Hintergrundpapier zur Verschlüsselungsdebatte

Berlin, 20. August 2019

Verschlüsselung ist ein zentraler Bestandteil der IT-Sicherheit. Moderne elektronische Kommunikationsdienste nutzen sie. Für Webseitenverbindungen ist sie mittlerweile weitgehend Standard (https). Wichtige Daten im Netz werden in Clouds verschlüsselt gespeichert. In einer Zeit, in der immer mehr Geräte und Dienste digital betrieben werden, und in der immer häufiger kritische Prozesse digital abgewickelt werden, und in der diese Geräte, Dienste und Prozesse durch das Internet miteinander verbunden werden, wird die Sicherheit dieser Dienste, Geräte und Prozesse zu einer wichtigen Frage. Mit zunehmender Bedeutung von IT-Sicherheit steigt die Bedeutung von Verschlüsselung. Bei Anwendern und Nutzern steigt zudem das Bewusstsein für sichere Dienste und der Wunsch, vertraulich miteinander kommunizieren zu können. Auch dies leistet der Verbreitung von verschlüsselter Kommunikation, insbesondere bei Messengerdiensten, Vorschub. Die Internetwirtschaft setzt aus diesem Grund auch in zunehmendem Maß in vielen Bereichen auf Verschlüsselung. Sie ist ein zentraler Baustein für das Vertrauen in digitale Dienste.

Dem gegenüber steht ein wachsendes Interesse von Regierungen und Ermittlungsbehörden, auf die Daten und Prozesse im Netz Zugriff zu haben, oder diese überwachen zu können. Durch Rechtsetzung und regulatorische Eingriffe in Netze, Dienste, Nutzermöglichkeiten und die Technologie selbst, versuchen sie, ihre Zugriffs- und Überwachungsmöglichkeiten aus unterschiedlichen Gründen zu fördern. Das ist problematisch. Denn auch wenn sich unter Umständen die Absichten für diese Anstrengungen unterscheiden mögen, so schaffen sie doch alle die gleichen, grundsätzlichen Probleme. Mit jeder Schwächung der IT-Sicherheit im Internet wird die angestrebte vermeintliche Erhöhung der öffentlichen Sicherheit zu einer Gefährdung der Gesellschaft durch Cyberkriminalität, Wirtschaftsspionage, Cyberwar.

In der Debatte über Verschlüsselung werden kontinuierlich die nachfolgenden Maßnahmen zur Einschränkung und Schwächung der Verschlüsselung diskutiert, mit denen das Vertrauen in die Sicherheit und die Integrität digitaler Dienste und Anwendungen geschwächt wird.

- **Vorgaben zum Niveau der Verschlüsselung:**

Immer wieder kommt die Forderung danach auf, dass Regierungen und Behörden im Stande sein müssten, „Verschlüsselung zu knacken“. Dies impliziert, dass starke Verschlüsselung nicht mehr vorkommen dürfte, so dass dies möglich ist. Die Vorgaben hätten einen regulatorischen Eingriff, der entsprechend anspruchsvolle Sicherheitslösungen untergraben könnte und das Sicherheitsniveau von Produkten, die auf dem Markt angeboten werden, nicht mehr gesteigert werden könnte.

Ein weiteres Problem ist, dass diese schwache Verschlüsselung nicht nur von den entsprechenden Regierungen und Behörden leichter geknackt werden kann, sondern auch von allen anderen Akteuren mit entsprechenden Kapazitäten. Zentrale Vorgaben zum Verschlüsselungsniveau sind dementsprechend schädlich für Verschlüsselung und für IT-Sicherheit. In diesem Kontext sollte auch klargestellt werden, dass zentral vorgegebene Sicherheitsniveaus, die Ausnahmen hierfür generell ausschließen und höchstens als Ausnahmetatbestand dulden, ähnliche Wirkung entfalten könnten und daher vermieden werden sollten.

- **Key Production**

Im Bereich der elektronischen Kommunikationsdienste hat sich Verschlüsselung etabliert. Fast alle verwenden unterschiedliche Formen von Verschlüsselung, die oft dynamisch ist, und als Ende-zu-Ende Verschlüsselung auch nicht ohne weiteres aufgelöst werden kann.

Vor diesem Hintergrund wird von verschiedenen Akteuren gefordert, dass Betreiber elektronischer Kommunikationsdienste im Stande sein müssen, die Nachrichten ihrer Nutzer zumindest auf Anforderung selbst entschlüsseln zu können und die Inhalte Ermittlungsbehörden zur Verfügung zu stellen. Ähnlich problematisch wäre es, wenn Teile des Schlüssels übermittelt werden müssten, so dass die Entschlüsselung der Nachrichten schneller oder einfacher erfolgen könnte. In diesem Fall könnte bei einer ausreichenden Anzahl an übermittelten Schlüsseln das mathematische Verfahren dahinter erkannt werden und die Verschlüsselung damit für alle Nachrichten aufgehoben werden. Zudem müsste in beiden Fällen ein Verschlüsselungsverfahren gewählt werden, das es dem Betreiber des Dienstes ermöglicht, die Nachrichten von dessen Nutzern zu entschlüsseln. Besonders sichere Verschlüsselungsverfahren, wie sie insbesondere bei OTT-Messengerdiensten zum Einsatz kommen, wären damit nicht mehr möglich.

- **Backdoors / Übergabeschnittstellen**

Es steht die Forderung im Raum, dass Betreiber von Diensten eine Schnittstelle zum Auslesen von Bestandsdaten und Inhalten zur Verfügung stellen müssen. Auch dies hätte das Problem, dass damit Ende-zu-Ende Verschlüsselung nicht möglich wäre und das Verschlüsselungsniveau dadurch geschwächt würde.

Ein weiteres Problem dieser Maßnahme wäre, dass eine solche Übergabeschnittstelle auch ein Einfallstor für Hacker sein könnte, die versuchen, Kommunikation abzufangen und diese für ihre eigenen Zwecke zu nutzen.

Fazit:
Maßnahmen, die Verschlüsselung schwächen, schwächen letzten Endes immer

auch die Sicherheit und Integrität digitaler Systeme und Dienste. Sie bieten in einer vernetzten Welt einen Ansatzpunkt für die Schädigung und Gefährdung weiterer Systeme und Netze, der Privatsphäre von Anwenderinnen und Nutzern und der wirtschaftlichen Tätigkeit. Sie untergraben das Vertrauen in diese Dienste, in digitale Technologien und darüber hinaus in Wirtschaft, Staat und Gesellschaft. Regierungen und internationale Organisationen sollten weltweit darauf hinwirken, dass eine regulatorische Schwächung von Verschlüsselung nicht durchgesetzt wird. Nutzerinnen und Nutzern muss die Möglichkeit gegeben werden, verschlüsselte Dienste und Anwendungen verwenden zu können, ohne, dass sie Sanktionen zu befürchten haben.

Verschlüsselung muss proaktiv gefördert werden, ihr Einsatz und ihre Verbreitung muss durch Forschungsvorhaben und Informationsangebote unterstützt werden. Verschlüsselungsverfahren dürfen nicht dahingehend reguliert werden, dass das Sicherheitsniveau abgesenkt oder eingefroren wird. Bekannte Schwachstellen und Sicherheitslücken müssen Betreibern von Diensten oder von Sicherheitslösungen gegenüber offengelegt werden, so dass Abhilfe geschaffen werden kann.
