SIEMENS

Presse

Wien, 7. Juli 2020

# Siemens und NATO CCDCOE vertiefen Zusammenarbeit bei Cyber-Sicherheit für kritische Infrastrukturen

- **Gemeinsame Schulungen gegen Cyber-Angriffe sind wesentlich für Schutz digitaler Stromnetze**
- **Wertvolle Erkenntnisse über Angriffe und Schwachstellen ermöglichen innovative Lösungen und sichere Produkte**

Siemens Smart Infrastructure und das NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) haben ein Memorandum of Understanding (MoU) unterzeichnet, um die Zusammenarbeit im Bereich der Cybersicherheit für kritische Infrastrukturen fortzusetzen. Die vom CCDCOE organisierte jährliche hochrangige Cyber-Verteidigungsübung „Locked Shields“ ist zentral für den gemeinsamen Aufbau von Verteidigungsfähigkeiten. Mit der neuen Vereinbarung intensivieren die beiden Parteien ihre bestehende Zusammenarbeit im Bereich Cyber-Sicherheits-trainings für Stromnetze. Durch das Training mit der Netzleittechnik Spectrum Power gewinnt Siemens wertvolle Erkenntnisse über mögliche Angriffspunkte. Gleichzeitig kann das Unternehmen neue, sicherheitsrelevante Funktionen oder Protokolle für seine Produkte und Lösungen umfassend testen.

Mit der Integration von mehr erneuerbaren und dezentralen Energiequellen hat sich in den vergangenen Jahren die Art und Weise, wie Stromnetze betrieben werden, grundlegend verändert. Deutlich zugenommen hat der Bedarf an Netzoptimierung, der Interaktion zwischen den Prosumern und die Anzahl neuer Marktteilnehmer. Da der Einsatz von Informations- und Kommunikationstechnologie in Übertragungs- und Verteilnetze zunimmt, führt die wachsende Zahl an Verknüpfungen zu mehr potentiellen Angriffspunkten in digitalen Stromnetzen. Folglich hat die Cyber-Sicherheit für Betreiber von Stromnetzen und Regierungsbehörden höchste Priorität.

**Intern Siemens AG Österreich**
Communications
Leitung: Katharina Swoboda

Siemensstraße 90
1210 Wien
Österreich

Seit 2010 findet die von der NATO CCDCOE organisiert jährliche Cyber-Verteidigungsübung „Locked Shields“ statt. Ziel ist es, Cyber-Reaktionsteams für die Verteidigung gegen massive Cyber-Angriffe auszubilden. Siemens arbeitet seit 2017 mit dem NATO CCDCOE zusammen, um Szenarien für Stromnetze in die Verteidigungsübung einzubeziehen. Dabei umfasst die Übung auch Systeme und Produkte von Siemens wie Spectrum Power oder Fernwirkgeräte des Typs Sicam A8000. Diese helfen dabei, komplexe Szenarien für das Stromnetz mit miteinander verbundenen und voneinander abhängigen Leitstellen und Umspannstationen zu bewältigen. In der Übung müssen die Verteidiger die Verteidigungslinien einer komplexen Infrastruktur mit verschiedenen Systemen und Anwendungen festlegen, die massiven Cyber-Angriffen standhalten sollen, die von einer großen Gruppe von Hackern ausgeführt werden. Die Cyber-Sicherheitsexperten lernen bei der Übung beispielsweise, wie die Stromversorgung aufrechterhalten werden kann, während sie Bedrohungen nachgehen, Angriffe melden und das System wiederherstellen. „Locked Shields“ ist eine Gelegenheit, durch Übungen, Schulungen und Zusammenarbeit im Bereich der Cyber-Verteidigungsoperationen zu lernen.

Robert Klaffus, CEO von Siemens Digital Grid sagte: "Stromnetze und alles, was mit ihnen verbunden ist, bilden das Rückgrat moderner Gesellschaften. Sie sind daher attraktive Ziele für Hacker. Die Erkenntnisse und Erfahrungen aus der Übung Locked Shields sind für die Sicherung und den Schutz von Stromnetzen von entscheidender Bedeutung. Durch die enge Zusammenarbeit mit dem NATO CCDCEO kann Siemens wertvolle Einblicke in neue Angriffsformen gewinnen und gleichzeitig herausfinden, wie wir den sich verändernden Herausforderungen der Cyber-Sicherheit in digitalen Stromnetzen begegnen können. Diese Erkenntnisse fließen in die Weiterentwicklung unseres Portfolios ein.“ Ein Beispiel für die Erprobung neuer Funktionen im Rahmen dieser Zusammenarbeit ist das offene Standardkommunikationsprotokoll OPC UA PUB/SUB, das bei vielen (IoT)Internet-of-Things-Anwendungen zum Einsatz kommt.

Oberst Jaak Tarien, Direktor des NATO CCDCEO sagte: „Unsere langfristige Zusammenarbeit mit Siemens bei der Schulung von Cyber-Experten zum Schutz kritischer Infrastrukturen im Allgemeinen und von Stromnetzen im Besonderen war ein wesentlicher Vorteil für die technischen Cyber-Verteidigungsübungen des NATO CCDCOE. Ziel der Vereinbarung ist, die Interaktion zwischen den verschiedenen Akteuren der Cyber-Verteidigung zu stärken sowie die Kooperation und den Ausstauch von Best Practice zu vertiefen. Dies hebt die Zusammenarbeit auf eine neue Ebene. Unsere Gesellschaften sind auf eine starke und resiliente kritische Infrastruktur angewiesen. Durch die Zusammenarbeit zur Verbesserung der Cyber-Sicherheit mit

wichtigen Partnern aus der Industrie wie Siemens Smart Infrastructure entsteht daher ein Mehrwert.“

**Ansprechpartner für Journalisten:**
Siemens AG Österreich
Johanna Bürger Tel.: +43 664 88555678
E-Mail: johanna.buerger@siemens.com

Folgen Sie uns auf Twitter: https://twitter.com/Siemens_Austria

**Siemens Smart Infrastructure (SI)** gestaltet den Markt für intelligente, anpassungsfähige Infrastruktur für heute und für die Zukunft. SI zielt auf die drängenden Herausforderungen der Urbanisierung und des Klimawandels durch die Verbindung von Energiesystemen, Gebäuden und Wirtschaftsbereichen. Siemens Smart Infrastructure bietet Kunden ein umfassendes, durchgängiges Portfolio aus einer Hand – mit Produkten, Systemen, Lösungen und Services vom Punkt der Erzeugung bis zur Nutzung der Energie. Mit einem zunehmend digitalisierten Ökosystem hilft SI seinen Kunden im Wettbewerb erfolgreich zu sein und der Gesellschaft, sich weiterzuentwickeln – und leistet dabei einen Beitrag zum Schutz unseres Planeten: SI creates environments that care. Der Hauptsitz von Siemens Smart Infrastructure befindet sich in Zug in der Schweiz. Das Unternehmen beschäftigt weltweit etwa 72.000 Mitarbeiterinnen und Mitarbeiter.

**Über Siemens Österreich**
Siemens Österreich zählt zu den führenden Technologieunternehmen des Landes. Insgesamt arbeiten für Siemens in Österreich rund 11.000 Menschen. Der Umsatz lag im Geschäftsjahr 2019 bei rund 3,5 Milliarden Euro. Die Geschäftstätigkeit konzentriert sich auf die Gebiete Elektrifizierung, Automatisierung und Digitalisierung. Dazu gehören im Wesentlichen Systeme und Dienstleistungen für die Energieerzeugung, -übertragung und -verteilung ebenso wie energieeffiziente Produkte und Lösungen für die Produktions-, Transport- und Gebäudetechnik bis hin zu Technologien für hochqualitative und integrierte Gesundheitsversorgung.
Automatisierungstechnologien, Software und Datenanalytik spielen in diesen Bereichen eine große Rolle. Mit seinen sechs Werken, weltweit tätigen Kompetenzzentren und regionaler Expertise in jedem Bundesland trägt Siemens Österreich nennenswert zur heimischen Wertschöpfung bei. Im abgelaufenen Geschäftsjahr betrug alleine das Fremdeinkaufsvolumen von Siemens Österreich bei rund 10.400 Lieferanten – etwa 6.500 davon aus Österreich – rund 1,2 Milliarden Euro. Siemens Österreich hat die Geschäftsverantwortung für den heimischen Markt sowie für weitere 20 Länder (Region Zentral- und Südosteuropa sowie Israel).
Weitere Informationen: www.siemens.at

Das **CCDCOE** ist ein von der NATO akkreditiertes Zentrum für Cyber-Verteidigung mit einem Fokus auf Forschung, Schulungen und praktische Übungen. Es repräsentiert eine Gemeinschaft von 25 Nationen, die einen 360-Grad-Blick auf die Cyber-Verteidigung bietet und über Fachwissen in den Bereichen Technologie, Strategie, Operationen und Recht verfügt.
Das Zentrum wird von seinen Mitgliedsstaaten personell und finanziell unterstützt, derzeit von Österreich, Belgien, Bulgarien, der Tschechischen Republik, Dänemark, Estland, Finnland, Frankreich, Deutschland, Griechenland, Ungarn, Italien, Lettland, Litauen, den Niederlanden, Norwegen, Polen, Portugal, Rumänien, der Slowakei, Spanien, Schweden, der Türkei, dem Vereinigten Königreich und den Vereinigten Staaten. Auch Kanada, Japan, Kroatien, Australien, Luxemburg, Irland, Montenegro, Slowenien, die Schweiz und Südkorea sind auf dem Weg, sich dem Zentrum anzuschließen.