Geostrategische Einflüsse in der IT

IT-Entscheidungen in Unternehmen haben auf den ersten Blick wenig mit Politik zu tun. Doch an vielen Stellen wirken sich Wirtschafts- und Sicherheitspolitik auch auf IT-Einkauf, -Betrieb und -Sicherheit aus. Dort ist dann eine offene und objektivierte Herangehensweise gefragt, mahnt unser Autor.

Von Florian Oelmaier, München

Wenn die Telekom ein 5G-Netz aufbaut, dann soll sie bitte den besten Netzwerkausrüster nehmen, egal wo er herkommt. Wenn die Europäische Zentralbank ihre Simulationsmodelle berechnet, dann soll sie das in der besten Cloud tun, egal in welchem Land die steht. Wenn ein Kraftwerkbetreiber Sicherheitssoftware kauft, dann ist es egal, wo sie programmiert wird – Hauptsache, sie ist zuverlässig. Und wenn DAX-Konzerne ihre Sicherheitsabteilung ins US-amerikanische Maryland verlegen (die Heimat der NSA), weil sie dort leichter Mitarbeiter finden, dann kann das doch nur gut für die Sicherheit sein, oder?

In Wirklichkeit lässt sich solchen Entscheidungen eine gewisse geopolitische Relevanz nicht absprechen. Wie aber soll man darauf reagieren? In einer Podiumsdiskussion meldete sich kürzlich ein Teilnehmer mit dem Beitrag zu Wort, dass er keiner Hardware vertraue, die aus China kommt – das schließt einen Großteil sämtlicher technischer Geräte aus. Und wie steht es mit der Software? Im „Clarifying Lawful Overseas Use of Data Act" (CLOUD Act) regeln die USA, dass ein US-amerikanisches Unternehmen auf Beschluss eines US-amerikanischen Richters sämtliche angeforderten Daten aushändigen muss, auch wenn diese im Ausland lagern – ganz ohne Amtshilfeersuchen bei ausländischen Behörden und ohne dass die betroffene Firma davon erfährt.

Muss man daraus nun folgern, keine Dienstleistungen US-amerikanischer Firmen mehr in Anspruch zu nehmen? Im Zeitalter von Office 365 und AWS erscheint das kaum noch realistisch. Und die heutige Wirklichkeit sieht auch ganz anders aus: Nach Recherchen von Corporate Trust befindet sich derzeit etwa ein Fünftel der gesamten von außen sichtbaren Rechnerkapazität der 30 größten deutschen Unternehmen in der Hand von Microsoft und Amazon (vgl. Abb. 1). Deutsche Firmen erwerben israelische Sicherheitstechnik, Google und Apple kaufen interessante Start-ups aus Deutschland und der Virenschutz stammt mitunter aus Russland. Viele, die darüber nachdenken, bekommen dabei ein mulmiges Gefühl im Bauch.

Vorgaben der Politik

Die USA haben die Diskussion auf politischer Ebene mit ihrem Boykott von Kaspersky und ZTE ins Rollen gebracht und mit der nachdrücklichen Forderung ausgeweitet, Huawei vom europäischen 5G-Netz auszuschließen. Doch auch Europa betreibt mit seiner Datenschutzgrundverordnung (DSGVO) eine gewisse extraterritoriale Einflussnahme: Denn der aktuelle Datenschutz gilt für alle Firmen, die Daten europäischer Bürger speichern, egal wo der Verarbeiter sitzt.

Russland und China haben ebenfalls Gesetze mit dem Ziel erlassen, dass bestimmte Daten im eigenen Land verarbeitet werden. Es ist davon auszugehen, dass in Zukunft noch mehr gesetzliche Regelungen Vorgaben für IT-Entscheidungen machen, besonders wenn es um Outsourcing und Cloudstrategien geht.

Der erste Schritt für jedes Unternehmen sollte daher eine Bestandsaufnahme der aktuellen und mittelfristig geplanten gesetzlichen Vorgaben und Regelungen in den Ländern sein, in denen man aktiv ist. Natürlich ist das Einhalten der diversen gesetzlichen und politischen Vorgaben die oberste Priorität – tatsächlich sind solche Überlegungen aber sehr wohl auch eine Frage der eigenen Firmenstrategie.

Geostrategische Risikoevaluation

Ein gutes Risikomanagement lässt sich nicht von Gefühlen leiten, sondern baut ein nachvollziehbares und für das Management parametrisierbares Bewertungsschema auf. Die wichtigste Grundlage ist es daher, sich von einer oft emotional geprägten Freund-Feind-Bewertung zu lösen: Weder sind die USA die Freunde deutscher Unternehmen noch stellen China oder Russland ihre Feinde dar. Auch für diese Art Risiken bietet es sich an, Eintrittswahrscheinlichkeit und Schadensszenarien beziehungsweise Schadenshöhe getrennt zu betrachten.

Zu den möglichen Schadensszenarien zählen folgende Aspekte:

_____ Sondersteuern und Zölle: Vor allem die in der EU diskutierten Sondersteuern auf IT-Dienstleistungen oder ihre zwangsläufigen Gegenreaktionen können sich künftig negativ auswirken.

_____ Ausfuhr- oder Zusammenarbeitsverbote: Hier gilt es auch auf indirekte Verbote zu achten – zum Beispiel sollte ein deutsches Unternehmen, das im Iran Geschäfte macht, derzeit besser kein Office 365 oder AWS nutzen.

_____ Verfügbarkeit der Infrastruktur: Sowohl in Russland als auch in China besitzt der Staat großflächig die Möglichkeit, Infrastrukturen zu kappen.

_____ Staatliche Eingriffsmöglichkeiten in die Vertraulichkeit von Daten: Nahezu alle Staaten sind auf verschiedene Arten in der Lage, im Land gelagerte Daten unbemerkt abzugreifen, oder haben Gesetze erlassen, um die Nutzung von Verschlüsselungsverfahren zu regeln (vgl. Abb. 2). Der CLOUD Act geht dabei sogar noch weiter und erlaubt der US-Justiz Zugriffe auch ins Ausland.

_____ Ungewollter Know-how-Transfer: Jede Beauftragung und jeder Aufbau von IT-Kapazitäten im Ausland bringen einen mehr oder weniger großen Know-how-Transfer in das Zielland mit sich.

_____ Informationsabfluss im Ausland: Egal ob ausländische Mitarbeiter abgeworben oder im Ausland Mitarbeiter eingeschleust werden – die Gefahr eines Informationsabflusses im Ausland besteht. Das gilt sowohl für ausländische Dienstleister als auch für eigene Niederlassungen. Meist ist die Gefahr umso höher, je weiter die Auslandsniederlassung organisatorisch von der Zentrale entfernt ist.

_____ Konkurrenzsituation / Aufkauf / zukünftige Konkurrenz: In einer Zeit, in der IT zunehmend wichtiger wird und ursprünglich auf IT fokussierte Unternehmen in immer mehr Branchen vordringen, besteht das Risiko, dass der Partner von heute ein Konkurrent von morgen ist.

_____ Manipulation: Die bewusste Manipulation von Daten und/oder Technik kann schwerwiegende Folgen nach sich ziehen und – wie am Beispiel der Sabotage des iranischen Atomprogramms gesehen – durchaus geopolitisch motiviert sein.

Hat man die für das eigene Haus relevanten Schadensszenarien definiert und priorisiert, ist der nächste Schritt die möglichst rationale Bewertung der Eintrittswahrscheinlichkeit jedes Szenarios. Dabei spielen bei der Bewertung potenzieller Partnerfirmen folgende Kriterien eine Rolle:

_____ eigene „Verdrahtung" im Partnerland
_____ Rechtsstaatlichkeit des Partnerlands
_____ politische Ziele des Partnerlands
_____ Korruption im Partnerland
_____ Historie staatlicher Eingriffe in die IT im Heimatland der Partnerfirma

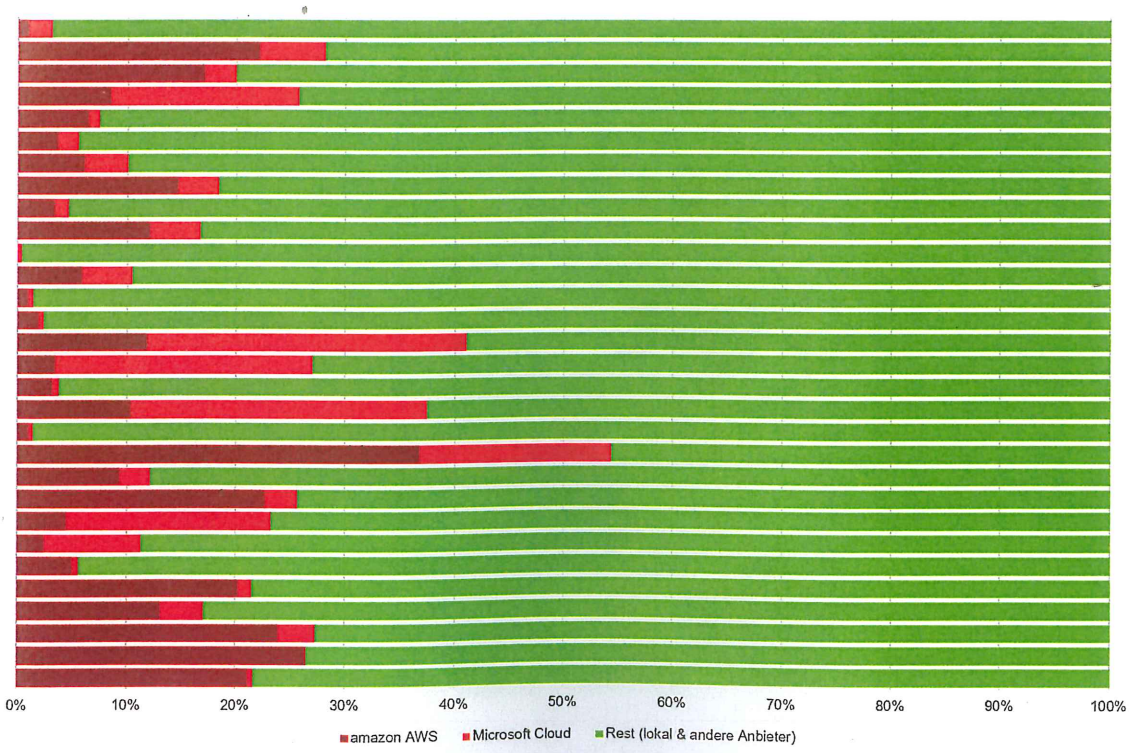

Abbildung 1: Nutzungsgrad von amazon AWS und Microsoft Cloudservices in den deutschen DAX-30-Unternehmen (gemessen an von außen sichtbaren, einem Unternehmen zuzuordnenden IP-Adressen)

_____ politische Exposition der Partnerfirma in ihrem Heimatland
_____ geopolitische Strategie der Partnerfirma
_____ Verquickung der Partnerfirma mit staatlichen Stellen und Aufträgen

Der wichtigste Punkt bei der geopolitischen Risikoevaluation in der IT sind aber die sogenannten Kumulrisiken: Da sich die genannten Risiken selten nur auf eine Geschäftsbeziehung auswirken, muss die Bewertung im Gesamtkontext aller Geschäftsbeziehungen erfolgen. Und während es für manche Firmen strategisch klug ist, sich fest an Unternehmen eines bestimmten Partnerlands zu binden (z. B., weil man außerhalb der IT ohnehin bereits große Abhängigkeiten geschaffen hat), bewährt sich normalerweise die Strategie, nicht alle Eier in ein Nest zu legen. In jedem Fall muss die Betrachtung der kumulativen Risiken regelmäßig und getrennt von den Einzelfallentscheidungen stattfinden!

Kaufentscheidungen

Selbstverständlich sind solche Fragen nicht für alle IT-Entscheidungen relevant. Neben den großen strategischen Überlegungen sollte der geostrategische Blickwinkel aber zumindest bei folgenden Themen in der IT eine Rolle spielen:

_____ Entscheidungen über Netzwerkdienstleister/Telekommunikationsanbieter: Dies gilt umso mehr, wenn diese auch eine Leitungsverschlüsselung versprechen oder WAN-Leitungen betreiben. Im zweiten Fall sind auch alle Transitländer und die Transitländer der Backup-Router in die Bewertung miteinzubeziehen.

_____ Entscheidungen über Cloud-Dienstleister und sämtliche „As-a-Service"-Angebote – hier müssen vor allem die Kumulrisiken betrachtet werden.

_____ Entscheidungen über Verlagerungen oder Outsourcing von IT-Administrationstätigkeiten oder anderen sensiblen Dienstleistungen

_____ Entscheidungen über den Kauf von Sicherheitshard- und -software

Auch bei allen anderen IT-Entscheidungen können geostrategische Überlegungen notwendig sein – im ersten Schritt ist dies aber eher nachrangig. Eine Sonderrolle nimmt die Anbindung von Niederlassungen im Ausland ein: Für solche Fälle ist das Risiko beider Kommunikationsrichtungen getrennt nach geostrategischen Erwägungen zu bewerten. Dabei muss man vor allem eine Replikation von Infrastrukturelementen (z. B. Active Directory) berücksichtigen.

Wie bei jeder Risikobetrachtung lassen sich auch geopolitische oder -strategische Risiken gegebenenfalls durch technische, organisatorische oder personelle Maßnahmen mindern. Das Restrisiko nach allen Minderungsmaßnahmen (Mitigation) sollte dann als einer der Einflussfaktoren in die Entscheidung mit eingehen. Um die aufgeführten Risiken transparent zu verwalten, muss es auch eine klare Verantwortlichkeit dafür geben.

Verantwortung beim CISO

Bereits heute haben viele CISO-Organisationen geostrategische Entscheidungen gefällt: nämlich in Bezug auf die Organisation der IT-Sicherheit an sich. Welcher Partner trägt welche Verantwortung mit welchen SLAs? Wie ist die Organisation der IT-Sicherheit zwischen Zentrale und Niederlassungen aufgeteilt? Gleichzeitig bringen sich zunehmend mehr CISO-Organisationen aktiv in das Vendor-Management ein, um die Auswahl von Dienstleistern und Zulieferern auch von IT-Sicherheitsüberlegungen abhängig zu machen.

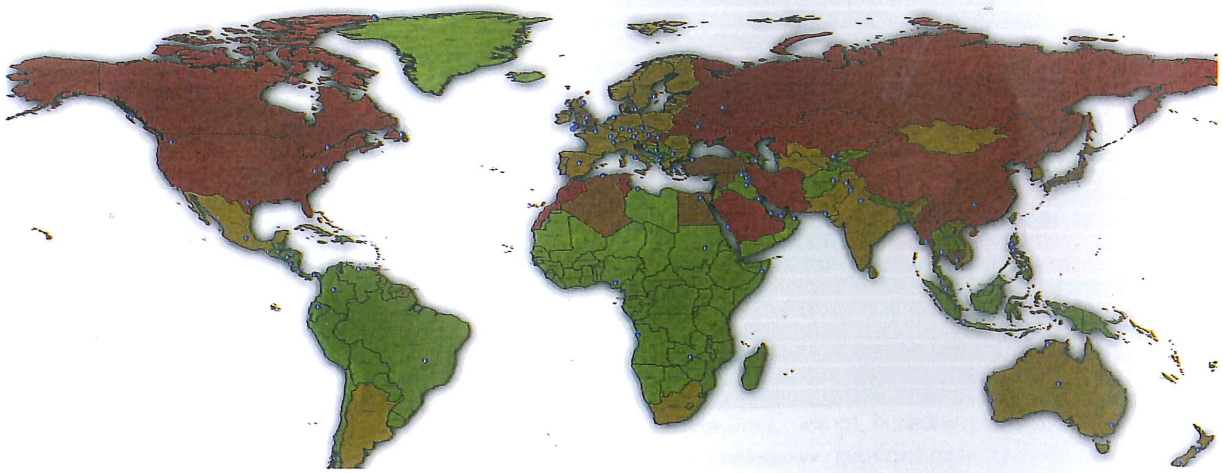

Abbildung 2: Strenge der Kryptogesetzgebung in den jeweiligen Ländern von rot (sehr viele staatliche Eingriffskompetenzen) bis grün (keine Gesetze) sowie NSA X-Keyscore Installationen (blaue Punkte)

Angesichts dieser Entwicklungen liegt es nahe, dass die CISO-Organisation auch das geostrategische Management von IT-Risiken übernimmt. Dabei sollte die Geopolitik nicht als von der Politik verordneter Hemmschuh, sondern als Chance begriffen werden: Mit einem aktiven Management von IT-Dienstleistern im geopolitischen Kontext lassen sich Sourcing-Alternativen schaffen und eine Monokultur vermeiden. Schließlich kann sich niemand wünschen, dass in einigen Jahren eine Situation entsteht, in der viele europäische Firmen weitgehend abhängig von nicht-europäischen Technologie-Unternehmen sind.

Zur Verdeutlichung stelle man sich nur einmal folgende Situation vor: Die EU hält weiterhin an dem Iran-Abkommen fest und ermuntert europäische Unternehmen, die wirtschaftlichen Beziehungen zum Iran aufrechtzuerhalten. Die US-Administration verbietet (analog zum ZTE-Fall) daraufhin den großen amerikanischen Technologie-Unternehmen von einem auf den anderen Tag die Zusammenarbeit mit europäischen Firmen, die aus Sicht der US-Administration gegen Iran-Sanktionen verstoßen haben. So etwas hätte schon heute massive Auswirkungen auf die IT dieser Unternehmen! In einigen Jahren führen dann gegebenenfalls auch selbstfahrende Autos europäischer Hersteller weltweit nicht mehr und autonome Produktionsanlagen deutscher Hersteller stünden still.

Der Drang der großen IT-Unternehmen zu immer weiterem Wachstum führt derzeit zu Quasimonopolen in unseren Firmen. Und während solche Monopole im Aufbau gute Preise versprechen, profitieren die Kunden doch auf Dauer nur selten davon. Hilfreich ist bei all diesen Überlegungen, dass wir in Deutschland und Europa gute IT-Firmen haben, die mit ihren Produkten qualitativ auf Augenhöhe mitspielen können – zumindest heute noch, denn diese Unternehmen benötigen natürlich hinreichend viele Aufträge, um sich am Markt zu halten. ■

Dipl.-Inf. Florian Oelmaier ist Prokurist und Leiter Cyber-Sicherheit & Computerkriminalität, IT-Krisenmanagement bei der Corporate Trust Business Risk & Crisis Management GmbH.