Amenazas internas en tu empresa: ¿Por qué es importante una defensa proactiva y protegerte del "insider"

OneseQ explica junto a Kymatio por qué es necesario evaluar las amenazas internas y el riesgo que pueden generar los propios usuarios y la importancia de la defensa proactiva en estos casos.

Madrid, 3 de febrero de 2021.- Según un estudio realizado por Ponemon Institute, tras el inicio de la pandemia, **el 76% de las organizaciones han experimentado una o más violaciones de datos**, sin embargo, más de la mitad (54%) no cuenta con planes para responder a los riesgos internos.

Razón por la cual OneseQ (el área de ciberseguridad de Alhambra IT) y Kymatio, compañía experta en gestión del ciberriesgo de empleados, se alían con el fin de impulsar la **proactividad de las organizaciones** frente a las posibles amenazas internas.

Aunque no se trata de un riesgo nuevo, sigue siendo una de las principales causas de **fuga de datos**. En este último año, por causas derivadas de la pandemia: menor seguridad a raíz del teletrabajo, aumento del agotamiento de los empleados, despistes… se ha vuelto una cuestión a tratar con prioridad ya que, según el mismo estudio, los empleados tienen **un 85% más de probabilidades de filtrar archivos confidenciales** ahora que antes de la COVID-19.

¿Cuáles son los riesgos internos?

A esta y otras preguntas dieron respuesta José María Ochoa, Cybersecurity Area Maneger de OneseQ y César González, Responsable de Ciberseguridad y Producto de Kymatio, en un webinar titulado **"¿No crees que confías demasiado en tus propios usuarios?**", celebrado el jueves 28 de enero de 2021.

Los ponentes, en primer lugar, explicaron en qué consiste una amenaza interna (supone un **compromiso de credenciales y sistemas** por parte de una entidad externa) y explicaron los distintos tipos que existen.

El Cybersecurity Area Manager de OneseQ, compañía especializada en **identificar, proteger, detectar, responder y recuperar en el ámbito de la seguridad de las compañías**, recalcó que para que esto ocurra, deben darse dos supuestos:

1. Tener o haber tenido **acceso de manera autorizada** a la red o a los datos de la empresa.
2. **Exceder o usar** intencionadamente, bajo extorsión o por descuido ese acceso.

Cuando se dan ambos supuestos es cuando se ven afectadas negativamente la **confidencialidad, integridad o disponibilidad** de la información, los sistemas o los recursos de la organización.

Además, Ochoa explicó que debemos tener muy en cuenta que el 20% de los ataques de ciberseguridad se deben a **usuarios indignados con poder de acción en las empresas**, por lo que cabe destacar que este tipo de *insiders* no solo conocen las políticas, procedimientos y tecnología de su organización, sino que también son conscientes de sus **vulnerabilidades**: políticas y procedimientos impuestos, fallos técnicos explotables, etc.

Sea cual sea el tipo de amenaza, **debemos superarla con inteligencia**.

¿Cómo detectar riesgos internos?

Ambas compañías identificaron la **defensa proactiva** como la clave para frenar este tipo de ataques. "Las empresas, por lo general, ejercen una respuesta reactiva cuando realmente debería ser proactiva, es la única forma de llevar a cabo una correcta gobernanza. Sobre todo, en estos momentos en los que nuestras compañías están **más expuestas**, a la vez que nuestros **entornos están menos controlados**", recalcó José María Ochoa.

Con el objetivo de evitar las amenazas internas, OneseQ, de la mano de Kymantio, ofrece la tecnología necesaria para poder localizar el riesgo y solucionarlo antes de que sea demasiado tarde. Todo ello, a través de la plataforma Kymatio, un SaaS que **identifica, analiza, evalúa y proporciona** todo lo necesario para tratar los **riesgos internos de origen humano** relativos a seguridad de la información**.**

César González, Responsable de Ciberseguridad y Producto de Kymatio, mostró cómo gracias a Kymatio podemos conocer los niveles de **formación, capacidad y actitud (entre otros) de los empleados**. Y es que solo a partir de ese punto podemos establecer mecanismos para paliar las deficiencias en estos ámbitos y avanzar en la gobernanza de la seguridad de la compañía.

El punto diferencial de esta herramienta frente a otras es su **aspecto social**, ya que, además de definir los privilegios de cada usuario y de definir los conocimientos sobre ciberseguridad que cada usuario debe tener, incorpora la **psicología para la generación de mapas de riesgo**, en los que se analiza a todos los empleados de la compañía. De tal forma que el departamento de RRHH está totalmente involucrado en este asunto, con el objetivo de proteger la compañía.

González explicó en detalle cómo Kymatio permite:

1. Gestionar el riesgo mediante un plan de prevención del ciberriesgo de empleados
2. Evaluar las necesidades de los usuarios
3. Fortalecer los conocimientos de los usuarios
4. Predecir el riesgo real

Cabe destacar cómo ambos ponentes coincidieron en la idea de que nos encontramos en un momento muy peligroso, en el que no podemos bajar la guardia, ya que la **ingeniería social** es cada vez más dirigida y eficaz.

"Hemos llegado a identificar ataques de *phishing* que se dirigían a personas con una gran carga de trabajo precisamente por ese hecho. A causa de la saturación y los despistes potenciados por la fatiga, el porcentaje de éxito de los atacantes es muy alto. Los atacantes son conscientes de

cómo afectan cuestiones como el estado de ánimo de los trabajadores o el malestar dentro de las compañías y lo usan a su favor", relató Ochoa.

Para finalizar, José María Ochoa, concluye: "Kymatio se trata del complemento perfecto del **control SIEM o del SOC**. Además, favorece el empoderamiento del CISO, ya que le permite centrarse en estrategias para prevenir el riesgo".

El webinar "¿No crees que confías demasiado en tus propios usuarios?" se enmarca en el ciclo de webinars **"Ciberseguridad 360"** organizado por OneseQ, junto a Kymatio, Netskope y Qualys, cuyo objetivo es mostrar a los asistentes cómo pueden **aumentar su seguridad de manera exponencial** teniendo en cuenta una serie de puntos clave como son: los ataques desde dentro, la seguridad del Cloud y Office 365 y la protección del Endpont.

Próximas fechas:

"Securiza tus entornos Cloud y Office 365" – Jueves 11 de febrero de 11h a 12h.

"Protege completamente tu endpoint de forma proactiva". – Jueves 18 de febrero 11h a 12h.

Inscríbete aquí

Más información sobre soluciones y servicios de ciberseguridad: www.oneseq.es