Pressemitteilung 15. November 2016

Cyber-Security – Staatliche Verantwortung oder Nutzerauftrag?

Vertreter aus Wirtschaft, Wissenschaft und Politik diskutierten beim Berliner Gespräch des MÜNCHNER KREIS das Spannungsfeld zwischen staatlicher Regulierung und Selbstverantwortung im Bereich Cyber-Security. (Foto: MÜNCHNER KREIS / EIT ICT)

München, 15. November 2016 – 100.000 – das ist die Anzahl der neuen Schadprogramme, die sich täglich über das Internet verbreiten. 61 Prozent der Deutschen sagen in der neuesten DIVISI-Studie, sie können sich ein Leben ohne Internet nicht mehr vorstellen. Diese beiden Zahlen machen deutlich, welche zentrale Rolle die Cyber-Security bereits heute spielt. In Zukunft wird die Datensicherheit eine noch größere gesellschaftliche Bedeutung haben. Die drängendsten Fragen zu diesem Thema diskutierten Experten aus Politik, Wirtschaft und Wissenschaft beim vom MÜNCHNER KREIS organisierten Berliner Gespräch am 13. Oktober 2016 unter der Überschrift „Cyber-Security – Neue Services im Spannungsfeld zwischen Regulierung und Selbstverantwortung" in den EIT ICT Labs.

Prof. Dr. Claudia Eckert, Fraunhofer Institut AISEC und TU München, brachte es am Ende des Abends auf den Punkt: „Cyber-Security ist nicht ausschließlich ein technisches Thema, sondern betrifft und beeinflusst alle Bereiche der Gesellschaft, Wirtschaft und Politik. Es gilt, die unterschiedlichen Bedürfnisse, Erwartungen und Forderungen in einem gemeinsamen Diskurs aufzuarbeiten und Lösungen zu finden, die mehrheitlich akzeptiert werden können. Das diesjährige Berliner Gespräch war ein erster wichtiger Schritt in diese Richtung. Der

Abend hat verdeutlicht, dass es im Interesse aller Beteiligten liegt, die Debatte intensiv fortzuführen."

Staatssekretär Klaus Vitt, Bundesbeauftragter für Informationstechnik, betonte, dass der Staat die Rahmenbedingungen für die gesamtgesellschaftlichen Veränderungen schaffen müsse und gleichzeitig die Aufgabe habe, Freiheit und Sicherheit zu garantieren. Dabei ist es notwendig, dass sich Regulierung und Selbstverantwortung die Balance halten. Mit der Fortschreibung der Cybersicherheitsstrategie 2016 will das Bundesministerium des Innern die Aktivitäten der Bundesministerien koordinieren und Leitlinien und Maßnahmen unter anderem zur Förderung der digitalen Souveränität, oder auch der Robustheit von kritischen Infrastrukturen festlegen. Der Schutz der IT-Systeme allein durch den Anwender genügt nicht mehr. Auch für effektiven Datenschutz ist die IT-Sicherheit eine wesentliche Voraussetzung.

Den Mittelstand sensibilisieren

Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnologie (BSI), wies auf den Anstieg um den Faktor 70 bei Ransomware-Angriffen hin. Hierbei verschlüsselt eine schädliche Software die Daten auf dem Computer und Kriminelle fordern Geld für die Entsperrung. Nach Ansicht Schönbohms sei der vertrauensvolle Informationsaustausch in Bezug auf Angriffe oder Angriffsversuche auf dem Weg zu einem sicheren Cyberraum unerlässlich. Nur wenn Angriffe auf die IT-Systeme gemeldet werden, können ein umfängliches Lagebild erstellt und Unternehmen rechtzeitig gewarnt werden, sodass eine angemessene und rechtzeitige Reaktion möglich ist. So kann die Sicherheit ohne weitreichende Regulierungen erhöht werden. Für das BSI sind hinsichtlich der IT-Sicherheit drei Säulen von Belang: Standardisierung, Zertifizierung und Verschlüsselung. Alle Teilnehmer waren sich einig, dass der Mittelstand, insbesondere die Geschäftsführung, für das Thema IT-Sicherheit sensibilisiert werden müsse, damit das Rückgrat der deutschen Wirtschaft nicht ins Hintertreffen gerät. „Um kleine und mittelständische Unternehmen fit für die Ära der Digitalisierung zu machen, benötigen wir die Unterstützung von Multiplikatoren und sollten die Anwendung von Sicherheitssoftware aus Deutschland fördern", so Arne Schönbohm.

Als Reaktion auf die immer komplexeren Problemstellungen im Bereich der IT-Sicherheit wurde 2004 die Europäische Agentur für Netz- und Informationssicherheit (ENISA) gegründet. Kernaufgaben der etwa 50 Mitarbeiter umfassenden in Griechenland ansässigen Agentur sind die Information und Beratung der europäischen Institutionen vor und während Gesetzgebungsprozessen im Bereich IT-Sicherheit. Der geschäftsführende Direktor Prof. Dr. Udo Helmbrecht sieht in einer Welt, in der Unternehmen zunehmend Nutzerdaten „ernten", den Schlüssel in technischen Lösungen sowie einer staatlichen Regulierung – die im IT-Bereich augenblicklich jedoch noch in den Kinderschuhen stecke. Die Probleme müssten endlich angegangen werden und Marktteilnehmer sollten sich nicht auf einigen wenigen Erfolgsbeispielen ausruhen.

Bequemlichkeit wichtiger als Sicherheit

„In der Gesellschaft gewinnt noch viel zu häufig die Convenience über die Sicherheit", berichtete Matthias Kammer, Direktor des Deutschen Instituts für Vertrauen und Sicherheit

im Internet (DIVISI), das im Juni eine neue Internetmilieustudie veröffentlichte. „Es macht sich in Deutschland ein Internetoptimismus breit." 72 Prozent der Befragten sehen bei der Nutzung des Internets mehr Chancen als Risiken; dabei tritt die Datensicherheit in den Hintergrund. Ein Indiz dafür ist, dass mehr als Dreiviertel der Deutschen wissen, dass sie bei kostenlosen Diensten mit ihren Daten bezahlen, aber diese dennoch nutzen. Die Internet-User sind sich bewusst (82 Prozent der Befragten), dass sie selbst die Verantwortung für ihre Daten in der Hand halten. Diese Verantwortungsphilosophie zeigt sich auch in den folgenden Ergebnissen: 66 Prozent der Umfrageteilnehmer würden gerne den Staat in die Pflicht nehmen, trauen ihm eine Lösungsfindung aber nicht zu; 88 Prozent verlangen mehr Datenschutz von der Wirtschaft, glauben aber nicht daran, dass diese ihn garantieren kann. Matthias Kammer warnte: „Ein Umbruch, wie er uns bevorsteht, erfordert einen breiten gesellschaftlichen Diskurs darüber, wie das Leben in einer digitalen Gesellschaft aussehen sollte und welche Werte dabei im Vordergrund stehen. Die technologische Gestaltung muss immer zusammen mit der gesellschaftlichen Entwicklung erfolgen und darf diese nicht abhängen."

Konkrete Forderungen an die Politik

Bei der abschließenden Paneldiskussion wurde nochmals deutlich, dass die Entgrenzung staatlicher Souveränität im Bereich der Cyber-Sicherheit eine zentrale Herausforderung im Rahmen der digitalen Transformation ist. Von der Politik ist angesichts der Uferlosigkeit des Internets neben technischer Weitsicht, Konfliktbereitschaft und Flexibilität gefordert, wobei eine staatliche Regulierung bis zu einem gewissem Grad nicht fehlen darf. Dennoch hoben die Teilnehmer hervor, dass zu viele Regelungen Wettbewerb verhindern und mahnten die Politik, Zertifizierungs- und Zulassungsprozesse für Produkte zu beschleunigen, damit die IT-Sicherheitsbranche in Deutschland nicht ins Hintertreffen gegenüber beispielsweise amerikanischen Unternehmen gerät. Darüber hinaus können zu viele Sicherheitsmaßnahmen ebenso Innovationsprozesse hemmen. Die Teilnehmer erörterten zudem die Frage nach der Notwendigkeit einer allumfassenden Vernetzung und die Forderung nach mehr Transparenz.

Ob eine solche Nachvollziehbarkeit der richtige Weg ist sowie weitere komplexe Fragen werden im kommenden Jahr auf einer Fachkonferenz des MÜNCHNER KREIS zum Thema Cyber-Security diskutiert. Aufgrund der gestiegenen Bedeutung des Themas Cybersicherheit hat der MÜNCHNER KREIS Anfang 2016 einen neuen Arbeitskreis Cyber-Security unter der Leitung von Prof. Dr. Claudia Eckert gegründet, um das Thema sowohl in der fachlichen Tiefe, als auch gesellschaftlichen Breite zu begleiten.

Über den MÜNCHNER KREIS

Der MÜNCHNER KREIS möchte die digitalisierte Wissens- und Informationsgesellschaft durch seine Arbeit aktiv mitgestalten. Als gemeinnützige, internationale Vereinigung an der Nahtstelle zwischen Wirtschaft, Wissenschaft, Politik und Gesellschaft bietet der MÜNCHNER KREIS eine unabhängige Plattform, die gleichermaßen Hersteller, Dienstleister und alle Anwenderbranchen wie Automotive, Energie etc. anspricht. Mit einer Vielzahl unterschiedlicher Aktivitäten setzt er sich konstruktiv mit den Chancen und Herausforderungen der Digitalisierung auseinander, um Orientierung in der digitalen Transformation zu geben.

www.muenchner-kreis.de

Pressekontakt

Mareike von Frieling
HeadlineAffairs
Rumfordstraße 5
D - 80469 München
T + 49. 89. 23 23 90 91
F + 49. 89. 23 23 90 99
vonfrieling@headline-affairs.de