Die Machtkonzentrierung geht (leider) weiter

Egg, 24. November 2023: *Offene Protokolle sind für den Austausch von Informationen in einer vernetzten Welt unerlässlich. Ohne das Internet gäbe es die Art und Weise, wie wir heute miteinander kommunizieren nicht. Die Standardprotokolle des Webs sind Garant dafür, dass wir aktuell und auch in Zukunft die Wahl haben, dass ein Austausch möglich ist und mit welchen Apps dies erfolgen soll. Die standardkonformen Protokolle des Internets sind bei den Tech-Konzernen jedoch mehr geduldet denn erwünscht. Aktuelles Beispiel bildet die neue Outlook-App unter Windows.*

Outlook mit IMAP neu nur über Microsoft-Cloud

Bislang war es möglich, Outlook mit jedem beliebigen Mail-Provider einzurichten. Neu ist dies faktisch nicht mehr möglich. Wird die neue Outlook App unter Windows aktiviert, so werden beim Einbinden des Mail-Dienstleisters, der die Mails für Kunden entgegennimmt und diese zur Outlook-App (E-Mail-Client) weiterleitet, die Kennwortdaten (inkl. Passwörter) immer in der Microsoft-Cloud gespeichert. Microsoft erfragt und verarbeitet danach sämtliche Mails des externen Mail-Providers in seiner eigenen Cloud.

Die Grundgedanke des Webs, dass Informationen standardkonform ausgetauscht werden, wird damit zerstört. Microsoft kann mit den Accounts schalten und walten, wie es dem Konzern beliebt. Und damit ist noch nicht einmal das Szenario gemeint, dass Outlook selber etwas gar neugierig wäre, sondern das Faktum, dass beliebige Dritt-Applikationen von Microsoft jederzeit auf diese Mails zugreifen können, dass diese Cloud-Dienste Inhalte verändern können, ohne dass der Endbenutzer/in dies überhaupt (z.B. durch erhöhte Aktivität auf dem eigenen Rechner) feststellen kann. Mehr

Informationen zum Thema finden sich bei **heise.de.**

Die Folgen sind nicht ganz nebensächlich

Natürlich werden nun wieder viele einwenden, alles halb so wild. Es muss ja niemand Microsoft-Produkte einsetzen, und schon gar nicht Outlook. Nun ist es aber doch so, dass die Outlook-Produkte derart gut in die Offfice-Apps und Teams von Microsoft integriert sind, dass die meisten Unternehmen letztlich genau darum auf Outlook setzen. Outlook im bisherigen Sinne war ein E-Mail-Client, der mit jedem beliebigen IMAP-Mail-Provider verwendet werden konnte.

Neu ist dies faktisch nicht mehr gegeben. Wer die Outlook-App einsetzt, kann einen alternativen IMAP-Provider nur noch dann verwenden, wenn Microsoft ungefragt mitliest, mitschreiben kann und überdies diese Daten immer in der Microsoft-Cloud speichert. Mit anderen Worten, wer die neue Outlook-App einsetzt, willigt immer dazu ein, dass alle Daten bei Microsoft gespeichert werden.

Hilft eine Verschlüsselung der Mails ?

Aktuell werden Mails z.B. über den S/MIME-Standard verschlüsselt. Dabei gibt es einen privaten und einen öffentlichen Schlüssel. Der private Schlüssel verbleibt beim Absender, der Empfänger erhält den öffentlichen Schlüssel und kann mit diesem die verschlüsselte Nachricht lesen.

Sofern der private Schlüssel nie ausser “Haus” geht und der öffentliche Schlüssel einzig beim Empfänger landet, bieten so verschlüsselte Mails einen recht guten Schutz gegen unbefugtes “Lesen” der Daten. Jedoch, der private Schlüssel muss im Mail-Client hinterlegt werden. Wie kann nun sicher gestellt werden, dass diese Schlüssel nicht doch an Microsoft weitergeleitet werden?

Bei Closed Source Software (der Quellcode ist nicht offengelegt) ist keine Aussage möglich, was ein entsprechendes Programm macht oder nicht. Immerhin kann über ein Aufzeichnen des Datenverkehrs (Logging) festgestellt werden, ob bzw. dass Informationen ausgetauscht werden. Solange Outlook folglich nur Daten zum Mail-Provider sendet, kann zumindest die Aussage gemacht werden, dass diese Informationen nicht an Microsoft gesendet werden.

Mit dem neuen expliziten “Verlangen” der Outlook-App über sämtliche Mail-Daten der nicht bei Microsoft gehosteten IMAP-Konten zu verfügen, lässt sich neu nicht mehr überprüfen, welche Daten an Microsoft gesendet werden und welche nicht, darin eingeschlossen sind auch die Schlüssel. Eine Verschlüsselung der Mails ergibt folglich keinen Sinn, Microsoft kann mitlesen. Kann heisst nicht, dass es so passiert. Kann heisst aber, es ist möglich, und dies sollte es nicht.

Abwürgen des IMAP-Protokolles

Das IMAP-Protokoll mit SSL/TSL-Verbindung (Port 993) bietet eine standardkonforme Mail-Kommunikation vom und zum Mail-Provider an. Vor etwa einem Jahr “würgte” Office365 den Zugriff für Dritte ab. Dies hatte zur Folge, dass die Mails nicht mehr mit dem Mail-Modul der ArchivistaBox archiviert werden konnten. Als Folge davon entstand in diesem Frühjahr das Office-365-Modul. Damit kann unsere Kundschaft die Mails weiter archivieren.

Kleine Randbemerkung an dieser Stelle: *An sich waren die meisten Mails bereits in der ArchivistaBox archiviert. Das Mail-Modul der ArchivistaBox löschte die Mails jeweils nach dem Verarbeiten im entsprechenden IMAP-Konto. Bei der Einführung des Office365-Moduls musste die Überraschung gemacht werden, dass diese Mails offensichtlich nur in der IMAP-Ansicht gelöscht (markiert) waren. Office365 spukte über Jahre zurück die Mails nochmals neu aus. Soviel zur Vertraulichkeit, dass Mails bei Microsoft gelöscht werden.*

Nun gibt es neben dem IMAP-Transportprotokoll Regeln zum Mailaufbau, d.h. es wird festgelegt, wie Mails inhaltlich aussehen. Damit ist sichergestellt, dass die Mail beim Empfänger auch lesbar ist. Eine verschickte Mail sollte nach Ankunft beim Empfänger (Mail-Provider) nicht mehr angetastet werden, der Job (Versenden einer Mail von X zu Y) ist ja abgeschlossen. Nur liefert Office365 Mail-Nachrichten nach eigenen Kriterien aus, d.h. eine einmal abgerufene Mail wird bei einem späteren Aufruf nicht gleich ausgeliefert. Zwar sind die Unterschiede nicht massiv, jedoch führen unterschiedliche IMAP-Inhalte der gleichen Mail dazu, dass niemand mehr die Eindeutigkeit einer Mail feststellen kann.

Tech-Konerne sind nicht an Standards interessiert

Warum macht Microsoft dies? Wie eingangs angeführt, die grossen Tech-Player sind nicht daran interessiert, dass Standard-Protokolle zur Anwendung kommen. Denn ist dies der Fall, liessen sich die Programme beliebig ersetzen. Werden dagegen mehr oder minder “geschlossene” Protokolle verwendet, lässt sich die Kundschaft deutlich einfacher an ein Produkt “binden”, da ein recht grosser Migrationsdruck zu überwinden ist, ehe ein Wechsel stattfinden kann.

Auch hier ein kurzer Verweis auf die Umstellung der Mail-Archivierung von IMAP zu Office365 bei Kundenprojekten. Mit dem IMAP-Protokoll konnten pro Sekunde Dutzende von Mails verarbeitet werden, mit dem neuen Office365-Protokoll spukt Office365 ca. 1 bis 2 Mails pro Sekunde aus. Überdies verweigert die Microsoft-Cloud nach ca. 25’000 Mails in Tagesfrist die Arbeit für einige Tage komplett. Daher gilt (und dies gilt nun nicht nur für Microsoft), sind die Daten erst einmal in der Cloud, wird es unter Umständen nur mit gröberem Aufwand gelingen (wenn überhaupt!), die Daten aus der Cloud heraus abzurufen.

Hoheit der Daten nur bei lokaler Speicherung

In diesem Kontext ist auch das neuerliche “Gebaren” der Outlook-App zu verstehen. Es geht nicht um Standards, sondern um Macht bzw. hier um die Daten der Kundschaft. Der Bogen kann aber gerne erweitert werden, es geht nicht darum, ob dass die Cloud sicherer oder einfacher ist, es geht um die Hoheit der Daten.

Betreffend Sicherheit sei hier gerne angeführt, dass die gesamte Microsoft-Cloud (sämtliche Dienste) diesen Sommer uneingeschränkt kompromittiert war, siehe dazu z.B. die **ARD-Tagesschau vom 8. September 2023.** Auch hier kann der Horizont erweitert werden, wie viele Meldungen gab es dieses Jahr, dass sensible Daten der schweizerischen Eidgenossenschaft (Bund) gehackt wurden? Stellvertretend für viele, die **BAZOnline mit einer aktuellen Meldung von heute.**

Abgesehen davon, dass sensible Daten nie und nimmer im Darknet landen sollten, stellt die Hoheit der Daten ein noch viel wichtigeres Element dar. Über die eigenen Daten verfügen zu können, ist für jedes Unternehmen wie Private von zentralster Bedeutung. In diesem Sinne, die Daten sollten immer lokal gespeichert werden.

Wenn nicht lokal, dann zumindest lokale Sicherung

Sollte das zentrale Pflegen der Programme und Daten als zu grosse Hürde erscheinen, so sollte zumindest darauf geachtet werden, die Daten immer auch lokal und in einem austauschfähigen Format zu speichern. Bei den Mails z.B. ist dies das IMAP-Format. Selbst bei unserer Office-Archivierung werden die Mails letztlich im IMAP-Format gesichert. Die entsprechenden Mails können so auch wieder aktiviert werden.

Unternehmen wie Private, die Daten nicht zumindest auch lokal speichern, laufen immer Gefahr, urplötzlich mit einem erheblichen Mass an Ärger eingedeckt zu werden. Schon mal darüber nachgedacht, was passiert, wenn ein Microsoft-Account dichtgemacht wird? Auch hier ein Verweis auf einen Artikel bei **PCSpezialist.de,** der darüber berichtet, warum dies passieren kann bzw. welche Folgen zu erwarten sind.

Letztlich geht es bei der neuen Outlook-App für Windows wohl darum, dass Microsoft sämtliche Mails in der Cloud mit “künstlicher Intelligenz” (KI) auswerten will. Der Nutzen dieser Technologien ist im besten Fall bescheiden, eher werden die Kollateralschäden erheblich sein. Aus all diesen Gründen kann die Outlook-App mit Cloud-Zwang für IMAP-Konten nicht empfohlen werden. Selbstverständlich erhalten aber Kunden, welche die Office-Cloud von Microsoft einsetzen, für das Office365-Modul Support, um die Mails sicher lokal speichern zu können.