GEFÖRDERT VOM BMBF

„Cyber-Safe – Schutz von Verkehrs-, Tunnel- und ÖPNV-Leitzentralen vor Cyber-Angriffen“ ist ein Forschungsprojekt, das vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen der Hightech-Strategie von 2015 bis 2018 unter den Förderkennzeichen 16KIS0168 bis 16KIS0172 gefördert wird. Cyber-Safe bezieht sich auf den Förderschwerpunkt „IT-Sicherheit für Kritische Infrastrukturen“.

VERBUNDPARTNER

STUVA

Straßen.NRW.

bast
Bundesanstalt für Straßenwesen

DÜRR
Tunnel- und Verkehrstechnik

RUHR UNIVERSITÄT BOCHUM
RUB

KONTAKT ZU CYBER-SAFE

Straßen und Tunnel/Verbundkoordination
Dipl.-Ing. Selcuk Nisancioglu
BASt – Bundesanstalt für Straßenwesen
Tel.: +49 2204 43-838 oder -883
cyber-safe@bast.de

ÖPNV und Tunnel
Dr.-Ing. Christian Thienert
STUVA e.V.
Tel.: +49 221 59795-24
cybersafe@stuva.de

cybersafe.stuva.de

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Cyber-Safe

Schutz von
Verkehrs-, Tunnel- und ÖPNV-Leitzentralen
vor Cyber-Angriffen

Cyber-Safe – Schutz von Verkehrs-, Tunnel- und ÖPNV-Leitzentralen vor Cyber-Angriffen

MOTIVATION

Die uneingeschränkte Mobilität von Personen und Gütern ist die Voraussetzung für wirtschaftliche Prosperität einer modernen Gesellschaft. Um einen reibungslosen und sicheren Normalbetrieb sicherzustellen werden daher wichtige Bereiche von Verkehrswegen durch Leitzentralen überwacht. Bei unplanmäßigen Vorkommnissen, wie Unfällen, übernehmen diese zudem die Koordination von Rettungskräften. Dabei bedienen sich die dort tätigen Operatoren und Disponenten moderner IT-Systeme. Der Ausfall von Leitzentralen durch Cyberangriffe würde daher nicht nur den Verkehr beeinträchtigen, sondern auch die Versorgung von betroffenen Personen gefährden.

ZIELE UND VORGEHEN

Ziel des Projektes Cyber-Safe ist es, die Sicherheit von Verkehrs-, Tunnel- und ÖPNV-Leitzentralen vor Cyberangriffen zu erhöhen. Die Betreiber sollen besser als bislang mögliche Gefährdungen erkennen und geeignete Schutzmaßnahmen ergreifen können. Hierzu werden zunächst bestehende Sicherheitskonzepte auf ihre Wirksamkeit hin überprüft. Anschließend werden Verbesserungen erarbeitet und deren Effektivität durch „White-Hats“ geprüft. Dies sind professionelle Hacker, die unter Beachtung des gesetzlichen Rahmens legal Hacker-Angriffe (sogenannte „Penetrationstests“) durchführen.

INNOVATIONEN UND PERSPEKTIVEN

Im Rahmen von Cyber-Safe werden erstmals IT-Systeme, Gefährdungen und Sicherheitskonzepte von Leitzentralen verschiedener Verkehrsträger untersucht. Die Erarbeitung neuer Konzepte zur Erhöhung der Sicherheit erfolgt unter Beachtung sich dynamisch verändernder Randbedingungen auf zeitlicher und inhaltlicher Basis ebenenübergreifend:

- Prävention,
  Verhinderung „erfolgreicher“ Angriffe
- Mitigation,
  Milderung der Folgen
- Rekonstruktion,
  Wiederaufnahme des Betriebs danach.

Durch ein innovatives Management-Tool mit zugehörigem Leitfaden sollen die Betreiber in die Lage versetzt werden, eine Bewertung des Sicherheitsniveaus eigenständig durchzuführen.

KRITISCHE INFRASTRUKTUREN

Sie sind das Rückgrat moderner Industrienationen: Kritische Infrastrukturen gewährleisten die grundlegende Versorgung von Wirtschaft und Gesellschaft in so wichtigen Bereichen wie Energie, Informationstechnik und Kommunikation, Transport und Verkehr, Medien und Kultur oder auch Staat und Verwaltung. Diese Infrastrukturen werden zunehmend von IT-Systemen gesteuert, die mit dem Internet verbunden sind. Damit ist ein Angriff von außen möglich und der Schutz vor Cyberangriffen zu einer neuen Herausforderung geworden.