IX Foro de la Ciberseguridad

“Estamos instalados en una sociedad de la inmediatez que no es capaz de contrastar la información que le llega”

23 de septiembre de 2020. ISMS Forum, junto con el Cyber Security Centre, celebró el IX Foro de la Ciberseguridad el pasado jueves 17 de septiembre de 2020. Más de 200 profesionales del sector se dieron cita de forma online en este evento que ha tratado temas como la creación del Foro Nacional de Ciberseguridad, la Revisión de la directiva NIS, o los retos para el CISO en la nueva Estrategia Digital.

Iván Sánchez, CISO de Sanitas y miembro de la Junta Directiva de ISMS Forum, fue el encargado de inaugurar el acto. “Como cada año, desde el Cyber Security Centre de ISMS Forum, organizamos el Foro de la Ciberseguridad con el objetivo de fomentar el intercambio de conocimientos entre los principales actores y expertos implicados en el sector para impulsar y contribuir a la mejora de la ciberseguridad en España. Promovemos la consolidación de un estado de conciencia sobre la necesidad de la Ciberseguridad para controlar y gestionar los riesgos derivados de la dependencia actual de la sociedad respecto a las Tecnologías de la Información y la Comunicación (TIC), siendo un aspecto clave para asegurar el desarrollo socio-económico del país”.

Una aproximación a la Revisión de la Directiva NIS

La ponencia que inauguró el encuentro fue impartida por **Boryana Hristova**, Legal Officer (European Commission), DG Communications Networks, Content and Technology, Cybersecurity and Digital Privacy, que realizó una aproximación de lo que conllevará la Revisión de la Directiva NIS.

“La Directiva NIS, aprobada en julio de 2016 por la Comisión Europea, es la primera legislación horizontal de ciberseguridad de la Unión Europea. Se basa en tres pilares, el primero relacionado con la capacidad de los Estados miembros para mejorar, a través de la redacción de estrategias nacionales de ciberseguridad, equipos de respuesta ante emergencias informáticas (CSIRTs), o un punto central de contacto (SPOC) para mantener la cooperación con la Unión Europea. El segundo pilar está dedicado a la cooperación europea, donde todas las autoridades se sientan juntas y discuten las diferentes formas de aplicar la directiva y cómo alinear sus enfoques hacia un punto en común. Por último, queda el tercer pilar, núcleo de la directiva, que está dedicado a la responsabilidad de las empresas, las cuales tienen que cumplir con ciertas medidas de seguridad y notificar los incidentes relevantes”, comentó Boryana al inicio de su presentación.

Desde su aprobación en 2016, la aplicación de la Directiva NIS se ha realizado de forma distinta en cada país y a ritmos diferentes. Por este motivo, se han realizado continuas visitas a todos los Estados miembros con el objetivo de encontrar las carencias y fortalezas, “todos los Estados miembros pudieron darnos su opinión de cómo veían la aplicación de la Directiva, cuáles eran las deficiencias en referencia al derecho internacional, si es que las había, y cuál era el valor añadido, con lo que pudimos

constatar que teníamos enfoques muy diferentes institucionalmente, centralizados en algunos Estados miembros y muy descentralizados en otros".

Las observaciones han concluido que los Estados miembros han recibido demasiada libertad a la hora de aplicar la directiva, transponerla y adaptarla a sus leyes nacionales. Si bien es cierto que cada país partía desde un punto diferente, ya que existían Estados miembros que ya estaban relativamente concienciados en materia de ciberseguridad y contaban con leyes y estrategias propias, para otros países, todo esto era completamente nuevo, "han aplicado metodologías muy diferentes que han conducido a la identificación de diferentes tipos de servicios, unos identificaron unos pocos servicios generales, mientras que otros consiguieron entrar más en detalle", comentó la experta, a lo que añadió "no contamos con un nivel uniforme, y desde la perspectiva del mercado interno esto es un problema, ya que el objetivo de la Directiva es asegurar que hasta el eslabón más débil estará protegido".

"Nos encontramos con una gran segmentación en la notificación de incidentes, recibiendo quejas de que las empresas no cumplen con los diferentes procedimientos de notificación, plazos, plantillas, etc. por lo que también estamos estudiando el papel de las autoridades competentes, CSIRTs, y corporaciones a nivel europeo", comentó Hristova. La Directiva NIS trata asegurar la respuesta a las nuevas necesidades en ciberseguridad de los países teniendo en cuenta la creciente digitalización de la sociedad a través de un aumento de la preparación nacional e internacional que permita mejorar la resiliencia de los sectores económicos clave y la reducción de la fragmentación de los mercados internos, todo esto mediante la armonización de los requerimientos aplicados a las entidades del sector.

"Todavía queda mucho trabajo por hacer, no puedo comentar nada en términos de contenido porque nadie sabe lo que va a salir de esta revisión, lo que sí puedo pediros es que participéis en la consulta pública que sigue abierta hasta el próximo 2 de octubre", concluyó la experta.

Contra los ciberatacantes: inteligencia de amenazas

La siguiente intervención la protagonizó **Staffan Truvé**, CTO & Co-founder de Recorded Future, que habló sobre la "inteligencia de amenazas", a través de la cual se puede identificar y analizar las ciberamenazas de una empresa. El ponente recalcó el proceso de cribado de datos que se lleva a cabo en este método, que consiste en la examinación de forma contextual de los datos para detectar problemas reales e implementar soluciones específicas para cada uno. "Cuando se produce un ciberataque, lo más importante es actuar rápido para tener la oportunidad no solo de estar informado sino de mantener el control y tomar medidas (…) saber qué vulnerabilidades están presentes en los productos, qué actores amenazantes las están utilizando y recabar información de todo tipo".

Según Staffan, "lo bueno de la inteligencia de amenazas es que te ayuda a ver tu empresa como la ven "los malos", puedes salir al "exterior", donde se encuentran los cibercriminales, para mirar en el interior de tu empresa y ver exactamente las mismas

cosas que los atacantes ven, así estableces un seguimiento de cómo está siendo usada o abusada tu marca y qué está pasando en Internet (…) es frecuente encontrar debates en los foros clandestinos donde se habla de los ataques, y si los rastreas, no solo puedes mejorar tu propia seguridad, también la de tus socios".

El experto también habló sobre la "inteligencia predictiva de amenazas", que consiste en ser capaz de entender que algo va a suceder antes de que lo haga, pasando de lo descriptivo a lo prescriptivo, "se puede empezar a recomendar lo que hay que evitar", comentó.

La primera mesa redonda, **"Security delivery acceleration with SECaaS"**, contó con la participación de **Elena Cerrada**, Country Manager (Forcepoint), **Pedro Viñuales**, Global Presales Manager (Cytomic), **José Luis Laguna**, Director Systems Engineering (Fortinet), **Fernando Anaya**, Country Manager (Proofpoint), **José de la Cruz**, Technical Director Iberia (Trend Micro), **Samuel Bonete**, Regional Sales and Technical Director Iberia (Netskope), **Joaquín Gómez**, NSX Sales Specialist (VMware), y como moderador **Iván Sánchez**, CISO (Sanitas) y miembro de la Junta Directiva de ISMS Forum. La mesa giró en torno al modelo Security as a Service.

Las empresas se han visto en la necesidad de acelerar sus procesos de transformación digital, específicamente en el entorno de las tecnologías de la información, para comenzar a consumir aplicaciones corporativas en formato SaaS y servicios de infraestructura (IaaS y PaaS). Este proceso ha generado la pérdida de control sobre las aplicaciones corporativas y sobre la propia infraestructura del *Data Center*, llevando a un aumento de los costes de la seguridad de red, entre otras posibles consecuencias a nivel de productividad, motivados por la deslocalización de los usuarios de la red corporativa. Esto desemboca en la necesidad de repensar la seguridad de red y comenzar a planificar un modelo de seguridad de red evolucionada del modelo on-prem a consumirla como un servicio.

De izquierda a derecha, Iván Sánchez, Elena Cerrada y Samuel Bonete.

Presentación del Foro Nacional de Ciberseguridad

La siguiente ponencia vino de la mano de **Mar López**, Jefa del Departamento de Ciberseguridad del Departamento de Seguridad Nacional (DSN), que realizó una presentación del Foro Nacional de Ciberseguridad.

"Señores, nos dijeron que nos coordináramos, ahora lo estamos, por lo que les toca a ustedes, los que están ahí sentados, asociaciones como ISMS Forum y otras que forman parte del foro, coordinarse y compartir conocimientos. El sector privado siempre nos ha demandado esto, pues ahora somos nosotros quienes se lo demandamos. Para apoyar los pasos en esa colaboración que necesitamos entre todos, se crea el Foro Nacional de Ciberseguridad, una iniciativa del Consejo de Seguridad Nacional que aparece por primera vez en la Estrategia Nacional de Ciberseguridad de 2019, y está compuesto por representantes de la sociedad civil, expertos independientes, el sector privado, la Academia, asociaciones y entidades sin ánimo de lucro, con el objetivo de generar conocimiento sobre oportunidades, desafíos y amenazas a la ciberseguridad nacional", comenzó Mar López.

"Tenemos una misión y visión concretas. En primer lugar, colaborar en el desarrollo de la Estrategia Nacional de Ciberseguridad y la consecución de sus objetivos, mediante el establecimiento de sinergias público-privadas que permitan dotar de una mayor protección a la sociedad española, y en segundo lugar, articular y cohesionar un entorno de colaboración público-privada que, a través de diferentes líneas de acción, genere el máximo conocimiento sobre los desafíos a la Seguridad Nacional en el ciberespacio, ya sean oportunidades o amenazas, y siempre en colaboración con el Consejo Nacional de Ciberseguridad", explicó la ponente.

El Consejo Nacional de Ciberseguridad es el principal líder del equipo, junto con una estructura basada en una Presidencia correspondiente al Departamento de Seguridad Nacional, y dos Vicepresidencias a cargo de INCIBE y el CCN, además de 16 Vocalías, la Comisión Permanente de Ciberseguridad y otros actores que representaran ampliamente a la sociedad civil, sin limitar la posibilidad de convocar a otros representantes. Se trata de un equipo multidisciplinar responsable de establecer la priorización de actuaciones que recoge la Estrategia de ciberseguridad y de elevar propuestas al Consejo para su ejecución y puesta en marcha.

Integración, flexibilidad, unidad de acción, transparencia y accesibilidad son algunos de los valores que constituyen este foro. Por este motivo, se plantea como un evento multidisciplinar y participativo, creando y dando acceso a diferentes oportunidades en materia de ciberseguridad. Para ello, "se han aprobado tres líneas específicas de la Estrategia Nacional de Ciberseguridad, que son: la Cultura de Ciberseguridad, el impulso a la industria y a la I+D+i, y la formación, capacitación y talento en ciberseguridad", según Mar.

"Nos queda mucho por hacer, pero para avanzar necesitamos la contribución de todos, y especialmente de marcos como este de ISMS Forum", añadió la experta al final de su presentación.

Mar López en el IX Foro de la Ciberseguridad.

"A río revuelto, ganancia de estafadores" es el título de la ponencia que impartió **Carles Solé**, CISO de Banco Santander España y miembro de la Junta Directiva de ISMS Forum.

Carles hizo eco de cómo los ciberdelincuentes se aprovechan de cualquier situación para cometer fraudes online. Ejemplo de ello fue el huracán Katrina, donde los estafadores online sacaron partido de la gran campaña de ayuda humanitaria que se creó para timar a miles de personas. Aunque el ejemplo más claro es el actual, puesto que, como señala el ponente, la situación de incertidumbre, desinformación, teletrabajo y confinamiento, ha llevado a que muchos se lancen al mercado online sin ser conscientes de sus consecuencias. "Estamos instalados en una sociedad de la inmediatez que no es capaz de contrastar la información que le llega o a la que accede (…) lo que se ha visto durante esta pandemia, más allá de las campañas de phishing bancario, han sido campañas de estafas, muchas de ellas provenientes de aplicaciones de seguimiento de la Covid-19 en un mapa, y la aplicación funcionaba, pero sin darte cuenta estaba entrando en tu equipo. También hemos visto el clásico pdf que entra por mail o el ataque a los equipos domésticos de los usuarios a través de los que consiguen entrar a las empresas", declaró el experto.

"Tenemos que erradicar este mal entre todos. La primera de las acciones es la concienciación, explicar a nuestros ciudadanos o clientes que estas cosas ocurren, nosotros somos la primera defensa para no caer en estas redes. La segunda de las acciones reside en la importancia de compartir información, el conocimiento de que otras compañías los han tenido y cómo funcionan nos hace estar un paso por delante. La tercera y última acción consiste en saber lidiar con lo anómalo, ya que siempre estamos expuestos a los riesgos, y al igual que nosotros avanzamos, los cibercriminales también", comentó Carles.

La ponencia de **Lucas Varela**, Digital Security en CaixaBank, trató sobre los orígenes del ramsonware. “Con un ramson pequeñito yo puedo afectar a uno o varios ordenadores de particulares, pero el premio que puedo sacar de eso es mucho más limitado que en la industria. Si yo infecto una máquina de una gran compañía, desde esa máquina puedo adentrarme en toda la organización para lanzar un malware masivo y obtener mayor beneficio” comentó el experto.

Asimismo, Lucas hizo referencia a la profesionalización de aquellos que se dedican al cibercrimen, "¿Qué te va a costar más, lo que yo te voy a cobrar o tener tu negocio parado durante x meses parado? (…) muchas veces la gente no entiende por qué los cibercriminales se dedican a eso, son gente muy profesional, que ganan mucho dinero, algo que les incentiva para crear aún más grupos, y cuentan con un gran nivel de sofistificación e industrialización".

Lucas Varela en el IX Foro de la Ciberseguridad.

Zetro Trust, supervisión frente a confianza

La siguiente ponencia vino de la mano de **John Kindervag**, Creator of Zero Trust y Field CTO en Palo Alto Networks, que explicó qué es Zero Trust y su importancia para la empresa.

“Zero Trust ha eliminado el concepto de confianza para la empresa”, declaró el experto. Según Kindervag, las empresas no deben confiar automáticamente en nada que se encuentre tanto dentro como fuera de sus limitaciones. Deben ser precavidas y verificar todo lo que intente conectarse a sus sistemas antes de darles acceso. “Zero Trust se basa en la focalización de los resultados empresariales, con un diseño de dentro hacia fuera, siempre vigilando quién o qué necesita acceso, e inspeccionando y registrando todo el tráfico”, comentó.

“Para conseguir un entorno Zero Trust es preciso definir la superficie que vamos a proteger, mapear los flujos de transacción, contar con un arquitecto experto en Zero Trust, crear una política Zero Trust y, por supuesto, mantener una supervisión constante de la red”, añadió Kindervag.

“Enabling Zero Trust for the new enterprise workflow” fue el título de la segunda mesa redonda, compuesta por **Enric Máñez**, Enterprise Security Sales Specialist, Senior (Akamai Technologies), **Ricardo Hernández,** Regional Sales Manager Spain & Portugal (ForeScout Technologies), **Jorge Hurtado**, Vice President EMEA (Cipher), **Álvaro García**, Senior Sales Engineer (Crowdstrike), y como moderador **Jesús Mérida**, CISO (Iberia).

Como ya venía diciendo John Kindervag en la ponencia anterior, en numerosas ocasiones se presupone la seguridad en los usuarios, los activos, y los recursos, cuando la realidad es que no existe ninguna confianza implícita en ubicaciones o redes específicas, sino que la autenticación y autorización son funciones previas y esenciales. Zero Trust es una respuesta a la necesidad actual en un contexto de pandemia en el que dependemos de usuarios remotos, dispositivos personales, y microservicios en Cloud en los que pueden circular datos sensibles. Por este motivo, se ha convertido en una prioridad el proteger recursos (activos, servicios, cuentas, permisos, etc.), y no segmentos de red. La mesa giró en torno a este debate con una conclusión muy clara para nuestros ponentes, “Zero Trust es una arquitectura, no un producto ni un fabricante, es un conjunto de soluciones que tienen que formar un todo para la seguridad, lo que tenemos ahora nos vale, pero en el nuevo mundo donde se está moviendo todo, no nos va a valer, busquemos la ventaja competitiva”.

De izquierda a derecha, Jesús Mérida, Jorge Hurtado y Ricardo Hernández.

La presentación del **Estudio del nivel de madurez en ciberseguridad de la empresa española** corrió a cargo del Observatorio de Ciberseguridad, y como representantes del mismo, contamos con **Toni García**, CISO en Grupo DAMM y miembro de la Junta

Directiva de ISMS Forum, **Santiago Minguito**, BISO Europe en PepsiCo y miembro de la Junta Directiva de ISMS Forum, y **Óscar Sánchez**, CISO en Puig y miembro de la Junta Directiva de ISMS Forum.

El objetivo de este estudio es analizar el nivel de madurez, evolución y nuevos fenómenos en el ámbito de la seguridad de la información, así como generar indicadores nacionales sobre el estado de la ciberseguridad en empresas y entidades privadas y públicas. Asimismo, se presenta como un divulgador de conocimiento e investigación a través de la creación de métricas y referencias nacionales, y la interlocución con instituciones y reguladores.

"Más del 60% de las empresas cuentan con una política donde se definen los roles y responsabilidades, junto con los requerimientos legales y regulatorios, dentro del marco de los procesos de gobierno y gestión del riesgo de ciberseguridad. Cerca del 50% de las empresas identifican y comunican las dependencias y los requisitos de los servicios y funciones críticas, asociadas a la misión, visión y objetivos de la organización. Sin embargo, el inventario de dispositivos, sistemas, aplicaciones y recursos de información solo es completo en un tercio de la muestra", comentó Santiago Minguito, a lo que añadió "hasta un 50% de las empresas mantienen identificadas y documentadas las vulnerabilidades y amenazas de ciberseguridad, analizando el riesgo en base a la probabilidad e impacto en el negocio, pero solo el 30% de la muestra manifiesta que los procesos de gestión del riesgo, así como el nivel de tolerancia, están establecidos, acordados e informados con las partes interesadas. En relación a los procesos de gestión del riesgo de la cadena de subministro, predomina (40%) la existencia de un proceso de gestión del riesgo de terceros y el establecimiento de las medidas en los contratos, pero no se auditan".

En cuanto a la protección de los sistemas y activos de información, más del 40% de las empresas manifiesta documentar los procesos y procedimientos, y más del 50% identifican los datos, pero los protegen de manera parcial. "Casi la mitad de las empresas encuestadas manifiesta la existencia de una gestión de identidades y accesos en base al principio de menor privilegio y segregación de funciones, sin embargo, en la gestión del cambio, si bien la mitad de los encuestados afirma la realización de un mantenimiento de los sistemas de información de forma controlada, los accesos no se auditan", declaró el ponente.

Thomas Rid, Professor of Strategic Studies en la Johns Hopkins University's School of Advanced International Studies fue el encargado de poner el broche final al IX Foro de la Ciberseguridad con su ponencia "Active Measures: The secret history of disinformation and political warfare". Thomas articuló su presentación alrededor de Ladislav Bittman y la operación "V-NEPTUN".

Un año más, el IX Foro de la Ciberseguridad del Cyber Security Centre e ISMS Forum se consolidó como uno de los mayores foros nacionales en el que más de 200 asistentes online disfrutaron de debates de alto rango en materia de Ciberseguridad.

Esta jornada ha sido posible gracias al apoyo de Palo Alto, Recorded Future, Akamai, Cipher, Crowdstrike, Cytomic, Forcepoint, Forescout, Fortinet, Netskope, Proofpoint, TrendMicro y VMware.

Esta jornada ha sido posible gracias al apoyo de Forcepoint, OneTrust Privacy, Riskrecon y Grupo SIA.

Sobre ISMS Forum

ISMS Forum -International Information Security Community- es una organización sin ánimo de lucro fundada en enero de 2007 para promover el desarrollo, conocimiento y cultura de la Seguridad de la Información en España y actuar en beneficio de toda la comunidad implicada en el sector. Creada con una vocación plural y abierta, se configura como un foro especializado de debate para empresas, organizaciones públicas y privadas, investigadores y profesionales donde colaborar, compartir experiencias y conocer los últimos avances y desarrollos en materia de Seguridad de la Información. ISMS Forum cuenta con más de 250 empresas asociadas y más de 1.250 profesionales asociados. La Asociación es ya, por tanto, la mayor red activa de organizaciones y expertos comprometidos con la Seguridad de la Información en España.

Contacto

Raquel García – Responsable de Comunicación Externa y Relaciones Públicas

rgarcia@ismsforum.es

Twitter: @ISMSForum

LinkedIn: ISMS Forum

Teléfono: +34 600 87 19 69