Comcrypto
Asynchrone Kommunikation durch neue Verschlüsselung zukunftssicher gemacht

PRISM hat uns Schwachstellen der Internetkommunikation und ihrer Verschlüsselung vor Augen geführt und dadurch aufgezeigt, dass bisher sicher geglaubte Prinzipien der Vertraulichkeit kompromittiert werden können. Der Codename PRISM bezeichnet eine von der US-amerikanischen National Security Agency (NSA) geführte Operation zur Überwachung der Internetkommunikation gemäß Abschnitt 702 des FISA-Änderungsgesetzes von 2008. Damals wie heute basieren die am weitesten verbreiteten Sicherheitsstandards auf über 20 Jahre alten Technologien, die - wenn nicht konsequent angewendet - von Akteuren wie der NSA relativ leicht zu entschlüsseln sind. Durch die Enthüllung von PRISM wurden Sicherheitslücken in asynchroner Kommunikation, Datensicherheit und Privatsphäre ins Rampenlicht gerückt. Diese Erfahrung inspirierte comcrypto – heute ein Unternehmen, das Pionierarbeit im Bereich zukunftsweisender Cybersecurity leistet - dazu, die Sicherheit von Kommunikation via Internet neu zu denken, um die Verschlüsselung unangreifbar zu machen, und um den Aufwand zum Betrieb von Security-Systemen um Größenordnungen zu reduzieren.

Comcrypto bietet heute eine Mischung aus innovativen, wohl definierten Sicherheitsprodukten für Endpunkte, Verbindungen, Backends, Rechenzentren und Kommunikation, die durchweg auf eigenen Implementierungen beruhen, die dieser Zielstellung folgen. Das Kernprodukt des Unternehmens, das Mail Exchange Gateway (MXG), wurde entwickelt, um asynchrone Ende-zu-Ende-Kommunikation im Zusammenspiel mit den bestehenden E-Mail-Servern von Unternehmen zu sichern.

„Unternehmen entwickeln auf der Basis von MXG leistungsfähige Netzwerke für geschützte E-Mail-Kommunikation: zwischen Unternehmen, zu ihren Mitarbeitern und zu ihren Kunden. Es gibt heute keinen Grund mehr, auch nur eine einzige E-Mail unverschlüsselt zu versenden. Mit MXG erfüllen wir schon heute Zukunftsszenarien für Sicherheitsstandards wie zum Beispiel Krypto-Agilität und dynamische Identitätsprüfung“, sagt Georg Nestmann, Geschäftsführer von comcrypto. Das Produkt MXG reduziert dabei durch seine Kapselung und Bereitstellung als Appliance die Installationskosten radikal und bietet seinen Anwendern ein Pay-per-Use-Modell ohne Fixkosten.

Die von comcrypto entwickelte Endpunktanwendung „Encurity“ arbeitet nicht nur nahtlos mit MXG zusammen, sondern erlaubt auch eine vertrauliche Kommunikation zwischen Personen in Peer-Netzwerken untereinander. „Wir freuen uns, unser Produkt „Encurity“ für den privaten Gebrauch kostenlos anbieten zu können und wollen damit unserer Gesellschaft, in der wir leben, auch etwas Wertvolles zurückgeben“, fügt Nestmann hinzu.

Während der Verschlüsselung kombinieren die Produkte von comcrypto mindestens zwei verschiedene Chiffrierungsverfahren, um den Datenschutz auch im Falle einer unwahrscheinlichen Offenlegung eines verwendeten Algorithmus zu gewährleisten. Comcrypto nutzt dazu modulare Bibliotheken, die ein Stacking und schnelles Umschalten kryptografischer Abläufe ermöglichen.

Mit seinen Lösungen unterstützt comcrypto seine Kunden bei der Einhaltung der Vorschriften der DSGVO. Das Beispiel eines großen deutschen Clearinghauses belegt das Potenzial und die Wirksamkeit der Sicherheitslösungen von comcrypto: Aufgrund fehlender Alternativen musste der Kunde seine bis dato ungeschützte Kommunikation kurzfristig auf Faxversand umstellen, um die Anforderungen der DSGVO zu erfüllen. Dies machte die tägliche Kommunikation teuer und chaotisch und belastete die Mitarbeiter mit zusätzlichen Aufgaben. Durch die kurzfristige Einführung von comcrypto verschlüsselt das Clearinghaus heute ausnahmslos die gesamte ausgehende Kommunikation und erreicht Vertraulichkeit sogar mit Kunden und Geschäftspartnern, die bislang noch keine eigene Sicherheitslösung implementiert haben. Monatelange Einführungs- und Onboardingprojekte gehören mit comcrypto der Vergangenheit an.

Als Erweiterung seines Angebots arbeitet comcrypto derzeit an einer Lösung, die das parallele Lesen und Schreiben verschlüsselter Nachrichten auf mehreren Endgeräten ermöglicht. Langfristiges Ziel von comcrypto ist die Absicherung seiner Chiffrate gegen die Entschlüsselung durch Quantencomputer. Damit sind comcrypto-Kunden zukunftssicher in punkto Geheimhaltung und Datenschutz. „Seit der Gründung von comcrypto im Jahr 2015 haben wir die Vision, quantensichere Technologie zu implementieren. Die durch comcrypto gesicherte Kommunikation widersteht den heutigen Entschlüsselungsansätzen von vornherein, doch das ist erst der Anfang unserer Reise. Wir erwarten, dass Quanten-Computing in Entschlüsselungsszenarien bis spätestens 2023 eingesetzt werden wird und arbeiten daher konsequent daran, unser quantenresistentes kryptografisches Design entsprechend weiterzuentwickeln.“, so Georg Nestmann weiter.