Weshalb der Einsatz von Microsoft Cloud Produkten rechtswidrig ist

Michael Georg Schmidt

ITS Explained
IT Sicherheit **einfach** erklärt

E info@its-explained.com
Threema-ID: WYH86UFA
Mastodon `@its_explained@mastodon.social`

9. September 2023

Inhaltsverzeichnis

1 Wie M365 und die Microsoft Cloud funktionieren

M365 und die gesamte Microsoft Cloud arbeiten auf Servern von Microsoft oder Servern unter deren Kontrolle. Damit haben amerikanische Behörden und Nachrichtendienste das Recht, von Microsoft die Herausgabe ***sämtlicher Kundendaten*** zu verlangen - auch der bei Microsoft gespeicherten Schlüssel. Das gilt für ***alle Server weltweit***.
Rechtsgrundlage sind folgende Gesetze:

- CLOUD ACT
- FISA Sec. 702, §1881 a
- USA Freedom Act

Damit sind die Kundendaten bei Microsoft nicht sicher, denn solche Anfragen kommen häufiger vor. Nicht dokumentiert sind die ***National Security Letters***, die geheim bleiben müssen (1,2).

2 Microsofts Verständnis von IT Sicherheit und Datenschutz

Microsoft bietet zwar die Möglichkeit seine Daten zu verschlüsseln, aber der Schlüssel muss in der Microsoft Cloud liegen. Bei einer teureren Lizenz gibt es die Möglichkeit des ***HYOK - Hold Your Own Key***, aber dies muss auf Hard- oder Software von Microsoft geschehen, womit Microsoft schon wieder Zugriff auf die Schlüssel hat.
Allerdings ist dies ohnehin nicht mehr relevant, da mit dem Hackerangriff, durch vermutlich chinesische Akteure, offenkundig geworden ist, dass Microsoft für alle Konten seiner Kunden einen „Nachschlüssel“ hat.
Das Microsoft IT Sicherheit und Datenschutz ohnehin nicht besonders ernst nimmt, beweist die Tatsache, dass Microsoft schon drei Monate vor dem Angriff von den Lücken wusste und nichts dagegen unternommen hat.
Der Vorfall ist so schwerwiegend, dass die amerikanische CISA (Cybersecurity & Infrastructure Security Agency) eine Untersuchung durch das Cyber Safety Review Board (CSRB) startete, die Präsident Biden per Dekret angeordnet hat.
Eine Stellungnahme von Microsoft stellt den Angriff als eine lange Reihe von ***Zufällen*** dar. Diese Darstellung erscheitn ausgesprochen unglaubwürdig.

3 Die Rechtslage

Die Rechtslage ist differenziert und nicht alles im Zusammenhang mit der Microsoft Cloud ist rechtswidrig, aber Entscheidendes ist es.

3.1 Übertragung Personen bezogener Daten in die USA

Personen bezogene Daten dürfen gem. Art. 45 Abs. 1 DSGVO in ein Drittland außerhalb Europas übermittelt werden, wenn die Europäische Kommission für dieses Drittland einen Angemessenheitsbeschluss gefasst hat. Das ist aktuell für die USA der Fall.
Diesen Beschluss sehen Datenschützer jedoch kritisch

- der ***Thüringer Landesbeauftragte für Datenschutz und Informationsfreiheit*** - Pressemitteilung vom 14.07.2023
- der Landesbeauftragter für den Datenschutz in Niedersachsen - Datenübermittlung in die USA: EU erläßt neuen Angemessenheitsbeschluss
- ***Datenschutz Hessen*** Angemessenheitsbeschluss zum EU-US Data Privacy Framework in Kraft getreten
- Heise Security - Krtik an „Wahnsinn“ : EU-Kommission gibt Datentransfer in die USA wieder frei

Es ist davon auszugehen, dass der ***Europäische Gerichtshof*** auch das EU-US Data Privacy Framework für rechtswidrig erklärt, da sich in den USA im Hinblick auf Datenschutz nichts zum Positiven gewendet hat. Es sind sogar schwerwiegende neue Verstöße gegen den Datenschutz bekannt geworden.

- Heise Security FBI beschlagnahmt unbeteiligten Mastodon Server - und behält ihn
- Heise Security Trotz Verbot: FBI hat über Vertragsfirma NSO-Spyware finanziert

Bis gegen das EU-US Data Privacy Framework beim Europäischen Gerichtshof Klage erhoben und diese entschieden wurde, können einige Jahre vergehen. Jedoch kann der Europäische Gerichtshof im Rahmen des Rechtsschutzes, die Aussetzung des Frameworks verfügen. Dann ist die Übermittlung Personen bezogener Daten in die USA - was beim Einsatz von Microsoft Cloud Produkten zwangsläufig geschieht - wieder rechtswidrig. Sobald eine Person hiergegen Beschwerde erhebt, ist die betreffende Institution verpflichtet, diese Daten rückstandslos aus den USA zurückzuholen und möglicherweise Schadenersatz zu leisten.

3.2 Konflikt mit Art. 24 DSGVO

Art. 24 Abs. 1 DSGVO, verlangt, dass der ***Verantwortliche*** „[...] geeignete technische und organisatorische Maßnahmen [...]“ umsetzt, die die Rechte natürlicher Personen schützen. Das heißt, dass der Nutzer der Microsoft Cloud dafür sorgen muss, dass die Daten bei Microsoft sicher sind. Das ist jedoch nicht möglich, da Microsoft ausgesprochen nachlässig mit der IT Sicherheit und dem Datenschutz umgeht.

3.3 Konflikt mit Art. 32 Abs. 1 Satz 1 1. HS DSGVO

Art. 32 Abs. 1 Satz 1 1. HS DSGVO verlangt „(1) Unter Berücksichtigung des Stands der Technik, [...] sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; [...]“
Das Risiko durch den Missbrauch Personen bezogener Daten ist unabsehbar groß. Die Eintrittswahrscheinlichkeit, dass die Daten missbraucht werden können ist durch den Angriff auf die Microsoft Clouddienste realisiert.
Somit ist es unerlässlich, das geeignete Schutzmaßnahmen, die ***dem Stand der Technik*** entsprechen getroffen werden. Dies wäre eine ***Ende-zu-Ende-Verschlüsselung (E2EE)***. Microsoft sieht diese jedoch in ***keinem Bereich*** vor. Damit liegt ein permanenter Verstoß gegen Art. 32 DSGVO vor.

3.4 Konflikt mit Art. 32 Abs. 1 Lit. b DSGVO

Art. 32 Abs. 1 Lit. b DSGVO schreibt vor, dass „die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;“ gegeben sein muss. Auch das ist auf Grund der bekannt gewordenen Tatsachen nicht möglich.

3.5 Fragwürdige Datenverarbeitungs-Praxis durch Microsoft

In seinen Datenschutzbestimmungen legt Microsoft folgendes fest:
„Wir kombinieren die erfassten Daten aus verschiedenen Kontexten (z. B. aus der Verwendung von zwei Microsoft-Produkten) oder von Drittanbietern, damit wir Ihnen eine nahtlose, konsistente und personalisierte Erfahrung bieten können, um fundierte Entscheidungen zu treffen oder diese zu anderen legitimen Zwecken zu verwenden.“

Es ist ausgesprochen fragwürdig, ob dieses Verständnis von Datenverarbeitung mit der Nutzung von M365 übereinstimmt. Eher ist davon auszugehen, dass hierfür ein Vertrag über eine ***gemeinsame Verantwortlichkeit*** gem. Art. 26 Abs. 1 DSGVO notwendig ist. Vielmehr ist zu befürchten, dass Microsoft unzulässiger Weise Nutzerprofile erstellt.

4 Alternativen zu M365

Als Alternativen zu M365 kommen folgende Angebote in Betracht

- Phoenix von Dataport
- grommunio
- LibreOffice | OpenOffice in Kombination mit Tresorit

5 Quellen

1. ACLU (American Civil Liberties Union) - https://www.aclu.org/documents/national-security-letters
2. CLOUD Act - https://www.justice.gov/criminal-oia/cloud-act-resources
3. CISA (Cybersecurity & Infrastructure Security Agency) - https://www.cisa.gov/
4. CSRB - Cyber Safety Review Board - https://www.cisa.gov/resources-tools/groups/cyber-safety-review-board-csrb
5. Dataport - https://www.dataport.de/
6. DSGVO Art. 24 - https://dejure.org/gesetze/DSGVO/24.html
7. DSGVO Art. 26 - https://dejure.org/gesetze/DSGVO/26.html
8. DSGVO Art. 32 - https://dejure.org/gesetze/DSGVO/32.html
9. EFF - National Security Letters - https://www.eff.org/de/issues/national-security-letters
10. EU-US Data privacy framework - https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf
11. FISA Sec. 702 §1881a - https://www.congress.gov/115/plaws/publ118/PLAW-115publ118.htm
12. Freedom Act - https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.htm
13. grommunio - https://grommunio.com/de/
14. Heise Security - Micorsoft Cloud: Weitere kritische Lücke - scharfe Kritik an Microsoft - https://www.heise.de/news/Microsoft-Cloud-Weitere-kritische-Luecke-scharfe-Kritik-an-Microsoft-9234573.html
15. Heise Security - Microsofts gestohlener Schlüssel mächtiger als vermutet - https://www.heise.de/news/Neue-Erkenntnisse-Microsofts-Cloud-Luecken-viel-groesser-als-angenommen-9224640.html

16. LibreOffice - https://de.libreoffice.org/

17. Micosoft Datenschutzbestimmungen (Stand August 2023)- https://privacy.microsoft.com/de-de/privacystatement

18. Microsoft Law Enforcement Requests Report - https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

19. Microsoft - Results of Major Technical Investigations for Storm-0558 Key Acquisition - https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/

20. OpenOffice - https://www.openoffice.org/de/

21. Phoenix von Dataport - https://www.phoenix-werkstatt.de/

22. Tresorit - https://tresorit.com/de