

IT-Sicherheit Kritischer Infrastrukturen: Deutschland schützt sich

Zwölf Projekte forschen für die Verbesserung der IT-Sicherheit

Kritische Infrastrukturen (*KRITIS*) müssen besonders geschützt werden, weil bei Störungen ein ganzer Staat lahmgelegt werden kann. Zu den KRITIS zählen insbesondere Wasser- und Elektrizitätswerke sowie Atomkraftwerke. Potenzielle Zwischenfälle stellen u. a. über Tage anhaltende Strom-, Telefon- oder Wasserausfälle dar, hohe gesellschaftliche und wirtschaftliche Schäden können das Resultat sein. An der Universität der Bundeswehr München wird in einem Verbund mit Kooperationspartnern zur IT-Sicherheit für KRITIS geforscht.

Wie in anderen Unternehmen hält die zunehmende Vernetzung der IT-Systeme auch in KRITIS relevanten Unternehmen Einzug. Aber wie kümmert man sich, bei diesen für die Öffentlichkeit relevanten Betrieben, um die Gewährleistung der IT-Sicherheit von IT-Systemen? Wie brisant und aktuell dieses Thema ist, zeigt der Beitrag „Kühler Krieg“ im Spiegel 39/2016. Dort wird anschaulich die These diskutiert, dass zukünftige Kriege nicht mehr mit Panzern und Flugzeugen, sondern digital mit Software und Computern ausgetragen werden.

Das Bundesamt für Bildung und Forschung (*BMBF*) sieht in diesem Bereich Forschungsbedarf, um die KRITIS in Deutschland zu schützen und so die fortwährende Versorgung mit Produkten und Dienstleistungen von KRITIS-Betreibern zu gewährleisten. Deshalb wurde mit dem Forschungsrahmenprogramm „Selbstbestimmt und sicher in der digitalen Welt 2015-2020“ der Förderschwerpunkt „IT-Sicherheit für Kritische Infrastrukturen (ITS|KRITIS)“ ausgeschrieben.

Im Förderschwerpunkt IT-Sicherheit für Kritische Infrastrukturen (*ITS|KRITIS*) sind elf Verbundprojekte sowie das Begleitforschungsprojekt „Vernetzte IT-Sicherheit Kritischer Infrastrukturen“ (*VeSiKi*) organisiert. Gemeinsames Ziel der zwölf Projekte ist die Verbesserung der IT-Sicherheit in KRITIS. Um möglichst viele der nach BSI definierten Sektoren von KRITIS zu erfassen, haben die Verbundprojekte unterschiedliche Fokussierungen und jedes Projekt im Förderschwerpunkt untersucht eine konkrete Forschungsfrage. Das Begleitforschungsprojekt *VeSiKi* bündelt die Ergebnisse der Verbundprojekte und legt dadurch unter anderem Synergieeffekte frei.

Die Forschung der Projekte im Förderschwerpunkt läuft bis Ende 2018. Die Erfahrungen und Resultate werden der Öffentlichkeit laufend über die Projektplattform <http://www.itskritis.de/> zur Verfügung gestellt.

Als große Veranstaltung präsentiert ITS|KRITIS am 23. November in Berlin das IT-Sicherheitsforum, bei dem Forschungsprojekte, Betreiber Kritischer Infrastrukturen sowie Vertreter aus Wirtschaft und Politik das Thema „IT-Sicherheit in Kritischen Infrastrukturen“ diskutieren. Begleitend präsentieren sich die Forschungsprojekte des Förderschwerpunktes in einer Ausstellung.

Informationen sind unter <https://www.itskritis.de/aktivitaeten.html#sicherheitsforum> verfügbar.

Was ist VeSiKi?

Im Begleitforschungsprojekt VeSiKi (Vernetzte IT-Sicherheit Kritischer Infrastrukturen) arbeiten die vier Projektpartner Universität der Bundeswehr München (UniBw), Universität Bremen (UniBre), Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) und VDE|DKE zusammen und begleiten den Förderschwerpunkt ITS|KRITIS („IT-Sicherheit in Kritischen Infrastrukturen“) sowohl koordinativ als auch mit wissenschaftlichen Maßnahmen. Nähere Informationen finden Sie auf den Webseiten www.itskritis.de und www.vesiki.de sowie via Twitter [@itskritis](https://twitter.com/itskritis).

Was ist ITSKRITIS?

ITSKRITIS ist der Förderschwerpunkt IT-Sicherheit in Kritischen Infrastrukturen des BMBF. In Rahmen des Förderschwerpunktes forschen die zwölf vom BMBF geförderten Forschungsprojekte AQUA-IT-Lab, Cyber-Safe, INDI, ITS.APT, MoSaIK, PREVENT, RiskViz, SecMaaS, SICIA, SiDate, SURF und VeSiKi.