Die DS-GVO kommt. Über den Tellerrand geschaut.

DS-GVO: Cyber-Police & Entführungsversicherung

Meldepflicht bei Datenmanipulation und Lösegeld absichern können – Fluch oder Segen ?

von Marc Latza

Der 25.05. und somit die Geburtsstunde der DS-GVO nähern sich. Die DS-GVO bringt neben vielen anderen Punkte auch die Meldepflicht bei einer möglichen Datenmanipulation mit sich.

Aber was passiert, wenn Daten „entführt" werden, eine „Lösegeld-Versicherung" über eine Cyber-Police besteht und die Meldepflicht dies ans Tageslicht bringt ?

Im September 2017 überdachten die obersten Finanzaufseher (BaFin) eine seit Jahren bestehende Entscheidung und änderte diese.

Die Bündelung von Lösegeldversicherungen mit Cyber-Policen ist seitdem möglich.

Bis dahin waren lediglich „reine" Lösegeldversicherung legal abschließbar.

Je nach Produktgeber handelt es sich dabei um sog. „Kidnap & Ransom"-Policen (K&R) oder um „Kidnap, Ransom & Extortion"-Policen.

Die Begriffe sind schnell erklärt:
Kidnap = Entführung
Ransom = Lösegeld
Extortion = Erpressung

Diese Absicherungen sind in Deutschland erst seit 1998 erhältlich und zählen daher zu einem relativ jungen Versicherungszweig.

Diese Policen fristeten ein eher untergeordnetes Dasein, bis der IS mit seinen Enthauptungsvideos für einen ordentlichen Boom mit Lösegeldversicherungen gesorgt hat.

Es geht hier um ein Millionengeschäft und perfider Weise verdienen also nicht nur die Entführer in ihren Ländern an dem Kidnapping, sondern auch die Assekuranz in den Heimatländern der Entführungsopfer bzw. an den Stammsitzen der jeweiligen Arbeitgeber von den ins Ausland entsendeten Mitarbeitern. Hierzu zählen auch Hilfsorganisationen (sog. NGO´s: Non Government Organisation / Nicht Regierungsorganisationen).

In Deutschland zählen die Großen der Versicherungsbranche zu den Anbietern: AIG, Allianz, Chubb, Ergo, HDI Gerling, Hiscox sowie XL Catlin.

Die Deckungskonzepte sind mittlerweile echte Alleskönner. Neben der Bezahlung eines Lösegeldes und die Kostenübernahme für Krisenberatern (das alles gehört schon fast zum guten Ton), sind z.B. auch die Absicherung von Umsatzrückgang, Gehälter, Flugkosten, Rehamaßnahmen nach überstandener Entführung usw.

Vorteil von diesem mittlerweile doch recht breit aufgestellten Markt ist der „günstige" Einstiegspreis von gut einem vierstelligen Jahresbeitrag. So können auch kleinere Unternehmen ihre wichtigsten (Auslands)Mitarbeiter absichern.

In der Spitze können Konzepte mit allen „Drum und Dran" auch locker sechsstellige Jahresbeiträge erreichen.

Die Wahl der Versicherungssumme ist schwierig zu beurteilen. Da sind neben den o.g. Kostenpositionen auch noch unbekannte Rechengrößen wie z.B. die Dauer einer Entführung.

Je länger die Entführung, desto höher die Kosten für das Krisenteam, Unterbringungs- und Flugkosten usw.

Nun ist nicht nur auf der Seite der Täter eine neue Zeitrechnung angebrochen.

Entführt wird immer noch, aber unblutig. Keine aufwendigen Schnipseleien mehr, um wie früher einen Erpresserbrief zusammen zu schustern. Jetzt läuft das gleiche Spiel digital ab ! Daten werden unzugänglich gemacht und nur gegen Zahlung eines „Lösegeldes“ wieder frei gegeben.

Diese Situation kann nun seit Neuestem laut dem BaFin mittels einer Cyber-Police abgesichert werden.

Es gibt zwar ein paar kleinere Spielregeln, so darf eine Cyber-Police nicht als Lösegeldversicherung beworben werden, aber immerhin ist hier nun die entsprechende Absicherung möglich. Zudem muss bei Einschluss einer Lösegeldversicherung in eine Cyberpolice weiterhin sichergestellt sein, dass die Ermittlungsarbeit der Polizei nicht beeinträchtigt wird.

Aber ist die Absicherung von Lösegeldern nun vorteilhaft oder wird damit erst recht das Geschäft mit Entführungen angeheizt ?

Bei den Entführungen von Menschen kann man sich bereits bestehender Statistiken bedienen.

So hat z.B. das BKA für das Jahr 2009 ermittelt, dass von den weltweit entführten Personen (bei denen die Behörden eingeschaltet wurden) in 68 % der Fälle ein Lösegeld bezahlt wurde und die Opfer freigekommen sind.
Nur 16 % kamen ohne Lösegeld frei (Täter haben aufgegeben oder das Opfer konnte erfolgreich fliehen). 9 % wurden befreit und 7 % konnte nur noch Tod vorgefunden werden.

Aber bei Cyber-Angriffen ?

Die Problematik liegt u.a. darin, dass der Angriff aus jeder Ecke der Welt erfolgen kann. Räumliche Distanzen stellen keine Hürde mehr da. Morgens eben schnell einen Cyber-Angriff starten, Lösegeldforderung versenden und danach ganz normal zur Arbeit gehen.

Selbst die Zahlungsmittel sind digital geworden und somit andere als bei den Entführungen der althergebrachten Art, bei denen man die Geldscheine hat manipulieren können. Lösegelder zahlt man mittlerweile in Bitcoins.

Ferner ist die Schwere des Angriffes eine andere Liga. Ein Hacker kann eine ganze Behörde oder sogar einen ganzen Staat erpressen. Dies wäre in der nicht digitalen Welt nur mit einer Armee möglich gewesen.

Die Erpressung eines Bundesstaates kann auch kuriose Züge annehmen.

So wurde z.B. im März 2018 der US-Bundesstaat Atlanta gehackt und erpresst:

Geforderte Zahlung:	6 Bitcoins.
Druckmittel:	Weite Teile der staatlichen IT wurden durch einen Krypto-Trojaner lahmgelegt.
Folge:	Behörden (darunter auch die Polizei) mussten wieder zu Stift und Papier greifen.
Problem:	Ein Nachrichtensender filmte die Forderung ab und veröffentlichte somit die von den Erpressern erstellte Internetadresse, mittels derer die Zahlung der Bitcoins veranlasst werden konnte.
Kurios:	Zahlreiche Dritte kontaktierten dann mittels der Internetadresse die Erpresser, was dazu führte, dass die Erpresser aufgrund zahlreicher Spams die Internetseite gelöscht haben. Eine Zahlung des Lösegeldes war somit nicht mehr möglich.

Sicherlich muss man zwischen den zahlreichen Varianten einer Entführung unterscheiden. Eine Kindesentführung läuft anders ab als eine Flugzeugentführung oder der Freiheitsentzug eines hochrangigen Managers durch den IS.

Gleichwohl werden wir uns den digitalen Entführungen verstärkt stellen müssen und sicherlich wird es zu Lösegeldzahlungen kommen.

Inwieweit der / die Täter dann noch Gentlemen sind und sich an ihr Versprechen hinsichtlich der Freigabe der Daten halten, wird die Zeit zeigen.

Wirklich fatal kann vor diesen Hintergrund nun die neue DS-GVO sein.

Durch die Meldepflicht besteht das Risiko, dass mögliche Lösegeldzahlungen erfolgreich waren. Anders als bei den Entführungen von Personen, die zumeist der Öffentlichkeit nicht mitgeteilt werden, kann hier bei „digitalen“ Entführungen eine regelrechte Sondierung der potentiellen Ziele erfolgen. Wenn es sich herumspricht, dass die Firma XY scheinbar eine Lösegeld-Versicherung hat, ist es nur eine Frage der Zeit, wann der nächste Angriff erfolgt.

Aufgrund des drohenden Reputationsschadens kann sich aber ein Gewerbetreibender eine „Aufgabe“ der entführten Daten nicht leisten.

Andererseits kann man auch gegen Lösegeld-Zahlungen argumentieren, da Daten kopiert werden können. Es ist so gesehen also egal, ob Lösegeld gezahlt wird oder nicht, die Daten sind so oder so „weg“. Entweder kommt die Firma nicht mehr an die Daten dran oder die „zurückgekauften“ Daten sind aufgrund einer möglicher Weise erstellten Kopie „wertlos“ geworden, da sie keine Exklusivität mehr für den ursprünglichen Benutzer haben.