Association de Banques Privées Suisses

Vereinigung Schweizerischer Privatbanken
Association of Swiss Private Banks

Wie kann die Privatsphäre in der digitalen Welt geschützt werden?

Schlusswort von Yves Mirabaud
Präsident der Vereinigung Schweizerischer Privatbanken
Private Banking Day - Luzern
17. Mai 2019

Es gilt das gesprochene Wort.

Sehr geehrte Damen und Herren

Zuerst möchte ich herzlich danken – unseren Referenten für die Qualität ihrer Reden und den Diskussionsteilnehmern für ihren wertvollen Beitrag zu unserer Reflexion über eine leistungsstarke Cybersecurity. Es ist erfreulich, dass der Bundesrat im Januar grünes Licht für die Schaffung eines Cybersecurity-Kompetenzzentrums auf Bundesebene gegeben hat. Dieses Kompetenzzentrum muss schnellstmöglich operativ und departementsübergreifend tätig sein. Die Kompetenzen von MELANI müssen ausgebaut werden, damit die Meldestelle auch reagieren und Cyperattacken abwehren kann – so wie das israelische CERT, das uns präsentiert wurde.

Gemäss der Schätzung einer grossen Schweizer Versicherungsgesellschaft von vergangenem November gehören Cyberangriffe zu den fünf grössten Risiken für Unternehmen und könnten diese in den kommenden fünf Jahren rund 8000 Milliarden Dollar kosten. Anlässlich ihrer Jahresmedienkonferenz 2018 erklärte die FINMA sogar, dass Cyberangriffe inzwischen «*das grösste operationelle Risiko für das Finanzsystem*» sind. Der FINMA-Direktor plädierte dafür, den interdisziplinären Austausch *«innerhalb des öffentlichen Sektors und mit der Branche»* bezüglich Cyberrisiken noch deutlich auszubauen. Wir sind der Ansicht, dass die Schweizerische Nationalbank die Koordination der verschiedenen Akteure im Krisenfall übernehmen sollte.

Über die rund hundert täglichen Angriffe auf E-Banking-Lösungen in der Schweiz hinaus, die glücklicherweise meistens scheitern, gibt es ausgeklügeltere Attacken, die über Monate hinweg sorgfältig geplant werden. Immer noch in den Köpfen aller präsent dürfte der Angriff auf die Zentralbank von Bangladesh sein, die über ihre Zugangssoftware zum Netzwerk von SWIFT infiziert wurde: mit vier falschen Überweisungsaufträgen wurden 81 Millionen Dollar von Konten abgezogen, während Dutzende anderer Überweisungen dank eines Rechtschreibefehlers im Namen des Empfängers blockiert werden konnten.

Dieses Beispiel zeigt, wie wichtig Details sind, und dass das Bankpersonal auf alle Formen von Angriffen vorbereitet sein muss, die heute angesprochen wurden. Das bedeutet auch ein entsprechendes Ausbildungsangebot, und es ist zu begrüssen, dass die Eidgenössischen Technischen Hochschulen ihr Angebot in diesem Bereich ausbauen. Allerdings ist zu befürchten, dass es nicht genügend Schweizer Cyberspezialisten gibt. Daher müssen die

erforderlichen Massnahmen getroffen werden, damit in der Schweiz ausgebildete ausländische Spezialisten auch in unserem Land arbeiten können, und die Einwanderung von im Ausland ausgebildeten Spezialisten muss gefördert werden.

Auch der Schweizer Gesetzgeber ist in der Pflicht: Das Parlament prüft zurzeit einen Gesetzesentwurf über die elektronische Identität. Wenn es möglich ist, einen Internetnutzer mit einer zertifizierten Identität zu identifizieren, so wie die Vorlage einer Identitätskarte oder eines Reisepasses als Identitätsnachweis dient, kann zahlreichen Missbräuchen ein Riegel geschoben werden. Wer geht heute noch davon aus, dass es sicher ist, sich über ein Facebook- oder Google-Konto zu identifizieren, wenn bekanntlich regelmässig Millionen von Daten bei diesen Unternehmen abgegriffen werden?

Ein weiterer Zukunftsbereich ist die «Blockchain»-Technologie bzw. die Technik verteilter elektronischer Register. Wenn die Daten an verschiedenen Orten aufbewahrt und geprüft werden, wird es viel schwieriger sein, diese illegal zu verändern. Der Bundesrat hat eine Vernehmlassung eröffnet, um das Schweizer Recht nur punktuell an diese neue Technologie anzupassen. Wir begrüssen diesen Ansatz, der den Rechtsschutz im Wesentlichen gewährleistet, ohne die Innovationen auszubremsen.

Die Schweiz hat somit alle Karten in der Hand, um auch weiterhin einen soliden Schutz für die uns anvertrauten Vermögenswerte zu gewährleisten, und sich gleichzeitig an die neuen Technologien anzupassen. Wir vertrauen darauf, dass der Finanzplatz Schweiz auch in der digitalen Welt ein Hafen der Sicherheit bleiben kann, wenn wir uns der Risiken bewusst sind und zusammenarbeiten, um diesen zu begegnen. Dies war das Ziel dieses vierten Private Banking Day, und ich denke, dass wir dieses angesichts ihres zahlreichen Erscheinens erreicht haben.

Ich danke Ihnen für Ihre Aufmerksamkeit. Nun wartet ein Cocktailempfang oben auf der Terrasse auf uns. Sie sind alle herzlich dazu eingeladen.