



ZIM-Erfolgsbeispiel

IT-Sicherheit auch für die Kleinen

IT-Sicherheit ist nicht nur ein Thema für Großunternehmen. Auch kleinere Unternehmen müssen ihre Daten und ihre Infrastruktur schützen, insbesondere wenn diese als „Kritische Infrastruktur“ zum Funktionieren der Gesellschaft beiträgt. Das Netzwerk DiSiNet hat es sich zur Aufgabe gemacht, an kleinere Unternehmen angepasste Sicherheitslösungen für kritische Infrastrukturen zu entwickeln.

Produkte und Innovationen

IT-Sicherheit ist schon lange kein Randthema mehr, auch werden die Angriffsszenarien immer komplexer. Die Betriebssicherheit von Kritischen Infrastrukturen kann aber nicht nur durch Angriffe auf IT-Systeme kompromittiert werden, schon kleine Unachtsamkeiten in der Bedienung oder fehlende Informationen zu Sicherheitsbestimmungen können zu Unfällen mit großen Schäden führen. Im ZIM-Kooperationsnetzwerk „Digitalisierung und Sicherung kritischer Infrastrukturen (DiSiNet)“ haben sich deshalb KMUs aus verschiedenen Bereichen und mehrere Forschungseinrichtungen zusammengetan, um durch neue Produkte und neue Verfahren mehr Sicherheit für Kri-

tische Infrastrukturen zu gewährleisten. Beispielhaft werden zwei Projekte skizziert:

Im Projekt **Nano-Firewall** wurde eine kompakte, robuste und energiesparende Firewall zur Absicherung von IT-Netzwerken entwickelt. Die Nano-Firewall soll den unautorisierten Fremdzugriff auf Maschinen, Sensoren oder Gebäudefunktionen unterbinden. Das Firewall-System besteht aus einer äußerst kompakten Hardware-Plattform mit einer Größe von nur 22 x 29 mm. Somit kann sie flexibel in andere Geräte, wie z. B. Produktionsmaschinen oder Sensorsysteme, integriert werden. Die der Hardware zu Grunde liegende Technologie ist die „Embedding Component Techno-

logy“. Diese wird im Projekt für die komplexen Strukturen eines leistungsfähigen Controllers und seiner Peripherie angepasst. Neben der sehr kompakten Bauform wird hierdurch auch eine hohe Robustheit erzielt. Die Firewall übernimmt die Überwachung von Verbindungsanfragen und die Analyse des Datenverkehrs (Deep Packet Inspection). Ebenso sind Protokollkonverter implementiert, um eine inhaltsgesteuerte heuristische Überprüfung der Code-Segmente zu ermöglichen.

Ziel des Projektes **Scanbox** war die Entwicklung eines intelligenten Analysesystems zur Erhebung der Netzwerk- und Informationssicherheit. Anhand der Analyseergebnisse und einer intelligenten

Verknüpfung mit Wissensdatenbanken gibt diese dem Nutzer konkrete Handlungsempfehlungen zum Beheben oder Minimieren der identifizierten IT-Sicherheitsrisiken und überprüft die Wirksamkeit der Gegenmaßnahmen. Dies versetzt KMUs, die keine eigene IT-Abteilung besitzen, in die Lage, ihrem Kompetenzlevel entsprechend konkrete Handlungsempfehlungen zu erhalten, die leicht umsetzbar sind.

Der Markt und die Kunden

Da die am Netzwerk teilnehmenden Unternehmen aus vielen verschiedenen Bereichen kommen, sind deren Kundenanforderungen auch sehr inhomogen. Dies bietet die Chance, fachübergreifende

Infos zum Projekt

Laufzeit: 07/2016 bis 09/2019

Projektform: Kooperationsnetzwerke

Technologiefeld: IuK-Technologien

Ansprechpartner

Joern Kinzel
Technologie- und Gründerzentrum
Potsdam-Mittelmark GmbH
Potsdamer Straße 18A, 14513 Teltow
Telefon 03328 430 270
www.tgz.pm

Aktuelle Netzwerkpartner

- Andres Industries AG , Berlin
- DECOIT GmbH, Bremen
- Fast Lane Institute for Knowledge Transfer GmbH, Hamburg
- FOC-fibre optical components GmbH, Berlin
- HGT Heizungs- und Gebäudetechnik GmbH, Berlin
- INCOstartec GmbH, Teltow
- LANTECH Informationstechnik GmbH, Klingenberg
- RWS Railway Service GmbH, Neuenhagen, Brandenburg
- TelcoTech GmbH, Teltow/Berlin
- Human-Factor-Consult GmbH, Berlin (Projekt)
- Hochschule für nachhaltige Entwicklung Eberswalde
- Technische Hochschule Wildau
- Kirchheimer Kreis e.V. Klingenberg
- Technische Hochschule Brandenburg
- Technische Universität Berlin
- Havelländische Eisenbahn GmbH, Berlin
- hanseWasser Bremen GmbH, Bremen
- ENSO NETZ GmbH, Dresden
- Wasserverband Strausberg-Erkner (WSE)



Bestückte nano-Firewall im Größenvergleich

Lösungen anzubieten. Als Beispiel sei die Scanbox genannt, die sowohl bei Stadtwerken und öffentlichen Einrichtungen, als auch bei Kunden aus der Bahnindustrie Anwendung finden kann. Die nano-Firewall kann nicht nur als zusätzliche Hardware-Firewall für kleine Netzwerke eingesetzt werden, es kann sogar jedes per TCP/IP (Transmission Control Protocol/Internet Protocol) angebundene IoT-Device zusätzlich abgesichert werden. Somit besteht ein in den nächsten Jahren stark wachsender Markt.

Das Netzwerk

Das Netzwerk umfasst 14 Unternehmen, vier Forschungseinrichtungen und einen Verein. Während der Laufzeit wurden bereits fünf ZIM-Projekte bewilligt, zwei weitere ZIM-Projekte sowie ein BMBF-Projekt befinden sich in der

Antragsphase und weitere Projekte in der Entwicklung. Das Netzwerk wurde der Öffentlichkeit von der Netzwerkmanagementeinrichtung Technologie- und Gründerzentrum Potsdam-Mittelmark und den Netzwerkpartnern auf mehreren Messen, u. a. der Sicherheitsmesse it-sa in Nürnberg, vorgestellt. Die mittlerweile 19 Netzwerkpartner arbeiten auch nach Beendigung der Förderung zusammen.

Infos zum Programm

Das Zentrale Innovationsprogramm Mittelstand (ZIM) des Bundesministeriums für Wirtschaft und Energie fördert technologie- und branchenoffen:

- Einzelprojekte
 - Kooperationsprojekte
 - Innovationsnetzwerke
- sowie im Vorfeld Durchführbarkeitsstudien.

Infos und Beratung zu Innovationsnetzwerken

VDI/VDE Innovation + Technik GmbH
Telefon 030 310078-341
www.zim.de

Impressum

Herausgeber

Bundesministerium für Wirtschaft und Energie
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Stand

November 2020

Gestaltung

VDI/VDE-IT, Berlin

Bildnachweis

© AdobeStock/kras99 (Seite 1)
© Technologie- und Gründerzentrum Potsdam-Mittelmark GmbH (Seite 2)