Prüfbericht

zur

Verschlüsselung von Microsoft Teams

August 2023

CONCEPTURE
GRUPPE | IHR ERFOLG. GESICHERT

1. Einleitung

In der digitalen Welt ist die Verschlüsselung zum Schutz von Informationen unerlässlich. Dieser Bericht konzentriert sich auf die Überprüfung der Verschlüsselung von Microsoft Teams - wie, wann und wo wird verschlüsselt und welche Art von Verbindungen werden aufgebaut?
Dabei hinterfragen wir, ob die tatsächliche Verschlüsselung den vom Hersteller beworbenen Standards entspricht.

Zur Durchführung der Untersuchung wurde ein Zugang zu Test-Accounts auf Microsoft Teams bereitgestellt. Unsere Untersuchung konzentrierte sich auf den Microsoft Teams Client in der Version 1.6.00.11166 und das Betriebssystem Windows in der Version 22H2 (Build 19045.2965).

Ziel war es, ein tieferes Verständnis darüber zu erlangen, wie und wann Verschlüsselung in dieser spezifischen Umgebung stattfindet. Die durch Microsoft oberflächlich bereitgestellten Informationen zur Verschlüsselung werden damit überprüft und ergänzt
(https://learn.microsoft.com/de-de/microsoftteams/teams-security-guide).

2. Verständnis der Verschlüsselung

Um die Anwendung der Verschlüsselung bei Microsoft Teams umfassend zu verstehen, ist es wichtig, die Grundlagen der Verschlüsselung und die damit verbundenen Anforderungen und Bedrohungen zu berücksichtigen. Verschiedene Angriffsszenarien erfordern unterschiedliche Verschlüsselungstechniken.

Zum einen gibt es die **Transportverschlüsselung**, die als erster Schutzmechanismus hauptsächlich dazu dient, Daten während ihrer Übertragung vor Dritten zu schützen. Bei der Kommunikation zwischen zwei Punkten, etwa zwischen einem Client und einem Server, werden die Daten so verschlüsselt, dass sie für Außenstehende unlesbar sind.
Dies ist besonders wichtig, wenn die Daten über unsichere Netzwerke, wie beispielsweise öffentliche WLANs, übertragen werden. Jeder, der versucht, die Daten während der Übertragung abzufangen, würde nur unverständlichen Code sehen.

Eine weitere Ebene der Sicherheit bietet die **Ende-zu-Ende-Verschlüsselung**. Hierbei werden die Daten so verschlüsselt, dass sie nur von den beabsichtigten Empfängern entschlüsselt und gelesen werden können. Selbst wenn die Daten während ihrer Übertragung abgefangen werden, können sie ohne den entsprechenden Schlüssel nicht entschlüsselt werden. Diese Form der Verschlüsselung ist besonders wichtig zum Schutz vor Angriffen, die darauf abzielen, Zugang zu vertraulichen Daten zu erlangen, indem sie in die Kommunikation zwischen den Beteiligten eindringen. Sie gewährleistet auch, dass selbst der Anbieter des Kommunikationsdienstes - in unserem Fall Microsoft - keinen Zugang zu den Inhalten der Kommunikation hat.
In der Praxis läuft das häufig so ab, dass Nachrichten schon vor dem Transport (der nochmal separat verschlüsselt ist), mit einem privaten Schlüssel verschlüsselt werden.

In unserem Kontext bedeutet dies, dass sowohl die Transportverschlüsselung als auch die Ende-zu-Ende-Verschlüsselung wichtig sind, um Microsoft Teams vor verschiedenen Arten von Angriffen zu schützen. Die richtige Implementierung und Anwendung dieser Verschlüsselungsmethoden ist daher entscheidend für die Sicherheit und Vertraulichkeit der Daten.

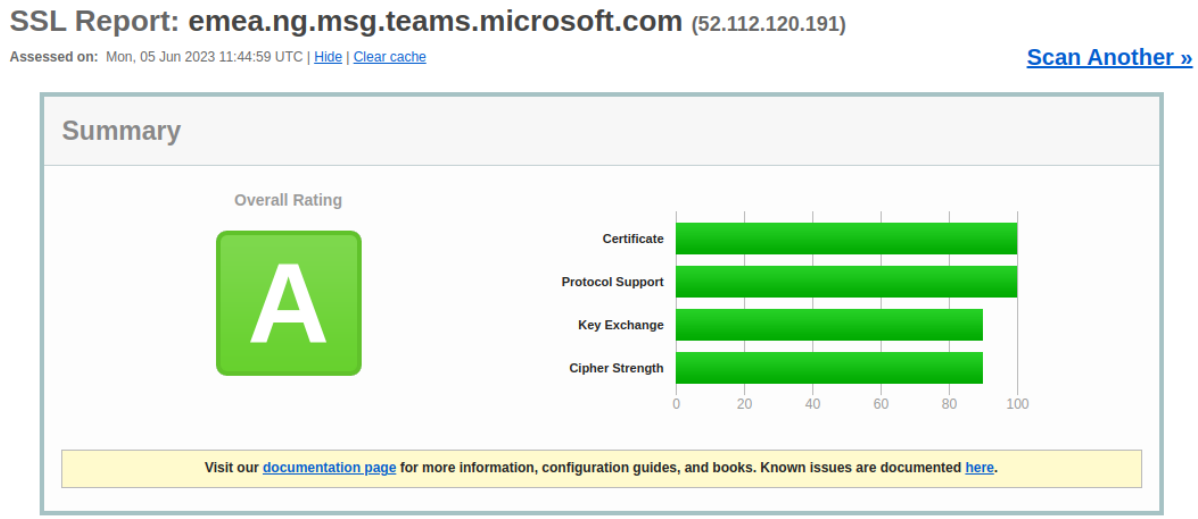
2.1 Transport Verschlüsselung

Die Analyse ergab, dass die Verschlüsselung von Microsoft Teams über das Transport Layer Security (TLS) Protokoll sichergestellt wird.
TLS ist ein kryptographisches Protokoll, das entwickelt wurde, um Kommunikationen über ein Computernetzwerk abzusichern. Es ist das am weitesten verbreitete Sicherheitsprotokoll und bildet die Grundlage für sichere (HTTPS) Verbindungen im Internet.

Für Nachrichten von Microsoft Teams wird beispielsweise der Endpoint: *https://de.ng.msg.teams.microsoft.com/v1/users/...* genutzt. Dieser Endpoint wird über HTTPS und somit über TLS gesichert.

Weitere Tests haben ergeben, dass alle getesteten Endpoints TLS die Version 1.2 verwenden.
Obwohl dies nicht die neueste Version ist (Aktuell ist TLS 1.3), bleibt TLS 1.2 ein robustes und weitgehend sicheres Protokoll.
So waren während der Tests keine bekannten Angriffe, wie beispielsweise Downgrade-Angriffe möglich. Bei einem Downgrade-Angriff versucht ein Angreifer, eine Verbindung auf eine ältere, weniger sichere Version eines Protokolls herabzustufen, um bekannte Schwachstellen auszunutzen. (Z.B. Downgrade von TLS 1.2 auf TLS 1.0)

Schließlich wurde noch die Sicherheit der Verbindung mit externen Diensten wie ssllabs.com überprüft, die eine detaillierte Analyse der Konfiguration von Webservern und der verwendeten TLS-Version bieten.
Die Ergebnisse waren durchweg positiv und zeigten ein gutes Rating, was auf eine korrekte und sichere Implementierung von TLS hinweist. Siehe Screenshot:



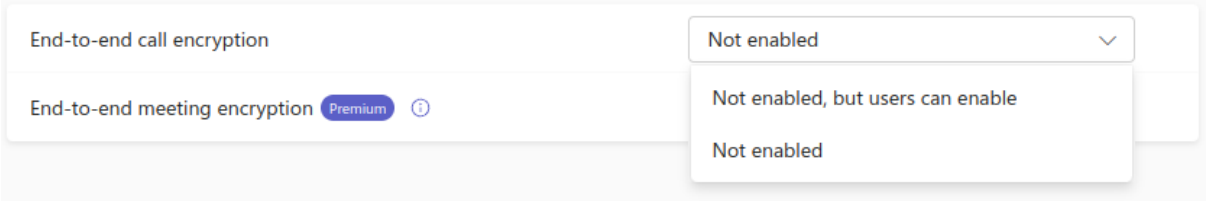
2.2 Ende zu Ende Verschlüsselung

Ende-zu-Ende-Verschlüsselung ist ein Kernelement in der sicheren Datenkommunikation. Es gewährleistet, dass Nachrichten ausschließlich von den beabsichtigten Empfängern gelesen werden können.
Für unsere Untersuchung wurde die Transportverschlüsselung (TLS 1.2) durch die Verwendung eines Root-Zertifikats temporär aufgebrochen, um den Inhalt und das Format der übermittelten Nachrichten genauer zu betrachten.

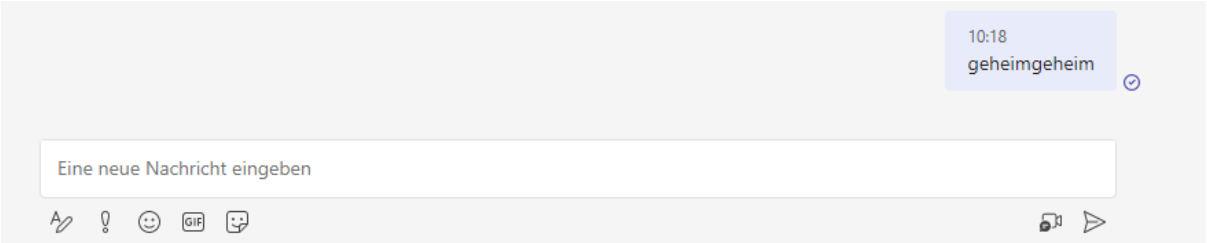
Die in Microsoft Teams versendeten Nachrichten zeigten das folgende json Format:

{
"content":" Test Nachricht ",
"messagetype":"RichText/Html",
"contenttype":"text",
"amsreferences":[ ],
"clientmessageid":"4160904686204616744",
"imdisplayname":"Lukas Sökefeld",
"properties":{... }
}

Überraschend war, dass die Texte nun unverschlüsselt sichtbar waren (Siehe Rote Hervorhebung). Das zeigt, dass eine Ende-zu-Ende-Verschlüsselung nicht vorliegt. Folglich kann Microsoft alle Nachrichten im Klartext lesen.
Um sicherzustellen, dass es kein Konfigurationsfehler ist, wurde in den Einstellungen geprüft, ob eine Ende-zu-Ende-Verschlüsselung aktiviert werden kann.
Das ist jedoch nur eingeschränkt in der Premium Version für Telefonate möglich, **nicht** für Nachrichten. Siehe Screenshot:

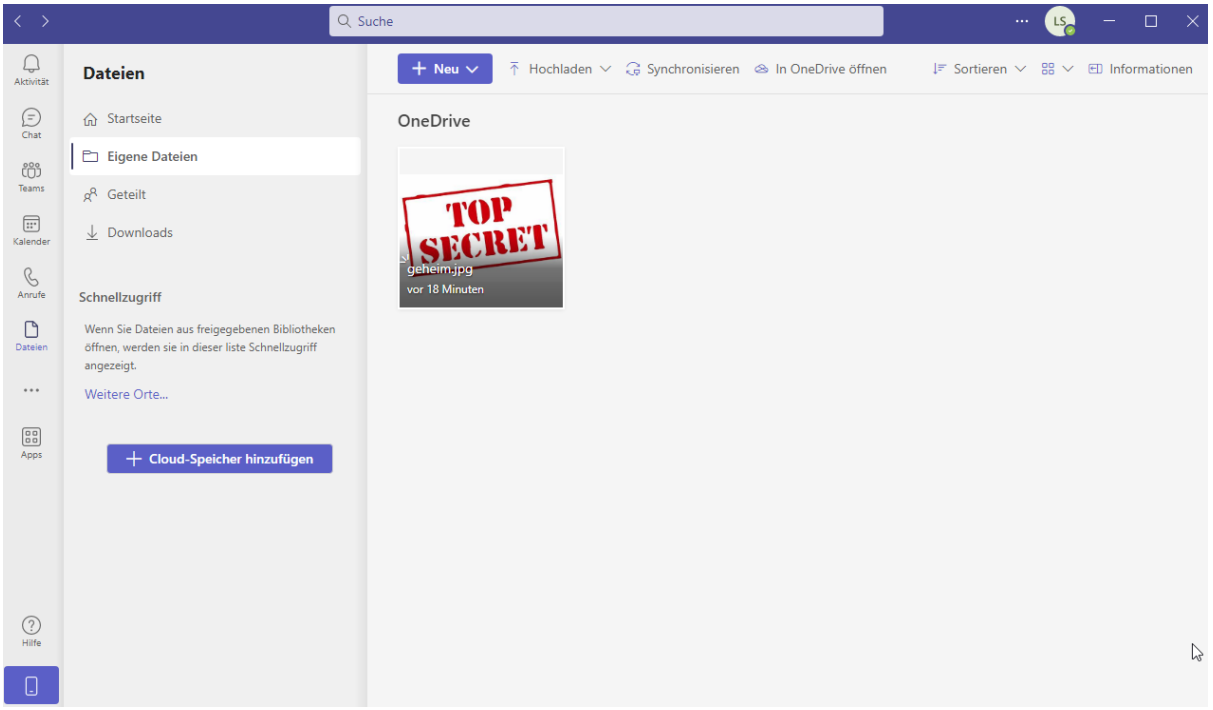


Zudem haben wir festgestellt, dass Nachrichten komplett unverschlüsselt auf dem Client gespeichert werden, was tatsächlich ein Sicherheitsrisiko darstellt. So können über den richtigen Windows-Dateipfad Nachrichten eingesehen werden, ohne dass ein Microsoft Teams Login notwendig ist.



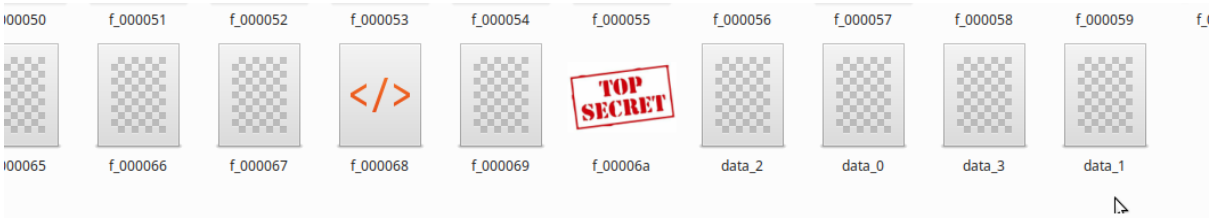
Letzte Nachricht im MicrosoftTeams Client, Windows

Im Cache unverschlüsselt hinterlegte Nachricht, Pfad: %AppData%\Microsoft\Teams\Cache\Cache_Data\IndexedDB\https_teams.microsoft.com_0.indexeddb.leveldb



Auch Dateien, die über Microsoft Teams gesendet wurden (mit OneDrive), werden unverschlüsselt auf dem Client abgelegt.

Datei in OneDrive im Windows Microsoft Teams Client



Die gleiche Datei im Cache Ordner von Microsoft Teams:
%AppData%\Microsoft\Teams\Cache\Cache_Data

2.3 Ende zu Ende Verschlüsselung, erweiterte Optionen

Microsoft Teams bietet erweiterte Optionen zur Ende-zu-Ende-Verschlüsselung (E2EE) in seinen administrativen Einstellungen. Administratoren haben dabei die Möglichkeit, die Verschlüsselung teilweise zu aktivieren. Die verfügbaren Optionen umfassen:

- End-to-end call encryption
- End-to-end meeting encryption (nur für Premium-Nutzer)

Es ist wichtig zu beachten, dass beide Optionen entweder auf "not enabled" oder "not enabled but user controlled" gestellt werden können. Eine Standardoption, die die Verschlüsselung für alle aktiviert, gibt es aktuell nicht.

Wird die Ende-zu-Ende-Verschlüsselung aktiviert, so werden folgende Aktionen verschlüsselt

- Audioanrufe
- Videoanrufe
- Das Teilen von Bildschirmen

Nachrichten und gesendete Dateien werden hingegen niemals Ende-zu-Ende verschlüsselt!

Es ist außerdem von entscheidender Bedeutung, dass beide Kommunikationspartner die E2EE in ihren Einstellungen aktiviert haben. Andernfalls findet keine Ende-zu-Ende-Verschlüsselung statt. Bei korrekter Aktivierung der E2EE wird dies durch ein Schloss-Symbol im Anruf angezeigt.

Auf technischer Ebene laufen Anrufe über die WebRTC-Schnittstelle.
Während des Tests konnte bei aktivierter Verschlüsselung der Inhalt des Anrufs nicht mehr eingesehen werden, was die Wirksamkeit der Ende-zu-Ende-Verschlüsselung unterstreicht.

3. Unterschiedliche Clients

Die Untersuchung zielte darauf ab, festzustellen, ob sich die verschiedenen Clients von Microsoft Teams - insbesondere Windows, MacOS und Web - in ihrem Verhalten unterscheiden. Unterschiedliche Clients könnten verschiedene Ansätze zur Datenverarbeitung und -sicherheit verwenden, was beispielsweise Auswirkungen auf die genutzte Verschlüsselung hat.

Die Analyse ergab jedoch, dass die nativen Windows- und MacOS-Clients nicht vollständig nativ sind. Sie nutzen stattdessen Electron, ein weit verbreitetes Framework, um Anwendungen zu erstellen.

Electron ist ein Open-Source-Framework, entwickelt von GitHub. Es ermöglicht Entwicklern, Desktop-Anwendungen mit bereits vertrauten Web-Technologien (HTML, CSS und JavaScript) zu erstellen. Mit dieser einheitlichen Codebasis können Anwendungen plattformübergreifend auf Windows, MacOS und Linux mit nur geringen oder gar keinen Änderungen ausgeführt werden.

Das erklärt, warum auf den verschiedenen Plattformen - Windows, MacOS und Web - das gleiche Verhalten beobachtet wurde.
Die Verwendung von Electron sorgt für eine hohe Konsistenz zwischen den verschiedenen Clients. Während dies aus Sicht der Anwendungsentwicklung und Nutzererfahrung Vorteile hat, kann es auch zu Sicherheitsbedenken führen. Beispielsweise haben vorangegangene Sicherheitslücken im Microsoft Teams Client direkt alle Plattformen betroffen, da sie durch die einheitliche Code-Basis von Electron entdeckt wurden.

Zusammenfassend lässt sich sagen, dass trotz der Unterschiede in den Betriebssystemen die verschiedenen Microsoft Teams Clients in ihrer Funktionsweise und ihrem Verhalten bemerkenswert ähnlich sind, was auf die Verwendung des Electron-Frameworks zurückzuführen ist.

4. Verbindungsaufbau

Die Analyse des Verbindungsaufbaus von Microsoft Teams offenbarte, dass der Client verschiedene Verbindungen zu unterschiedlichen IP-Bereichen herstellt. Hier ist ein Auszug der Ziel-IP-Adressen, zu denen Verbindungen beim starten des Clients aufgebaut wurden:

- 20.67.143.122 MS Datacenter, Dublin Ireland
- 20.42.65.88 MS Datacenter, Washington USA
- 52.113.199.174 MS Datacenter, Amsterdam, Holland
- 52.112.120.191 MS Datacenter, Gavle, Sweden
- 20.189.173.12 MS Datacenter, San Francisco, USA

Interessanterweise ist zu erkennen, dass der Client nicht nur mit europäischen IP-Adressen Kontakt aufnimmt. Dies könnte bedeuten, dass Daten über verschiedene geografische Standorte hinweg übertragen und verarbeitet werden, was möglicherweise Auswirkungen auf Datenschutz und Datenhoheit hat, abhängig von den geltenden lokalen Gesetzen und Bestimmungen.

5. Fazit

Nach eingehender Analyse können wir festhalten, dass Microsoft Teams eine solide Transportverschlüsselung bietet. Die Datenübertragung erfolgt über TLS 1.2, was einen effektiven Schutz vor Dritten während der Übertragung sicherstellt. Die Angaben Microsofts entsprechen also der Realität.

Allerdings offenbarte die Untersuchung signifikante Sicherheitsprobleme auf den Client-Geräten selbst.
Es gibt keine Ende-zu-Ende-Verschlüsselung und auch keine Möglichkeit, diese über die Einstellungen zu aktivieren. Dies bedeutet, dass Nachrichten und Dateien auf dem Client gespeichert und durch den Hersteller Microsoft eingesehen werden können. Das stellt ein erhebliches Risiko für die Privatsphäre und Sicherheit der Nutzer dar.
Dieser Punkt ist in den Werbematerialien so nicht sichtbar und konnte durch diesen Bericht aufgezeigt werden.

Im Kontrast dazu nutzen andere Messaging-Diensten wie WhatsApp oder Signal bereits seit langem Ende-zu-Ende-Verschlüsselung, um ihre Nutzer zu schützen. Diese Praxis stellt sicher, dass nur die Kommunikationspartner - und nicht der Anbieter des Dienstes oder potenzielle Angreifer - Zugang zum Klartext der Nachrichten haben.

.