Symbolbild: Kryptographie-Kommentar zum Taurus-Skandal

28.03.2024 09:00 CET

Auch Verschlüsselung will gelernt sein – ein Kryptographie-Kommentar zum Taurus-Skandal

Ein Statement von Martin Oczko, Geschäftsführer der procilon GROUP

Vor knapp vier Wochen, am 1. März, machte der russische Fernsehsender RT ein am 19. Februar abgehörtes Konferenzgespräch von vier Offizieren der deutschen Bundeswehr öffentlich, in dem diese die Möglichkeit der Lieferung von Taurus-Marschflugkörpern an die Ukraine diskutiert hatten. Die nun einsetzende ‚Taurus-Abhöraffäre' fand rasch einen Niederschlag – in nationalen und internationalen Medien, in den deutsch-russischen

diplomatischen Beziehungen und schließlich sogar im deutschen Bundestag.

Wie genau die Gesprächsaufzeichnung zustande kam, das ermittelt derzeit die Abwehrabteilung des MAD. Fest steht bislang nur eines: Informationen – und damit Daten – konnten abgeschöpft werden.

Die Arbeitsbesprechung war als Telefonkonferenz über die Anwendung Cisco WebEx erfolgt. Cisco WebEx ermöglicht eine sichere Kommunikation über verschlüsselte Kanäle und ist vom BSI nach dem Cloud Computing Compliance Controls Catalogue (BSI C5) zertifiziert.

Rasch brachten Medien eine ganze Reihe möglicher Abhörszenarien ins Spiel, wie einen Spion oder eine Wanze im Zimmer eines der Konferenzteilnehmer oder einen Trojaner auf einem der angeschlossenen Smartphones. Am 5. März äußerte sich dann Verteidigungsminister Boris Pistorius und erklärte, dass das ‚Datenleck' wahrscheinlich durch einen Anwendungsfehler eines der Konferenzteilnehmer zustande gekommen sei.

Diese Möglichkeit ist durchaus gegeben. Nicht alle Einwahlarten in eine WebEx-Konferenz sind gleich gut abgesichert. So heißt es in einem Artikel von heise online zur Taurus Abhöraffäre: Wählt sich ein Teilnehmer beispielsweise nicht direkt über die Anwendung selbst, sondern über ein Telefon in die WebEx-Konferenz ein, so erfolgt seine Verbindung ohne Ende-zu-Ende-Verschlüsselung. Bei der Einwahl über einen Browser lässt sich eine verschlüsselte Verbindung zwar herstellen, doch müssen die zuständigen IT-Teams dafür zuvor bei der Client- und Server-Software manuell für WebEx eine Ende-zu-Ende-Verschlüsselung eingerichtet und aktiviert haben. Sonst erfolgt die Verbindung auch hier nicht wie erhofft – unverschlüsselt.

Das Beispiel der Taurus-Abhöraffäre zeigt: damit Datensicherheitsmaßnahmen wie erhofft greifen können, müssen sie so implementiert sein, dass Fehlverhalten – auch Unbewusstes – so weit wie

möglich ausgeschlossen werden kann. Das gilt auch und gerade für die Verschlüsselung von Daten. Vielerorts mangelt es hier aber immer noch am erforderlichen Sicherheitsbewusstsein – bei den Herstellern, den IT-Administratoren, und den Endanwendern selbst.

Im Bereich der E-Mail-Kommunikation sind die meisten Behörden da mittlerweile glücklicherweise schon einen Schritt weiter. Automatisierte Verschlüsselungslösungen ver- und entschlüsseln ein- und ausgehende Emails, erzeugen und prüfen Siegel, ohne dass die einzelnen Endnutzer hier noch selbst Hand anlegen müssen. Das Prinzip ‚Security by Design' hat bei ihrer Entwicklung Pate gestanden. Das Risiko eines unbeabsichtigten Fehlverhaltens von Seiten der Nutzer kann so spürbar reduziert werden.

Dass die Verschlüsselung von Daten für staatliche Institutionen mittlerweile von existenzieller Bedeutung ist, haben die vergangenen Jahre klar gezeigt. Cyberangriffe auf staatliche Stellen häufen sich. Meist handelt es sich hierbei um Ransomware-Angriffe, um Erpressungsversuche also. Doch sind auch erzwungene Datenabflüsse mittlerweile keine Seltenheit mehr. Erinnert sei hier nur an den Angriff auf das Berliner Kammergericht von 2020 oder auf die Schweizer Kantonspolizei Bern von 2023. Leicht können die Daten, welche die Cyberkriminellen bei solchen Angriffen erbeuten, im Darkweb verkauft, für Phishing, Spear Phishing und Social Engineering-Angriffe genutzt, oder – wie im Fall der Taurus-Abhöraffäre – für eine antideutsche Medienkampagne eingesetzt werden.

Nur mit einem Mehr an Sicherheitsbewusstsein und Sicherheitslösungen, deren Entwicklung dem Prinzip Security by Design verpflichtet ist, wird sich Datensicherheit an deutschen Behörden in Zukunft noch erfolgreich aufrechterhalten lassen.

Seit Jahrzehnten gilt die procilon GROUP als verlässlicher Ansprechpartner, wenn es um den Auf- und Ausbau einer sicheren digitalen Kommunikation im deutschen Rechtsraum geht.

Sowohl Unternehmen als auch Behörden setzen zur sicheren Identifizierung,

Übertragung und Aufbewahrung ihrer Daten auf Lösungen der Anbietergruppe. Ihr SaaS- und On-Premises-Portfolio ermöglicht es ihnen, digitale Inhalte sicher, niederschwellig, vertraulich, nachvollziehbar und beweisbar zu signieren, auszutauschen und zu archivieren. Die Stärke der procilon GROUP-Produktpalette basiert dabei zum einen auf der strikten Einhaltung deutscher und europäischer Richtlinien und Vorgaben, zum anderen auf dem Einsatz kryptografischer Spitzentechnologien made in Germany, sowie – last but not least – auf seiner Cloud First-Strategie.

Ein wichtiges Mitglied der Anbietergruppe ist die intarsys GmbH. Sie entwickelt und vertreibt qualitativ hochwertige und technologisch führende Softwareprodukte und -komponenten zur Erzeugung und Prüfung von elektronischen Signaturen, Siegeln und Zeitstempeln sowie zur beweissicheren Langzeitarchivierung von digitalen Dokumenten.

Gemeinsam haben es sich die Mitglieder der Anbietergruppe zum Ziel gesetzt, die procilon GROUP zu einem der führenden deutschen Anbieter elektronischer Vertrauensdienstanwendungen auszubauen.

Sie möchten mehr über die procilon GROUP erfahren? Klicken Sie hier – oder abonnieren Sie den procilon Newsletter.

Kontaktpersonen

Henrike Ewald
Pressekontakt
Marketing Manager
presse@procilon.de
034298 4878 10