Pressemitteilung

Stellungnahme zu Ransomware-Infektionen im Zusammenhang mit TeamViewer

Göppingen, 23. März 2016. In den letzten Tagen sind einige Berichte über Ransomware-Infektionen aufgetaucht, die in Zusammenhang mit TeamViewer gebracht werden. Wir verurteilen kriminelle Machenschaften auf das Schärfste, können aber besonders zwei Aspekte unterstreichen:

(1) Keiner der bislang beschriebenen Fälle basiert auf einer Sicherheitslücke von TeamViewer
(2) Mit einigen wenigen Schritten kann man Missbrauch vorbeugen

Ad (1.): Wir haben die Fälle, die uns zur Kenntnis gebracht wurden detailliert betrachtet. Die entstandenen Sicherheitsproblematiken gehen danach nicht auf TeamViewer zurück. Wir haben bislang keinen Hinweis darauf, dass sich Angreifer in diesem Szenario eine Sicherheitslücke von TeamViewer zu Nutze machen. Durch die Ende-zu-Ende Verschlüsselung von TeamViewer ist zum Beispiel auch eine Man-in-the-Middle-Attacke nahezu ausgeschlossen. Ferner haben wir keinen Grund zu der Annahme, dass eine Brute-Force-Attacke den berichteten Infektionen zugrunde liegt. Zur Abwehr von Brute-Force Angriffen erhöht TeamViewer exponentiell die Wartezeit zwischen Verbindungsversuchen. Für 24 Versuche werden so bereits 17 Stunden benötigt. Die Wartezeit für Verbindungsversuche wird erst nach der erfolgreichen Kennwort-Eingabe zurückgesetzt. TeamViewer bietet seinen Kunden nicht nur Schutz vor Angriffen eines bestimmten Computers, sondern auch vor sogenannten Botnetz-Angriffen, bei denen versucht wird, von mehreren Computern aus auf eine spezielle TeamViewer ID zuzugreifen.

Im Übrigen gilt es, festzuhalten, dass keiner der aktuell im Umlauf befindlichen Artikel auf ein strukturelles Defizit oder eine Sicherheitslücke von TeamViewer hinweist.

Bei den Fällen, die wir gegenwärtig überprüft haben, liegt leichtsinnige Nutzung zu Grunde. Dazu zählt insbesondere die Mehrfachverwendung der selben Kennwörter über mehrere Benutzerkonten bei verschiedenen Anbietern hinweg.

Bei vielen Anbietern erweist sich das als kein Problem, weil entsprechende Sicherheitsvorkehrungen dafür sorgen, dass Benutzerdaten gut geschützt werden - so zum Beispiel bei TeamViewer. Bei anderen Anbietern sind Kundendaten jedoch schlecht oder gar nicht geschützt. Solche Anbieter sind eine einfache Zielscheibe für Hacker und Datendiebe, die ihre Beute über einschlägige Portale zum Kauf anbieten oder einfach nur unentgeltlich veröffentlichen.

Da TeamViewer eine weit verbreitete Software ist, versuchen viele Online-Kriminelle, sich mit Daten von kompromittierten Konten, die sie über derlei Quellen bezogen haben, einzuloggen, um herauszufinden, ob

ein entsprechendes TeamViewer-Konto existiert. Ist dies der Fall, können sie sich leider oft Zugriff auf alle zugeordneten Geräte verschaffen, um dann Malware oder auch Ransomware dort zu installieren. Diesem Problem können Benutzer jedoch vorbeugen.

Ad (2.) TeamViewer distanziert sich aufs Schärfste von jedweden kriminellen Machenschaften und rät Benutzern dazu, sich durch entsprechende Gegenmaßnahmen zu schützen:

- Das beginnt beim Download: TeamViewer rät Benutzern dazu, nur auf die offiziellen TeamViewer-Kanäle zurückgreifen.

- Darüber hinaus sollten Benutzer unbedingt jedes Benutzerkonto - ganz gleich ob bei TeamViewer oder anderswo - durch einzigartige und sichere Kennwörter schützen.

- Des Weiteren empfiehlt TeamViewer seinen Benutzern, ihre Konten mittels zwei Faktor-Authentifizierung wirksam zu schützen. http://www.teamviewer.com/de/help/402-How-do-I-activate-deactivate-two-factor-authentication-for-my-TeamViewer-account.aspx

- Schließlich sollten Benutzer sicherstellen, dass ihre Geräte nicht etwa durch Mal-, Spyware oder sonstige Schadsoftware verunreinigt sind, mittels derer sich Hacker unautorisiert Zugriff auf geheime und sensible Daten verschaffen können.

Für technische Anfragen steht Benutzern der TeamViewer Support jederzeit unter support@teamviewer.com zur Verfügung.

Benutzern, die Opfer krimineller Aktivitäten wurden, empfiehlt TeamViewer, sich mit der zuständigen Polizeibehörde in Verbindung zu setzen und ihren Fall zur Anzeige zu bringen. Dies ist besonders wichtig, weil TeamViewer aufgrund der strengen Datenschutzregularien, denen das Unternehmen unterliegt, sensible Daten nur an autorisierte Personen oder Behörden herausgeben darf.

Über TeamViewer
Die deutsche TeamViewer GmbH mit Sitz in Göppingen wurde 2005 gegründet. Das Unternehmen beschäftigt sich mit der Entwicklung und dem Vertrieb von Systemen für den Online-Support, die webbasierte Zusammenarbeit und das Remote-Monitoring von IT-Komponenten. Die Fernwartungssoftware TeamViewer ist in über 30 Sprachen verfügbar und hat weltweit über 200 Millionen Nutzer. airbackup, eine Online-Backup-Lösung, und ITbrain, eine Lösung für Remote-Monitoring, Anti-Malware und Inventarisierung, ergänzen das Produkt-Portfolio von TeamViewer.

Weitere Informationen sind erhältlich unter: www.teamviewer.com
Folgen Sie TeamViewer bei Twitter unter @TeamViewer und dem Unternehmensblog blog.teamviewer.com.