“Es clave el papel de los CISOs en las empresas para gestionar los incidentes de seguridad”

Daniel García, director gerente de ISMS Forum, explica el momento actual que vive la ciberseguridad en las organizaciones

Daniel García, director gerente de ISMS Forum, explica el momento actual que vive la ciberseguridad en las organizaciones desde el primer **Cyber Resilience Forum** que tendrá lugar en Madrid el próximo 30 de enero para ahondar en este concepto clave de ciberresiliencia como capacidad de recuperar el negocio tras un incidente.

Para este experto, el impacto de la normativa nueva como el Reglamento Dora y la NIS 2 van a ayudar a que las empresas consideren como estratégico las políticas de ciberseguridad.

¿Podría explicarnos qué objetivos y qué temas se van a abordar a lo largo de este I Cyber Resilience Forum, evento que abre la temporada de su entidad?

Es importante destacar que desde ISMS Forum veníamos trabajando en la seguridad de la información y en el área de la protección de datos, pero quizás uno de esos dominios no tenía una presencia mayor, sobre todo ahora con la nueva regulación comunitaria que se avecina como es el Reglamento Dora a nivel financiero, el recientemente aprobado de Inteligencia Artificial o la directiva NIS 2.

Estas normativas son palancas que nos hacen pensar que la resiliencia cobra mayor relevancia ahora, que hace unos años. No solo viene acompañada de un nivel de compliance sino que además se han desarrollado buenas prácticas en las empresas para generar la posición o el nivel de control de nuestros activos y resolución de incidentes.

Nosotros venimos haciendo buenas prácticas al respecto como son los ciberejercicios, el proyecto que elaboramos, en colaboración con el Departamento de Seguridad Nacional, en el cual ponemos la atención en una crisis de componente ciber.

En estos ejercicios, los participantes, siendo grandes empresas, deben poner a prueba sus estrategias y manuales de gestión de crisis para resolver graves situaciones. En ella, deben poner a prueba su capacidad de resiliencia. Esto es demostrar que entrenando sus capacidades de gestión e incidentes pueden volver de forma rápida a su situación de negocio inicial.

Este nuevo entorno regulatorio nos ha hecho pensar que era necesario celebrar un evento donde la ciberresiliencia tuviera su protagonismo, entendida en su componente normativo por su adaptación futura a varios reglamentos, pero también porque tendremos en unos meses a disposición la NIS 2 donde conoceremos el texto definitivo.

En este entorno, el entrenamiento de capacidades a día de hoy es una realidad e invitamos a las empresas a que hagan este tipo de simulacros para que sepan realmente que sus protocolos de actuación funcionan ante la llegada de cualquier ciberincidente.

Uno de los platos fuertes de este primer evento será la firma del acuerdo de colaboración establecido recientemente entre ISMS Foum y Business Continuity Institute (BCI). Cuando se habla de ciberresiliencia hay que tener en cuenta dos conceptos: la gestión de crisis y la continuidad del negocio.

Estamos hablando de que el BCI es la mayor referencia a nivel global y continuidad de negocio. Allí estará presente el presidente del BCI España , Manel Herrer.

¿Cuál es el papel del CISO en este concepto de ciberresiliencia?

Nosotros pensamos que es clave. De hecho, en este I Cyber Resilience Forum del próximo 30 de enero habrá una mesa redonda que aborde su involucración en esta actividad clave para las empresas.

Gran parte de estas amenazas son ciberincientes, así lo ha dicho el propio World Economic Forum en su in-

forme anual donde en su Top 5 hay hitos relacionados con la ciberseguridad donde la IA y su impacto es un elemento clave, al igual que la continuidad de negocio y la ciberresiliencia.

Llegar a la figura del CISO nos permite elevar a la categoría de gobierno la responsabilidad sobre este tipo de entrenamientos y de capa de protección que insisto, no solo son protección, sino que está basada en la mejora de las capacidades para dar respuesta a esos ciberincidentes.

Desde el punto de vista de la ciberresiliencia, ¿cuáles son esas claves que debe tener en cuenta una organización para una pronta recuperación del negocio, una vez sufre el ciberataque?

Uno de los puntos de interés para una mayor efectividad de nuestra actividad, no es tanto elevar el mensaje desde un punto de vista técnico, sino de forma más inteligible.

En este evento de ciberresiliencia tendremos un primer panel donde contaremos con CISOs, expertos de gran relevancia (cada uno en su sector de actividad), donde van a explicar al resto de asistentes el nivel de responsabilidad y concienciación que tiene la figura del responsable de seguridad para captar las amenazas y gestionar de manera eficiente un incidente.

Creemos que es importante que las empresas inviertan en esa materia y se den cuenta de lo importante que es tener políticas de ciberseguridad, claras y alineadas con su negocio respectivo. No es un prisma técnico, sino que queremos dar un mensaje de gobierno a nivel de ciberseguridad para conocer, de la mejor manera posible, cuáles son las estrategias que nos pueden ayudar a reforzar ese nivel de resiliencia lo mejor posible.

En este contexto, el entorno regulatorio se complica con la llegada del Reglamento Dora y la directiva NIS 2.

¿Cómo cree que va a impactar en las organizaciones el cumplimiento de este nuevo marco normativo?

Son dos directivas muy exigentes que profundizan en lo estratégico que es la ciberseguridad y la ciberresiliencia.

El Reglamento Dora está más centrado en el sector financiero, como ámbito acotado de aplicación. En el caso de la NIS 2 puede afectar a pequeñas y grandes empresas al mismo tiempo.

En este primer evento que organizamos tenemos una mesa debate en el que pedimos a los reguladores que nos expliquen lo que está por venir y cómo nos tendremos que adaptar a este marco normativo, donde la protección es clave tanto a nivel propio como respecto a terceros.

Al final ese mensaje que queremos lanzar, no es solo dirigido al CISO, sino que también queremos que llegue a todas las organizaciones. Estamos seguros que hay empresas que no conocen que NIS 2 es aplicable a ellos y que habrá un órgano supervisor que establezca sanciones sino cumplen con la normativa.

Al final, responder a un ciberataque supone a las empresas contar con un protocolo propio, muy específico a cada empresa.

¿Qué rasgos a nivel general lo definen desde su punto de vista?

Hace algunos años, el nivel de madurez en este ámbito era limitado, salvando el sector financiero que siempre ha estado muy regulado, lo que ha hecho que su desarrollo llegase antes que en otras actividades económicas.

En aquel momento sus manuales de gestión de crisis estaban orientados a otras cuestiones como un incendio u otro tipo de problemas de inoperatividad relacionado con su actividad. Al final la evolución de esa problemática es distinta, ahora hay que destacar que ciertos incidentes han generado una alerta en el sector que ha permitido un nivel de madurez mayor.

En 2019 sucedieron una serie de incidentes que generaron un nivel de alerta sobre el que podría ocurrir en nuestro entorno, sobre esas empresas que colaboran en nuestra gestión de activos y que forman parte de esa cadena de suministros.

Por ello, desde ISMS Forum lanzamos un primer estudio llamado ***Guía para la gestión de crisis por ciberincidente en la cadena de suministro*** donde evaluábamos situaciones posibles y generamos un procedimiento de actuación. Dicho procedimiento de actuación fue creado por un grupo de CISOs lo que nos permitía tener un punto común de actuación que podría ser aplicable en otras empresas. Hay que darse cuenta que aunque la figura del CISO se entendía como un elemento estratégico para determinadas compañías con una facturación destacada, el resto de las empresas aun no lo había asimilado.

Todo ha sido como consecuencia de una evolución lógica de las actividades que venimos realizando en los últimos años A partir de ahí, nos dimos cuenta que era necesario el entrenamiento y la mejora de las capacidades para una mejor respuesta.

En ese entorno realizamos e impulsamos algunos entregables y pusimos en marcha el ejercicio ya comentado, en colaboración con el Departamento de Seguridad Nacional, convirtiéndose en el más grande que se hace a nivel multisectorial en España, donde sometemos a cierto estrés a unas 35 empresas.

Desde esta perspectiva les pedimos a estas organizaciones, que involucrasen al resto de la organización. Se trataba de que tanto la dirección financiera, como de recursos humanos, comunicación y marketing estén alienados con lo que hacen las empresas en materia de ciberseguridad

En todo este escenario el papel del Delegado de Protección de Datos es importante para saber en qué momento hay que notificar la brecha de seguridad y también gestionar el momento previo a esta situación. Las empresas deben gestionar canales de comunicación interna para mejorar dichos ciberincidentes y reducir su inoperatividad tras sufrir un ciberincidente.

ISMS Forum, en colaboración con la cátedra de la Universidad Complutense de Madrid, trabajan en el ***Indicador de Ciberinseguridad***, donde se busca analizar el impacto económico global de que las organizaciones no adopten medidas para frenar esos ciberincidentes. Es otra llamada de atención que hacemos a las organizaciones. No es tanto un gasto como una inversión para protegerse frente a los ciberincidentes.