrundlage ist nicht ersichtlich.

Die vorliegende Analyse beschreibt kein Datensendeverhalten bzgl. Telemetrie-, Diagnosedaten und ähnlichen Daten. Bei der Durchführung der Prüfung wurden allerdings zahlreiche Verbindungen zu entsprechenden Endpunkten wie

- https://mobile.pipe.aria.microsoft.com/Collector/3.0/
- https://olmprodpowerlift-cdn.azureedge.net/powerlift-analysis-systems/ oder
- https://gate.hockeyapp.net/v2/track

festgestellt, aber aufgrund des Fokus dieser Untersuchung nicht weiter analysiert.

Beteiligt an der Prüfung: [redacted]

---

[1] Internet Message Access Protocol, standardisiert in RFC 3501

[2] Simple Mail Transfer Protocol, standardisiert in RFC 5321

**Vorgehen:**
Es wurde ein bestehendes E-Mail-Konto via IMAP mit der offiziellen Outlook App verknüpft. Der Test und die Untersuchung fand auf den beiden Plattformen Android und iOS statt. Als Server für IMAP und SMTP kommt ein Server von FRE zum Einsatz, da unser Abteilungs-Server derzeit noch kein IMAP bietet.
Nachfolgend sind die Ergebnisse für die Outlook App in der Version 4.2030.3 für Android beschrieben. [iOS ist noch zu ergänzen]

Die verwendeten Login-Daten für das IMAP-Konto lauten wie folgt:

- E-Mail-Adresse: lft2@[redacted]
- Username: lft2
- Passwort: - - - Teschtle0816 - - -
- IMAP- / SMTP-Server: [redacted] (IP-Adresse [redacted])

Innerhalb der Outlook App lassen sich E-Mail-Konten von diversen Anbietern verknüpfen. Zu Testzwecken wurde das oben genannte IMAP-Konto verwendet. Am E-Mail-Server (Cyrus Imapd und Exim) wurde im Server-Log geprüft, welcher Client sich mit dem Server verbindet. Der Datenverkehr vom Smartphone wurde mitgeschnitten, um die Zugriffe zu prüfen.

**Erwartetes Verhalten:**
Die App sollte sich direkt mit dem angegebenen Server über IMAP verbinden und ansonsten keine weiteren Verbindungen durchführen. Es sollten keine Datenabflüsse stattfinden. Wenn doch, muss dies dem Nutzer klar und deutlich kommuniziert, begründet werden. Nutzer müssen auf damit einhergehende Risiken (insbesondere Offenbarung von Kommunikationsinhalten und Metadaten) hingewiesen werden. Solche Funktionen sollten wenn überhaupt nur manuell nach entsprechender Aufklärung aktiviert werden können. Dies gilt sowohl für das Senden als auch das Abrufen von E-Mails.

**Festgestelltes Verhalten:**

Nach Eingabe der erforderlichen Daten (Username, Passwort etc.) verbindet sich nicht die App direkt sondern ein Microsoft-Server mit dem konfigurierten E-Mail-Server, wie aus den Protokolldateien des Servers ersichtlich ist:

```
Aug 28 11:07:56 cyrus imaps[68216]: login: [52.125.140.74] lft2 LOGIN+TLS User
logged in SESSIONID=<[redacted]-68216-1598605676-1-7251846154066095578>
```

```
[...]
Aug 28 11:12:39 cyrus imaps[75933]: login: [52.125.138.94] lft2 LOGIN+TLS User
logged in SESSIONID=<[redacted]-75933-1598605959-1-1865504613446843484>
```

Die IP-Adresse 52.125.141.94 ist Microsoft zuzuordnen, siehe Anlage 1 (Auszug aus dem Whois).

Zu späteren Zeitpunkten erfolgen weitere Zugriffe von Microsoft-Servern:

```
Aug 28 13:40:18 cyrus imaps[88817]: login: [52.125.138.94] lft2 LOGIN+TLS User
logged in SESSIONID=<[redacted]-88817-1598614817-1-10708460015531101292>
Aug 28 13:40:18 cyrus imaps[87882]: login: [52.125.138.94] lft2 LOGIN+TLS User
logged in SESSIONID=<[redacted]-87882-1598614818-1-8872240340624646673>
```

Über den Zeitraum von etwa viereinhalb Stunden wurden Zugriffe von sechs verschiedenen IP-Adressen aus dem Netz von Microsoft festgestellt; innerhalb mehrerer Tage (28. bis 31. August) kamen keine weiteren hinzu:

```
52.125.138.29
52.125.138.94
52.125.140.101
52.125.140.74
52.125.141.101
52.125.141.99
```

Auch beim Versenden erfolgt der Versand über Microsoft-Server (Ausschnitt aus dem Protokoll des SMTP-Servers):

```
Aug 28 11:08:49 exim exim[75221]: no host name found for IP address 52.125.140.74
Aug 28 11:08:49 exim exim[75221]: 1kBaNN-000JZF-ET <= lft2@[redacted]
H=(mail.outlook.com) [52.125.140.74]:36622 P=esmtpsa L- X=TLS1.2:ECDHE-RSA-AES256-
SHA384:256 CV=no SNI="[redacted]" A=sasl_login:lft2 S=1242 M8S=0 RT=0.161s
id=5EADD75739850053.400b0a2c-3232-458a-85c4-4b71ab5a11a9@mail.outlook.com from
<lft2@[redacted]> for [redacted]
Aug 28 11:13:49 exim exim[75221]: SMTP command timeout on TLS connection from
(mail.outlook.com) [52.125.140.74]:36622
```

Die Microsoft-Server halten permanent Verbindungen zum IMAP-Server offen, auch wenn die Anwendung schon mehrere Tage nicht mehr genutzt wurde:

```
# netstat -n | egrep '(52.125.1|Active Inter|Proto)'
Active Internet connections
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4       0      0 10.23.42.103.993       52.125.138.94.56460    ESTABLISHED
tcp4       0      0 10.23.42.103.993       52.125.138.94.56440    ESTABLISHED
tcp4       0      0 10.23.42.103.993       52.125.140.112.48010   ESTABLISHED
tcp4       0      0 10.23.42.103.993       52.125.140.112.47990   ESTABLISHED
tcp4       0      0 10.23.42.103.993       52.125.140.74.51654    ESTABLISHED
tcp4       0      0 10.23.42.103.993       52.125.140.74.51592    ESTABLISHED
```

(Hinweis: bei der “Local Address” handelt es sich um eine lokale Adresse aus dem 10/8er Netz, da TCP-Verbindungen von draußen in das entsprechende Jail mit dieser Adresse weitergeleitet werden.)

Ob E-Mails weiterhin auf Microsoft-Servern verarbeitet, werden wenn die App bereits gelöscht wurde, wurde bisher nicht geprüft.

In der App finden Nutzer keine Hinweise darauf, dass sowohl alle E-Mails als auch die verwendeten Passwörter Microsoft im Klartext vorliegen. Eine informierte Einwilligung wird nicht eingeholt. Welche Verarbeitungen durch Microsoft stattfinden ist nicht transparent.

Ein Datenmitschnitt mit Wireshark bestätigt die Analyse. Die App kontaktiert bei der Verknüpfung mit dem E-Mail-Konto, beim Versenden und auch Empfangen von E-Mails nicht einmal den E-Mail-Server ([redacted]. Daraus lässt sich folgern, dass jegliche Kommunikation bzw. auch der Versand und Empfang von E-Mails stets über Server von Microsoft verläuft.

**Verbindungen nach Löschen der App**

Für einen weiteren Test wurde die App am 01.09.2020 auf dem Smartphone gelöscht. Der Microsoft-Server meldet sich aber dennoch permanent weiterhin am E-Mail-Server an, um E-Mails abzuholen, wie in den Logfiles ersichtlich:

```
Sep  2 10:38:16 cyrus imaps[41490]: login: [52.125.138.94] lft2 LOGIN+TLS User
logged in SESSIONID=<[redacted]-41490-1599035896-1-11058160043874696523>
Sep  2 11:10:15 cyrus imaps[50291]: login: [52.125.140.74] lft2 LOGIN+TLS User
logged in SESSIONID=<[redacted]-50291-1599037815-1-9325482903716871814>
```

```
Sep  2 11:10:16 cyrus imaps[11887]: login: [52.125.140.74] lft2 LOGIN+TLS User
logged in SESSIONID=<[redacted]-11887-1599037815-1-958401625021725865>
Sep  2 11:39:22 cyrus imaps[56138]: login: [52.125.138.94] lft2 LOGIN+TLS User
logged in SESSIONID=<[redacted]56138-1599039561-1-16356951987953391022>
Sep  2 11:39:23 cyrus imaps[39440]: login: [52.125.138.94] lft2 LOGIN+TLS User
logged in SESSIONID=<[redacted]-39440-1599039562-1-1267589854112029711>
```

Eine tiefergehende Analyse der abgesetzten IMAP-Befehle und übertragenen Datenmengen könnte feststellen, welche Mails aus welchen Ordnern abgeholt werden. Eine solche Analyse wurde bisher nicht durchgeführt.

**Datenschutzerklärung von Microsoft:**

In der Datenschutzerklärung von Microsoft unter https://privacy.microsoft.com/de-de/privacystatement heißt es:

> *Bei Verwendung der mobilen Outlook-Anwendungen werden diese Daten ebenfalls mit Microsoft-Servern synchronisiert, um zusätzliche Funktionen zu aktivieren. Dazu gehören schnellere Suchergebnisse, personalisiertes Filtern weniger wichtiger E-Mails und die Möglichkeit, E-Mail-Anlagen von verknüpften Dateispeicheranbietern ohne Verlassen der Outlook-App hinzuzufügen. Bei der Verwendung der Desktop-Outlook-App können Sie auswählen, ob Ihre Daten mit unseren Servern synchronisiert werden sollen. Sie können jederzeit ein Konto entfernen oder die Daten ändern, die von Ihrem Konto synchronisiert werden.*

Unabhängig davon, ob eine simple Erwähnung in der Datenschutzerklärung ausreicht: Diese Beschreibung macht nicht deutlich, dass Microsoft sowohl vollen Zugriff auf alle E-Mails des Nutzers hat, ebensowenig dass auch alle gesendeten E-Mails über Microsoft-Server abgewickelt werden und dort selbst dann verarbeitet werden, wenn die App gar nicht genutzt wird. Ebenso ist nicht klar, dass Microsoft die Zugangsdaten einschließlich der Passwörter auf ihren Servern speichert.

**Bewertung:**

Durch dieses Vorgehen hat Microsoft vollen Zugriff sowohl auf alle empfangenen als auch auf die gesendeten E-Mails. Ebenso hat Microsoft Zugriff auf die Klartext-Passwörter, die

nach obiger Analyse auch auf dem Microsoft-Server gespeichert werden. Aus technischer Sicht ist dies nicht notwendig.

Ein durchschnittlicher Nutzer geht davon aus, dass eine E-Mail-Anwendung sich direkt mit dem eingetragenen E-Mail-Server verbindet und nicht die Zugangsdaten zu einem Server des Anbieters überträgt und der gesamte Datenverkehr über Server des Anbieters läuft.

Eine transparente Information über dieses Verhalten ist nicht ersichtlich. Insgesamt ist für den Nutzer nicht transparent erkennbar, zu welchem Zweck sich Microsoft mit den sensiblen Zugangsdaten direkt auf dem E-Mail-Server beim Provider anmeldet, wie es mit den Inhalten der E-Mails umgeht und wie diese sensiblen Kommunikationsdaten (auch vor Zugriffen Dritter) geschützt werden. Die oberflächlichen Erklärungen dazu in der Datenschutzerklärung sind nicht ausreichend. Eine informierte Einwilligung der Nutzer wird nicht eingeholt.

Verfügung:

1. z.V.

**Anlage 1:**

Whois zur IP-Adresse 52.125.140.74, gültig für den gesamten Netzbereich 52.125.0.0 - 52.127.255.255:

```
Using server whois.arin.net.
Query string: "n + 52.125.140.74"


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2020, American Registry for Internet Numbers, Ltd.
#


NetRange:       52.125.0.0 - 52.127.255.255
CIDR:           52.126.0.0/15, 52.125.0.0/16
NetName:        MSFT
NetHandle:      NET-52-125-0-0-1
Parent:         NET52 (NET-52-0-0-0-0)
NetType:        Direct Assignment
OriginAS:
Organization:   Microsoft Corporation (MSFT)
RegDate:        2015-11-24
Updated:        2015-11-24
Ref:            https://rdap.arin.net/registry/ip/52.125.0.0


OrgName:        Microsoft Corporation
OrgId:          MSFT
Address:        One Microsoft Way
City:           Redmond
StateProv:      WA
PostalCode:     98052
Country:        US
```

RegDate:        1998-07-10
Updated:        2017-01-28
Comment:        To report suspected security issues specific to traffic emanating from Microsoft online services, including the distribution of malicious content or other illicit or illegal material through a Microsoft online service, please submit reports to:
Comment:        * https://cert.microsoft.com.
Comment:
Comment:        For SPAM and other abuse issues, such as Microsoft Accounts, please contact:
Comment:        * abuse@microsoft.com.
Comment:
Comment:        To report security vulnerabilities in Microsoft products and services, please contact:
Comment:        * secure@microsoft.com.
Comment:
Comment:        For legal and law enforcement-related requests, please contact:
Comment:        * msndcc@microsoft.com
Comment:
Comment:        For routing, peering or DNS issues, please
Comment:        contact:
Comment:        * IOC@microsoft.com
Ref:            https://rdap.arin.net/registry/entity/MSFT


OrgTechHandle: MRPD-ARIN
OrgTechName:   Microsoft Routing, Peering, and DNS
OrgTechPhone:  +1-425-882-8080
OrgTechEmail:  IOC@microsoft.com
OrgTechRef:    https://rdap.arin.net/registry/entity/MRPD-ARIN

OrgAbuseHandle: MAC74-ARIN
OrgAbuseName:   Microsoft Abuse Contact
OrgAbusePhone:  +1-425-882-8080
OrgAbuseEmail:  abuse@microsoft.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/MAC74-ARIN


#

```
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2020, American Registry for Internet Numbers, Ltd.
#
```