Comunicado de prensa conjunto

Press

Siemens, AES, Airbus, Allianz, Atos, Cisco, Dell Technologies, Deutsche Telekom, IBM, MHI, MSC, NXP, SGS, Total y TÜV SÜD

Munich, 14 de febrero, 2020

Los socios de la Carta de Confianza deciden nuevas medidas para una mayor seguridad cibernética

- **Ciberseguridad por defecto: Los productos de la próxima generación deben estar equipados con seguridad preconfigurada**
- **Nuevos socios: NTT, Infineon y el Instituto Hasso Plattner de Ingeniería Digital se unen en la Carta de Confianza**
- **La ciberseguridad se extendió a lo largo de la cadena de suministro: Numerosos proveedores cumplen los requisitos básicos de las empresas de la Carta de Confianza**
- **Campaña de educación para las pequeñas y medianas empresas y las escuelas: Los asociados de la Carta de Confianza proporcionan materiales de seguridad cibernética**

Los socios de la Carta de Confianza (CoT) han acordado entregar productos de próxima generación con una seguridad cibernética preestablecida, siguiendo una clara filosofía de "Seguridad por defecto". En la actualidad, no existen normas uniformes que regulen esta cuestión; muchos productos salen de la fábrica dependiendo únicamente de sistemas de seguridad que no ofrecen una protección integral. Los usuarios a menudo tienen que ajustar la configuración de seguridad después. Como primer paso, las empresas asociadas a la Carta han definido ahora qué características de seguridad deben estar presentes y activadas por defecto ben los productos de la próxima generación, desde las características de autenticación fuerte hasta la identidad única del producto y el requisito de que las contraseñas deben cambiarse en el primer uso.

Siemens AG
Werner-von-Siemens-Str.
180333 Munich
Germany

Siemens, AES, Airbus, Allianz, Atos, Cisco, Dell Technologies, Deutsche Telekom, IBM, MHI, MSC, NXP, SGS, Total and TÜV SÜD

The Los socios del CdT también creen que ninguna funcionalidad o posibilidad de conexión remota no documentada debe formar parte de la configuración inicial del dispositivo, otro aspecto que aún no es una regla general hoy en día. Todos estos requisitos se están desplegando ahora paso a paso dentro de las carteras pertinentes de las empresas miembros de la Carta de Fideicomiso.

"La ciberseguridad es un ingrediente clave para la confianza de nuestros clientes en todos nuestros negocios que ofrecen productos conectados digitalmente. También es la base para el éxito sostenible y el fundamento de un fuerte ecosistema", dice Roland Busch, director general adjunto, CTO, CHRO y miembro del consejo de administración de Siemens AG.

En la Conferencia de Seguridad de Munich en febrero de 2018, Siemens y ocho socios del sector industrial lanzaron por primera vez una carta conjunta para una mayor seguridad cibernética. Dos años después de la firma, la Carta de Confianza ha crecido a 17 miembros. Además de Siemens y la Conferencia de Seguridad de Munich, las empresas AES, Airbus, Allianz, Atos, Cisco, Dell Technologies, Deutsche Telekom, IBM, Mitsubishi Heavy Industries, NXP Semiconductors, SGS, Total y TÜV SÜD se han comprometido con el documento. Además, la Oficina Federal de Seguridad de la Información (BSI), el Centro Criptológico Nacional (CCN) y la Universidad Tecnológica de Graz acompañan el trabajo de la Carta como Socios Asociados. Hoy, la Carta de Confianza está ganando dos nuevos miembros en NTT, un proveedor de consultoría y servicios gestionados de TI de origen japonés, y el fabricante alemán de semiconductores Infineon Technologies AG. Con el Instituto Hasso Plattner de Ingeniería Digital GmbH (HPI), uno de los principales institutos de TI de Alemania también contribuye ahora a la iniciativa de ciberseguridad como Socio Asociado.

El año pasado, los asociados ya acordaron 17 requisitos básicos concretos con los que pueden aumentar la seguridad de sus cadenas de suministro. Desde entonces, numerosos proveedores de empresas de CdT ya se han comprometido a cumplir estos requisitos.

Siemens AG
Werner-von-Siemens-Str.
180333 Munich
Germany

Siemens, AES, Airbus, Allianz, Atos, Cisco, Dell Technologies, Deutsche Telekom, IBM, MHI, MSC, NXP, SGS, Total y TÜV SÜD

Siemens los ha estado introduciendo paso a paso desde el 15 de febrero de 2019, y han sido anclados internacionalmente y hechos vinculantes como parte de las condiciones generales de pedido. Esto afecta principalmente a los proveedores de componentes críticos para la seguridad, como software, procesadores o componentes electrónicos. Se espera que los proveedores existentes implementen los requisitos gradualmente si no se están cumpliendo ya. El objetivo es proteger mejor la cadena de suministro digital de los piratas informáticos. Entre los requisitos básicos figuran, por ejemplo, que los proveedores incorporen normas, procesos y métodos de seguridad en sus productos o servicios. Esto se refiere tanto a las características técnicas como a las medidas organizativas pertinentes a los productos, servicios y la correspondiente infraestructura de tecnología de la información. El objetivo en este caso es reducir los riesgos causados por las deficiencias de los programas informáticos y el malware. Los proveedores tienen la responsabilidad de llevar a cabo controles, pruebas y correcciones de seguridad con regularidad. Los socios del CdT también han acordado estos requisitos para ellos mismos. La cadena de suministros es el punto más débil del ecosistema de ciberseguridad de una empresa: El origen del 60 por ciento de esos incidentes cibernéticos, son las empresas más pequeñas las que se ven afectadas, según un estudio de Verizon.

Los asociados del CdT también han decidido promover la educación y la capacitación en cuestiones de seguridad cibernética, incluso para las pequeñas y medianas empresas (PYMES), que son cada vez más blanco de los ciberataques. Por ejemplo, en Alemania, la Carta de Confianza se asoció con la “Alianza para la Ciberseguridad” y elaboró un conjunto de materiales con una tarjeta de emergencia que explica rápida y fácilmente qué hacer en caso de un ciberataque. Además, los asociados han elaborado material de capacitación adicional que se pone a disposición de la PYME de forma gratuita. Con ello pretenden prevenir el ciberdelito, pero sobre todo poner de relieve las posibilidades de adoptar medidas eficaces de seguridad cibernética. Los asociados han elaborado una simulación especial de seguridad cibernética para las escuelas, a fin de que los estudiantes y los maestros tengan una visión general clara y fácilmente digerible de los problemas.

Siemens AG
Werner-von-Siemens-Str.
180333 Munich
Germany

Siemens, AES, Airbus, Allianz, Atos, Cisco, Dell Technologies, Deutsche Telekom, IBM, MHI, MSC, NXP, SGS, Total y TÜV SÜD

Según el Centro de Estudios Estratégicos e Internacionales, los ciberataques causarán más de 500.000 millones de euros en daños globales en 2018. Y las amenazas aumentan constantemente en un mundo digitalizado: Según Cisco, hay alrededor de 50.000 millones de dispositivos en red en uso en 2020, el doble que en 2015, y se espera que la cifra aumente a 500.000 millones en 2030.

El texto de la Carta de Fideicomiso se puede encontrar en:
www.charteroftrust.com
Puede encontrar este comunicado de prensa en sie.ag/2w9OXOs

Síguenos en Twitter: www.twitter.com/siemens_press

Persona de contacto para periodistas

Siemens
Florian Martini; Teléfono: +49 89 636 33446;
E-mail: florian.martini@siemens.com

AES
Gail Chalef; Teléfono: +1 703 682 6428 ; E-Mail: gail.chalef@aes.com

Airbus
Florian Taitsch; Teléfono: +49 89 3179 4644; E-mail: florian.taitsch@airbus.com
Ambra Canale; Teléfono: +49 89 31 79 99 29; E-mail: ambra.canale@airbus.com

Allianz
Daniel Aschoff; Teléfono: +49893800-18900;
E-mail: Daniel.Aschoff@allianz.com

Siemens, AES, Airbus, Allianz, Atos, Cisco, Dell Technologies, Deutsche Telekom, IBM, MHI, MSC, NXP, SGS, Total y TÜV SÜD

Atos

Lucie Duchateau; Teléfono: +33 7 62 85 35 10;

E-mail: lucie.duchateau@atos.net

Cisco

Jessica Tompkinson; Teléfono: +44 20 8824 3701;

E-mail: jetompki@cisco.com

Dell Technologies:

Media.Relations@Dell.com

Deutsche Telekom

Christian Fischer; Teléfono: +49 151 121 85073;

E-mail: christian.fischer03@telekom.de

IBM

Jonathan Sage; Teléfono: +44 7738310713;

E-mail: jonathan.sage@uk.ibm.com

MHI

Daniela Stawinoga-Carrington, Teléfono: +44 20 3480 7521,

E-mail: daniela_stawinoga-carrington@mhie.com

MSC

Johannes Schmid; Teléfono: +49 89 379794920;

E-mail: j.schmid@securityconference.de

NXP

Svend Buhl; Teléfono: +49 40 5613 2289;

E-mail: svend.buhl@nxp.com

SGS

Daniel Rüfenacht; Teléfono: +41 22 739 94 01;

E-mail: Daniel.Rufenacht@sgs.com

TÜV SÜD

Sabine Krömer; Teléfono: +49 151 5587 3235;

E-mail: Sabine.Kroemer@tuev-sued.de

Siemens AG (Berlín y Múnich) es una potencia tecnológica global que ha sido sinónimo de excelencia en ingeniería, innovación, calidad, fiabilidad e internacionalidad durante más de 170 años. La compañía está activa en todo el mundo, centrándose en las áreas de generación y distribución de energía, infraestructura inteligente para edificios y sistemas de energía, y la automatización y digitalización en las industrias de proceso y manufactura. A través de la empresa Siemens Mobility, gestionada por separado, es un proveedor líder de soluciones de movilidad inteligente para el ferrocarril y la carretera. transporte, Siemens está dando forma al mercado mundial de servicios de pasajeros y de carga. Debido a su participación mayoritaria en las empresas que cotizan en bolsa Siemens Healthineers AG y Siemens Gamesa Renewable Energy, Siemens es también un proveedor líder mundial de tecnología médica y servicios de salud digital, así como de tecnología respetuosa con el medio ambiente soluciones para la generación de energía eólica en tierra y en el mar. En el año fiscal 2019, que terminó el 30 de septiembre de 2019, Siemens generó unos ingresos de 86.800 millones de euros y unos ingresos netos de 5.600 millones de euros. A finales de septiembre de 2019, la compañía tenía alrededor de 385.000 empleados en todo el mundo. Más información en Internet en: www.siemens.com.

Siemens AG
Werner-von-Siemens-Str.
180333 Munich
Germany