Die Bekanntmachung in Zahlen

LAUFZEIT BIS
2018

12
PROJEKTE

17
BETREIBER KRITISCHER INFRASTRUKTUREN

23
MILLIONEN EURO FÖRDERVOLUMEN

Impressum

Herausgeber
Bundesministerium für Bildung und Forschung (BMBF)
Referat Kommunikationssysteme; IT-Sicherheit
53170 Bonn

Bestellungen
schriftlich an
Publikationsversand der Bundesregierung
Postfach 48 10 09
18132 Rostock
E-Mail: publikationen@bundesregierung.de
Internet: http://www.bmbf.de
oder per
Tel.: 030 18 272 272 1
Fax: 030 18 10 272 272 1

Stand
Februar 2017

Gestaltung
VDI/VDE-IT, AZ

Druck
MKL Druck GmbH & Co. KG, Ostbevern

Bildnachweis
Aliaksei Dzeiko: AQUA-IT-Lab
Bundesanstalt für Straßenwesen: CyberSafe
Bundesdruckerei: SECMaaS
Fotolia.com:
Aleksey Stemmer: MoSaIK, Nonwarit: Die Bekanntmachung in Zahlen , viappy: VeSiKi
Hochschule Augsburg: RiskViz
pixelio.de/Uwe Schlick: SIDATE
Presse- und Informationsamt der Bundesregierung, Steffen Kugler: Porträt Prof. Dr. Johanna Wanka
RGtimeline / Thinkstock: Titel
Stadtwerke München GmbH: SURF
UKSH: ITS.APT
Vattenfall GmbH: INDI
Vattenfall GmbH, Katrin Rößler: SICIA

Dieser Flyer ist Teil der Öffentlichkeitsarbeit des Bundesministeriums für Bildung und Forschung; er wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

Mehr Informationen:
https://www.bmbf.de/de/sicher-in-der-digitalen-welt-849.html

Bundesministerium
für Bildung
und Forschung

DIE NEUE HIGHTECH STRATEGIE
Innovationen für Deutschland

Sicherheit geht vor

IT-Sicherheit für Kritische Infrastrukturen

Projekte für sichere Versorgung mit Energie, Kommunikation und sicheren Straßenverkehr

Ampeln sind richtig geschaltet, es kommt genügend Strom aus der Steckdose und lebenswichtige Geräte in Krankenhäusern funktionieren: Kritische Infrastrukturen gewährleisten, dass wir uns auf Energie, Kommunikation, Transport, Kultur oder auch Verwaltung verlassen können. Diese Infrastrukturen werden zunehmend von IT-Systemen gesteuert, die mit dem Internet verbunden sind.

Die Vernetzung der IT-Systeme birgt auch Risiken. Vor allem für kleinere Betreiber von Kritischen Infrastrukturen wie kommunale Energie- oder Wasserversorger rückt die IT-Sicherheit in den Fokus. Der Schutz vor Cyberangriffen ist zu einer neuen Herausforderung geworden. Das Bundesministerium für Bildung und Forschung fördert daher im Förderschwerpunkt „IT-Sicherheit für Kritische Infrastrukturen“ zwölf Forschungsprojekte. Zentrale Inhalte sind: 1. Werkzeuge und Verfahren, die es Betreibern Kritischer Infrastrukturen ermöglichen, das aktuelle Sicherheitsniveau zuverlässig zu beurteilen. 2. Maßnahmen zur IT-Sicherheit, die auf die Anforderungen dieser Nutzer eingehen. 3. das Berücksichtigen vorhandener Systeme.

„IT-Angriffe auf kritische Infrastrukturen wie die Strom- und Wasserversorgung oder Krankenhäuser geschehen immer häufiger und können große Schäden verursachen, wenn sie nicht rechtzeitig erkannt werden. Gerade kleine oder mittelgroße Unternehmen sind jedoch oftmals noch nicht ausreichend auf Hackerangriffe vorbereitet. Das Bundesministerium für Bildung und Forschung fördert daher die Erforschung und Erprobung alltagstauglicher und bezahlbarer IT-Sicherheitslösungen, um diese zentralen Infrastrukturen jeglicher Größe fit für die Zukunft zu machen.“

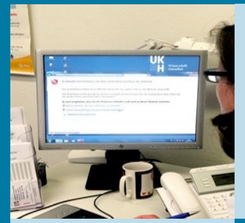
Johanna Wanka

Prof. Dr. Johanna Wanka
Bundesministerin für Bildung und Forschung

Wasser

AQUA-IT-Lab

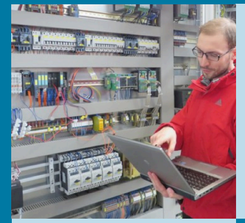
Das Niveau der IT-Sicherheit zuverlässig ermitteln: Dazu entsteht ein Testlabor, in dem Forscherinnen und Forscher die Infrastruktur eines Wasserversorgers rekonstruieren. Simulierte Angriffe geben Aufschluss über Schwächen und Verbesserungspotenziale.



Gesundheit

ITS.APT

Um die Sicherheit von Kritischen Infrastrukturen zu bewerten, wird nach Schwachstellen in Systemen und Software gesucht. Doch oft ist der Mensch die „Schwachstelle". Dies untersucht ein interdisziplinäres Team aus der Informatik und Psychologie.



Energie, Wasser und Transport

RiskViz

Industrielle Kontrollsysteme (ICS) sind ein wichtiger Bestandteil Kritischer Infrastrukturen und immer häufiger über das Internet erreichbar. Damit sind sie ein Angriffspunkt für Hacker. Die Projektpartner entwickeln eine Suchmaschine, die ICS findet und deren Bedrohungslage einschätzt.

Energie und Wasser

SIDATE

Kleine Energieversorger haben oft beschränkte Ressourcen, Sicherheit sollte aber nicht zu kurz kommen. Die Projektpartner entwickeln Wissenswerkzeuge zur Selbsteinschätzung und eine Datenbank für Betreiber. Diese erfahren, wo sie im Vergleich zu anderen stehen oder sich verbessern sollten.

CyberSafe

Verkehrs-, Tunnel- und ÖPNV-Leitzentralen stehen auf dem Prüfstand. Was ist gute Angriffsprävention? Wie mildere ich die Folgen im Fall der Fälle ab? Oder: Wie wird der Betrieb nach einem Angriff wieder aufgenommen?

Transport und Verkehr

MoSaIK

Kommunen leisten viel: Ohne sie fährt kein Bus, ohne sie bricht der Deich, ohne sie gelangt kein Strom in die Haushalte. Die Projektpartner entwickeln Werkzeuge, die vor allem kleine Kommunen bei der Analyse der IT-Sicherheit ihrer Leit- und Steuerungssysteme unterstützen.

Staat/Verwaltung, Energie, Wasser

SecMaaS

Im Projekt werden zentrale, cloudbasierte Sicherheitsdienste für Bürgerämter entwickelt, damit diese in Zukunft sagen können: Komplexe Aufgaben wie Verschlüsselung von E-Mails oder das Management von Zertifikaten sind in besten Händen.

Staat und Verwaltung

SURF

Viele Schutzsysteme greifen in Kritischen Infrastrukturen ineinander. Genau dieses Zusammenspiel wird im Projekt betrachtet: von der Härtung von Netzkomponenten über den Einsatz spezieller Sicherheitschips bis hin zur Risikobewertung von Systemzuständen.

Energie und Transport

Energie

INDI

Viele Cyberangriffe erkennt man an einem veränderten Kommunikationsverhalten. Im Projekt werden solche Anomalien in Industrienetzen mit Algorithmen des maschinellen Lernens untersucht. Ergebnis sind Modelle, die verdächtiges Kommunikationsverhalten in der digitalen Welt erkennen.

Finanz- und Versicherungswesen

PREVENT

Verbessert wird die Bewertung der Sicherheit von Rechenzentren in Banken. Echtzeitmessungen, Ergebnisse von Sicherheitstests und Simulationen von Bedrohungsszenarien werden zu einem Lagebild zusammengeführt.

Energie

SICIA

Wie bewertet ein Kraftwerkbetreiber seine IT-Sicherheit? Im Projekt werden Systeme zuerst auf Geräteebene analysiert, um relevante Sicherheitsindikatoren zu ermitteln. Die Analyse setzt sich auf höheren Ebenen fort und führt so zu aussagekräftigen Kennzahlen.

Begleitforschung: VeSiKi

Die Projekte verfolgen ambitionierte Ziele, die Begleitforschung VeSiKi bearbeitet die übergeordneten Fragestellungen, z. B.: Wie müssen sich Standards und Normen entwickeln? Wie ist aktuelles Recht zu bewerten? Wie können neue Ansätze in der Sicherheitsforschung entstehen?