Datenschutz vs. Informationssicherheit?

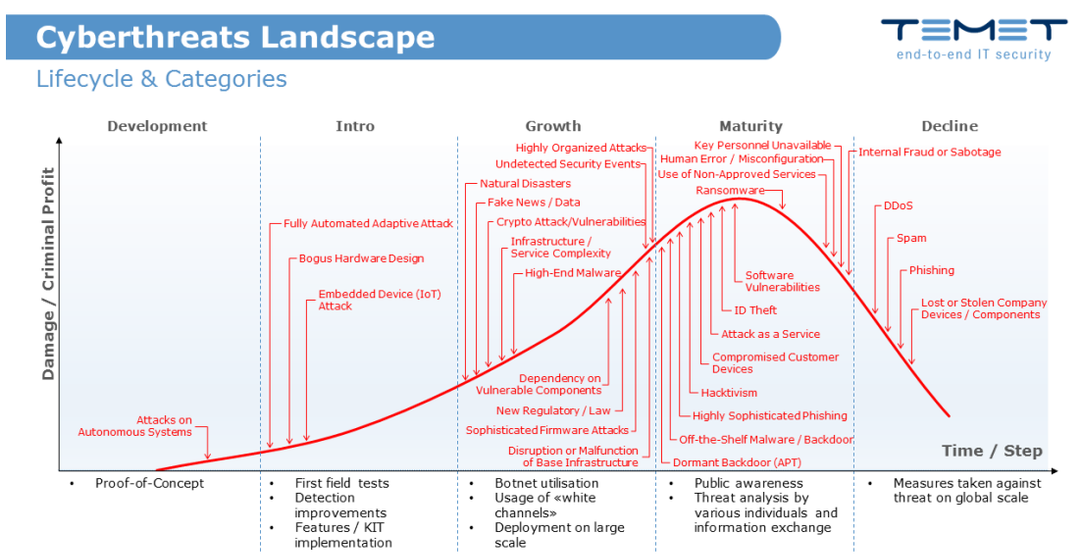
Der Themenkomplex Datenschutz spielt im Design und Betrieb der Informationssicherheit immer wieder eine Rolle – nicht immer zur Freude der Geschäftsverantwortlichen.

In der Beratung zur Informationssicherheit geht es üblicherweise um Themengebiete wie Cyber Security, Identitäts- und Zugriffsmanagement oder Managementsysteme zur Informationssicherheit. Diese Bereiche sind meist in IT- oder in Business-Einheiten der Kunden angesiedelt und sollen die Informationen der Unternehmen vor allen möglichen Verletzungen schützen.

Integrale Betrachtungsweise

Datenschutz als Disziplin des Zivilrechts bezweckt dagegen den Schutz der Personen, die mit den Informationen verbunden sind; er ist selten der Katalysator für Sicherheitsprojekte und wird bestenfalls als Rahmenbedingung berücksichtigt. Die Ziele der beiden Betrachtungsfelder sind also unterschiedlich, überlappen sich aber in weiten Teilen. Sie können deshalb kaum isoliert bearbeitet werden.

In der Regel müssen bei Mandatserfüllung bestehende interne und externe Rahmenbedingungen der Kunden berücksichtigt werden. Dazu gehören Sicherheitsstrategien und Richtlinien wie etwa anwendbare Standards oder Klassifizierungsvorgaben. Ausserdem gelten immer rechtliche Anforderungen an die Bearbeitung von Personendaten, meist auch für andere Daten des Unternehmens. Es ist deshalb bei allen Arbeiten in einer der beiden Domänen zwingend, die Fragestellung integral anzugehen und dazu die Anforderungen der anderen Domäne nicht ausser Acht zu lassen. Beispiele dazu finden sich zuhauf, insbesondere in stark regulierten Wirtschaftsbereichen wie der Finanzindustrie oder dem Gesundheitswesen.



Mögliche Bedrohungen der Informationssicherheit

Standards und Compliance

Oft bezwecken Projekte eine Standortbestimmung der eigenen Informationssicherheit bezüglich Branchenüblichkeit und Stand der Wissenschaft. Dazu können etablierte Standards gute Dienste leisten, etwa der Standard ISO/IEC 27001, das NIST Cybersecurity Framework oder branchenspezifische Referenzen wie HIPAA für das Gesundheitswesen oder PCI-DSS für Kreditkartentransaktionen. Alle diese Standards umfassen auch Anforderungen an die Umsetzung des Datenschutzes, der sich aus dem nationalen oder anderem anwendbaren Recht ergibt.

Umgekehrt umfasst auch das Datenschutzrecht praktisch immer generische Massnahmen der Informationssicherheit (technische und organisatorische Massnahmen); im Schweizerischen Recht finden sie sich in Artikel 7 DSG, in der europäischen DSGVO etwa gleichlautend im Artikel 32. Muss ein Gericht die Angemessenheit von Massnahmen zum Datenschutz prüfen, wird es zu deren Bestimmung mit hoher Wahrscheinlichkeit auf die erwähnten oder vergleichbare (Branchen)Standards abstützen. Dasselbe gilt erfahrungsgemäss für mehr oder weniger konkrete Anforderungen des relevanten Regulators.

Es gibt daher eine hohe Wechselwirkung zwischen faktischen und formellem Recht zu Informationssicherheit und Datenschutz; beide Quellen für Massnahmen der Datenbearbeitung können nicht isoliert betrachtet werden.

Kooperation statt Abgrenzung

Im Alltag des Informationssicherheits-Beraters ergibt sich diese Wechselwirkung selten von selbst. Informationssicherheit ist inzwischen verbreitet als Business Enabler anerkannt und wird meist seriös konzipiert wie betrieben – auch, weil sie weitestgehend nur internen Anforderungen genügen muss. Datenschutz wird dagegen nach wie vor als klassische (rechtliche / externe) Rahmenbedingung betrachtet, mithin als Bremse des Geschäfts.

Dennoch ist klar: trennbar sind die Disziplinen nicht; sie bedingen und erfüllen sich gegenseitig, das zugrundeliegende System kann auf der einen Seite selten ohne Auswirkungen auf der anderen Seite verändert werden. Die formelle Verknüpfung der beiden Gebiete ist inhaltlich richtig und nötig. Ein Projekt zur Einführung eines IAM Systems oder einer rechtkonformen Archivierung nach GeBüV oder anderer Aufbewahrungsvorschriften ist nicht denkbar ohne die vertiefte Prüfung der verbundenen Datenschutzanforderungen.

Dieser Ausgangslage sollten Projektaufträge Rechnung tragen. Das Projektsetup, die Zieldefinition und -messung sowie die Auswirkungen der Projektergebnisse müssen entsprechend umgesetzt werden, allenfalls sollten sie erweitert werden. Der Rechtsdienst des Unternehmens, idealerweise die Datenschutzbeauftragten, können dabei unterstützen.

IM INTERVIEW

Erik Küng
Senior IT Security Consultant
TEMET AG
T: +41 (0)44 302 24 42
E: info@temet.ch

www.temet.ch