Wolkig mit Aussicht auf Datenlecks

Neues Outlook überträgt Passwörter an Microsoft

Das neue Outlook macht einiges anders als das alte: Wer es ausprobiert, überträgt sensible Zugangsdaten und Mails in die Microsoft-Cloud. Datenschützer sind alarmiert.

Von Ronald Eikenberg

Nutzt man die aktuelle Windows-11-Version, empfiehlt das Startmenü ein neues Mailprogramm namens „Outlook (new)“ (siehe auch FAQ auf Seite 164). Es soll die „Mail“-App von Windows langfristig ersetzen. Auch Office-Nutzer machen schnell Bekanntschaft mit der neuen App, schon weil Microsoft den Schiebeschalter „Testen Sie das neue Outlook“ prominent im alten Outlook platziert hat.

Doch der jüngste Outlook-Spross machte zuletzt mit einer Datenschutzfalle Schlagzeilen, in die Nutzer leicht tappen: Anders als von Outlook und anderen Mailclients gewohnt, baut die neue App keine direkte Verbindung zu den eingerichteten Mailservern auf, sondern überlässt das der Microsoft-Cloud. Trägt man die Zugangsdaten für ein IMAP-Mailkonto ein, schickt die App diese Daten an Microsoft. Die Microsoft-Cloud nutzt die Zugangsdaten, um selbst Kontakt zu den Mailservern aufzubauen und die Mails abzuholen sowie zu speichern.

Mailpasswort in der Microsoft-Cloud

Dies belegt eine Analyse von c’t mit einem sogenannten Man-in-the-Middle-Proxy, mit dem wir uns lokal in den TLS-verschlüsselten Datenverkehr der App eingeklinkt haben. Dabei zeigte sich, dass die App die Microsoft-URL https://outlook.office.com/ows/beta/ShadowService/getShadowToken kontaktiert und Usernamen sowie Passwörter dorthin überträgt. Kurz darauf meldeten sich die IP-Adressen 52.98.204.101 und 52.98.207.109 mit unseren Zugangsdaten am Mailserver an, wie dessen Logdateien belegen. Der Eigentümer der IP-Adressen ist die Microsoft Corporation aus Redmond.

Informiert wurden wir über die Übertragung der Zugangsdaten und die daraus resultierenden Konsequenzen nicht. Die Outlook-App wies uns lediglich darauf hin, dass unser Mailkonto synchronisiert werden müsse: „Um Ihr IMAP Konto zu Outlook hinzuzufügen, müssen wir Ihre E-Mails mit der Microsoft Cloud synchronisieren.“ Kein Wort zur Preisgabe der Log-in-Informationen.

Besonders überrascht hat uns, dass wir die Übertragung auf einem System beobachten konnten, auf dem wir gar kein Cloudkonto von Microsoft eingerichtet hatten: Windows 11 hatten wir ohne Microsoft-Konto eingerichtet und auch die Outlook-App verlangte keines. Offenbar hat Microsoft ungefragt eine Art Schattenkonto in seiner Cloud für uns erstellt, um damit unsere Mails abzurufen und zu speichern.

Als wir das Unternehmen mit unseren Beobachtungen konfrontierten, verwies es auf den Hinweis zur Synchronisierung der Daten und den darin verlinkten Support-Artikel (siehe ct.de/yqyu). Der Artikel erklärt (Stand: 21.11.2023), dass Nutzer anderer Mailanbieter nun von Microsoft 365 und Exchange Online bekannte Komfortfunktionen wie „E-Mail-Suche“, „Posteingang mit Relevanz“ oder auch „E-Mails als gelesen/ungelesen markieren“ nutzen können.

Was er jedoch nicht erklärt, ist die Übertragung und Speicherung der Zugangsdaten. Diese räumte Microsoft in der Stellungnahme etwas verklausuliert ein: „Bei IMAP-Providern, bei denen Microsoft die Verbindung mit BasicAuth herstellt, speichern wir die Zugangsdaten als User-Token in verschlüsselter Form.“ Mit BasicAuth meint das Unternehmen die klassische Authentifizierung mit Benutzername und Passwort, wie das bei IMAP und SMTP der Fall ist.

```
POST /ows/beta/ShadowService/getShadowToken?
Host: outlook.office.com
{
  "emailAddress":"rei@ct.de",
  "providerType":"GenericImap",
  "remoteImapServer":{
    "hostname":"imap.ct.de",
    "port":993,
    "secure_connection_type":"ssl"
  },
  "remoteSmtpServer":{
    "hostname":"smtp.ct.de",
    "port":587,
    "secure_connection_type":"ssl"
  },
  "remoteImapCredentials":{
    "UserId":"rei@ct.de",
    "Secret":"GeheimesPasswort!"
  },
  "remoteSmtpCredentials":{
    "UserId":"rei@ct.de",
    "Secret":"GeheimesPasswort!"
  }
}
```

Die neue Outlook-App überträgt die sensiblen Zugangsdaten zum Mailkonto in lesbarer Form an Microsoft.

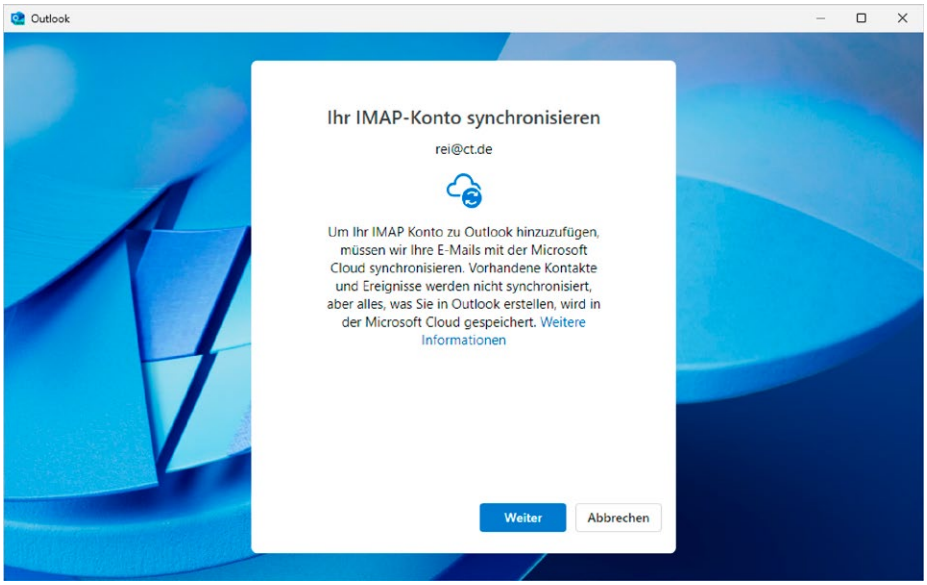
Kein Zugriff aufs Klartextpasswort?

Das Unternehmen will jedoch selbst keinen Zugriff auf die Zugangsdaten haben: „Nur die Benutzer selbst und die Microsoft-Dienste, die mit der Mailbox interagieren, um die Daten abzurufen, haben Zugriff auf dieses Token. Das bedeutet, dass Microsoft keinen Zugriff auf das Klartextkennwort hat.“ Diese Aussage ist mindestens irreführend, denn natürlich benötigt Microsoft das Kennwort im Klartext, um sich gegenüber den externen Mailservern zu authentifizieren und die Mails abrufen zu können.

Zur Speicherung der Daten äußert sich das Unternehmen wie folgt: „Diese Informationen werden gespeichert, solange der Benutzer den E-Mail-Client aktiv nutzt. Bei Inaktivität werden die Kontodaten gemäß dem Kontolebenszyklusprozess entfernt. Der Nutzer hat auch die Möglichkeit, die Löschung von Daten (einschließlich Zugangsdaten) bei Bedarf zu beantragen, indem er das Konto löscht und die Option ‚von allen Geräten entfernen‘ wählt.“ Das ist ein wichtiger Hinweis, der auch dem in Outlook verlinkten Support-Artikel gut zu Gesicht stünde.

Wer das neue Outlook im Startmenü oder in der Oberfläche des alten Outlook entdeckt und ausprobiert, dem dürfte nicht klar sein, dass er damit nicht länger einen lokalen Mailclient verwendet, sondern im Prinzip eine Art Webmaildienst wie Outlook.com oder Gmail. Grundsätzlich hat die neue App durchaus ihre Daseinsberechtigung und einige Vorteile, denn das Cloudkonto bietet gegenüber IMAP diverse Komfortfunktionen und eine flotte, globale Suchfunktion. Die Nutzung muss jedoch stets eine bewusste Entscheidung sein, da sie mit der Herausgabe sensibler Zugangsdaten und Mails verbunden ist.

Für Microsoft ist es nicht der erste Vorfall dieser Art: Bereits im Jahr 2015 führten die damals veröffentlichten Outlook-Apps für iOS und Android zu Schlagzeilen, als herauskam, dass sie ebenfalls die Cloud für den Mailabruf und -versand nutzten. Die Apps wurden daraufhin vielerorts untersagt oder gesperrt, etwa an deutschen Universitäten. Als wir Ende 2022 Mail-Apps für iOS testeten (siehe ct.de/yqyu) zeigte sich, dass Microsoft dieses Verhalten abgestellt hatte und die Outlook-App direkt mit eingestellten Mailservern spricht. Auch die Android-App baut die Verbindungen inzwischen direkt auf. Bei den Outlook-Apps für Windows und auch macOS schlägt Microsoft jetzt wieder den entgegengesetzten Kurs ein.



Wer hier zustimmt, gewährt Microsoft umfassenden Zugriff auf das Mailkonto.

Datenschützer sind besorgt

Datenschützer zeigen sich besorgt über die aktuellen Entwicklungen: „Die Meldungen über ein vermutetes Datensammeln von MS über Outlook sind alarmierend“, schrieb der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Ulrich Kelber auf Mastodon. Kurz danach hat das BfDI die für Microsoft in der EU zuständige irische Datenschutzbeauftragte um einen Bericht gebeten.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) warnte in einer Pressemitteilung vor der Datenübertragung: „Momentan rät der TLfDI [...] dringend dazu, sich die Genehmigung für diesen tiefgreifenden Eingriff in die Privatsphäre durch die App ‚Neues Outlook‘ bestens zu überlegen und die richtigen Schlüsse [...] zu ziehen. Nehmen Sie das von Microsoft selbst ins Spiel gebrachte Wahlrecht wahr und verzichten Sie auf die neue Outlook-Version!“

Auch der ehemalige Landesdatenschutzbeauftragte Baden-Württembergs Stefan Brink, der heute das Wissenschaftliche Institut für die Digitalisierung der Arbeitswelt leitet, hat Bedenken: „Das kann sogar ein Rechtsverstoß des Nutzers sein, etwa wenn er als Mitarbeiter des öffentlichen Dienstes oder Träger von Geschäftsgeheimnissen seines Unternehmens bestimmten Geheimhaltungsvorschriften unterliegt. Zudem gibt der Nutzer damit Microsoft Zugriff auf die Inhalte der Mails – und das darf er in aller Regel nicht.“

Brink hält sogar einen DSGVO-Verstoß für möglich: „Dass personenbezogene Daten in einer für die betroffene Person nachvollziehbare Weise verarbeitet werden, gehört zu den Grundsätzen der DSGVO (Art. 5 Abs. 1 DSGVO). Dass die hier gezeigte Vorgehensweise von Microsoft dem gerecht wird, kann man mit Fug und Recht bezweifeln.“

Was Sie jetzt tun können

Aktuell helfen nur individuelle Maßnahmen: Unternehmen, öffentliche Institutionen & Co. müssen sich bewusst entscheiden, ob sie der neuen Outlook-App und damit auch der Weitergabe sensibler Zugangsdaten und Mails an die Microsoft-Cloud zustimmen und ihre Mitarbeiter entsprechend informieren. Zudem sind technische Maßnahmen möglich, etwa das Entfernen des im alten Outlook angezeigten Schalters „Testen Sie das neue Outlook“ per Gruppenrichtlinie oder das Blockieren der Microsoft-Zugriffe auf den Mailserver (siehe ct.de/yqyu). Wer die neue App bereits ausprobiert hat, kann Microsoft über das Zahnradsymbol oben rechts und „Konten verwalten/Verwalten/Entfernen/Von allen Geräten entfernen“ bitten, die Daten aus der Cloud zu löschen. *(rei@ct.de)* c't

Hintergründe & Schutz: ***ct.de/yqyu***