KURZPOSITION CYBERSICHERHEIT

DIE JUNGEN UNTERNEHMER

Cybersicherheit – eine Kernaufgabe des Staates

Die Sicherstellung von innerer und äußerer Sicherheit gehört mit gutem Recht zu den klassischen Staatsaufgaben. Auch wirtschaftspolitisch betrachtet gehört die Aufrechterhaltung der öffentlichen Ordnung zu den grundlegenden Rahmenbedingungen, für die der Staat verantwortlich ist. Die Bedeutung von Sicherheit als Standortfaktor lässt sich vor allem erahnen, wenn die Kosten für wirtschaftliches Handeln in unsicheren Ländern betrachtet werden: Unternehmen müssen mitunter erhebliche Summen aufwenden, um ihre Betriebsstätten und Sachwerte zu schützen, und sich gegebenenfalls auch um die Sicherheit ihrer Mitarbeiter kümmern. Zum Glück hat die Sicherheitspolitik im wirtschaftspolitischen Diskurs in Deutschland lange kaum eine Rolle gespielt – die Bedingungen waren im Großen und Ganzen gut. Dies hat sich in den letzten Jahren jedoch leider geändert. Neben anderen Entwicklungen hat dazu auch das Thema Cybersicherheit beigetragen.

Die weltweite Vernetzung im Zuge der Digitalisierung hat neben vielen positiven Effekten den Nachteil, dass auch Straftaten im digitalen Raum kaum durch physische Grenzen behindert werden. Von der Beleidigung über das Hacking von Online Banking bis zur Wirtschafts-spionage – die Täter können aus einem beliebigen Land Opfer in anderen Ländern ins Visier nehmen. Dies erschwert die Strafverfolgung, sobald eine Tat begangen wurde. Es macht aber auch die Einschätzung der Risikolage und die Vorsorge schwierig.

Digitale Technologie ist, wie auch jede analoge Technik, nie absolut sicher. Ein Türschloss gibt es beispielsweise in unterschiedlichen Sicherheitsstufen, die es Einbrechern immer schwerer machen. Aber selbst das sicherste Türschloss kann – Zeit, Werkzeug und Können vorausgesetzt – aufgebrochen werden. Im Unterschied zur analogen Welt ist es im Cyberraum jedoch grundsätzlich möglich, jedes „Türschloss“ im Netz von jedem beliebigen anderen vernetzten Ort anzugreifen. Täter müssen für einen Einbruch nicht mehr physisch vor Ort sein. Dies erhöht die Sicherheitsrisiken natürlich erheblich.

Hinzu kommt, dass im Zuge der Digitalisierung immer mehr Geräte ans Internet angeschlossen werden. So werden einerseits immer mehr Anlagen ans Netz geschlossen, die in wichtigen Lebensbereichen zentrale Steuerungsfunktionen übernehmen (vom vernetzten Auto über Industrieanlagen bis zur Strom- und Wasserversorgung). Zum anderen werden immer mehr einfache Geräte vernetzt – vom Toaster über den Sensor bis zur Armbanduhr (Stichwort „Internet of Things“). Cybersicherheit ist damit längst nicht nur eine Frage der Sicherheit von einzelnen Computern, sondern betrifft alle Lebensbereiche.

Aus Sicht von DIE JUNGEN UNTERNEHMER kommt dem Thema Prävention und Strafverfolgung im digitalen Raum eine hohe Priorität zu. Dies gilt auch für den Schutz von Bürgern und Unternehmen vor Spionage und Datenbetrug. Deutschland ist als Hochtechnologieland schließlich ein besonders attraktives Ziel für Wirtschaftsspionage. Um die Cybersicherheit zu erhöhen, wird eine Vielzahl von verschiedenen Maßnahmen nötig sein. Ohne einen Anspruch auf Vollständigkeit zu erheben, stellen DIE JUNGEN UNTERNEHMER im Folgenden eine Reihe von Ansatzpunkten vor, die hierzu beitragen können.

DIE JUNGEN UNTERNEHMER
DIE FAMILIENUNTERNEHMER e.V.
Justus Lenz
Charlottenstraße 24 | 10117 Berlin

Tel. 030 300 65-443
Fax 030 300 65-390
lenz@junge-unternehmer.eu
www.junge-unternehmer.eu

Stand: 27. November 2017

Cyberpolizei

Ein zentraler Baustein zur Verbesserung der Cybersicherheit ist die Ertüchtigung der Polizeibehörden. Zur effektiven Prävention von Straftaten gehört neben technischen Sicherheitsmaßnahmen auch der Verfolgungsdruck nach dem Begehen einer Straftat. Auch für die bessere Betreuung der Opfer von Cyberkriminalität ist es unabdingbar, dass die Strafverfolgungsbehörden auf diesem Gebiet kompetenter werden. DIE JUNGEN UNTERNEHMER fordern deswegen:

- Die Polizeibehörden müssen technisch und personell so gut ausgestattet sein, dass sie Kriminalität im digitalen Raum effektiv erschweren und verfolgen können.
- In der digitalen Gesellschaft muss die internationale Kooperation von Polizeibehörden weiter verstärkt werden, um grenzüberschreitende Kriminalität besser verfolgen zu können.
- Das Bundesamt für Sicherheit in der Informationstechnik soll aus der Zuständigkeit des Innenministeriums herausgelöst werden und stattdessen dem Bundeskanzleramt unterstellt werden. Dieser Schritt soll das Amt unabhängiger machen und eine stärkere Konzentration auf den Schutz von Bürgern und Unternehmern vor Cyberkriminalität und Spionage ermöglichen.

Spionageabwehr im Cyberraum

Deutsche Unternehmen haben immer wieder mit den Folgen von Wirtschaftsspionage zu kämpfen. Auch wenn nur einzelne Fälle öffentlich werden, so ist die Dunkelziffer vermutlich hoch. Gerade für einen High-Tech-Standort kommt es aber darauf an, seine immateriellen Güter zu schützen. Dies liegt natürlich zunächst vor allem in der Hand jedes einzelnen Unternehmens. Der Staat sollte jedoch dazu beitragen, Wirtschaftsspionage zu erschweren. Zudem hat zuletzt der NSA-Skandal gezeigt, dass auch die Kommunikation jedes normalen Bürgers abgehört werden kann. Auch aus diesem Grunde ist es aus Sicht der jungen Unternehmer unerlässlich, die Spionage im Cyberraum zu bekämpfen. Wir fordern deswegen:

- Die deutschen Geheimdienste dürfen unter keinen Umständen dazu beitragen, dass Wirtschaftsspionage seitens Dritter, auch befreundeter Staaten, möglich wird. Ganz im Gegenteil: Die Abwehr von Wirtschaftsspionage sollte weit oben auf der Prioritätenliste der deutschen Dienste stehen.
- Sicherheitslücken in Softwareprogrammen dürfen von Behörden nicht verschwiegen und für die eigene Aufklärung genutzt werden. Stattdessen sollen Sicherheitslücken, die staatlichen Stellen bekannt werden, gemäß den Prinzipien einer verantwortungsvollen Offenlegung den Herstellern mitgeteilt und zu angemessener Zeit veröffentlicht werden, damit sie geschlossen werden können.

DIE JUNGEN UNTERNEHMER
DIE FAMILIENUNTERNEHMER e.V.
Justus Lenz
Charlottenstraße 24 | 10117 Berlin

Tel. 030 300 65-443
Fax 030 300 65-390
lenz@junge-unternehmer.eu
www.junge-unternehmer.eu

- Europa sollte endlich das sogenannte „Schengen-Routing“ einführen. Dieses würde sicherstellen, dass Datenverkehr zwischen beliebigen Endpunkten innerhalb Europas nicht über Drittstaaten weitergeleitet würde. Dies würde es Geheimdiensten außerhalb Europas erschweren, den gesamten innereuropäischen Datenverkehr abzuhören. Das Schengen-Routing alleine würde zwar gezielte Spionage nicht verhindern, aber immerhin das massenhafte Abhören und Auswerten von Daten erschweren.

Sicherheit in der Verwaltung

Neben der Ertüchtigung der Polizei muss sich die gesamte öffentliche Verwaltung im Zuge der Digitalisierung mit dem Thema Cybersicherheit beschäftigen. Dies ist unerlässlich, um die Integrität von eGovernment-Verfahren zu gewährleisten. Auch steht die öffentliche Verwaltung in der Pflicht, von ihr gesammelte Daten über Bürger und Unternehmen angemessen zu schützen. DIE JUNGEN UNTERNEHMER fordern deshalb:

- Die öffentliche Verwaltung muss dem Eigenschutz einen höheren Stellenwert einräumen. Nur wenn sich Politik, Regierung und Verwaltung effektiv selbst schützen, können sie Partner für den Kampf der Wirtschaft gegen Kriminalität und Spionage im digitalen Raum sein.

- Öffentliche Stellen sollten vermehrt Lösungen einsetzen, deren Quellcode sie unabhängig auditieren und auf Sicherheitslücken hin überprüfen lassen können. Dies können neben Open Source-Programmen auch private Lösungen sein, die überprüft werden können.

Stärkung des IT-Sicherheitsmarktes

Gerade für kleinere Unternehmen ist es sehr schwierig, sich effektiv vor Cyberangriffen zu schützen. Kleinere Unternehmen können schließlich nicht eigene teure IT-Spezialisten beschäftigen. Dies gilt natürlich auch für Privatleute. Umso wichtiger ist es, dass kleinere Unternehmen und Privatleute am freien Markt IT-Produkte mit einem hohen Sicherheitsstandard kaufen können. Diese verhindern zwar keine spezialisierten Angriffe, unterbinden jedoch einen Großteil der automatisierten Massenangriffe. Als großer Nachfrager kann die Verwaltung dazu beitragen, dass sich ein Markt für sichere IT-Produkte entwickelt. DIE JUNGEN UNTERNEHMER fordern deswegen:

- Öffentliche Stellen sollten in der Beschaffung von IT-Technik hohe Sicherheitsstandards einfordern und zu einem zentralen Auswahlkriterium machen. So können sie dazu beitragen, dass ein Markt für sichere IT-Komponenten und -Produkte entsteht.

- Die Bundesregierung sollte die Entwicklung und Verbesserung von hohen Sicherheitsstandards entsprechenden Open Source Lösungen unterstützen. Sie erhält so selbst gute Sicherheitslösungen, die gleichzeitig von Bürgern und Unternehmen genutzt werden können. Hierzu sollten im Rahmen der Forschungsförderung Programme zur Open Source Unterstützung seitens Universitäten und Forschungsinstituten eingerichtet werden.

DIE JUNGEN UNTERNEHMER
DIE FAMILIENUNTERNEHMER e.V.
Justus Lenz
Charlottenstraße 24 | 10117 Berlin

Tel. 030 300 65-443
Fax 030 300 65-390
lenz@junge-unternehmer.eu
www.junge-unternehmer.eu

Gleichzeitig sollte die Bundesregierung regelmäßige Sicherheitsaudits von Open Source Software fördern, in denen diese auf Sicherheitslücken überprüft werden. Die Ergebnisse dieser Audits sollten veröffentlicht werden.

- Zur Stärkung der deutschen IT-Sicherheitsbranche sollten die Prozesse der Ausfuhrkontrolle verbessert werden. Über einen Antrag zum Export von Verschlüsselungstechnik sollte wie in vielen unserer Nachbarländer innerhalb von 30 Tagen entschieden werden. Sollte es innerhalb dieser Frist keinen begründeten Negativbescheid geben, gilt der Antrag als genehmigt.

Internet of Things – Dringender Handlungsbedarf

Mit dem Schlagwort „Internet of Things“ (IoT) wird der Trend beschrieben, dass zunehmend mehr Geräte ans Internet angeschlossen werden. Dies reicht von der Industriesteueranlage über Sensoren bis hin zur Armbanduhr. Sicherheitskritisch ist dabei zunächst natürlich die Integrität der einzelnen Geräte. Um nur einige mögliche Beispiele zu nennen: Ein gehackter Toaster könnte einen Brand auslösen oder ein selbstfahrendes Auto zum Unfall gebracht werden. Je weiter IoT-Geräte verbreitet werden, desto mehr werden sie jedoch auch für die Sicherheit des Netzes selbst relevant. Denn viele Geräte mit Sicherheitslücken können von Angreifern zu Botnetzen mit großer Schlagkraft zusammengeschaltet werden, um z. B. Denial of Service Attacken durchzuführen. Dieses Problem besteht umso mehr, da schon heute viele IoT-Geräte nicht regelmäßig mit Sicherheitsupdates versorgt werden.

DIE JUNGEN UNTERNEHMER sehen diese Entwicklung mit großer Sorge. Es ist aus unserer Sicht unerlässlich, dass die Anbieter von IoT-Geräten einen größeren Fokus auf die Sicherheit ihrer Geräte legen. Gleichzeitig besteht jedoch die Gefahr, dass gesetzliche Regelungen über das Ziel hinaus schießen. Innovationen sollten durch Sicherheitsstandards nicht behindert werden. Zudem dürfen kleine Anbieter nicht über Gebühr belastet werden. Zum jetzigen Zeitpunkt ist es deshalb unserer Meinung nach zu früh, gesetzliche Verpflichtungen, beispielsweise für Sicherheitsupdates, einzuführen. Wir plädieren jedoch dafür, dass sich Branchen im Zuge der Selbstregulierung auf bessere Sicherheitsstandards einigen. Auch die Einführung von Prüfzeichen, mit denen die Einhaltung von Sicherheits-Mindestanforderungen bestätigt wird, sollte vorangetrieben werden.

DIE JUNGEN UNTERNEHMER
DIE FAMILIENUNTERNEHMER e.V.
Justus Lenz
Charlottenstraße 24 | 10117 Berlin

Tel. 030 300 65-443
Fax 030 300 65-390
lenz@junge-unternehmer.eu
www.junge-unternehmer.eu