

S2 Grupo y Cryptonics lanzan un sello de calidad pionero en ciberseguridad en blockchain para empresas

La empresa española S2 Grupo (especializada en ciberseguridad y gestión de sistemas críticos) junto a Cryptonics (spin-off de S2 Grupo especializada en ciberseguridad en blockchain) han lanzado sello de calidad pionero en ciberseguridad en la tecnología blockchain de las empresas. Asimismo, ambas compañías han anunciado la creación del Enterprise Blockchain Security Council (EBSec), una alianza abierta de empresas con un interés compartido en la adopción segura de sistemas blockchain y DLT

Bajo el nombre de Enterprise Blockchain Security Specification (EBSS), su objetivo es establecer una guía de buenas prácticas en este campo para mejorar la seguridad en este tipo de tecnología. Esto será de gran utilidad para los expertos de tecnologías de la información de las compañías que utilizan blockchain porque les permitirá seguir parámetros esenciales para ciberproteger adecuadamente sus negocios y organizaciones.

Para ello, ambas compañías han anunciado la creación del Enterprise Blockchain Security Council (EBSec), una alianza abierta de empresas con un interés compartido en la adopción segura de sistemas blockchain y DLT (Distributed Ledger Technology, registros de transacciones distribuidos). Por el momento, forman parte de esta alianza empresas de referencia internacional en el sector como son Solidified, empresa de auditoría de contratos inteligentes y de una plataforma bug bounty (programa de recompensas) que se especializa en auditorías de contratos inteligentes, y PARSIQ, líder en análisis de blockchain y especializada en la monitorización en tiempo real de activos digitales implementados en esta tecnología.

“Hasta ahora no existían estándares ni certificaciones de calidad en blockchain y cada vez son más las empresas que la utilizan. Esto dejaba un vacío en la ciberprotección de las empresas que hemos decidido cubrir con la creación de este sello de calidad pionero, que permitirá poder seguir una guía de buenas prácticas para la ciberprotección de blockchain”, ha explicado José Rosell, socio-director de S2 Grupo.

“Las blockchain están protegidas por criptografía avanzada que muchas veces se cree, erróneamente, que es irrompible con la tecnología actual. Esto significa que, en teoría, los activos digitales almacenados en libros de contabilidad distribuidos deberían ser extremadamente seguros. Sin embargo, hemos visto cómo los incidentes de ciberseguridad conducen al robo de activos de manera constante”, ha declarado Miguel A. Juan, socio-director de S2 Grupo.

“Prácticamente, cada semana nos encontramos con incidentes importantes o se revelan nuevas vulnerabilidades. La aparente inseguridad del espacio público de las blockchain ha empezado a afectar la reputación de la tecnología de contabilidad distribuida y, por tanto, obstaculiza gravemente la adopción empresarial. Esto hace que empresas e industrias enteras no vean con claridad cómo

utilizarla y, por tanto, es fundamental disponer de estándares que permitan hacerlo de forma cibersegura”, ha afirmado Stefan Beyer, CEO de Crytonics.

Tres problemas de ciberseguridad en DLT (Distributed Ledger Technology, registros de transacciones distribuidos)

Según han afirmado expertos de ciberseguridad de S2 Grupo y Crytonics los principales problemas de ciberseguridad de la tecnología ledger son:

1.- Cambio de paradigma: las empresas tienen que lidiar con nuevos paradigmas de seguridad a los que no están acostumbradas y carecen de directrices de buenas prácticas. Los sistemas descentralizados de blockchain se diferencian de los sistemas de TI tradicionales en que la seguridad de los activos ya no es un concepto centralizado, en el que los datos y otros recursos están encerrados en un servidor de caja negra en un escenario de tipo bóveda. Ahora, los activos están protegidos de forma transparente por protocolos criptográficos, claves criptográficas gestionadas por el usuario e incluso mediante reglas complejas en contratos inteligentes. Esto significa que

2.- Las malas prácticas: las malas prácticas en seguridad de la información son muy frecuentes en todos los sistemas, pero el impacto es peor en sistemas transparentes y descentralizados que dependen de la seguridad de las claves privadas.

3.- Falta de seguridad de los sistemas de información convencionales: los libros de contabilidad distribuidos y los contratos inteligentes son solo una pequeña parte de las aplicaciones típicas de blockchain. Por lo general, hay varias capas de software convencionales, que incluyen interfaces web, API, el software de nodo y las bases de datos. En muchos incidentes, el sistema es atacado a través de vulnerabilidades de los software tradicionales, no a través de la tecnología blockchain.

“El EBBS ha nacido por la necesidad de directrices generales de seguridad que las empresas puedan utilizar para aplicar un estándar mínimo de seguridad en sus operaciones. La especificación no pretende reemplazar las normas de seguridad existentes, como ISO / IEC 27001: 2013. Tampoco ofrece medidas de seguridad de bajo nivel para proporcionar código seguro, ya existen otras recomendaciones que cubren tecnologías específicas. Sin embargo, el EBSS se centra en las pautas generales y las políticas operativas que deberían estar en vigor en una empresa que desee adoptar la tecnología de ledger distribuida de forma cibersegura”, ha asegurado Stefan Beyer.

Datos de contacto:

Luis Núñez
667574131

Nota de prensa publicada en: [Madrid](#)

Categorías: [Telecomunicaciones Ciberseguridad](#)

<https://www.notasdeprensa.es>