Der Cyber-Angriff

Berlin (BB). Am 12.05.17 erfolgte eine erhebliche Cyber-Sicherheitsvorfälle, die durch so genannte „Ransomware“ ausgelöst wurden. Schadsoftware, die beim Angegriffenen seine Dateien verschlüsselt und vorgibt, diese erst gegen eine Zahlung wieder zu entschlüsseln, wurden von Anwendern gemeldet. Dieser Angriff ist nicht der erste seiner Art, auch wenn er besonders schwerwiegend ist. Er fügt sich in die angespannte Cyber-Bedrohungslage, auf die BSI und BMI immer wieder hingewiesen haben, ein. Das BKA hat die strafrechtlichen Ermittlungen übernommen.

Es gibt aber auch gute Nachrichten: Die Regierungsnetze sind von dem Angriff nicht betroffen, ihr hochprofessioneller Schutz durch das BSI zahlt sich aus. Zudem sprechen die jetzigen Erkenntnisse dafür, dass wer unserem Rat folgt, regelmäßige Software-Updates durchzuführen, eine gute Wahrscheinlichkeit hatte, dem Angriff zu entgehen.

Wenn wir uns die Zielrichtung des Angriffes ansehen, sind wir mit unserer Cybersicherheitsstrategie und dem IT-Sicherheitsgesetz, das besonders den Schutz **Kritischer Infrastrukturen im Blick hat**, auf dem richtigen Weg.

„Die Zeit drängt: Es ist deswegen besonders wichtig, dass wir nun auch die noch ausstehende Einigung bei der Festlegung der dem IT-Sicherheitsgesetz unterfallenden kritischen Infrastrukturen in den Bereichen Transport und Verkehr, Gesundheit, Finanz- und Versicherungswesen bis zum Ende der Legislaturperiode erzielen, um hier zügig den Schutz weiter erhöhen zu können. Zwei von diesen Bereichen waren jetzt in besonderer Weise betroffen, in Deutschland mit der Deutschen Bahn und mit Schenker als wichtiger Akteur des Transport- und Logistiksektors. Ich hoffe, dass spätestens jetzt alle Beteiligten zügig ihrer Verantwortung nachkommen und meinen längst auf dem Tisch liegenden Vorschlägen zustimmen.“

Text: Bundesministerium des Innern; Dr. Tobias Plate LL.M.

THEMENINFO

„Cyber-Raum“ – offensive und defensive Cyberstrategie

Im Rahmen der kritischen Infrastruktur wird auch der Katastrophen- und Bevölkerungsschutz sich mit den Cyber-Angriffen beschäftigen müssen. Zunehmend sind Infrastrukturen auf computer- und IT-gestützten Systemen aufgebaut, sodass diese damit auch auf Cyber-Angeriffe schon präventiv reagieren müssen.

Das Schlagwort „Cyberware“ stand bisher für T-Angriffe auf überwiegend computergestützt betriebene Systeme von mitlitärischen oder regierungsbehördlichen Systemen. „Hierbei kann es sich um mittelbare und unmittelbare Einwirkungen auf Waffen- oder sonstige militärische Systeme handeln, aber auch um (gegebenenfalls völkerrechtswidrige) Angriffe mit Auswirkungen auf wichtige zivile Infrastruktureinrichtungen wie Krankenhäuser oder Energieversorgungssysteme. Der Begriff des Cyberangriffs ist dabei weit gefasst und meint z. B. auch Daten-Spionage, das Zerstören von Hardware oder das Einschleusen schadhafter oder kompromittierter Hard- und Software in fremde Systeme. Neben sogenannten offensiven Strategien, die darauf zielen, die Systeme anderer Staaten anzugreifen, sie zu sabotieren, die Kontrolle über sie zu erlangen, sie außer Kraft zu setzen oder Fehlfunktionen hervorzurufen, geht es zudem darum, durch sogenannte defensive Ansätze, die eigenen IT-Strukturen, Kommunikations- und Waffensysteme zu sichern und aufrechtzuerhalten und sie vor Einwirkungen und Angriffen zu schützen.“

Für den zivilen Bereich sind kriminelle sowie wirtschaftliche Straftaten zunehmend feststellbar. Aber auch die Verletzung von Persönlichekeitsrechten und der Privatphäse zum Zwecke von Verschaffung von persönlichen oder wirtschaftenlichen Vorteilen wird die Cyberkriminalität eingesetzt.

Auch der Bevökkerungsschutz muss sich aktiv mit dem Thema Cyber-Angriffe auseinandersetzen.

Themen wie externe Beeinflussung von Lagemeldungen, Alarmierungen, Warnungen und logistischen Aufgaben, alle diese Bereiche werden derzeit elektronisch-comuptergestützt abgewickelt, unterliegen damit der möglichen Gefahr der Cyber-Angriffe.

Da entsprechend definierte Abhängigkeiten auch Auswirkungen auf die nichtpolizeiliche Gefahrenabwehr haben, muss hier von einer kritischen Infrastruktur ausgegangen und eine entsprechende präventive Vorsorge getroffen werden.