Swisscom verschwieg nach Datenklau den Kunden die Risiken

ZÜRICH. Es seien «nicht besonders schützenswerte Daten», betonte die Swisscom 2018 nach der grossen Panne. Nun zeigt sich, wie die Firma die Risiken gegenüber den Behörden beurteilte.

«Handel mit Kundenangaben im Darknet», «Vermehrte Werbeanrufe», «Enttarnung von VIPs»: Das sind drei von elf aufgelisteten Gefahren für Swisscom-Kunden. Sie stammen aus einer bisher unter Verschluss gehaltenen Risikoanalyse, die die Swisscom im Nachgang des 2018 bekannt gewordenen Datendiebstahls dem Eidgenössischen Datenschutzbeauftragten (EDÖB) liefern musste. Kriminelle hatten Ende 2017 die Zugriffsrechte einer Partnerfirma genutzt und Name, Adresse, Telefonnummer und Geburtsdatum von 800 000 Swisscom-Kunden geklaut.

Als die Swisscom die Panne 2018 kommunizierte, versuchte sie zu beruhigen. Beim gestohlenen Material handle es sich gemäss Datenschutzgesetz um «nicht besonders schützenswerte Daten». Es gehe um Daten, die man oftmals freiwillig in Telefonverzeichnissen, in sozialen Medien oder bei Wettbewerben angebe.

Ganz so harmlos klang es bei der Swisscom intern nicht. In der auf Geheiss des Datenschutzbeauftragten Adrian Lobsiger erstellten Risikofolge-Abschätzung führt der Telecomriese eine Reihe von Punkten auf. So heisst es unter dem Titel «vermehrte Werbeanrufe»: «Es besteht das Risiko, dass die vom unberechtigten Datenzugriff betroffenen Personen mehr Werbeanrufe erhalten.» Die Eintretenswahrscheinlichkeit bezeichnet die Swisscom als hoch, das Schadenspotenzial als mittel.

Hohe Wahrscheinlichkeit und hohes Schadenspotenzial machte die Swisscom beim «SMS Phishing» aus. «Es besteht das Risiko, dass Betroffenen personalisierte SMS zugesandt werden, um diese zu verleiten, eine schädigende Aktivität vorzunehmen.» Und unter «Enttarnung von VIPs oder gefährdeten Personen» hält die Swisscom fest, es bestehe das Risiko, dass Angaben von bekannten oder gefährdeten Persönlichkeiten veröffentlicht werden könnten. Eine Gefährdung an Leib und Leben könne nicht ausgeschlossen werden.

Lobsiger geht heute davon aus, dass die beschriebenen Risiken grösstenteils nicht eingetreten sind: «Die Swisscom und die 800 000 Kunden hatten Glück.» Wichtig sei, dass man den Schutz dieser Art von Daten künftig ernster nehme. **SANDRO SPAETH**

3.5 Vermehrte Werbeanrufe

Es besteht das Risiko, dass die vom unberechtigten Datenzugriff betroffenen Personen mehr Werbeanrufe erhalten als Personen, die nicht betroffen sind. Um eine vermehrte Werbeaktivität mit Bezug auf die betroffenen Personen frühzeitig zu erkennen und das Risiko für die betroffenen Personen zu reduzieren, führt Swisscom bis auf weiteres regelmässige Kundenbefragungen und Stichproben durch.

Eintretenswahrscheinlichkeit: hoch;

Schadenspotential: mittel.

3.1 Handel mit Kundenangaben im Darknet

Es besteht das Risiko, dass die Daten von den Swisscom-Systemen kopiert und gesamthaft oder teilweise auf einschlägig bekannten Plattformen im Internet und im Darknet um Verkauf angeboten werden. Swisscom überwacht bekannte Seiten, um ein entsprechendes Angebot zeitnah identifizieren und reagieren zu können.

Eintretenswahrscheinlichkeit: mittel;

Schadenspotential: hoch.

Oben sind zwei von elf Gefahren aus der Risikoanalyse zum Datendiebstahl aufgelistet. KEYSTONE

Das sagt die Swisscom zum Fall

Wieso hat die Swisscom die Kunden nicht besser über mögliche Risiken aufgeklärt?
Wir haben seinerzeit Medien und Kunden über den Vorfall informiert. Insbesondere auf das Risiko von ungewollten Werbeanrufen haben wir hingewiesen. So haben wir empfohlen, den Callfilter zu installieren, und haben zu Vorsicht bei ungewöhnlichen Kontaktaufnahmen aufgerufen. Glücklicherweise sind diese Risiken nach derzeitigem Kenntnisstand nicht eingetroffen.

Kann die Swisscom garantieren, dass keiner der 800 000 Betroffenen künftig mehr Werbeanrufe erhält oder Daten im Darknet landen?
Unsere Sicherheitsexperten sind auch im Darknet unterwegs. Bisher konnten wir nicht feststellen, dass diese Kundenangaben dort aufgetaucht sind. Aber natürlich können wir einen potenziellen Missbrauch nicht ausschliessen.

Könnte sich ein solcher Datendiebstahl heute noch ereignen?
Als Sofortmassnahme wurden die betroffenen Zugänge des Partners gesperrt. Zudem werden etwa die Zugriffe durch Partnerfirmen stärker überwacht und bei ungewöhnlichen Aktivitäten wird Alarm ausgelöst, grössere Abfragen wurden unterbunden. Weiter wurde eine 2-Faktoren-Authentisierung eingeführt. Ein ähnlicher Fall ist praktisch ausgeschlossen. **SAS**

Datenschützer sieht besonderes Interesse der Öffentlichkeit

ZÜRICH. 20 Minuten hat nach Bekanntwerden des Datendiebstahls beim EDÖB Adrian Lobsiger um Dokumenteneinsicht ersucht. Dieser stimmte dem Ansinnen grundsätzlich zu. Er argumentierte, es bestehe ein besonderes Informationsinteresse der Öffentlichkeit, da die Anzahl Betroffener hoch sei und die Medien breit über den Fall berichtet hätten. Die Swisscom versuchte die Veröffentlichung zu verhindern. Das Unternehmen verwies in seiner Beschwerde etwa auf Geschäftsgeheimnisse oder Reputationsrisiken. Das Bundesverwaltungsgericht teilte diese Ansicht nicht und gab die Dokumente – auch wenn in gewissen Teilen geschwärzt – frei. SAS