IT-Sicherheitslücken schließen

Bis Ende 2017 wird im BVT ein Cyber-Security-Center eingerichtet. Dort sollen Lagebilder zur Internetsicherheit erstellt und Unternehmen bei der Schließung von IT-Sicherheitslücken unterstützt werden.

Die meisten Unternehmen sehen bei der Cyber-Sicherheit den Ausschnitt, der sie selbst betrifft. Es ist jedoch sinnvoll, als Staat ein gesamtes, sektorenübergreifendes Bild zur aktuellen Cyber-Lage zu haben und es Entscheidungsträgern in Verwaltung und Wirtschaft zur Verfügung zu stellen“, sagt Mag. Peter Gridling, Direktor des *Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT)*. Dabei werden vor allem Unternehmen der kritischen Infrastruktur unterstützt, bei deren Ausfall oder Störung es zu schwerwiegenden Folgen wie Versorgungsengpässen kommen könnte oder zu einer Beeinträchtigung der öffentlichen Sicherheit.

Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT): Bis Ende 2017 wird ein Cyber-Security-Center aufgebaut.

Lagebild. Das Cyber-Security-Center, das bis 2017 im BVT errichtet wird, soll periodisch Trends bei Cyber-Bedrohungen analysieren. „Wir können Unternehmen nicht vorschreiben, ob und wie sie Sicherheitsprobleme zu lösen haben. Durch das Aufzeigen von Trends soll aber ablesbar sein, wie hoch das Risiko ist und welche Auswirkungen ein Nichthandeln für Unternehmen haben könnte“, sagt Gridling. Das Lagebild soll in enger Zusammenarbeit zwischen Verteidigungsministerium, Bundeskanzleramt und Innenministerium in Abstimmung mit den Unternehmen gestaltet werden.

Neben staatlichen Daten zu Cyber-Zwischenfällen werden Cyber-Informationen von Unternehmen zusammengeführt. „In Gesprächen mit Unternehmerinnen und Unternehmern haben wir den deutlichen Wunsch wahrgenommen, dass vom Staat eine Koordinationsfunktion zum Thema Cyber-Sicherheit erwartet wird. Mit dem Aufbau des Cyber-Security-Centers wollen wir diese Rolle wahrnehmen“, sagt der BVT-Direktor. Dafür ist der Aufbau von Personal, Know-how und technischen Ressourcen notwendig.

Im Projektteam für das Cyber-Security-Center sind EDV-, Kommunikations- und Personalexperten sowie Juristen. „Die Gesetze gehen auf die neuen Herausforderungen in der Cyber-Sicherheit nicht ausreichend ein. Es sind viele rechtliche Fragen zu klären“, erklärt Projektleiter Dipl.-Ing. Philipp Blauensteiner. „IP-Adressen gelten in Österreich als personenbezogene Daten. Das ist ein Hindernis, wenn wir etwa Warnungen weiterleiten wollen.“ Ohne Anpassung der rechtlichen Grundlagen werde es in weiten Bereichen der Präventionsarbeit schwierig, den Erwartungshaltungen der Bedarfsträger gerecht zu werden.

Handlungsempfehlungen. Ein weiterer Arbeitsbereich des Cyber-Security-Centers ist die Erarbeitung von Handlungsempfehlungen. „Wir nehmen dabei eine Koordinationsrolle ein: Unternehmen informieren uns, wie sie mit einem Cyber-Angriff erfolgreich umgegangen sind. Wenn ein anderes Unternehmen mit einer ähnlichen Herausforderung an uns herantritt, können wir die Erfahrungen weitergeben“, erklärt Blauensteiner. „Wir sind gerade dabei, uns anzusehen, unter welchen Voraussetzungen Unternehmen bereit sind, in einem solchen System mitzuarbeiten.“

Kooperation mit dem C⁴. Die Mitarbeiterinnen und Mitarbeiter des Cyber-Security-Centers werden in ihrer täglichen Arbeit eng mit dem *Cyber-Crime-Competence-Center (C⁴)* im Bundeskriminalamt zusammenarbeiten. Die Mitarbeiter des C⁴ beschäftigen sich mit der Bekämpfung von Straftaten, die mithilfe des Internets verübt werden, wie zum Beispiel Onlinebetrug, Hacking und Schadsoftware. Im Jahr 2014 gingen beim C⁴ mehr als 12.000 Meldungen ein. „In unserer täglichen Arbeit können wir als Cyber-Security-Center nicht jede Meldung des C⁴ im Detail kennen“, erklärt Blauensteiner. „Wichtig ist für uns, mit den Trends und Entwicklungen vertraut zu sein und ins Cyber-Lagebild einfließen zu lassen.“ Das C⁴ ist neben dem Cyber-Security-Center wichtiger Bestandteil der operativen Cyber-Koordinierungsstruktur in Österreich. *M. L.*

CYBER-SICHERHEIT

ÖSCS

Die *Österreichische Strategie für Cyber-Sicherheit (ÖSCS)* und das Arbeitsprogramm der Bundesregierung bilden das Fundament der Maßnahmen zur Stärkung der Cyber-Sicherheit. Mit der ÖSCS wird eine operative Cyber-Koordinierungsstruktur festgelegt. Die Errichtung des Cyber-Security-Centers im BVT ist eine Maßnahme, um dieses Vorhaben umzusetzen. Das Innenministerium wird auf der operativen Ebene vom Verteidigungsministerium unterstützt, auf das die Federführung im Cyber-Defence-Fall übergehen würde.

FOTO: EGON WEISSHEIMER