Abhörskandal

Das Problem liegt tiefer

[25.03.2024] In Deutschland fehlt eine zentrale Kommunikationslösung für Sicherheitsbehörden. Dieses Dilemma steht hinter dem Abhörskandal bei der Bundeswehr. Ein Kommentar des Sicherheitsexperten Christian Pohlenz.

Die Debatte um den Abhörskandal bei der Bundeswehr ist richtig und wichtig – sie darf sich aber nicht den Luxus leisten, nur die bekannten Symptome zu thematisieren. Das eigentliche Problem liegt tiefer und wird seit Jahrzehnten mehr oder weniger bewusst verschleppt. Statt mit dem Finger auf die Nutzer zu zeigen und auf mögliche Anwendungsfehler hinzuweisen, sollte das Übel an der Wurzel gepackt werden: einer zersplitterten Kommunikationsinfrastruktur, die eine funktionierende Vernetzung der Sicherheitsbehörden in Deutschland verhindert.

Vor allem dürfen die Anbieter die Anwender bei Bundeswehr, Polizei und anderen Behörden nicht länger mit der schwerwiegenden Verantwortung allein lassen, ihre Kommunikationskanäle selbst absichern zu müssen. Aus den offiziellen Erkenntnissen geht nämlich auch hervor, dass das Abhören des WebEx-Datenverkehrs durch einen Anwenderfehler überhaupt erst möglich wurde.

Jedes Bundesland nutzt seine eigene Technologie

Dahinter steht die strukturelle Misere einer fehlenden zentralen Lösung. Während jede Organisation, jede Behörde und jedes Bundesland seine eigene Technologie nutzt, bleiben das dringend notwendige Zusammenspiel und die Sicherheit der Software auf der Strecke. In der Folge greifen die Mitarbeiterinnen und Mitarbeiter auf Behelfslösungen zurück, etwa auf nicht zugelassene Messenger und Collaboration-Tools – mit fatalen Folgen.

Hochsensible Themen wie mögliche Taurus-Lieferungen an die Ukraine über Plattformen wie WebEx zu diskutieren, zeugt zudem von einer gewissen Sorglosigkeit und mangelnder Sensibilisierung aller Beteiligten für die ganz realen Gefahren aus dem digitalen Raum. Deutschland hat die Bedrohung durch Spionage und Cyber-Angriffe viel zu lange unterschätzt, vielleicht hat der Vorfall rund um den Taurus-Leak zumindest die positive Konsequenz, dass wir uns der Risiken im Zeitalter der digitalen Kommunikation bewusst werden und angemessen reagieren.

Zentrale Kommunikationsplattform

Die vollständige Abschaffung von Insellösungen ist jedoch kein realistisches Ziel. Vielmehr sollte die Bundesregierung die Implementierung einer zentralen Plattform anstreben, die als zentraler Betreiber die Sicherheit und Interoperabilität der angebundenen Anwendungen gewährleistet und den Anwendern alle benötigten Funktionen in einem geschützten Raum zur Verfügung stellt. Entscheidend für die erfolgreiche Abwehr zukünftiger Cyber-Angriffe wird darüber hinaus die intensive Schulung und Sensibilisierung der Mitarbeiterinnen und Mitarbeiter sein, die bereits den aktuellen Skandal hätte verhindern können.

Bei der Nutzung unbekannter Collaboration-Tools kann bereits eine kurze Recherche im Vorfeld die nötige Klarheit bringen, ob es sich um einen sicheren Kanal handelt und über welche Sicherheitsstandards die Lösung verfügt. Damit Mitarbeiterinnen und Mitarbeiter in Zukunft gar nicht erst in diese Situation kommen,

braucht Deutschland eine zentrale und ganzheitliche Cyber-Sicherheitsstrategie, die eine sichere Kommunikationsinfrastruktur vom Bundeskanzleramt über die Bundeswehr bis hin zu Polizei, Feuerwehr und anderen Behörden gewährleistet.

(al)

Stichwörter: Innere Sicherheit, Materna Virtual Solution, Abhörskandal, Behördenkommunikation