

Bahn stellt Funk-Daten selbst ins Netz

Brauchte man wirklich Fachwissen, um das Funknetz der Bahn in Herne und Berlin anzugreifen?

Arne Poll

Welche interne Kenntnis brauchten Täter wirklich, um das Funknetz der Bahn anzugreifen? Der Konzern stellt weiter – auch nach der Attacke auf die Kabelstränge in Herne und Berlin vom Wochenende – etliche Daten zu seinen Systemen und Havarieabläufen im Internet öffentlich zur Verfügung. Der renommierte IT-Experte Karsten Zimmer sagt auf Nachfrage unserer Redaktion: „Das ist eine ganz gefährliche Sache.“ Die Bahn will sich nicht zum Thema äußern, sieht das Thema aber offensichtlich deutlich gelassener.

Eine dabei wesentliche Datenquelle ist das Infrastrukturregister. Das ist so etwas wie eine riesige digitale Straßenkarte für die Bahn. Hier lassen sich auf den Meter genau wie bei Google Maps Bahnlinien anzeigen, aber auch Zusatzinformationen wie interne Wege, der Verlauf von Elektrifizierung, Streckenneigung und die detaillierte Ausstattung der Linien mit Kommunikationssystemen wie dem jetzt betroffenen GSM-R-Funk. Die DB Netz stellt das Infrastrukturregister öffentlich zu Verfügung.

„Das darf man nicht für die Öffentlichkeit zugänglich machen“, sagt IT-Forensiker Karsten Zimmer, der sich mit der Redaktion die vorliegenden Daten angesehen hat. „Aus Sicherheitssicht ist das ganz gefährlich.“ Dabei denke er weniger an Geheimdienste und Top-Agenten. Staatlich organisierte Kriminelle oder Hacker kämen mit ihren Kenntnissen auch an diese Daten, wenn sie mehr geschützt seien. Dieses Verzeichnis aber ermögliche es selbst halbwegs versierten Normalbürgern, an mutmaßlich sicherheitsrelevante Daten zu gelangen und damit Schindluder zu treiben.

Richtlinie zum GSM-R-Funknetz legt Details zum System offen

Sicherheitskreise bis hin zum Verkehrsministerium und Spitzenpolitiker hatten nach dem Angriff davon gesprochen, dass man wohl tiefgreifende Kenntnisse der Systeme benötige, um das Funknetz so gezielt anzugreifen. Nach dem Vorfall wollten Bahn und Ermittler auch einige Fragen aus Sicherheitsgründen nicht beantworten, die sich aus den Daten im Netz klären.

Noch mehr Informationen über das jetzt betroffene Funknetz der Bahn liefert die „Richtlinie 481.0205“ – ebenfalls öffentlich einsehbar. Darin sind bis ins Detail die Verhaltensweisen im Umgang mit dem Bahnfunknetz GSM-R erklärt,



Eine Lok bei Herne: Die Bahn nutzt das Kommunikationssystem GSM-R in den Führerständen. Die Daten mit etlichen Details dazu stehen offen im Internet (Archivfoto).

RALPH BODEMER / FF5

einschließlich der Handynummer des dafür Verantwortlichen. Die Richtlinie nennt bis ins Detail mit schematischen Zeichnungen Rufnummernprinzipien und interne Kennzeichen, mit denen sich Lokführer bei den Leitstellen ausweisen, Prioritäten und Notrufabfolgen. Mit etwas Kombinationsfähigkeit kommt man an komplette Rufnummern. Auch weitere Richtlinien sind öffentlich.

Karsten Zimmer, der auch die Verhaltensweisen von Profi-Kriminellen studiert, hält das für fatal. Gerade in einer Notfallsituation sei

Stress angesagt. Da könne selbst ein simpler betrügerischer Anruf das System und damit auch Menschen in Gefahr bringen. Die Bahn erlaubt es laut Richtlinie, den Zugführern bei Ausfall des Bahnfunknetzes und stehendem Zug sogar „ein öffentliches Mobiltelefon“ zu nutzen. Es müsse allerdings sichergestellt sein, „dass die Teilnehmer selektiv sowie störungs- und zweifelsfrei miteinander sprechen können“, heißt es in der Richtlinie.

Die Befürchtung: Mutmaßliche Täter könnten – unabhängig vom aktuellen Fall – das Chaos eines



Das darf man nicht für die Öffentlichkeit zugänglich machen. Aus Sicherheitssicht ist das ganz gefährlich.

Karsten Zimmer, IT-Experte

GSM-R-Ausfalls nutzen und die öffentlich erreichbaren Telefonnummern, zum Beispiel der Fahrdienstleitungen, wählen. Im schlimmsten Fall könnten Täter unter falscher Flagge agieren und Schaden anrichten. Im einfachsten Fall könnte jemand mit böser Absicht schlichtweg immerhin wichtige Rufnummern lahmlegen. Die Bahn weist selbst in ihrer Richtlinie auf die Sensibilität der Verfahrensweise hin: „Zugfunkgespräche über Bürotelefone dürfen nur bei Störungen geführt werden, da hier keine Sprachaufzeichnung stattfindet.“

Für Karsten Zimmer ist die Veröffentlichung „eine Anleitung für Kriminelle, wie man vorgehen kann“. Auch andere Unternehmen gingen mit Anleitungen zu ihrer Infrastruktur teils sehr fahrlässig um.

Bahn will sich nicht zu möglicher Gefährdung äußern

Die Bahn will sich auf Anfrage der WAZ nicht zu den Vorwürfen äußern. Intern soll man die Veröffentlichung der Daten eher gelassener sehen, erfuhr unsere Redaktion aus dem Umfeld der Bahn. Ein Problem soll sein, dass die DB Netz die Streckendaten auch anderen Verkehrsunternehmen zur Verfügung stellen muss. Warum der Austausch nicht über interne Systeme geschieht, bleibt offen. Auch nach der Anfrage der Redaktion standen die Daten weiter frei zugänglich online.

Aktuell bleibt weiter offen, wer für die Attacke verantwortlich ist. Der polizeiliche Staatsschutz in Bochum ermittle in alle Richtungen. Die Beamten untersuchen, ob die Kombination der Angriffe in Herne und Berlin wirklich ein gezieltes Vorgehen war – oder ob die Leitungen zufällig beispielsweise bei einem Kabeldiebstahl in Mitleidenschaft gezogen wurden.