Funkkolleg 2016/2017

Sicherheit

Zusatzmaterial zur Sendung 21:

Kritische Infrastrukturen – wo Gesellschaften verletzlich sind

vhs Die Volkshochschulen in Hessen

TECHNISCHE UNIVERSITÄT DARMSTADT

HESSEN Hessisches Kultusministerium

hr iNFO

Zusatzmaterial zur Folge 21
Kritische Infrastrukturen – wo Gesellschaften verletzlich sind

Livestream und Podcast: www.hr-inforadio.de

Interessierte Hörerinnen und Hörer finden auf dieser Seite weiterführende Informationen zu den einzelnen Sendungsthemen als Zusatzmaterial. Die Materialien wurden zum Zugriffszeitpunkt 27.03.2017 erstellt von:
Markus Stegeman, Fachgebiet Wirtschaftsinformatik | Software Business & Information Management, Technische Universität Darmstadt

Inhalt

1. Forschungsstudien

Neue Studie zeigt Bedrohungspotential

Die IT-Sicherheit Kritischer Infrastrukturen ist bedroht. Eine große Anzahl der Betreiber Kritischer Infrastrukturen mussten im letzten Jahr Angriffe verzeichnen. Die Betreiber investieren viel in die IT-Sicherheit und schätzen ihre Fähigkeit Angriffe abzuwehren als hoch ein. Zu diesen Ergebnissen kommt eine Studie von Prof. Ulrike Lechner mit ihrem Team des Forschungsprojekts „Vernetzte IT-Sicherheit Kritischer Infrastrukturen“ an der Universität der Bundeswehr München. Prof. Lechner möchte mit ihrer Forschung die Gesellschaft und Politik für die möglichen Konsequenzen von erfolgreichen IT-Angriffen sensibilisieren und auch IT-Lösungen zur Abwehr von Angriffen finden.

In diesem kurzen Artikel werden die wichtigsten Erkenntnisse der Forschung von Prof. Ulrike Lechner und ihrem Team zusammengefasst. Zudem enthält er einen Link zu den detaillierten Ergebnissen der vorgestellten Studie. Das Forschungsprojekt „Vernetzte IT-Sicherheit Kritischer Infrastrukturen“ wird in Abschnitt 3.4 näher vorgestellt.

Quelle: Universität der Bundeswehr München: Neue Studie zeigt Bedrohungspotenzial, 07.04.2017

Link: https://www.unibw.de/willkommen/startseite-meldungen/neue-studie-zeigt-bedrohungspotenzial

2. Industrienahe Studien

Kaspersky sieht kritische Infrastrukturen in Gefahr

Mit dem Internet der Dinge nehmen auch immer mehr industrielle Kontrollsysteme Kontakt zum Internet auf. Damit wachse aber auch die Gefahr von Cyberattacken erheblich, warnen IT-Sicherheitsexperten von Kaspersky Lab. Je größer die Infrastrukturen seien, desto größer sei das Risiko empfindlicher Sicherheitslücken, sagte Andrey Suvorov von Kaspersky Lab.

Das Unternehmen hat zu der Problematik eine weltweite Studie durchgeführt. Demnach waren im Juli 2016 220.000 Komponenten von industriellen Kontrollsystemen über das Netz weltweit verfügbar. 91,6 Prozent der Systeme nutzen unsicherer Internetverbindungsprotokolle, die Angreifer für Attacken oder der Möglichkeit der Fernsteuerung ausnutzen könnten. In den vergangenen fünf Jahren seien Schwachstellen innerhalb von Industrie-Komponenten um das zehnfache gestiegen.

Quelle: WELT Online: Kaspersky sieht kritische Infrastrukturen in Gefahr, 11.07.2016

Link:
https://www.welt.de/newsticker/dpa_nt/infoline_nt/computer_nt/article156951358/Kaspersky-sieht-kritische-Infrastrukturen-in-Gefahr.html

3. Sonstiges

3.1. Literatur

Kritische Infrastrukturen, Cybersicherheit, Datenschutz

Als die EU im Jahr 2013 beabsichtigte, eine Meldepflicht für Cyberattacken auf kritische Infrastrukturen einzuführen, gab es zwar in Wirtschaft und Politik Widerstände gegen diesen Vorschlag. Doch einiges sprach dafür, dass mit einer solchen Meldepflicht kritische Infrastrukturen präventiv geschützt werden können. Ausschlaggebend hierfür ist, dass die nationalen und europäischen Behörden die erlangten Informationen vertraulich behandeln und verarbeiten. Mit einem umfangreichen Maßnahmenkatalog setzte die EU Maßstäbe für eine europäische und internationale digitale Standortpolitik.

Dieser Artikel der Stiftung Wissenschaft und Politik in „SWP-Aktuell“ stammt aus dem Jahr 2013, verdeutlicht jedoch anschaulich, welche politischen Aspekte in Diskussionen über kritische Infrastrukturen eine Rolle spielen.

Quelle: Bendiek, Annegret: Kritische Infrastrukturen, Cybersicherheit, Datenschutz. Die EU schlägt Pflöcke für digitale Standortpolitik ein. SWP-Aktuell, 2013

Link: https://www.swp-berlin.org/fileadmin/contents/products/aktuell/2013A35_bdk.pdf

3.2. Video/Audio

Cyberangriffe - Wasserwerke und Energieversorger als Ziel

Kritische Infrastrukturen wie Energieversorger, Wasserwerke und Stromnetzbetreiber sind zunehmend Ziel von Cyberangriffen. Die Digitalisierung schafft Einfallstore für Hacker. Das Risiko wird von Betreibern und Unternehmen unterschätzt.

Die Sendung „plusminus“ (ARD) befasst sich in dieser Ausgabe mit der Sicherheit kritischer Infrastrukturen und zeigt anhand verschiedener Beispiele auf, wie einfach Infrastrukturen durch Hacker manipuliert werden können.

Link: http://www.ardmediathek.de/tv/Plusminus/Cyberangriffe-Wasserwerke-und-Energiev/Das-Erste/Video?bcastId=432744&documentId=38016072

Cyberangriffe auf Deutschland

Experten sorgen sich um die Sicherheit der Datennetze von Bundeswehr und Bundesregierung. So wurde das IT-Netz der deutschen Streitkräfte im Jahr 2015 71 Millionen mal von Hackern angegriffen. Das Datennetz der Bundesregierung wird rund 1,8 Millionen mal pro Jahr attackiert.

In dieser Ausgabe der Sendung „Frontal 21“ (ZDF) wird am Beispiel eines Cyberangriffs im Dezember 2015, welcher die Energieversorgung der westukrainischen Stadt Iwano-Frankowsk zum Ziel hatte, deutlich, welche Folgen eine unzureichende IT-Sicherheit für kritische Infrastrukturen haben kann.

Link: https://www.zdf.de/politik/frontal-21/cyberangriffe-auf-bundeswehr-und-bundesregierung-russische-100.html

3.3. Webseiten

Themenseite „Kritische Infrastrukturen“ des BBK

Infrastrukturen sind bedeutsame Versorgungssysteme unserer Gesellschaft. Sie sind nicht nur alltäglichen Störungen und Gefahren, sondern auch Extremereignissen zum Beispiel durch Naturgefahren, technischem oder menschlichem Versagen oder vorsätzlichen Handlungen ausgesetzt. Infrastrukturen sind komplexe Systeme, von denen eine Vielzahl von Versorgungsfunktionen abhängen. Häufig sind Infrastrukturen voneinander abhängig. Beispielsweise ist bei einem Ausfall der Stromversorgung auch die Informations- und Telekommunikationstechnologie betroffen und umgekehrt.

Auf den Informationsseiten des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) finden Sie u.a. Definitionen, Ansprechpartner, Aufgabenbereiche, Projekte sowie Publikationen zum Thema „Kritische Infrastrukturen“.

Link:
http://www.bbk.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html

3.4. Forschungsgruppen

Vernetzte IT-Sicherheit Kritischer Infrastrukturen (VeSiKi)

VeSiKi ist das wissenschaftliche Begleitforschungsprojekt des Förderschwerpunktes IT-Sicherheit für Kritische Infrastrukturen (ITS-KRITIS), welches vom Bundesministerium für Bildung und Forschung gefördert wird. Es beschäftigt sich mit neuen, sektorübergreifenden Ansätzen zur Beurteilung der IT-Sicherheit von kritischen Infrastrukturen, erarbeitet Verbesserungsvorschläge für bestehende technische sowie etablierte Prozesse, begleitet die Verbundprojekte und koordiniert die Zusammenarbeit.

VeSiKi verfolgt folgende Ziele:
• Entwicklung eines Rahmenwerks für Infrastrukturbetreiber
• Ausarbeitung von Empfehlungen für die Fortschreibung der Gesetzgebung
• Erstellung einer Standardisierungs-Roadmap

Nähere Informationen und eine Liste von Publikationen finden Sie unter folgendem Link:
https://www.itskritis.de/vernetzte-it-sicherheit-kritischer-infrastrukturen.html

3.5. Zeitschriften

Deutsche Wasserwerke ungeschützt im Internet

Auf ihrer Webseite Internetwache.org decken die Studenten Sebastian Neef und Tim Philipp Schäfers seit Jahren Sicherheitsprobleme im Netz auf. Jetzt haben die beiden Enthusiasten die digitalen Steuerungen mehrerer deutscher Wasserwerke, Blockheizkraftwerke und Biogasanlagen offen zugänglich im Internet entdeckt.

In einigen Fällen wäre es Unbefugten nach Analyse der IT-Experten offenbar möglich gewesen, die Anlagen nicht nur auszuspähen, sondern auch zu manipulieren - etwa die Pumpen in einem Wasserwerk. "Mich schockiert, wie leicht diese Anlagen zu finden waren und wie einfach Hacker sie mit Standardmethoden hätten sabotieren können", sagt Schäfers.

Quelle: Rosenbach, Marcel: Sicherheitslücke. Deutsche Wasserwerke ungeschützt im Internet, SPIEGEL Online, 15.07.2016

Link: http://www.spiegel.de/netzwelt/web/deutschland-sicherheitsluecke-wasserwerke-ungeschuetzt-im-internet-a-1103147.html

Eichhörnchen gegen Hacker 623 : 1

Eine neue Website macht mit einem Augenzwinkern auf eine bislang unterschätzte Gefahr für Stromnetze aufmerksam. Weltweit 623 Angriffe habe man schon Eichhörnchen zuschreiben können, heißt es auf cybersquirrel1.com. Hingegen gab es erst eine einzige erfolgreiche Infrastruktur-Attacke eines Staates. Mithilfe einer Übersichtskarte macht die Seite anschaulich, wo es in den vergangenen Jahrzehnten schon zu Problemen kam.

In die Wertung gehen nicht nur die Attacken von Eichhörnchen ein, die offenbar gern auf Strommasten klettern und an Kabeln nagen, sondern auch Fälle, in denen Vögel, Mäuse, Ratten und Waschbären für Betriebsstörungen verantwortlich waren. Für die Auflistung der Vorfälle dienen jeweils Meldungen örtlicher Zeitungen als Beleg.

Quelle: SPIEGEL Online: Angriffe auf kritische Infrastruktur. Eichhörnchen gegen Hacker 623 : 1, 14.01.2016

Link: http://www.spiegel.de/netzwelt/web/usa-eichhoernchen-sind-gefaehrlicher-fuer-stromnetze-als-hacker-a-1071832.html

Kritische Infrastrukturen und wie kritisch sie wirklich sind

Wie sicher sind Industrial Control Systems (ICS) – die Steuerungssysteme in industriellen Anlagen? Die Frage stellt sich besonders für kritische Infrastrukturen, die in den letzten Jahren wurden immer wieder zum Ziel von Cyberattacken wurden. Diese Anfälligkeit gefährdet den störungsfreien Betrieb von Prozessen, die für unsere moderne Welt überlebensnotwendig sind.

Die Webseite „Security-Insider“ stellt in diesem Artikel u.a. verschiedene Verwundbarkeits-Level und mögliche Ansätze zur Abhilfe (z.B. durch Patches) vor.

Quelle: Weyrauch, Rüdiger; Schmitz, Peter: Risiken für Industrial Control Systems. Kritische Infrastrukturen und wie kritisch sie wirklich sind, Security Insider, 05.01.2017

Link: http://www.security-insider.de/kritische-infrastrukturen-und-wie-kritisch-sie-wirklich-sind-a-569489/

IT-Sicherheitsgesetz: Wer was wann zu melden hat

Mit dem am 25. Juli 2015 in Kraft getretenen IT-Sicherheitsgesetz ist Deutschland Vorreiter im Kampf um die "Cybersicherheit". Die wichtigen Betreiber kritischer Infrastrukturen wurden damit verpflichtet, IT-Sicherheitsvorfälle dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden.

Wer dazu gehört und melden muss, wird in einer Messtabelle ermittelt, die vom BSI, dem Bundesamt für Bevölkerungsschutz und den Leitern der Branchenarbeitskreise der „UP KRITIS“ festgelegt wurde. Diese Tabelle wurde von Stefan Paris, dem für IT- und Cybersicherheit zuständigen Unterabteilungsleiter des Bundesinnenministeriums in Berlin vorgestellt. Zu den Meldepflichtigen gehören 70 deutsche Rechenzentren und Server-Farmen.

Quelle: Borchers, Detlef: IT-Sicherheitsgesetz: Wer was wann zu melden hat, heise online, 08.02.2016

Link: https://www.heise.de/newsticker/meldung/IT-Sicherheitsgesetz-Wer-was-wann-zu-melden-hat-3096885.html