Evalúa el estado de la ciberseguridad en tu organización

Los riesgos en cuanto a la ciberseguridad en tu organización se incrementan, en la medida que el ecosistema digital se expandiendo a nivel global. En esta línea, y desde una perspectiva de ciberseguridad, los dos últimos años han presentado desafíos en distintas áreas.

El “Boom” del trabajo remoto ha multiplicado la cantidad de conexiones y puntos de trabajo en línea, pero con un costo. Las brechas de seguridad han sido muy importantes y publicitadas, con importantes impactos económicos y reputacionales.

Pero la ciberseguridad no es un problema de unos pocos, o sólo de las grandes corporaciones; el Ransomware ha estado en su pico más alto (con un aumento del 105% durante el 2021 de acuerdo con Fortune) y atacando de manera preferente a la pequeña y mediana empresa.

El trabajo remoto y el trabajo híbrido han demostrado que son factibles y están para quedarse. Sin embargo, pese a presentar muchas bondades, también presentan un incremento del riesgo para la ciberseguridad en tu organización.

Y los ciberdelincuentes así lo han hecho notar. Ellos, han sabido tomar ventaja de las brechas y vulnerabilidades de

seguridad que presentaron las empresas y negocios, Sobre todo, en esta primera etapa de acomodo a la nueva realidad de entornos híbridos y remotos.

Es de destacar que, aunque muchas empresas grandes y corporaciones han sufrido brechas de seguridad, han sido las pequeñas y medianas empresas las victimas más fáciles; debido a su falta de recursos y conocimiento de seguridad.

Si a esto le añadimos que los ataques a este segmento de empresas (y a todas en general) se están convirtiendo en más frecuentes, dirigidos y complejos; tenemos una realidad particularmente dura para el segmento de pequeña y mediana empresa.

Consecuencias de un ataque para la ciberseguridad en tu organización

Las consecuencias de un ciberataque pueden ser devastadoras para la ciberseguridad en tu organización, pudiendo generar:

- Daños reputacionales al publicarse información confidencial o conversaciones privadas.
- Pérdida de negocios o de propiedad intelectual debido a que información confidencial llega a la competencia.
- Demandas o sanciones por incumplimiento de contratos o regulaciones, como acuerdos de confidencialidad o leyes de protección de datos personales.
- Pérdida total de información vital para la operación.
- Horas, días o semanas durante las cuales no se podrá

operar ya que los equipos han sido afectados
- Pérdida de dinero por robos o engaños.

Y estas consecuencias no se limitan a solamente la empresa afectada, ya que cualquier impacto que afecte las operaciones de una empresa puede perjudicar a otras que dependan de sus servicios o productos, o, en casos más graves, puede poner en riesgo el bienestar del público en general.

Debido a esto es necesario ver a la ciberseguridad como una necesidad general, siendo vital fortalecer la postura de ciberseguridad a nivel país.

Esta noción tiene que ser acompañada de legislaciones fuertes que exijan a los distintos sectores económicos generar controles de ciberseguridad apropiados de acuerdo con su nivel de riesgo.

En el caso de nuestro país contamos con ciertas legislaciones e iniciativas en proceso de implementación (por ejemplo: ley de delitos informáticos, ley de protección de datos personales, iniciativas de protección de activos críticos nacionales, CSIRT nacional y reglamento de ciberseguridad para el sistema bancario, entre otras.).

Sin embargo, todavía nos encontramos en un nivel de madurez inicial en comparación con otros países, incluso de la región.

Como empresas privadas, uno de los primeros pasos que debemos

tomar es el de entender nuestro estado de ciberseguridad, ya que cada empresa forma parte de un sistema de múltiples dependencias, y cómo nos encontramos tanto con respecto al "benchmark" de empresas de nuestra misma categoría y sector, como respecto al estado esperado de ciberseguridad (aquel estado objetivo que nos indica que estamos lo suficientemente seguros, para el tipo de actividades que realizamos).

Estudio sobre ciberseguridad en empresas peruanas

En respuesta a esta necesidad, Axus con el patrocinio de la Cámara de Comercio e Industria de Lima (CCL) está desarrollando un estudio que reflejará la realidad del **estado de la ciberseguridad en el Perú**. Éste estudio está basado en hechos (fact-based) y servirá como guía y punto de referencia para mejorar la postura de ciberseguridad en las empresas peruanas en general.

Creemos que este estudio es importante, ya que la información a la que se puede acceder actualmente se encuentra sesgadas a marcas específicas, no considera a las pequeñas y microempresas (las cuales son el grueso de las empresas peruanas) o son estudios a nivel regional y carecen de la granularidad necesaria sobre la realidad peruana.

Axus Advisory Group y la **Cámara de Comercio de Lima** han desarrollado una metodología de análisis que permite conocer el grado de concientización que poseen las empresas peruanas sobre la ciberseguridad, así como medir qué tan preparadas se encuentran para defenderse ante la creciente ola de ciberataques.

El estudio se encuentra basado el Modelo de Cultura Organizacional en Ciberseguridad desarrollado por la Dra. Keri Pearlson y el Dr. Keman Huang del MIT, y evalúa los mecanismos de gestión de las organizaciones y los comportamientos de los colaboradores para prevenir y proteger a la organización ante ataques cibernéticos.

Adicionalmente, evalúa, considerando herramientas y procedimientos, el nivel de control y de implementación de buenas prácticas que tiene cada organización, respecto a los requerimientos de normativas y directrices como ISO 27001, NIST y los Controles Críticos de Seguridad del *Center for Internet Security*.

El estudio del **estado de la ciberseguridad en el Perú** tiene como objetivo convertirse en el informe de referencia sobre la ciberseguridad en el país, proporcionándole a las empresas peruanas una visión sobre los principales puntos de mejora a nivel Perú, los cuales, unidos a sus respectivas realidades individuales, les permitirán orientar y alinear sus esfuerzos individuales de fortalecimiento frente a las amenazas cibernéticas existentes.

Para completar la encuesta, ***Ingresa aquí***.

Asimismo, las personas que participen del estudio automáticamente serán consideradas en el sorteo de una Tablet (fecha de sorteo: 31 de mayo). Y además, podrán gestionar una reunión con el equipo de especialistas de **Axus**, para analizar sus resultados en el estudio, y evaluar cómo se encuentra su

organización respecto a la industria.