Identificación de necesidades de monitoreo de ciberseguridad enfocado en el segmento PyMEs

Eduardo Casanovas, Carlos Tapia

Instituto Universitario Aeronáutico, Facultad de Ingeniería, Av. Fuerza Aérea 6500, Córdoba, Provincia de Córdoba, Argentina
ecasanovas@iua.edu.ar, ctapia@iua.edu.ar

Resumen. Habiendo relevado las necesidades comunes de las organizaciones respecto de Ciberseguridad, con foco en el rubro PyME, se procederá a clarificar los recursos, metodologías y know-how necesario para crear un Centro de Operaciones de Ciberseguridad que permita monitorear aspectos de Seguridad Informática de organizaciones, adaptado a la realidad de cada tipo de organización, por lo que se plantearán diferentes casos de uso.

Palabras clave. ciberseguridad, SOC, Security Operations Center, Centro de Operaciones de Seguridad, logs, monitoreo.

1 Introducción

Las organizaciones, ya sean con fines de lucro o sin fines de lucro y de cualquier rubro de industria, en su enorme mayoría no cuentan con un área de Seguridad Informática y mucho menos poseen personal especializado dedicado para monitorear los eventos de ciberseguridad o ataques informáticos que pudieran surgir. Por ataques informáticos, se entiendo infecciones de virus informáticos, robo de información, acceso no autorizado a sistema, suplantación o robo de identidad, interrupción o corte total del servicio de sistemas y daño a imagen en sitios web. Todas estas son potenciales vicisitudes que cualquier organización, más específicamente en el segmento PyME, con un mínimo de infraestructura tecnológica o exposición a Internet puede sufrir y justamente un Centro de Operaciones de Ciberseguridad puede ayudar a mitigar los riesgos.

5 Referencias bibliográficas:

[1] Pulgar Luntero, R. (2016). Plan de negocios para la creación de una empresa que oferte servicios de monitoreo de incidentes informáticos llamado SOC (security operation center) para instituciones financieras en la ciudad de Quito. Recuperado el 07/03/2018. http://dspace.udla.edu.ec/bitstream/33000/5809/1/UDLA-EC-TIC-2016-78.pdf

[2] Bidou, R. (2002). Security Operation Center Concepts & Implementation. Recuperado el 07/03/2018. http://iv2-technologies.com/SOCConceptAndImplementation.pdf

[3] Zimmerman, C. (2014, Octubre 2014). Ten Strategies of a World-Class Cybersecurity Operations Center. Recuperado el 04/03/2018. https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf

[4] Crowley, C. (2017, Mayo 2017). Future SOC: SANS 2017 Security Operations Center Survey. Recuperado el 04/03/2018. https://www.sans.org/reading-room/whitepapers/analyst/future-soc-2017-security-operations-center-survey-37785

[5] Aliyev, I. (2016, 24/10/2016). Security Operations Center (SOC) mission and success factors. Recuperado el 09/03/2018. https://www.linkedin.com/pulse/security-operations-center-soc-mission-success-ilgar/