KRYPTOGRAFIE

MULTI-TOOL DES DATENSCHUTZES

In den letzten Jahren sind die Anforderungen an den Datenschutz ständig gewachsen. Nicht nur sind zahlreiche Gesetze und Vorgaben aufgestellt und präzisiert worden, auch neuere Entwicklungen im Geschäftsleben legen verstärkten Wert auf den Schutz sensibler Daten. Unternehmen und Behörden müssen sich dieser Anforderungen bewusst werden und entsprechende Maßnahmen ergreifen. Grundsätzlich liegt es im Interesse eines Unternehmens, die Kontrolle über seine Daten zu behalten und diese entsprechend zu sichern.

Environmental, Social & Corporate Governance (ESG)

ESG ist ein relativ neuer Ansatz, um zu bewerten, in welchem Maße Unternehmen sich für Ziele einsetzen, die über die Gewinnmaximierung für ihre Aktionäre, Eigentümer oder Stakeholder hinausgehen. Innerhalb der ESG-relevanten Aspekte gewinnt in zunehmendem Maße auch der Umgang mit Daten an Bedeutung. Unternehmen werden auch daran gemessen, wie sorgfältig sie mit sensiblen Daten ihrer Angestellten, Kunden und Partner umgehen. Die bestgeeignete Technik, um diesen sorgfältigen Umgang zu gewährleisten, ist die Verschlüsselung, bevor die sensiblen Daten die geschützte Unternehmensumgebung verlassen.

KRYPTOGRAFIE IST DER SCHLÜSSEL ZU EINER REIHE VON THEMEN, DEREN BEDEUTUNG STÄNDIG WEITERWÄCHST.

Elmar Eperiesi-Beck, Gründer und CEO, eperi, https://eperi.com/de/

DSGVO, Schrems-II-Urteil und die Cloud

Die Datenschutzgrundverordnung (DSGVO) legt einen noch viel größeren Wert auf den sorgfältigen Umgang mit Daten und hält diesen juristisch verbindlich fest. Insbesondere das Schrems-II-Urteil hat geklärt, welche Folgen die DSGVO für die Nutzung von Cloud-Diensten hat:

- Die Nutzung nichteuropäischer Cloud-Dienste ist ohne weitere Maßnahmen nicht DSGVO-konform (auch wenn die Server in Europa stehen).
- Standardvertragsklauseln sind nicht mehr ausreichend, um DSGVO-Konformität zu gewährleisten.
- Die von Cloud-Anbietern angebotenen Sicherheitslösungen (wie Microsoft E5 Lizenz) sind nicht ausreichend, um DSGVO-Konformität zu erreichen.

Der Europäische Datenschutzausschuss (EDSA) hat beschlossen, dass Unternehmen weiterhin personenbezogene Daten an außereuropäische Cloud-Dienste übertragen dürfen, wenn sie geeignete technische Maßnahmen zum Schutz dieser Daten treffen. Explizit nennt der EDSA die Verschlüsselung oder Pseudonymisierung von Daten nach dem aktuellen Stand der Technik, bevor diese an die Cloud übertragen werden. Auch hier ist also Verschlüsselung das Mittel der Wahl.

Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)

Einen bisher wenig beachteten Grund für den Einsatz von Verschlüsselungstechnologien liefert das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG), das seit 2019 entsprechende EU-Richtlinien in deutsches Recht umsetzt. In die Definition fließt unter anderem die Bestimmung ein, dass nur dann ein Geschäftsgeheimnis vorliegt, wenn das Unternehmen angemessene Geheimhaltungsmaßnahmen getroffen hat. Was als angemessene Geheimhaltungsmaßnahme gilt, kann sich dabei von Fall zu Fall unterscheiden, nicht zuletzt in Abhängigkeit von der Wichtigkeit der fraglichen Geheimnisse. Auch in diesem Fall gilt allerdings, dass Unternehmen mit Verschlüsselung der Daten nach dem aktuellen Stand der Technik auf der sicheren Seite sind.

Die richtige Lösung

Eine selbst kontrollierte Verschlüsselung ist also die beste Möglichkeit für ein Unternehmen, sich beim Thema ESG zu profilieren, außereuropäische Cloud-Dienste DSGVO-konform zu nutzen sowie seine Geschäftsgeheimnisse On-Premises und in der Cloud zu schützen. Alle anderen Systeme sind fallibel. Verschlüsselte Daten sind zwar auch nicht vor Diebstahl geschützt, aber sie sind (kommerziell) unbrauchbar für Kriminelle. Einen stärkeren technischen Schutz kann es nicht geben.

Die technisch effizienteste und einfachste Umsetzung der Verschlüsselung besteht dabei in der Nutzung eines Kryptogra-

fie-Gateways, das die Daten verschlüsselt, bevor sie On-Premises gespeichert oder in die Cloud übertragen werden. Der Vorteil der Datenverschlüsselung innerhalb eines Gateways liegt per se in der Tatsache, dass das Unternehmen jederzeit die Kontrolle über die Verschlüsselungsmethode und die verwendeten Schlüssel behält und so die Einhaltung der DSGVO gewährleisten kann.

Indexierung

Mit dem richtigen Gateway lassen sich auch Nachteile vermeiden, die eine herkömmliche Datenverschlüsselung mit sich bringt. Verschlüsselte Daten sind an sich nicht entzifferbar, auch nicht für die Anwendung, in der diese erstellt wurden. Eine Suche in verschlüsselten Daten zum Beispiel stellt darum eine technische Herausforderung dar. Diese lässt sich durch die interne Indexierung der Datenfelder in der Anwendung bewältigen. Hierbei werden die Datenfelder bei der Verschlüsselung im Gateway indexiert und die entsprechenden Indizes in einer separaten, dedizierten Datenbank beim Unternehmen abgelegt. Sucht ein Anwender nach einer bestimmten verschlüsselten Information, findet das Gateway die Indizes in der Datenbank und sendet eine entsprechend modifizierte Suchanafrage an die Anwendung. Die Anwendung sendet die betroffenen Datensätze zurück an das Gateway, das diese entschlüsselt und dem Anwender zur Verfügung stellt. Bei diesem Prozess verlassen zu keinem Zeitpunkt Daten im Klartext das Unternehmen. Bei entsprechender technischer Umsetzung nimmt der Prozess nicht mehr als wenige Millisekunden in Anspruch.

Flexibilität

Je nach (Cloud-) Anwendung müssen die Verschlüsselung und Indexierung angepasst werden, weil dieselbe Art Daten, abhängig von der Anwendung, an verschiedenen Stellen im Datenstrom zu finden ist – eine Adresse in SAP beispielsweise an anderer Stelle als bei Salesforce. Diese Anpassung lässt sich am besten durch Templates bewerkstelligen. In dem Template kann ein Unternehmen dann auf einfache Weise definieren, welche Art von Daten es als sensibel erachtet und darum verschlüsseln will. Es wird sich dabei immer nur um einen verhältnismäßig kleinen Teil der Daten handeln. Das Motto lautet: So wenig wie möglich und so viel wie nötig verschlüsseln.

Das Template generiert eine Beschreibung, die festlegt, wo im Datenstrom der jeweiligen Anwendung das Kryptografie-Gateway die zu verschlüsselnden Daten finden kann. Für viele gängige Anwendungen sind vorgefertigte Templates vorhanden, und es ist kein Hexenwerk, ein neues Template auch für Eigenentwicklungen von Unternehmen oder Behörden zu erstellen.

Multi-Tool Datenverschlüsselung

Kryptografie ist der Schlüssel zu einer Vielzahl verschiedenster Themen, deren Bedeutung ständig weiterwächst. Auch Unternehmen, denen ihr Eigeninteresse nicht ausreicht, strikte Maßnahmen zum Schutz ihrer sensiblen Daten zu ergreifen, erhalten durch ESG, DSGVO und Schrems-II-Urteil sowie GeschGehG mehr als ausreichend Gründe für den Einsatz von Kryptografie. Wie jedes gute Multi-Tool kann ein Kryptografie-Gateway hohe Gebrauchsfreundlichkeit gewährleisten: die gewohnten Geschäftsabläufe bleiben erhalten, die Prozesse laufen effizient mit minimalen Latenzzeiten und Plugins sind nicht erforderlich.

Elmar Eperiesi-Beck