Conoce los cinco pensamientos clave sobre la ciberseguridad en 2018

Los datos nos rodean cada vez más, desde la forma en que los médicos los utilizan para comprender mejor a sus pacientes hasta los retailers que recopilan datos sobre las interacciones de los clientes en sus transacciones.

Frente a las conversaciones sobre cómo hacer la mayor parte de los datos disponibles ha surgido una necesidad urgente de que las empresas consideren cómo pueden proteger y satisfacer las demandas de privacidad de los consumidores.

De hecho, nuestro propio informe "Tech in a Transforming Britain" reveló que una quinta parte del Reino Unido cree que el cibercrimen es el mayor reto al que se enfrentan en la actualidad, tanto por encima de la incertidumbre económica mundial como del desempleo y déficit de conocimientos. Desde WannaCry hasta Equifax y Uber llevan todo el año 2017 centrados en la seguridad, esta preocupación no es una sorpresa.

Pero ante la inminente aproximación de las legislaciones sobre Regulación General de Protección de Datos (GDPR) y Sistemas de Información y Redes (NIS), ¿Qué pueden hacer las empresas y organizaciones para proteger sus negocios, clientes y trabajadores contra los ciberataques en 2018?

Aquí están nuestras cinco predicciones principales:

1 Usar CTI para respaldar un regreso a los enfoques básicos

La inteligencia de amenaza cibernética (CTI) se puede definir de muchas maneras diferentes. En el próximo año será importante utilizar Threat Intelligence para proporcionar un sistema de alerta temprana a los clientes y observar el contexto de las amenazas.

En resumen: realizar un trabajo exhaustivo para que los clientes no tengan que depender del servicio y el nivel de acceso, los proveedores pueden actualmente bloquear las amenazas antes de que tengan la posibilidad de causar daños.

En la mayoría de los casos, Threat Intelligence simplemente proporciona una guía sobre protección usando defensas básicas como la administración de parches. Supone un reto en cualquier entorno corporativo expresar la gravedad de una vulnerabilidad no sólo como riesgo técnico, sino también como un riesgo financiero, humano y comercial.

En un mundo perfecto pondríamos parches y repararíamos todas las cosas, pero la realidad dista mucho de un entorno así. La mayoría de las veces parchear un sistema financiero para una vulnerabilidad crítica en Java el día antes del cierre financiero anual no resultará muy interesante por miedo a romper el sistema, a pesar del parche de preproducción exitoso.

La combinación de la gestión de vulnerabilidades con Threat Intelligence es un gran ejemplo de uso para la protección de entornos corporativos. Los clientes tienen derecho a estar preocupados por la próxima cepa de incidentes de ciberseguridad global, pero con los brotes de Petya y Wannacry del año anterior el malware utilizó una vulnerabilidad SMB para la propagación conocida meses atrás y que simplemente necesitaba un parche.

Por ejemplo, aquí en Fujitsu proporcionamos un aviso de amenazas sobre ese parche a los clientes de CTI tres meses antes de que se extendiera Petya.

Además, también hemos proporcionado, con varios meses de antelación, a nuestros clientes de CTI asesoramiento para la vulnerabilidad Apache Struts que Equifax utilizó, una amenaza que generó un gran impacto.

2 Noticias falsas y manipulación

La línea que divide la seguridad cibernética y la política está distorsionada por continuos informes de manipulaciones electorales o incumplimientos de los organismos y departamentos gubernamentales.

Las investigaciones en torno a las elecciones de EE.UU. se prolongarán durante el 2018 con preocupaciones centradas en la manipulación de los controles de seguridad y la "prestidigitación". Hubo informes sobre actividades disruptivas similares durante las elecciones francesas de 2017.

En los últimos años, responsables de los partidos políticos en todo el mundo se han familiarizado con los conceptos de "Phising" o "Incident Response"". En el caso del Comité Nacional Demócrata (DNC), el coste mensual para dar respuesta a los incidentes para eliminar a los atacantes de la red de DNC era de $ 50 K al mes.

Los Estados Nación continúan creciendo en experiencia en ciberseguridad con el talento, voluntad y recursos para rentabilizar sus esfuerzos.

No todos los modelos de amenazas necesitan proteger contra adversarios que buscan desestabilizar una nación, pero con la creciente adopción de los servicios digitales y la frecuente atribución de ciberataques a los Estados Nación, los ataques contra entidades comerciales para apoyar objetivos políticos seguirán aumentando.

3 El Peligro del día cero

Los vendedores de Boutique Zero day, como Zerodium, ofrecen importantes recompensas a los investigadores, como los $ 1.5 millones que se ofrecieron en 2017 por un "exploit" en iOS.

Las iniciativas emprendidas por el gobierno de los Estados Unidos, tales como "hackear al ejército", demuestran una buena disposición para encontrar vulnerabilidades en los servicios digitales del país. Este es un enfoque ético donde el ejército de EE.UU. aceptó el riesgo de que se explotasen sus vulnerabilidades y, lo que es más importante, recompensó a quiénes informaron de las mismas.

Shadowbrokers saltó a la fama en 2017 como un grupo que lanzó ataques con información robada a la Agencia de Seguridad Nacional de los Estados Unidos. El grupo lanzó varios ataques de día cero, como ETERNALBLUE y DOUBLEPULSAR, que posteriormente se utilizaron en ciberataques como WannaCry y Adylkuzz.

La confirmación política del "acaparamiento de días cero" por parte del gobierno de EE.UU. se hizo pública en 2017 en la Política de Renta Variable (VEP). Esta política significa esencialmente que el gobierno puede optar por retener una divulgación si cree que es en interés de la seguridad.

Afortunadamente, para los principales ataques observados en 2017, los parches estaban disponibles para las numerosas vulnerabilidades explotadas, lo que permitió un elemento de protección o mitigación contra daños significativos.

4 Monitorización eficaz de la seguridad

A medida que los datos y nuestra vida digital continúan creciendo y conectándose, existe un Internet "Expandido" con líneas cada vez más borrosas para los perímetros de la red. Una consecuencia de esto es tener más datos para administrar y un aumento de los ciberataques para detectar y analizar.

Un requisito fundamental para cualquier empresa es la monitorización de la seguridad, pero a fin de abordar y mantener el ritmo del continuo aumento de los ciberataques, las organizaciones deben seguir siendo innovadoras para monitorizar con eficacia.

El panorama de las amenazas continúa creciendo en velocidad y complejidad y los Centros de Operaciones de Seguridad (SOC) tienen dificultades para mantenerse al día con la variedad de ataques a los que se enfrentan las empresas en la actualidad.

Las tecnologías tradicionales que utilizan un enfoque manual ya no son suficientes y es necesario un nuevo enfoque proactivo para contrarrestar el cibercrimen hoy en día.

Estos incluyen servicios analíticos tales como entidad de usuario o analítica de comportamiento (UEBA), detección y respuesta de punto final (EDR) y detección y respuesta gestionada (MDR) en un ecosistema de amenaza avanzada y fuerte.

Se necesitarán enfoques combinados de habilidades analíticas respaldadas por la seguridad de la automatización y la orquestación (SAO) para abordar problemas reales que enfrentan los SOC, como la fatiga de las alarmas.

En el futuro los SOC se aprovecharán de la inteligencia artificial, el aprendizaje automático y del API, un manual modelo controlado para una eficaz supervisión de la seguridad. El enriquecimiento automatizado de la Threat Intelligence para los incidentes que liberan un valioso tiempo de los analistas será necesario a medida que la industria se enfrenta a la creciente brecha cibernética.

5 Métricas de respuesta a incidentes "para ganar"

Mientras que un acuerdo de nivel de servicio (SLA) siempre será vara de medir para cualquier servicio entregado, las organizaciones adoptarán cada vez más nuevas métricas para medir la respuesta a incidentes.

La orientación del Gobierno del Reino Unido define la capacidad de reaccionar a los ciberataques de la siguiente manera:

"una respuesta eficaz ante un ataque depende de que primero seamos conscientes de que un ataque ha ocurrido o está ocurriendo. Una respuesta rápida es esencial para detener el ataque y para responder y minimizar el impacto o el daño causado"

Una métrica de respuesta a incidentes que se adoptará gradualmente y se utilizará para esto es el tiempo medio de respuesta (MTTR), para poder ver reducciones demostrables a lo largo del tiempo.

La respuesta a los incidentes y, lo que es más importante, la rapidez con que las organizaciones pueden responder a los incidentes será cada vez más importante con la inminente legislación del Reglamento General de Protección de Datos (GDPR) y los Sistemas de Redes e Información (NIS).

Una infracción de declaración obligatoria ha de ser reportada a la Oficina de Comisionados de Información (ICO) dentro de las 72 horas siguientes, por lo que la reducción del MTTR se volverá crítica y las empresas deben contar con un sólido plan de respuesta a incidentes.

El tiempo medio de permanencia (MTTD) es un término utilizado para describir el número de días que un atacante se encuentra dentro de una red antes de ser detectado. Un estudio de FireEye en las organizaciones EMEIA encontró que el MTTD promedio era de 489 días. Esto aumenta la importancia de la opinión de que el enfoque actual de los SOCs tradicionales no es tan efectivo como debería ser.

Los atacantes continuamente encuentran métodos innovadores para atacar y excretar datos a través de las capas de la red. La industria de la seguridad debe seguir siendo innovadora para reducir el MTTD general.

Contacto

FUJITSU
Camino Cerro de los Gamos, 1
28224, Pozuelo de Alarcón, Madrid (Spain)
info.spain@ts.fujitsu.com
www.fujitsu.com/es