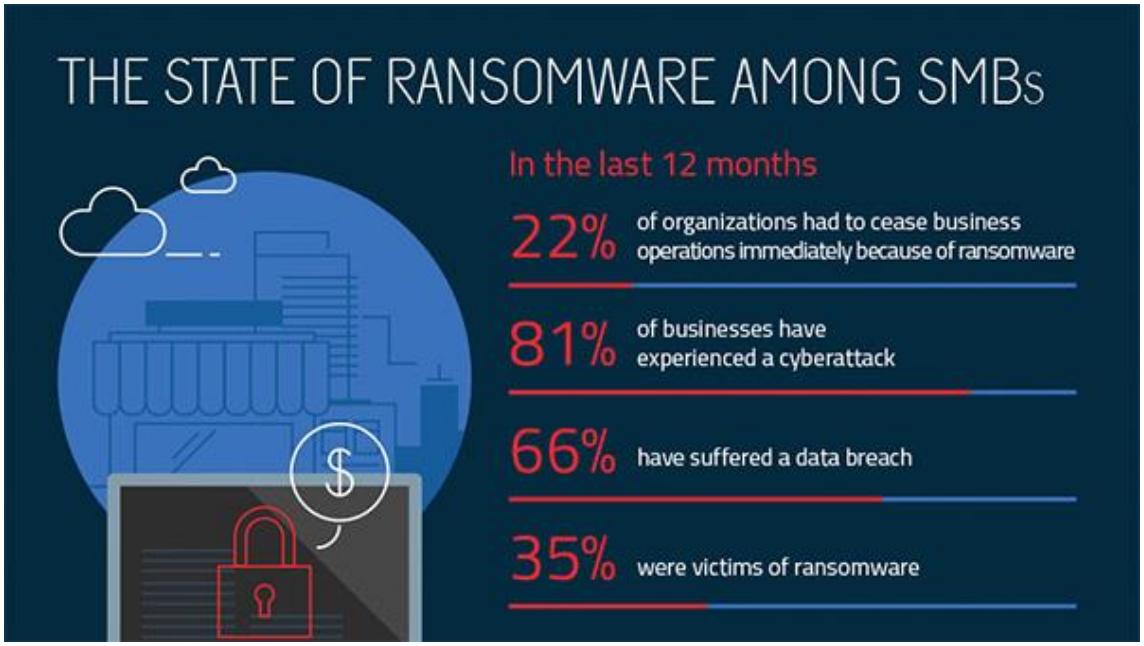
AREAS DE LA SEGURIDAD INFORMATICA

Hardware: Los ataques contra todo tipo de hardware y firmware continuarán y el mercado de las herramientas que los hacen posibles se expandirá y crecerá.

Ransomware: Las redes de anonimato y métodos de pago continuarán alimentando a la importante y creciente amenaza de ransomware, ataque que consiste en "secuestrar" archivos y pedir rescate para liberarlos. En 2016, un mayor número de ciberdelincuentes inexpertos aprovecharán las ofertas de ransomware como un servicio.



Wearable: Los wearables sin protección de seguridad incorporada serán los principales objetivos de los ciberdelincuentes, debido a que recolectan datos muy personales. Lo más importante, el hecho de que se sincronizan con teléfonos inteligentes crea el potencial para acceso a datos más valiosos. Y debido a que frecuentemente se emparejan con aplicaciones web con el propósito de compartir, las máquinas virtuales de nube y las aplicaciones web de soporte representan superficies adicionales de ataque.

Automóviles: Los investigadores de seguridad seguirán enfocándose en nuevas formas de explotar hardware de automóviles conectados que carecen de capacidades fundamentales de seguridad. Las áreas de ataque de automóviles podrían incluir unidades de control de motor, acceso al vehículo, dirección y frenado, sistemas de llaves remotas y acceso al teléfono inteligente del usuario, entre otras.

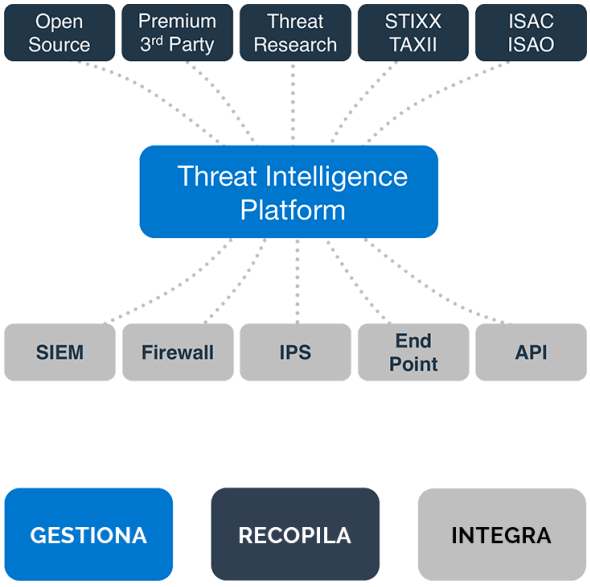
Almacenes de datos robados: El conjunto de información personal robada se está reuniendo en grandes almacenes de datos, haciendo que los registros sean más valiosos para los ciberatacantes. El próximo año observaremos el desarrollo de un mercado negro aún más robusto para el robo de información personal identificable, así como nombres de usuario y contraseñas.

Ataques a través de los empleados: Las organizaciones continuarán mejorando sus posturas de seguridad, implementando las últimas tecnologías de seguridad, trabajando para contratar a personas con talento y experiencia, creando políticas efectivas y permaneciendo vigilantes. Sin embargo, los atacantes probablemente cambien su enfoque y ataquen cada vez más a las empresas a través de sus empleados, dirigiéndose entre otras cosas, a los relativamente inseguros sistemas del hogar de los empleados para acceder a las redes corporativas.

Servicios de nube: Los ciberdelincuentes y competidores corporativos cada vez más se dirigirán a los servicios en nube que gestionan una cantidad creciente de información confidencial de negocios. Esta información podría contener la estrategia de negocios de la organización, estrategias del portafolio de la compañía, innovaciones de próxima generación, finanzas, planes de adquisición y desinversión, datos de empleados y otros datos.

Ataques de integridad: Uno de los más significativos nuevos vectores de ataque será la puesta en riesgo sigilosa y selectiva de la integridad de sistemas y datos. Estos ataques consisten en apoderarse y modificar transacciones o datos a favor de los cibercriminales, como por ejemplo, el cambio de la configuración de un depósito de nómina directo a la cuenta de cheques de la víctima para que se deposite en una cuenta diferente.

Intercambio de inteligencia de amenazas: El intercambio de inteligencia de amenazas entre las empresas y los proveedores de seguridad crecerá rápidamente y madurará. Se emprenderán medidas legislativas para hacer posible que las compañías y los gobiernos compartan inteligencia de amenazas. El desarrollo de mejores prácticas en esta área se acelerará, surgirán métricas de éxito para cuantificar la mejora de protección, y la cooperación de inteligencia de amenazas entre los proveedores de la industria se ampliará.



Áreas de la seguridad informática. (2015, Noviembre 10). Recuperado 8 de abril de 2020, de https://www.infobae.com/2015/11/10/1768685-las-9-areas-clave-la-seguridad-informatica-2016/