

Link: <http://mundoenlinea.cl/2018/10/11/la-seguridad-es-un-habilitador-de-negocios/>

Sin duda la ciberseguridad se ha vuelto un tema relevante en la actualidad para las distintas industrias, esto por los exitosos casos de ciberataques en que se han visto vulnerados distintos sistemas, ya sea en la industria bancaria, de salud, de energía, entre otros. Ante esto, y en el marco de una nueva edición de Cybersec, Congreso de Ciberseguridad organizado por la **Universidad de Santiago**, Stephen Fallas, Advanced Security Architect for the Cisco Global Security Group for Latin America, se refirió a cómo los hackers atacan infraestructura crítica y las implicancias para la IoT industrial. En esa línea entregó distintas recomendaciones para los procesos y advertencias que deben tener en cuenta las distintas industrias para evitar ser víctimas de ataques cibernéticos. "Durante el 2017 al menos el 47% de la industria de infraestructuras críticas, como energía, transporte o salud, por ejemplo, tuvieron dos brechas de ciberataques. Ante esto lo importante es que las empresas se pregunten ¿qué están dejando de hacer? y de esta manera poder construir una estrategia correcta", aseguró Fallas. Junto con esto, el profesional identificó tres elementos importantes que resultan claves para evitar ciberataques en las Infraestructuras Críticas: Visibilidad para analizar el tráfico de la red "A la hora de proteger una infraestructura crítica es importante saber cómo funciona, con que elementos opera y conocer los que son parte en este flujo de negocios, porque no se puede proteger lo que uno no ve. En ese sentido la visibilidad es fundamente en este tipo de entornos para poder mitigar esa situación", comentó el ejecutivo. Monitorear la infraestructura. Identificar y alertar sobre flujos de tráfico anormales. Inteligencia amenazas. Conocimiento de los ataques existentes y los vectores de comunicación. Prevención instrucciones. Bloquee ataques, explotación e inteligencia. Seguridad DNS. Asegurar la comunicación saliente a dominios seguros. Segmentar asegura el ecosistema: "Con la segmentación podemos buscar una estrategia para aislar componentes que están generando un comportamiento malicioso. Hoy en día todos tenemos equipos de capa 2 y 3 y es importante utilizarlos para poder aislar de una forma más automatizada este tipo de amenazas que se están generando", afirmó el experto. Infraestructura. Proteja las comunicaciones entrantes, salientes y entre sí. Escalable. Separe los sistemas y usuarios basados por roles y políticas, reducir la complejidad de la ciberseguridad. Acceso basado identidad. Restrinja la conexión de sistemas y dispositivos conocidos. Perfiles. Evalúe y determine las características y la postura para ver si un dispositivo se está portando de forma anómala.



The screenshot shows the article page on the 'Mundo en Línea' website. The article title is "La seguridad es un habilitador de negocios" by Stephen Fallas, dated October 11, 2018. The article text is partially visible, discussing the importance of cybersecurity in critical infrastructure. The page also features a sidebar with product recommendations, including a Miele robotic vacuum cleaner and a SanDisk Connect Wireless Stick. The website's navigation menu and search bar are visible at the top.