BSI

Maßnahmen nach globalen IT-Ausfällen

[31.07.2024] Nach der globalen IT-Sicherheitspanne vom 19. Juli formuliert das BSI einen klaren Aktionsplan. Künftig will die Sicherheitsbehörde Softwarehersteller stärker in die Pflicht nehmen. Langfristig will das BSI erreichen, dass die Systemarchitekturen von Sicherheitstools resilienter und weniger fehleranfällig werden.

Nach den weltweiten IT-Störungen am 19. Juli 2024 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) erste Maßnahmen entwickelt, um vergleichbare Vorfälle künftig zu vermeiden. Dem zugrunde lagen laut BSI Gespräche mit den Software-Unternehmen Crowdstrike und Microsoft; auch mit Herstellern vergleichbarer Softwarelösungen will das BSI Gespräche führen und seine Maßnahmen entsprechend weiterentwickeln. Dabei will die Cybersicherheitsbehörde darauf hinwirken, dass das jeweilige Betriebssystem auch bei schwerwiegenden Fehlern immer mindestens in einem abgesicherten Modus gestartet werden kann. Damit soll eine etwaige Fehlerbehebung für die Betroffenen künftig erleichtert werden.

Langfristig beabsichtigt das BSI, neue und resiliente Komponenten konzipieren und umsetzen zu lassen, welche die gleiche Funktionalität und Schutzwirkung entfalten wie bisher – und dabei weniger tiefgreifende Eingriffsrechte in die Betriebssysteme benötigen. Damit sollen die Auswirkungen etwaiger Softwarefehler minimiert werden. Darüber hinaus kündigt das BSI an, dass es mit Crowdstrike Maßnahmen vereinbaren wolle, durch welche die Betriebsstabilität von Kundensystemen auch bei der Installation kurzfristig notwendiger Software-Updates sichergestellt wird. Bereits umgesetzte Maßnahmen will die Cybersicherheitsbehörde auf Wirksamkeit überprüfen.

Ein strengerer Blick auf die Softwareentwicklung

Um diese Ziele zu erreichen, hat das BSI einen Zeitplan mit kurz-, mittel- und langfristigen Maßnahmen entworfen. Bis **spätestens 15. August 2024** soll eine Analyse der Betroffenheit vom Sicherheitsvorfall in Deutschland erfolgen; die Wiederherstellungsquote betroffener Systeme verfolgt werden (mit Stand 25. Juli 2024 21:54 Uhr MESZ sind laut Crowdstrike bereits 97 Prozent aller Systeme mit Windows-Sensoren wieder online) und eine Zusammenführung bereits erfolgter kurzfristiger Warnungen mit erwarteten häufigen Schwachstellen und Risiken (Common Vulnerabilities and Exposures, kurz: CVEs) zum Vorfall auf Basis des etablierten Meldeprozesses erfolgen.

Bis **spätestens 30. September 2024** plant das BSI die Auswertung des folgenden ausführlichen und abschließenden Analyseberichts (Root Cause Analysis) sowie eine Überprüfung des aktuellen und weiterentwickelten Testkonzepts von Crowdstrike durch das BSI in Abstimmung mit weiteren internationalen Partnerbehörden sowie Diskussionen zu erforderlichen Anpassungen mit Crowdstrike. Ebenfalls vorgesehen ist die Klärung künftiger Maßnahmen zur Sicherstellung eines zügigen Roll-outs der Logiken/Signaturen unter strikter Gewährleistung der Betriebsstabilität von Kundensystemen und die Prüfung der Wirksamkeit des von Crowdstrike bereits angekündigten Ausrollprozesses von Updates bei Kunden. Organisationen, die Crowdstrike-Produkte nutzen, sollen hinsichtlich der grundsätzlichen Betriebsrisiken sensibilisiert werden.

Langfristig – **bis Jahresende** – will das BSI konkrete Möglichkeiten zur Evaluierung der Softwareentwicklungsprozesse der Hersteller (basierend auf BSI TR-03185) durch unabhängige Dritte diskutieren und beruft sich dabei auf bereits erfolgte Ankündigungen von Crowdstrike. Zudem soll eine Zusammenarbeit des BSI mit Crowdstrike und Microsoft etabliert werden, um auch bei schwerwiegenden Fehlern eines eingesetzten Endpoint Detection and Response-Tools (EDR) ein Starten des Systems zu ermöglichen. Mit allen relevanten Stakeholdern zur Architektur von EDR-Tools sollen Erstgespräche zur Erhöhung derer Resilienz erfolgen.

Diese Maßnahmen sollen im Jahr 2025 fortgesetzt und vertieft werden. So sollen Konzeption und Umsetzungen neuer, resilienterer Architekturen zur Ausführung von EDR-Tools mit minimal erforderlichen Privilegien bei gleicher Funktionalität und Schutzwirkung erfolgen. Dabei sollen dann auch alle weiteren Hersteller dieser Produktkategorie, aller relevanten Betriebssystemplattformen sowie ganz allgemein der Hersteller von Produkten mit (derzeit noch) hohen Privilegien einbezogen werden.

(sib)

Stichwörter: IT-Sicherheit, BSI, Bundesamt für Sicherheit in der Informationstechnik, Crowdstrike, Cybersicherheit, Microsoft