Puntos ciegos y conceptos básicos de seguridad: bajar la guardia le puede costar caro en 2017

Informe de predicciones de amenazas del centro de operaciones de seguridad de Fujitsu

shaping tomorrow with you

FUJITSU

Contenido

Introducción

» En el mundo de la seguridad cibernética, mirar hacia atrás es tan importante como mirar hacia adelante. Necesitamos examinar las lecciones del pasado para estar preparados frente las amenazas del futuro.

Por lo tanto, este informe volverá la vista atrás hacia nuestras predicciones para el 2016, para comprobar si se ajustaron a los acontecimientos reales y también recogerá nuestras ideas para el 2017.

Espero que este informe le sirva a su organización no solo como una retrospectiva práctica, sino también para echar un vistazo a lo que está por venir, para que pueda continuar protegiendo a su empresa".

Rob Norris
Jefe de seguridad empresarial y cibernética, EMEIA

¿Fueron exactas nuestras predicciones para el 2016?

Predijimos que habría un mayor número de ataques DDoS graves como resultado del crecimiento continuo del Internet de las cosas (IoT). Algunas de las principales organizaciones se vieron afectadas durante 2016 por los ataques DDoS desde una botnet de IoT, incluyendo los DVR y las cámaras de CCTV. Los ataques afectaron a DynDNS, que interrumpieron los servicios en línea de Spotify, Twitter, GitHub y PayPal, entre otros, en octubre. KrebsOnSecurity también sufrió uno de los mayores ataques de la historia.

También planteamos que las aplicaciones web se encontrarían bajo un ataque creciente y, lamentablemente, se produjeron muchos ataques con éxito continuados, en los que la red social rusa VK y el Qatar National Bank se vieron afectados por los ataques de inyección SQL a principios de 2016.

Los atacantes continuaron centrando sus objetivos en los datos importantes para las organizaciones. Las universidades y los despachos jurídicos fueron objetivos importantes de los ataques durante 2016, utilizando como estrategias principales el robo de datos y el ransomware. La Universidad de Calgary reconoció que pagó 20 000 dólares para desencriptar los archivos afectados por el ransomware.

Predijimos que la biometría aumentaría.

Fujitsu continúa desarrollando algunas de las principales tecnologías del mundo en biometría y muchos proveedores están ahora tratando de mejorar sus soluciones de hardware. Apple incluyó la biometría de las huellas dactilares en su iPhone durante algún tiempo y finalmente añadieron la biometría a sus Macbooks en 2016, poco después de que el NIST anunciara que ya no admitirían los SMS como un método secundario de autenticación de dos factores.

También pensamos que Flash sería un foco de atención, ya que seguía siendo un objetivo de los ataques mediante los exploit kits. Los principales navegadores eliminaron la tecnología Flash de las opciones predeterminadas, mientras que YouTube se cambió a HTML5 de forma predeterminada, así que nuestras suposiciones fueron correctas en lo referente a esta aplicación.

Además, predijimos correctamente que la información personal estaría cada más ligada a los ataques informáticos. La lotería nacional de Reino Unido fue una de las víctimas de estos ataques. Fueron hackeadas 26 500 cuentas de jugadores, poniendo en riesgo información como las fechas de nacimiento o los datos de las tarjetas.

Creemos que las empresas deberán estar alerta ante los desafíos de seguridad informática en 2017. En las siguientes páginas se describen nuestras 10 predicciones principales.

Las 10 predicciones principales de seguridad informática de Fujitsu para 2017

1

Muchas empresas seguirán teniendo un punto ciego

Podemos predecir que los ataques continuarán teniendo éxito en 2017, ya que las organizaciones siguen sin abordar los puntos ciegos que existen en cuanto a los ataques a través de canales cifrados no atendidos debido a la falta de capacidades de inspección SSL. En 2016 también hubo un enorme aumento de los ataques contra las empresas que utilizan Microsoft PowerShell.
PowerShell es un marco de referencia y un lenguaje de programación que se instala de forma predeterminada en todos los equipos Windows y se está utilizando para los ataques debido a que muchas organizaciones carecen de una protección adecuada contra el uso malintencionado.

Al formar parte del sistema de Windows, es más fácil que los atacantes lo utilicen como parte del ciclo de ataque y es difícil que los defensores de la red detecten el uso malintencionado, si no lo están supervisando. Las herramientas como PowerShell Empire, normalmente utilizadas por los equipos de pruebas de penetración, también se utilizan en los ataques para superar el perímetro, crear puertas traseras y desplazarse lateralmente a través de una red. Las organizaciones deben revisar sus capacidades de supervisión, los niveles de registro y también trabajar para identificar qué scripts "buenos" conocidos se utilizan en sus redes para tener la capacidad de detectar ataques maliciosos cuando sea posible.

2

La inteligencia artificial cambiará el análisis en los centros de operaciones de seguridad (SOC)

A medida que las organizaciones intenten utilizar la inteligencia artificial (IA) y las capacidades de aprendizaje automático, el modo en que las organizaciones analizan eventos de seguridad cambiará en 2017. El principio de "qué se entiende por bueno" en términos de seguridad informática lleva años tratándose.
El aprendizaje automático es una extensión de este concepto con algoritmos de lo que se considera un buen comportamiento, por ejemplo, cómo deberían o no deberían hacerse ciertas llamadas de sistema o cómo ciertos tipos de archivos se combinan para que cualquier desviación se considere sospechosa.

La supervisión de la red principal en busca de un comportamiento anómalo, como las transacciones grandes o los primeros intentos de acceder a una base de datos será un cambio en el enfoque de los centros de operaciones de seguridad que necesitan avanzar hacia un enfoque basado en la inteligencia. Dejarán de reaccionar y clasificar el tráfico "malo" conocido a través de un antivirus o una alerta de detección de intrusos, pero habrá que investigar sobre una alerta que advierta de que ha ocurrido algo inusual basada en un algoritmo de aprendizaje automático. También habrá que tener en cuenta para 2017 que los atacantes utilizarán las mismas capacidades de IA, ya que tratan de acabar con los controles de seguridad y de las redes.

3 Los delincuentes seguirán atacando las aplicaciones de core bancario

Las aplicaciones de core bancario fueron uno de los objetivos en 2016. En los principales acuerdos de los institutos bancarios internacionales se perdieron millones de dólares que fueron robados directamente como consecuencia de las deficiencias en la red global de pago de SWIFT. En el caso más destacable fueron 81 millones de dólares de un banco de Bangladesh. También observamos el crecimiento de los troyanos bancarios que los delincuentes dirigen contra las aplicaciones de administración para explotar las tecnologías heredadas y robar las bonificaciones financieras directamente de los bancos.

Consideramos que esto será un riesgo importante para el sector bancario en 2017. SWIFT ha introducido 16 controles obligatorios e inspeccionará los bancos en 2018 para asegurar el cumplimiento, pero aún sigue siendo una oportunidad para los delincuentes informáticos. Los investigadores detectaron que el troyano Odinaff tenía como objetivo SWIFT a finales de 2016 y es probable que este año veamos nuevas variantes y métodos de ataque.

4 Los atacantes aumentarán el foco contra el mercado móvil

Las mejoras de seguridad de los nuevos sistemas operativos y el uso creciente de los dispositivos inteligentes para los datos personales y empresariales harán que las plataformas móviles se conviertan en un mayor objetivo en 2017. Muchas organizaciones están actualizando ahora los sistemas operativos heredados de Microsoft que han sido con frecuencia uno de sus puntos débiles y están aprovechando las funciones de seguridad mejoradas de los sistemas operativos de servidor mejorados y el navegador Edge integrado en Windows 10.

Las pequeñas aplicaciones, como Adobe Flash, que también suelen ser uno de los objetivos, especialmente, de los exploit kits, también están siendo retiradas de las redes empresariales y los proveedores con el navegador Google Chrome, convirtiendo HTML5 en la opción predeterminada en diciembre de 2016. Actualmente se suelen tener varios dispositivos inteligentes, muchos con enormes cantidades de datos personales y empresariales gracias a las modernas capacidades de almacenamiento y, por ello, los atacantes seguirán desarrollando nuevos ataques contra las plataformas móviles utilizando el ransomware para móviles, que exige un pago para la devolución o la desencriptación de fotos personales. La gestión de dispositivos móviles tendrá que complementarse con controles de seguridad sólidos, especialmente en los dispositivos empresariales.

Los hackers tendrán como objetivo las ciudades inteligentes

5

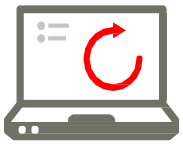
A medida que los dispositivos del Internet de las cosas siguen creciendo exponencialmente, seguiremos descubriendo problemas de seguridad que antes ni habíamos considerado. Cuando un arquitecto diseñó los paneles inteligentes de las autopistas, ni siquiera pensó que los hacktivistas los pudieran utilizar para mostrar mensajes con motivos políticos en lugar de advertencias para los conductores. Esto también se aplica a los fabricantes de IoT que crearon cientos de miles de cámaras de CCTV, DVR y los routers SOHO que ahora son parte del botnet "Mirai" de IoT.

Se aprenderán bien las lecciones tras lo ocurrido con Mirai, como evitar las contraseñas predeterminadas incrustadas directamente en el código, pero muchos de los protocolos diseñados para dispositivos inteligentes conectados contarán con sus propios defectos potenciales y debilidades, como hemos visto con los routers Zyxel. Veremos más debilidades como estas en 2017.

Los atacantes han aprovechado estas vulnerabilidades, de forma que, aunque hace 12 meses parecía imposible e improbable tener la capacidad de apagar el alumbrado conectado de una ciudad "inteligente" mediante el ransomware, los últimos acontecimientos han cambiado esa percepción.

No solo deben controlarse las posibles debilidades de los dispositivos inteligentes, sino que también estas plataformas y la normativa con respecto a la gestión de estas plataformas de control jugarán un papel fundamental. Esto incluye los controles de seguridad de la cadena de suministro involucrados en las prestaciones y en el control de cualquier parte de las ciudades inteligentes que estamos conectando. Si estas plataformas de gestión de los dispositivos inteligentes se ponen en riesgo únicamente con la vulneración de la seguridad de una parte de la cadena de suministro, entonces es de esperar que veamos más ataques como estos. Los atacantes quizás no intenten explotar las debilidades de las ciudades conectadas, pero pueden tratar de instalar ransomware en una parte fundamental de la infraestructura.

6



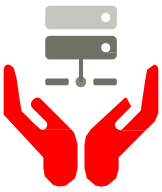
La resistencia y la recuperación serán diferenciadores comerciales

Los ataques informáticos son ahora tan potentes que incluso las organizaciones más seguras podrían verse afectadas. En 2017, la pregunta será: ¿con qué rapidez se pueden recuperar?

Una recuperación rápida y plena atraerá el apoyo y el respeto de los mercados, mientras que una mala recuperación desencadenará críticas y demandas.

A finales de noviembre, las autoridades de transporte municipal de San Francisco sufrieron un importante ataque de ransomware, pero, gracias a un proceso de copia de seguridad sólido, consiguieron restaurar gran parte de la funcionalidad en un solo día.

El próximo año, veremos qué empresas se toman en serio el reto de adoptar un enfoque coordinado que combine la protección, la detección y la respuesta.



7

La conservación de datos, no solo de aquellos con grandes cantidades de información, se convertirá en un punto clave para todas las organizaciones

En 2017, cada vez más inversores, accionistas, clientes y reguladores querrán que se les garantice que se están protegiendo los datos confidenciales. Esto será especialmente importante en el enfoque de la Regulación general de protección de datos. Las herramientas especializadas en la prevención de pérdida de datos (DLP) funcionan bien si se utilizan correctamente, pero muchas empresas utilizan las DLP de manera irregular o piensan que el uso de una sola herramienta DLP es suficiente.

Las organizaciones deben considerar los riesgos, identificar los datos principales que quieren proteger y vigilar sus redes atentamente. También tendrán que proteger los datos vulnerables de terceros de la misma manera que protegen los suyos propios.

8

Los clientes globales exigirán inspeccionar sus cadenas de suministro de seguridad de datos

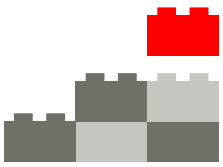
La mayoría de las organizaciones saben que sus datos confidenciales no se conservan solo internamente. Sino que también se encuentran en su cadena de suministro. Sin embargo, a menudo existe una gran diferencia entre lo que las organizaciones esperan de sus proveedores y lo que los proveedores tienen que hacer contractualmente.

Según aumenta la toma de conciencia de los riesgos informáticos, estamos empezando a ver cómo las empresas globales buscan una prueba clara de una seguridad de datos correcta de los principales asesores profesionales. Esto incluye los despachos jurídicos, las gestorías y las consultorías empresariales. Los principales clientes están bien situados para exigir una buena seguridad de los datos como condición de trabajo con esos asesores. Parece que esta tendencia crecerá mucho en 2017 y en el futuro.

9 Las juntas directivas tratarán la seguridad de TI de forma rutinaria

Con tantos ataques informáticos contra las principales organizaciones, ni siquiera los directivos más tecnofóbicos podrán evitar esta cuestión como si fuera algo que solo debe tratar el departamento de TI. 2017 será el año en que las juntas directivas comprendan que una seguridad de TI escasa podría perjudicar a las empresas.

Las organizaciones deberán formar al personal de TI de categoría superior para que entiendan las necesidades de la junta directiva y cómo la TI puede ser tratada de forma que puedan entenderla.



10 Las malas prácticas de TI rutinarias seguirán causando la mayor parte del daño evitable

La mayoría de las veces, los problemas de seguridad informática que afectan a las organizaciones no son obra de las nuevas técnicas de ataques informáticos o de infiltrados con malas intenciones. Un sorprendente número de empresas no llevan a cabo las tareas de organización que reducen los riesgos, que resultan tan simples como fundamentales.

No disponen de parches eficaces para las debilidades ni una inteligencia adecuada contra las amenazas. No usan un sistema de gestión de acceso que solo refleje los usuarios actuales. No utilizan accesos con "privilegios mínimos" ni implementan las recomendaciones de las pruebas de penetración. Esto los hace vulnerables ante la pérdida de datos, el robo de datos o la interrupción externa de sus sistemas de forma innecesaria.

Desgraciadamente, esto continuará ocurriendo en 2017, lo que significa que la mayoría de las vulneraciones de seguridad serán evitables.

Los ataques seguirán ocurriendo. ¿Está preparado?

En 2017 se producirán vulneraciones de seguridad más potentes de forma frecuente. Se verán afectadas las empresas de los principales sectores empresariales de todo el mundo. Incluidas las megacorporaciones consolidadas, los gobiernos y las principales marcas. Algunos serán fruto de la mala suerte. Pero muchos otros sufrirán ataques que se podrían haber evitado con un poco más de cuidado y atención.

Visite el sitio web de Secure Thinking si desea obtener más información sobre cómo mantener su empresa segura y cómo Fujitsu le puede ayudar a gestionar el cambiante panorama de las amenazas de ciberseguridad

shaping tomorrow with you

FUJITSU

FUJITSU
22 Baker Street
London W1U 3BW
Tel: +44 (0) 1235 79 7711
Email: askfujitsu@uk.fujitsu.com
Web: **uk.fujitsu.com/securethinking**
Ref:3684