Sicherheitspolitisches Frühstück: Wolfgang Ebner, Martin Schallbruch, Wilhelm Sandrisser.

Cybersecurity und innere Sicherheit

Beim fünften sicherheitspolitischen Frühstück des Innenministeriums am 28. Februar 2012 referierte IT-Experte Martin Schallbruch über Aspekte zur Cyber-Sicherheit.

Innere Sicherheit sei ohne Sicherheit im Cyberspace nicht mehr möglich, sagte Dr. Wilhelm Sandrisser, Leiter der Gruppe I/B (Sicherheitspolitik, Internationales, EU, Öffentlichkeitsarbeit) im Innenministerium. Da hier aber verschiedene staatliche wie nicht staatliche Akteure angesprochen werden, sei ein breiter sicherheitspolitischer Ansatz notwendig. Ziel dieses „Sicherheitspolitischen Frühstücks" sei es daher, die Erfahrungen aus Deutschland näher zu betrachten und Rückschlüsse für diesbezügliche Arbeiten in Österreich zu ziehen.

Martin Schallbruch, IT-Beauftragter des deutschen Bundesministeriums des Innern, ging auf die großen Themen der nächsten Jahre in der IT- und Cyber-Sicherheit ein und erläuterte, wie sich Deutschland auf diese Herausforderungen vorbereitet. Er hob die Rolle des deutschen Innenministeriums hervor, sprach über die deutsche Cyber-Sicherheitsstrategie und gab in einer Einschätzung wieder, was Österreich aus den Erfahrungen in Deutschland lernen könne. Schallbruch verwies auf die Bedeutung des internationalen Austauschs im Bereich Cyber-Sicherheit. Da es aber in jedem Staat unterschiedliche Voraussetzungen gebe, seien bis zu einem gewissen Grad nationale Lösungen notwendig. Grundsätzlich sei es wichtig festzuhalten, dass Cybersecurity eine Frage der Sicherheit des Staates, der Wirtschaft und der Bürgerinnen und Bürger sei, da es mittlerweile um die Grundlagen des Staates gehe.

Die staatlichen Organisationen müssten diesen Prozess unterstützen und für die Rahmenbedingungen sorgen. Dabei sei wesentlich, dass sowohl bei der Planung als auch bei der Umsetzung ein breiter Ansatz verfolgt werde, also staatliche und nicht staatliche Akteure in den Prozess eingebunden würden.

Dies sei unter anderem deshalb so wichtig, da es sich beim Thema Cyber-Sicherheit nicht nur um ein komplexes Thema handle, sondern um ein zusammenwachsendes System. In der Folge sei man daher oftmals überrascht, was alles passiere, da die Zusammenhänge zuvor unbekannt waren. Dies lasse sich auf die hohe Arbeitsteilung in der heutigen Gesellschaft zurückführen. Diese Komplexität würden sich Kriminelle im Rahmen ihrer Cybercrime-Aktivitäten zu Nutze machen. Schallbruch verwies darauf, dass unterschiedliche Täter unterschiedliche Motivationen hätten. Diese würden von Cyber-Kriminalität über Cyber-Spionage bis zu Cyber-Extremismus reichen.

Das Grundproblem lasse sich darauf reduzieren, dass die Systeme von Anfang an nicht sicher konzipiert worden seien und somit zahlreiche Schwachstellen enthielten. Ein damit zusammenhängendes häufiges Problem sei, dass die im Einsatz befindlichen Systeme nicht die aktuelle Software hätten und oftmals erweitert würden, ohne zu prüfen, was dies für das Gesamtsystem bedeute.

Schallbruch zitierte Richard Clarke, der Gast des dritten „Sicherheitspolitischen Frühstücks" war, mit folgender Aussage: „Was nützt uns Cyber-Aufrüstung, mit der wir überall eindringen, wenn wir den Trojaner im eigenen Stromnetz haben und davon

FOTO: EGON WEISSHEIMER

nichts wissen.“ Es sei daher grundsätzlich wichtig, dass die infor-mationstechnischen Systeme sicher gemacht würden. Hier käme den Betreibern strategisch wich-tiger Infrastruktur eine besondere Rolle zu, so wie der Schutz dieser Infrastrukturen im Rahmen der deutschen Cybersecurity-Maßnahmen überhaupt oberste Priorität habe.

Schallbruch sagte, dass Cyber-Sicherheit ein Thema sei, das alle betreffe und nicht allein von den IT-Sicherheitsverantwortlichen behoben werden könne. Man brauche auch Prozessverantwortliche. Cyber-Sicherheit benötige eine neue Intensität der Zusammenarbeit, die man bislang nicht gekannt habe. Ein zentraler Punkt bei der Zusammenarbeit von staatlichen Akteuren und Vertretern der Wirtschaft sei der wechselseitige Informationsaustausch. Dieser Prozess würde aber eine gewisse Zeit in Anspruch nehmen, da erst das wechselseitige Vertrauen aufgebaut werden müsse. Es müssten auch kritische Punkte angesprochen werden dürfen, die die Unternehmen betreffen. So wüssten viele Unternehmer oft nicht, wo ihre Daten abgespeichert werden. Dies sei einer der Gründe, warum die betrieblichen Schutzmaßnahmen häufig unzureichend seien.

Laut Schallbruch müsste auch die Verantwortung der Internet-Provider stärker betont werden. So sollte überlegt werden, ob sie künftig ihre Kunden informieren müssen, sollten diese beispielsweise in ein Botnetz geraten. Weiters sollte der Frage nachgegangen werden, ob die Haftungsregelungen für Provider geändert werden müssten.

Auch die IT-Systeme des Staates müssten besser geschützt werden, da viele Aufgaben ohne IT nicht mehr erfüllbar wären. Schließlich müssten sich die Menschen organisieren und ihren Beitrag zur Cyber-Sicherheit leisten.

Teilnehmerinnen und Teilnehmer des 5. „Sicherheitspolitischen Frühstücks“ im Innenministerium.

Eine Cyber-Übung im November 2011 in Deutschland habe gezeigt, dass ein allgemein übergreifendes IT-Sicherheitsmanagement notwendig sei. Zwar sei das IT-Management von Bund und Ländern nicht verknüpft, die Systeme aber sehr wohl. Ein weiteres Ergebnis sei die Erkenntnis gewesen, dass die Fähigkeiten, mit Cyber-Bedrohungen umzugehen, ausgebaut werden müssten. Im internationalen Bereich könne man den Bereich am ehesten mittels „Soft Law“ begleiten, in dem geregelt ist, wie Staaten sich im Cyberspace zu verhalten hätten (Norms and State Behaviour).

Cyber-Abwehrzentrum. In Deutschland ist das Bundesministerium des Innern für IT-Sicherheit zuständig und damit „ein wesentlicher Akteur innerhalb der deutschen Netzpolitik“, sagte Schallbruch. Die deutsche Cybersecurity-Strategie wurde mit anderen Ministerien ausgearbeitet. Ein Ausfluss dieser Strategie ist das Cyber-Abwehrzentrum. Hier bearbeiten Vertreter des Innen- und Verteidigungsministeriums sowie anderer Ministerien und Vertreter der Wirtschaft Cybersecurity-Vorfälle. Die Struktur des Cyber-Abwehrzentrums sei zwar noch nicht perfekt, die Handlungsfähigkeit sei allerdings gegeben, betonte Schallbruch.

Neben dem Abwehrzentrum wurde der Cyber-Sicherheitsrat geschaffen. Seine Aufgabe ist es, die präventiven Instrumente und die zwischen Staat und Wirtschaft übergreifenden Politikansätze für Cyber-Sicherheit zu koordinieren.

Vorbildwirkung für Österreich hätten vor allem die Arbeiten an der Cybersecurity-Strategie sowie der Cyber-Sicherheitsrat, sagte Schallbruch. Die Strategie habe dazu geführt, dass die Akteure ihre Sicht auf das Problem einbringen konnten und dieses Phänomen in seiner gesamten Breite analysiert wurde. Der Cyber-Sicherheitsrat habe sich als gemeinsame Plattform etabliert, auf der wesentliche Punkte der Cyber-Sicherheit besprochen und abgestimmt werden könnten.

Aufgrund der unklaren Zurechenbarkeit von Angriffen sei Cybersecurity in erster Linien Aufgabe der inneren Sicherheit. Trotzdem müsse man sich der Fragen stellen, was die Rolle des Militärs sei und ob der Staat eine aktive oder reaktive Rolle einnehmen solle? Wie man sich auch entscheiden möge, Vorsicht bei der Ausweitung der staatlichen Möglichkeiten im Cyberspace sei geboten. Hinsichtlich Cyber-Sicherheit sei eine Selbstregulierung durch die Unternehmen gut und wünschenswert, rechtliche Rahmenbedingungen seien jedoch notwendig, erläuterte Schallbruch.

Mag. Wolfgang Ebner, Leiter der Abteilung Grundsatz und Strategie der Generaldirektion für die öffentliche Sicherheit, berichtete über die Arbeiten zum Thema Cyber-Sicherheit des Bundesministeriums für Inneres. „Das Innenministerium ist das zuständige Ressort in Sachen Cybersecurity, da es sich hier praktisch immer um Straftaten handelt“, sagte Ebner. Er wies darauf hin, dass bereits verstärkt Polizistinnen und Polizisten im Bereich Cybersecurity ausgebildet würden.

Im Bundeskriminalamt werde das Cyber-Crime-Competence-Centre (C4) aufgebaut. Ebner erwähnte auch die Kooperation mit der Wirtschaft über die *Wirtschaftskammer Österreich (WKO)*. Darüber hinaus betonte er die gute Zusammenarbeit mit dem *Kuratorium Sicheres Österreich (KSÖ)*.

Dr. Wilhelm Sandrisser fasste die wesentlichen Punkte des Sicherheitspolitischen Frühstücks zusammen und hob hervor, dass die einzelnen Aktivitäten des Bundeskanzleramts, des Bundesministeriums für Landesverteidigung und Sport und des Bundesministeriums für Inneres langfristig zusammengeführt werden sollten.

Nieves Kautny/Karl Srnec

FOTO: EGON WEISSHEIMER