

Siemens e NATO CCDCOE insieme per la cybersecurity delle infrastrutture critiche

- **Formazione congiunta contro i cyberattacchi per la protezione delle reti digitali**
- **Insight strategici su attacchi e vulnerabilità abilitano soluzioni innovative e prodotti più sicuri**

Siemens Smart Infrastructure e NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) hanno firmato un Memorandum of Understanding (MoU) per proseguire la cooperazione sulla cybersecurity delle infrastrutture critiche. CCDCOE ha organizzato l'esercitazione annuale di alto livello per la difesa cibernetica Locked Shields, pilastro fondamentale per lo sviluppo congiunto delle capacità difensive. Con il nuovo accordo, l'esistente cooperazione tra le parti in tema di formazione sulla cybersecurity delle reti digitali fa un ulteriore passo avanti. Facendo sperimentazione con il software per il controllo della rete Spectrum Power, Siemens è in grado di acquisire insight strategici su potenziali vettori di attacco e di testare approfonditamente nuove funzionalità o protocolli di sicurezza per i propri prodotti e soluzioni.

Negli ultimi anni le modalità con le quali si gestiscono le reti sono profondamente cambiate con l'integrazione di una quota crescente di rinnovabili e fonti di energia decentralizzate. Le necessità di ottimizzazione della rete e di interazione tra i prosumer e i nuovi attori presenti sul mercato sono in costante e significativa crescita. Con la tecnologia ICT sempre più presente nelle reti di distribuzione e trasmissione, le crescenti interconnessioni generano più vettori per potenziali attacchi alle reti elettriche digitali. Di conseguenza, la cybersecurity sale in cima alle priorità degli operatori e degli enti governativi.

Dal 2010, Locked Shields rappresenta l'esercitazione annuale sulla difesa cibernetica organizzata da NATO CCDCOE per la formazione di gruppi di esperti nella difesa dai cyberattacchi di notevole portata. Siemens ha iniziato a collaborare con NATO CCDCOE nel 2017 inserendo nell'esercitazione difensiva scenari relativi alla rete elettrica, attraverso sistemi e prodotti quali il Siemens Spectrum Power e le unità terminali remote Sicam A8000. Questi aiutano a prendere contatto con i complessi scenari della rete elettrica tramite centri di controllo e sottostazioni interconnesse e interdipendenti. Nell'esercitazione, i difensori devono impostare linee di protezione per un'infrastruttura complessa, inclusi diversi sistemi e applicazioni che dovrebbero resistere a massicci cyberattacchi eseguiti da un ampio gruppo di hacker. Mantenere accesi i riflettori in fase di ricerca delle minacce, segnalare gli attacchi e recuperare il sistema sono alcuni dei compiti impegnativi che gli esperti di sicurezza informatica imparano ad affrontare nel corso di questa esercitazione. Locked Shields è un'opportunità per imparare attraverso l'esercizio, la formazione e la cooperazione nel campo della difesa informatica.

Robert Klaffus, CEO di Siemens Digital Grid: "Le reti elettriche e tutto ciò che interconnettono danno forma alla spina dorsale delle società moderne e rappresentano quindi obiettivi attrattivi per gli hacker. L'apprendimento e l'esperienza tramite l'esercitazione Locked Shields sono essenziali per assicurare e proteggere le reti elettriche. Grazie alla cooperazione con NATO CCDCOE, Siemens può acquisire insight strategici su nuove forme di attacco e su come affrontare le nuove e in continua evoluzione sfide di cybersecurity nell'ambito delle reti elettriche digitali. Questi insight sono utilizzati per sviluppare ulteriormente il nostro portfolio." Un esempio di test su nuove funzionalità all'interno di questa cooperazione è il protocollo standard aperto di comunicazione OPC UA PUB/SUB, impiegato in molteplici applicazioni IoT.

Il Colonnello Jaak Tarien, Direttore di NATO CCDCOE: "La nostra cooperazione di lungo periodo con Siemens nella formazione di cyber esperti per la protezione delle infrastrutture critiche in generale e delle reti elettriche in particolare è stata una risorsa importante per le esercitazioni tecniche di difesa informatica di NATO CCDCOE. Con l'obiettivo di rafforzare l'interazione tra i diversi attori nell'ambito della difesa informatica, di approfondire la cooperazione e lo scambio di best practice, questo accordo porta la nostra cooperazione ad un nuovo livello. Le nostre società si basano su infrastrutture critiche forti e resilienti. Di conseguenza, c'è un valore reale nella nostra partnership che mira a far progredire la sicurezza informatica insieme ai partner industriali chiave quali Siemens Smart Infrastructure".

Contatti per i giornalisti:

Siemens Italia

Marco Latorre, mobile: +39 3421424322

e-mail: marco.latorre.ext@siemens.com

Le immagini sono disponibili sul sito www.siemens.it/press

Seguici su Twitter: www.twitter.com/Siemens_stampa

Siemens Smart Infrastructure (SI) dà forma al mercato delle infrastrutture intelligenti di oggi e di domani. Collegare sistemi energetici, edifici e industrie è la risposta alle sfide dell'urbanizzazione e del cambiamento climatico. SI offre ai clienti un portafoglio end-to-end completo da un'unica fonte - con prodotti, sistemi, soluzioni e servizi dal punto di generazione di energia fino al consumatore finale. Con un ecosistema sempre più digitalizzato, permette ai clienti di crescere e alle comunità di progredire, contribuendo a proteggere il pianeta. SI crea ambienti che si prendono cura di te. Siemens Smart Infrastructure ha la sua sede globale a Zug, in Svizzera, e conta circa 71.000 collaboratori in tutto il mondo.

Siemens è una multinazionale che si distingue per eccellenza ingegneristica, innovazione, qualità, affidabilità e internazionalità da oltre 170 anni. La società è attiva in tutto il mondo, concentrandosi nelle aree delle

infrastrutture intelligenti per edifici e sistemi energetici distribuiti, automazione e digitalizzazione nell'industria di processo e manifatturiera. Attraverso le società a gestione separata Siemens Energy, il business globale dell'energia di Siemens e Siemens Mobility, fornitore leader di soluzioni di mobilità intelligenti per il trasporto ferroviario e stradale, Siemens dà forma ai sistemi energetici di oggi e domani così come al mercato mondiale dei servizi passeggeri e merci. Grazie alla sua controllata quotata in borsa Siemens Healthineers AG e a Siemens Gamesa Renewable Energy (come parte di Siemens Energy), Siemens è tra le prime al mondo anche nel mercato della tecnologia medica e dei servizi sanitari digitali nonché nelle soluzioni ecocompatibili per la generazione di energia eolica onshore e offshore. Nell'anno fiscale 2019, conclusosi il 30 settembre 2019, Siemens ha generato un fatturato di 86,8 miliardi di euro e un utile netto di 5,6 miliardi di euro. Alla fine di settembre 2019, la società contava circa 385.000 collaboratori in tutto il mondo. www.siemens.com

Presente in Italia dal 1899, Siemens è una delle maggiori realtà industriali nel nostro Paese con centri di competenza su software industriale e mobilità elettrica, un centro tecnologico applicativo per l'Industria 4.0 e due stabilimenti produttivi. La società ha chiuso l'esercizio fiscale 2019 con un fatturato di oltre 2 miliardi di Euro. Per il secondo anno consecutivo, Siemens è certificata Top Employer Italia. www.siemens.it

CCDCOE è un hub per la difesa informatica accreditato dalla Nato che si focalizza su ricerca, formazione ed esercitazioni. Rappresenta una comunità di 25 nazioni fornendo una panoramica a 360° sulla cyber defence, con competenze tecnologiche, strategiche, operative e legali.

Il Centro è gestito e finanziato dagli stati membri, attualmente Austria, Belgio, Bulgaria, Repubblica Ceca, Danimarca, Estonia, Finlandia, Francia, Germania, Grecia, Ungheria, Italia, Lettonia, Lituania, Paesi Bassi, Norvegia, Polonia, Portogallo, Romania, Slovacchia, Spagna, Svezia, Turchia, Regno Unito e Stati Uniti. Canada, Giappone, Croazia, Australia, Lussemburgo, Irlanda, Montenegro, Slovenia, Svizzera e Corea del Sud stanno per aderire al Centro.