NOTA DE PRENSA

ISMS Forum presenta los Ciberejecicios Multisectoriales 2022 poniendo a prueba las capacidades de detección y respuesta de 30 compañías españolas

ISMS Forum -International Information Security Community-, a través de su iniciativa Cyber Security Centre (CSC), ha realizado la Octava Edición de los Ciberejercicios Multisectoriales, también denominados como "CiberMS 2022", con el objetivo de generar concienciación sobre los riesgos en ciberseguridad y fomentar las buenas prácticas entre 30 grandes organizaciones participantes, que se fundamentan en la evaluación de la resiliencia, la medición del estado de madurez y la mejora de las capacidades de detección y respuesta de las organizaciones en materia de ciberseguridad.

La presente edición del proyecto ha sido organizada por ISMS Forum junto con el apoyo de terceras entidades privadas. Entre ellas, se encuentra KPMG como empresa evaluadora, la cual ha analizado los resultados obtenidos en el desarrollo del ejercicio. Asimismo, Riskrecon, Cymulate, ISMSForum y en conjunto SMARTFENSE y BeyGoo, han participado bajo el rol de atacantes a las entidades con el objetivo de poder evaluar su respuesta.

La iniciativa se ha desarrollado a través de un ejercicio de ciberseguridad consistente en la realización de un conjunto de pruebas de seguridad y simulacros de ataque a los sistemas de las 30 grandes compañías españolas participantes de este año. Las pruebas

han estado exclusivamente orientadas a poner a prueba los mecanismos de seguridad lógica de la entidad, así como la cultura de seguridad de los empleados y su capacidad para detectar y comunicar de forma correcta estos incidentes a los equipos de respuesta.

La primera prueba se basa en el reconocimiento, en dicha prueba se podrá ver el Rating de ciberseguridad de las compañías participantes, así como evaluar su situación de riesgo IT. La segunda prueba se centra en la seguridad perimetral de correo electrónico, seguridad de navegación y adaptación a amenazas recientes. En tercer lugar, se buscan credenciales expuestas de los usuarios en la Dark web, sitios de leaks, phishing en redes sociales y dominios y subdominios expuestos que están siendo desatendidos por la organización y pueden generar un riesgo. La prueba final está basada en la exfiltración, a través de un autoejecutable.

Las pruebas han permitido contrastar la relación entre ataques lanzados y el impacto originado en la entidad participante, a la vez que comparar los resultados con otras entidades.

Para la valoración de los ejercicios se están siguiendo estándares de mercado como MITRE ATT&CK y NIST CSF, que permiten ofrecer un reflejo de las empresas participantes frente a las evaluaciones generales de mercado emitidas por los diferentes analistas más relevantes.

La Octava Edición de los Ciberejercicios Multisectoriales continúa progresando, de manera que las evaluaciones parciales realizadas en base a los ataques ya han dejado de manifiesto una idea general sobre el estado del arte y algunos aspectos a tener en cuenta para la continua mejora de la protección y respuesta ante incidentes.

La finalidad de los Ciberejercicios Multisectoriales es generar concienciación sobre los riesgos existentes a todos los niveles, reforzar la comunicación y la coordinación, entrenar a las empresas en la gestión de incidentes de ciberseguridad y generar buenas prácticas sobre ciberseguridad en las organizaciones.

Aunque hay un mantenimiento de la probabilidad de sufrir un Data Breach Event y un Ransomware Event, la tendencia es positiva en la gestión del riesgo, aunque hay aspectos importantes a seguir trabajando.

Un año más, los CiberMS ponen de manifiesto el importante papel que tiene el sector privado en la ciberseguridad nacional y el bienestar de los ciudadanos, así como los beneficios de la colaboración público-privada. Para ello, es necesario seguir innovando y fomentando estas iniciativas, por este motivo, la Asociación insta a las compañías españolas del sector a participar en la siguiente edición de los Ciberejercicios Multisectoriales.