TEMA: EMPRESAS PROPENSAS A LA CIBERDELINCUENCIA

PROBLEMÁTICA: Las Mypes no se encuentran preparadas para la ciberdelincuencia

INTEGRANTES:

Yossi Evelyn Jauregui Quispe

Juan Saul Natividad Villanueva

Francisco Jose Hernández Alarcón

Joseph Eduardo Flores Solis

Franklin Alí Moza Villalobos

INTRODUCCIÓN:

Hoy en día la tecnología es parte fundamental de las funciones vitales para el desarrollo de una empresa y su ejecución. La información y los diversos procesos se encuentran almacenados en complejos sistemas informáticos, los cuales tienen que tener diversas características para su funcionamiento y calidad, una de ellas y muy importantes es la seguridad, ya que la filtración de esos datos puede ser perjudicial en ámbitos personales, sociales y económicos para la organización.

Es asi que, una empresa siempre está vulnerable, pues con la evolución de la tecnología para el desarrollo adecuado de cualquier actividad, existe también una contraparte que evoluciona con ella, esta viene hacer la delincuencia cibernética. ¿Pero que es la delincuencia cibernética?, mas adelante se explicara ello

Por otro lado, Esta problemática a afectado a grandes empresas, las cuales se encuentran activas bastantes años y con la experiencia necesaria para hacer frente a este tipo de delincuencia, sin embargo, muchas han tenido serias perdidas por ello

Un ejemplo la Alerta Integrada de Seguridad Digital de la Presidencia del Consejo de ministros (PCM) alertó la filtración de datos sensibles de más de 40 mil usuarios del Ministerio de Salud (Minsa). Los datos se estarían ofertando en el foro ‘breached.to’, por el usuario “Leriwey”, en la base de datos se ofertaba información sensible de los pacientes del Minsa como, nombres completos, documentos de identidad, historial clínico, dirección entre otros. Incluso incluso datos sensibles del Ministerio de Salud.

En este contexto, que nos preguntamos si las grandes empresas con experiencia y más preparación están propensas a sufrir a taques, las empresas pequeñas o pymes ¿Se encuentran preparadas para afrontar dicho problema?

DESARROLLO:

DESARROLLO 1:

Respondiendo a la primera pregunta En la actualidad, es bastante habitual escuchar sobre delitos cometidos a través de las tecnologías digitales. Unos ilícitos que no solo afectan cada vez a más personas, sino que son altamente dañinos. Estos son delitos de cibercriminalidad, que se efectúan a través de una red, ya sea pública o privada, y que atentan contra la seguridad. A estas prácticas ilegales se les conoce más comúnmente como ciberdelincuencia**.** Existen varios tipos de ciberdelincuencia como por ejemplo los más comunes: **Malware**: actuaciones en las que entran en juego todos los tipos de virus informáticos que tienen como fin dañar, suprimir o bloquear algunos datos de un sistema informático. **Robo de identidad.** Quizás la forma más común de ciberdelincuencia. Puede presentarse de diferentes maneras. Por mencionar algunas de las más practicadas, tenemos: **Phishing o suplantación de identidad**: es un tipo de delito de cibercriminalidad que persigue engañar al usuario para hacerse con sus datos de acceso de diferentes cuentas personales, así como datos bancarios y de tarjeta de crédito, haciéndose pasar por una entidad o empresa de su confianza. **Keylogging:** práctica de spyware silencioso mediante el cual se registran las pulsaciones en el teclado o la información introducida en distintos campos, con el fin de robar los datos personales de acceso de un usuario como el nombre, las contraseñas o los códigos bancarios, sin que este lo sepa. Mediante el uso indebido de la tecnología, los delincuentes cibernéticos pueden llevar a las empresas a la ruina e incluso arruinar la vida a las personas. Muchos países y organizaciones de todo el mundo luchan para poner un alto a los delincuentes cibernéticos y contribuir a la seguridad de los sistemas. Nosotros debemos tener mucho cuidado con nuestras informaciones personales para no ser víctima de los ciberdelincuentes.

DESARROLLO 2:

En segundo lugar, respondiendo a la segunda pregunta, Diversos estudios afirman que todas las industrias y organizaciones, no importando el tamaño o sector son susceptibles a padecer delitos informáticos cuyos daños podrían ser del orden de U$ 6 billones anuales para 2021. Es así como, las pequeñas y medianas empresas (pymes) son cada vez más vulnerables en términos de seguridad informática.

Las pymes se enfrentan a los mismos problemas de ciberseguridad que presentan las grandes empresas, sin embargo, la dificultad radica en que las primeras no cuentan con los recursos necesarios para abordar los riesgos de manera eficiente, y sus equipos y presupuestos de seguridad son inadecuados, por lo tanto, tienen en una desventaja significativa para lidiar con las amenazas cibernéticas. Las pymes suelen actuar como proveedores, contratistas y socios de organizaciones más grandes y están conectadas digitalmente. Es así como, los ciber atacantes las utilizan como puertas de enlace para vulnerar los sistemas de organizaciones más grandes. Es así que para los directivos de las pymes la ciberseguridad no es una prioridad; más aún, estos no comprenden los riesgos, y no ven a su organización como un objetivo probable, subestimando el valor de su información para la competencia, y considerando la seguridad informática un problema de las grandes empresas y no de la suya. Es así como, a menudo los directivos no justifican el gasto de recursos en ciberseguridad, lo que conduce a presupuestos insuficientes en el área

Los líderes de tecnología de la información y directivos de las pymes padecen de la falsa creencia que poseen una adecuada capacidad de defensa en su organización;Segun la RSM US,consultoría enfocada en el mercado medio en los Estados Unido , encontró en su estudio que el 95% de las pymes consideran que poseen mecanismos de seguridad informática superior al promedio, y su riesgo de sufrir ataques informáticos es muy bajo; sin embargo, el estado real de preparación y madurez en ciberseguridad de estas pymes puede ser bastante insatisfactorio. Esto se evidencia en el estudio de Cyber Security Breaches Survey 2019, donde se señala que solo el 15% de las pymes poseen un proceso formal de gestión de incidentes cibernéticos, y el 50% de los líderes de TI dicen que no saben por dónde empezar para mejorar su postura de seguridad. Bajo este panorama, las organizaciones no realizan evaluaciones permanentes, sistemáticas y exhaustivas del riesgo cibernético

Por ejemplo para el caso de Colombia,se destaca el riesgo de seguridad informática de las pymes en Colombia y se afirma que los errores comunes que se comenten al interior de las instituciones en materia de seguridad informática son, entre otros: no valorar la información, considerar que la seguridad equivale a un antivirus, y confiar en tecnología no adecuada. Así mismo, se ratifica la importancia de los mecanismos de ciberseguridad para todas las organizaciones e instituciones que hoy en día ejecutan sus funciones mediante el tratamiento de datos. Por lo tanto, las pymes en Colombia son altamente vulnerables a riesgos en seguridad informática y es necesaria una adecuada gestión de estos (. Ahora bien, cada día surgen nuevas vulnerabilidades que afectan todo tipo de programas, servicios y sistemas operativos, las cuales son agregadas a las bases de datos específicas. "The MITRE Corportation" ,Organización que Provee ingeniería de sistemas, investigación y desarrollo , cuenta con una base de datos de vulnerabilidades denominada CVE (Common Vulnerabilities and Exposures), que permite identificar debilidades en un producto, al proporcionar identificadores estandarizados para cada vulnerabilidad o exposición. Sin embargo, aunque existen este tipo de bases de datos, a menudo las organizaciones de pequeño y mediano tamaño no están permanentemente al margen de ellas, teniendo brechas de seguridad.

SOLUCIONES.

Entonces cómo podemos amortiguar dicha problemática, para ello es necesario contar con:

Equipo de seguridad: Sin importar el tamaño de tu negocio, debes asignar una persona y equipo líder responsable de la ciberseguridad del negocio. Este equipo debe contar con un especialista de seguridad TI externo o interno e incluir personas de áreas claves de la empresa.

Análisis y respuesta: Una vez que ya tienes un equipo, el siguiente paso es analizar las diversas situaciones de crisis que se puedan generar, a raíz de los incidentes de seguridad como: fugas de información, clonación de identidad, infección de malware, depósitos falsos, suplantación de identidad, etc. Después de ello ejecuta y mejora continuamente el plan de respuesta a través de pruebas reales, definiendo el paso a paso a seguir para gestionar la crisis.

Asegura tu WiFi: Es muy común que en una pequeña empresa se comparta la red por WiFi, pero debemos asegurarnos de configurar el punto de acceso inalámbrico o enrutador, para que esté encriptada y oculta para externos.

Filtros de seguridad: Recuerda que es necesario tener una política de seguridad desde el registro de tus clientes hasta el proceso de venta. Usa contraseñas alfanuméricas fuertes, implementa certificado de seguridad SSL a tu página web e implementar antivirus y software licenciado para todos tus equipos.

Capacita a tus colaboradores: Debido a que muchos fraudes pueden concretarse por un error humano, es necesario capacitar al personal, en especial a las áreas que se encarga de las transacciones financieras, pagos a proveedores, ventas digitales y sepan cómo actuar ante posibles casos de fraude cibernético.

Proveedores: Al contratar servicios móviles, datos, internet y/o telefonía, lo mejor es indagar por los servicios complementarios de seguridad y certificaciones de seguridad que tienen. Recientemente, Entel fue una de las pocas empresas en el Perú en lanzar en pandemia un portafolio de soluciones y/o servicios de ciberseguridad para mypes , además de recibir la certificación FIRST a su CyberSOC que garantiza una efectiva y eficaz respuesta ante incidentes cibernéticos.

Copia de seguridad: Respaldar la información es fundamental, por lo que es recomendable utilizar la nube para crear copias de seguridad de tu información crítica y base de datos de información.

CONCLUSIONES:

En síntesis, la ciberdelincuencia es un peligro latente en las pequeñas y medianas empresas y la principal causa es la falta de decisión en implementar sistemas de ciberseguridad. Las empresas de ahora deben ver este desembolso no como un gasto sino como una inversión.

Las grandes empresas lo ven siempre desde esa perspectiva y es por ello que se traduce en menos pérdidas a largo plazo. Las pymes padecen de la falsa creencia que poseen una adecuada capacidad de defensa en su organización; RSM US (2018), encontró en su estudio que el 95% de las pymes encuestadas consideran que poseen mecanismos de seguridad informática superior al promedio, y su riesgo de sufrir ataques informáticos es muy bajo; sin embargo, el estado real de preparación y madurez en ciberseguridad de estas pymes puede ser bastante insatisfactorio.