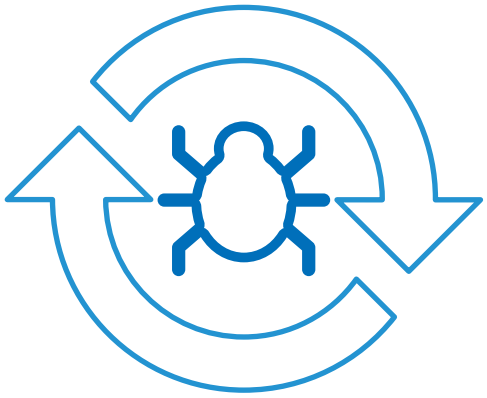
SOPHOS
Security made simple.

Tendencias amenazas de seguridad 2015

Predicciones sobre ciberseguridad en el 2015 y siguientes

Por James Lyne, director de investigaciones globales de seguridad, Sophos



Ciberseguridad en el 2015

La ciberseguridad está experimentando un crecimiento importante, tanto dentro de la industria como en la vida de las personas y las empresas que usan medios tecnológicos modernos. Y debido a que la tecnología no cesa de cambiar a un ritmo vertiginoso, las amenazas tampoco dejan de evolucionar con rapidez - con cibercriminales encontrando formas nuevas y creativas para aprovecharse en su propio beneficio tanto de los usuarios como la tecnología todo el tiempo.

Ahora es el momento del año en el que se publican las predicciones para la tecnología y todos los cambios y las amenazas que vendrán el año que viene. Algunas pueden estar muy lejos, mientras que otras ya pueden estar produciéndose. Sin embargo, nos parece que es útil analizar las tendencias claves de la ciberseguridad, así que a continuación presentamos las 10 áreas que pensamos tendrán un impacto significativo en el año 2015 y siguientes.

SOPHOS
Security made simple.

Para encontrar recursos adicionales, visite
sophos.com/es-es/

Las mitigaciones de vulnerabilidades reducen el número de vulnerabilidades útiles.

Durante años los cibercriminales se han venido aprovechando de distintas vulnerabilidades para difundir de forma inadvertida su código malicioso. Remontándonos a los inicios, el principal vector de distribución de código malicioso era el spam, pero hoy en día son los ataques basados en web y el aprovechamiento de las brechas de seguridad de los navegadores los que están claramente a la cabeza. Afortunadamente, Microsoft ha investigado en mitigaciones de vulnerabilidades como DEP (prevención de ejecución de datos, para evitar la ejecución de código del atacante en determinadas áreas de la memoria de un ordenador), ASLR (ejecución aleatoria de la disposición del espacio de direcciones, que hace más difícil escribir código de ataque cambiando las direcciones de la memoria) y un número considerable de mejoras en Windows 8 y Windows 8.1 (analizar estas en profundidad no es el objetivo de este análisis, aunque se puede encontrar documentación completa al respecto online).

A medida que la dificultad para aprovechar las vulnerabilidades aumenta, los exploits para aplicaciones muy codiciadas por los atacantes, como Internet Explorer en plataformas importantes como Windows 7, cada vez son más escasos y su valor de mercado está aumentando. La consecuencia directa son cambios en las pautas de comportamiento como las que ya hemos podido ver y otras consecuencias que podemos anticipar. Los exploits de alto valor se están vendiendo para ataques más específicos y desplegando de forma más selectiva, dejando a una parte del mercado del cibercrimen con menos opciones.

De allí que algunos atacantes estén regresando a la ingeniería social dejando atrás el uso de exploits. Por lo tanto, deberemos estar alerta ante fraudes de ingeniería social más efectivos a medida que los cibercriminales encuentran nuevas cargas más innovadoras. También es posible que veamos cómo algunos atacantes centrarán su atención en plataformas distintas a Microsoft que en ocasiones presentan menos mitigaciones. Otra cuestión que es necesario considerar es el gran número de usuarios que seguirán usando plataformas ya anticuadas durante algún tiempo (después de todo, muchos todavía están usando XP). Las nuevas mitigaciones están haciendo que el precio de los exploits en el mercado negro sea cada vez más alto, unido a un secretismo todavía mayor en la industria sumergida. Yo estaría alerta ante ataques de ingeniería social más sencillos y efectivos en el 2015 y estaría más encima de la política de parches y los procesos de contención en dispositivos de plataformas distintas a Microsoft.

Los ataques al Internet de las cosas se convertirán en un riesgo general.

En el 2014 hemos podido constatar que los fabricantes de dispositivos IoT (Internet de las cosas) no han estado a la altura a la hora de implementar estándares de seguridad básicos - o no han aprendido de la dilatada y lamentable historia de fallos de la informática convencional o debido a la rapidez del mercado sencillamente no les importa.

Yo mismo he atacado routers inalámbricos con ataques web como inyección de comandos, cámaras de CCTV que no tenían implementado ningún bloqueo de cuentas y puntos de conexión inalámbricos sin nombres de usuario ni contraseñas y que en cambio confiaban explícitamente en la red local. A pesar de que brechas como estas se hayan ejemplificado hasta la saciedad en distintas conferencias de seguridad, todavía no han despertado un interés generalizado entre los cibercriminales. No obstante, creemos que no tardarán en aparecer ejemplos más serios fuera las pruebas de concepto de los investigadores de seguridad.

Sin una seguridad mejor, es más que probable que los ataques contra estos dispositivos tengan un impacto global real muy desagradable. Es fundamental que la industria de seguridad evolucione para englobar también este tipo de dispositivos, que los distribuidores de las aplicaciones correspondientes maduren para reconocer la importancia de la seguridad (tanto como Microsoft se vio obligada en su día) y que la preocupación de los consumidores por la seguridad siga creciendo para que se convierta en un requisito comercial y deje de ser solo una preocupación de los profesionales de la seguridad.

Posiblemente, la razón por la que el nivel de explotación de las vulnerabilidades del Internet de las cosas sea tan bajo es que los cibercriminales todavía tienen que encontrar el modelo de negocio que les permita hacer dinero. Sin embargo, a medida que aumente la diversidad de aplicaciones, la probabilidad de que estos puedan emerger será mucho mayor. Y viendo la trayectoria hasta ahora de la industria de IoT, se puede decir que cuando esto suceda todavía no habrán acordonado la seguridad. Y lo que todavía es peor, estos distribuidores no tendrán ni la infraestructura necesaria para distribuir actualizaciones a tiempo, a diferencia con Microsoft que sí pudo parchear su sistema a las malas.

El cifrado se convertirá en un estándar, pero no satisfará a todos.

En el 2013 predijimos que el cifrado completo de discos se convertiría en un estándar muy difundido por los fabricantes de SO o en discos duros y administrado por fabricantes de seguridad, y esta tendencia se ha hecho realidad a gran escala en las empresas modernas.

La creciente preocupación por la seguridad y la privacidad surgida a raíz de las revelaciones de espionaje gubernamental y los titulares de violaciones de datos han convertido el cifrado en un estándar generalizado.

Así, un análisis rápido de las aplicaciones móviles de Android revela que un gran número de ellas usan cifrado para proteger los datos a nivel local en los dispositivos y al conectarse de vuelta a los servicios en Internet. Este número ha crecido de forma notable desde hace unos cuantos años y puede parecer un motivo de celebración.

Desafortunadamente, aunque muchas de estas aplicaciones han hecho el esfuerzo de usar SSL (por ejemplo), pocas lo han implementado correctamente. Por ejemplo, muchas no usan el “pineado” de certificados, por lo que el cifrado es más de cara al público en lugar de proporcionar seguridad y privacidad real. Son los detalles los que diferencian un cifrado efectivo de un cifrado de «marketing», pero la realidad es que gran parte del cifrado obedece más bien a cuestiones de marketing.

Muchas empresas y consumidores quieren cifrar los datos que suben a los servicios de alojamiento en la nube desde dispositivos móviles u ordenadores, pero los defectos en el despliegue deberían hacer que las empresas se pregunten algo más que «¿está cifrado?». Es probable que los estándares y los procesos de auditoría sean lentos a la hora de detectar estos detalles, como fue el caso cuando DES se consideró (más bien tarde) como inapropiado.

Por otra parte, algunas agencias estatales de seguridad no están contentas con esta tendencia de mayor cifrado, ya que piensan que afectará negativamente a la seguridad. Sin duda alguna su objetivo de seguridad se opone a la privacidad, pero mantener todo sin seguridad para permitir su trabajo forense en defensa de la legalidad no es una estrategia sensata.

Además, en lo que se refiere a los proveedores de seguridad de redes independientes, se plantea otra problemática interesante en tanto que el aumento creciente del cifrado del tráfico impide que este pueda ser interceptado y escaneado en la red. Es probable que esto tenga un impacto significante en la forma en la que deba de proporcionarse la seguridad en un futuro cercano.

Más fallos importantes en software de gran difusión no detectados por la industria de seguridad durante los últimos 15 años.

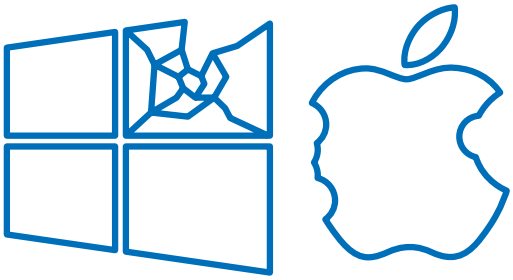
Este año ha visto un número relevante de brechas importantes en plataformas distintas a las de Microsoft en las que la industria de seguridad centra su atención. Desde Heartbleed a Shellshock, se ha hecho evidente que la cantidad de código no seguro usado en un gran número de sistemas informáticos de la actualidad es importante.

Muchos se alarmaron cuando se detectó que el proyecto OpenSSL (un software muy difundido integrado en más sitios de lo que uno puede imaginar) no disponía la mayoría de las veces de los recursos para realizar auditorías y comprobaciones de código de forma correcta, a pesar de su gran difusión.

Muchos de estos defectos posiblemente no alcancen la gravedad de los que vimos en el 2014, aunque no por eso dejarán de ser un reto interesante para las empresas. Las empresas han desarrollado y llevado a la práctica protocolos para la distribución de parches o la gestión de riesgos en sistemas Windows, pero no disponen de nada similar para otras plataformas. Esto se hizo patente en la lentitud extrema de muchas empresas a la hora de intentar responder a Heartbleed. Lamentablemente, todavía hoy muchas marcas siguen presentando vulnerabilidades, a pesar del tiempo transcurrido desde que este fallo copó los titulares a nivel internacional.

Desafortunadamente, no veo que se hayan aprendido las lecciones y el descubrimiento de más vulnerabilidades en sistemas distintos a Microsoft conllevará periodos largos de exposición para un elevado número de usuarios.

Los sucesos del 2014 han disparado el interés de los cibercriminales en el software y sistemas normalmente menos considerados que además se mantendrá durante los próximos años, de modo que es necesario preparar una estrategia de respuesta también en este ámbito. Esta situación planteará sin dudas retos para muchos de los procesos y procedimientos que las empresas tienen implantados.

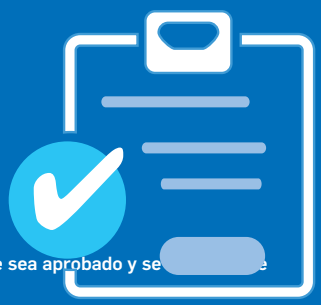


El panorama legislativo exigirá más divulgación y responsabilidad, particularmente en Europa

La legislación avanza de forma más lenta que la tecnología y la seguridad, pero cambios importantes que han tardado mucho en llegar prácticamente ya están aquí. Tras años hablando sobre la divulgación obligatoria de violaciones, responsables de protección de datos y sanciones importantes, la Unión Europea está a punto de implementar nuevos estándares exigentes en el 2015, que entrarán en vigor en el 2016.*

Encuestas recientes realizadas en Europa han relevado que la mayoría de las empresas no saben lo que está por venir, aunque un fallo en la protección de datos puede conllevar sanciones de hasta 100 millones de euros o el 5 % de los beneficios anuales. Un sorprendente 77 % de las empresas encuestadas incluso no sabían si estaban cumpliendo la legislación sobre protección de datos vigente, por no hablar de la que está por venir. Es probable que estos cambios también lleven a considerar una legislación de protección de datos más progresiva en otras jurisdicciones.

Los retos con respecto a la legislación contra el cibercrimen son importantes, cuya aplicación es ostensiblemente nacional a pesar del carácter internacional del cibercrimen. Creo que se producirán más quejas sobre las limitaciones y la idoneidad de leyes nacionales como la Ley de Fraude y Utilización Indebida de la Informática (CFAA) de los EE. UU. y similares en todo el mundo. Aunque este no es el momento para desarrollar un enfoque más internacional.



***Al tratarse de un borrador puede que los plazos y el alcance cambien, aunque es muy probable que sea aprobado y se [illegible] según se describe.**

Los atacantes se centrarán más en los sistemas de pago móviles, aunque seguirán explotando el fraude tradicional en el pago durante algún tiempo.

Los sistemas de pago móviles fueron el centro de atención del 2014 después de que Apple abriera la veda con Apple Pay. Sin duda se producirán errores de implementación en estos nuevos protocolos, aunque la incursión de Apple parece proporcionar más ventajas y mejoras con respecto a los estándares de seguridad de muchas de las tarjetas de crédito o débito del mundo, particularmente en los EE. UU., donde se mantienen unos estándares más bien arcaicos y susceptibles de fraude.

Los cibercriminales buscarán fallos en estos sistemas, aunque los diseños presentes incorporan varias funciones de seguridad positivas: hardware especial que convierte en mucho más difícil extraer la información; el uso de PIN, contraseñas o huellas dactilares para la autenticación (mucho más seguros que una firma); y un token para representar su autorización (lo que significa que los cibercriminales no pueden robar el equivalente de un número de una tarjeta de crédito para usarlo repetidamente incluso si logran acceder al monedero electrónico).

Está claro que estos sistemas de pago son una mejora con respecto a las tarjetas fáciles de clonar. Ataques como el de Target demuestran las debilidades más importantes de los esquemas usados actualmente en América. Los nuevos sistemas de pago opondrán una mayor resistencia al robo. Es de esperar que los cibercriminales continúen explotando las tarjetas de crédito y débito tradicionales durante un periodo de tiempo importante, ya que por ahora son un objetivo más fácil. Permanezcan atentos ante nuevos fallos en estos sistemas nuevos a medida que los cibercriminales encuentran nuevas formas para aprovecharse.

7

La brecha de conocimientos especializados a nivel global seguirá aumentando, la capacidad de respuesta ante incidentes y la formación serán claves.

Cada vez más violaciones de datos y ataques llegan a las noticias. Una tendencia que probablemente crecerá a medida que se extienda la obligatoriedad de la divulgación de este tipo de incidentes con las empresas debiendo responder públicamente por sus errores.

Con la tecnología cada vez más integrada en nuestras vidas diarias y como pilar de la economía global, la deficiencia de conocimientos especializados en ciberseguridad cada vez es más crítica. Tanto los gobiernos como la industria reconocen que esta deficiencia es un problema.

Esta brecha está aumentando en lugar de decreciendo. Algunos gobiernos vaticinan que necesitarán hasta el 2030 para satisfacer las necesidades actuales de profesionales de seguridad. Combinando esto con el flujo de ataques y el requisito de atender los incidentes en cuanto se producen, se puede deducir que la lucha por profesionales de seguridad es feroz.

Las empresas deberían analizar su estrategia de búsqueda de estos profesionales y la industria en su conjunto debería convencer a los estudiantes de las buenas perspectivas de futuro del ámbito de la ciberseguridad.

Surgirán servicios de ataque y kits de exploits para plataformas móviles (y otras).

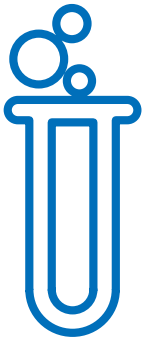
Los últimos años del cibercrimen han estado marcados por el auge de productos y servicios que han convertido los ataques y la explotación de vulnerabilidades en algo tan sencillo como apuntar y disparar. Algunos de estos paquetes criminales han ampliado sus capacidades para atacar dispositivos móviles, pero hasta ahora ninguno de forma importante o con un enfoque específico.

Aunque con la creciente popularidad de los dispositivos móviles (y la cantidad cada vez mayor de datos jugosos almacenados en los mismos), sospecho que no tardarán en aparecer paquetes y herramientas criminales centrados explícitamente en estos dispositivos. También es posible que veamos cómo esta tendencia se extenderá a otras plataformas en el espacio IoT, a medida que estos dispositivos proliferan alrededor de nuestras vidas.

En este momento, la mayor parte del malware para plataformas distintas a Windows está dirigido contra Android, con la mayoría del malware presentándose como aplicaciones legítimas y engañando a los usuarios para que instalen su código malicioso. Esta tendencia continuará sin duda alguna, pero el ecosistema de entrega de aplicaciones validadas se está reforzando, haciendo que la carga indirecta de aplicaciones presente más dificultades para los cibercriminales. Esto a su vez puede volver la atención hacia el desarrollo de exploits para estas plataformas y el desarrollo de kits de exploits para comercializar esta capacidad y convertirla en algo sencillo.

Se debe observar que las últimas versiones de software móvil tienen ASLR (espacio de usuario y Kernel) y funciones de espacios seguros (entre otros controles de seguridad). Al tiempo que estas plataformas están lejos de ser perfectas y muchos usuarios están ejecutando versiones antiguas sin estas mejoras, hay que decir que la actualización automática se está convirtiendo en un estándar cada vez más frecuente. Con lo que atacar estas plataformas resulta cada vez más difícil, a la vez que el volumen de exploits se mantiene mucho más bajo que el de exploits basados en web dentro el mundo del PC.

Sin duda veremos que la atención se seguirá centrando en los dispositivos móviles y supongo que durante los próximos años aparecerán novedades por parte de los cibercriminales con la comercialización de herramientas para plataformas distintas al PC y con un modelo de amenazas madurado.



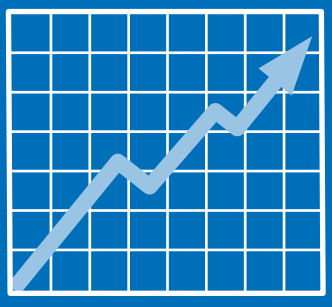
La brecha entre ICS/SCADA y la seguridad del mundo real se hará más grande.

Normalmente, los sistemas de control industrial (ICS) están 10 años o más por detrás de los entornos de sobremesa convencionales en lo que se refiere a la seguridad. Es bastante normal que al analizar estas plataformas se detecte que faltan mecanismos de autenticación, cifrado o comprobación de integridad y que la única estrategia de seguridad viable es mantenerlas aisladas en redes separadas.

Desafortunadamente, son muchas las ocasiones en las que estos sistemas han terminado conectados de forma inadvertida a redes exteriores. Solo es necesario un escaneado rápido con herramientas como Shodan para descubrir un número sorprendente de sistemas de control conectados a Internet. Afortunadamente, hasta ahora los incidentes serios no han sido muchos.

La realidad es que muchos de estos dispositivos y distribuidores están acostumbrados a definir un conjunto de criterios centrados en resiliencia o control y que no han aprendido a hablar el lenguaje de seguridad que otras áreas tecnológicas ya han tenido que absorber. También se han apoyado en gran medida en el aislamiento y la separación de redes para prevenir ataques.

Aunque que hay iniciativas de seguridad de los actores más importantes, la brecha entre el mundo real de la seguridad y los ICS no deja de crecer. Preveo que durante los años siguientes veremos que saldrán a la luz fallos mucho más serios, que serán aprovechados por atacantes, mientras que las motivaciones seguirán evolucionando para dejar de ser solo de tipo financiero. Creo que esto impulsará una mayor regularización y estandarización de la industria en este ámbito, aunque el cambio tardará en producirse debido a lo elevado de los costes y la complejidad y, frecuentemente, el hecho de que se trate de soluciones a medida. Resumiendo, creo que es un ámbito con un riesgo elevado y en el que la seguridad está más relegada de lo que se podría esperar.



Capacidades interesantes de rootkits y bots podrían dar lugar a nuevos vectores de ataque

Muchos de los ataques de los últimos años se han producido en la capa de aplicación (inclusos los ataques DDoS han estado centrados más en la capa de aplicación en lugar de en la capa de transporte). Muchos de los protocolos más importantes, como IPv4, llevan con nosotros desde hace bastante tiempo y nos hemos acostumbrado a sus carencias y errores de diseño. No obstante, se está acercando un importante periodo de cambios.

Una versión completamente nueva de HTTP (2.0 el sucesor de 1.1) está de camino y el protocolo IPv6 se ha introducido de forma generalizada en las redes sin que la mayoría de los administradores lo hayan notado.

Estamos en el proceso de cambiar las plataformas y los protocolos más importantes en los que hemos confiado algún tiempo y estos cambios de nivel inferior probablemente traigan consigo fallos interesantes que los cibercriminales posiblemente puedan aprovechar. Las áreas a las que esto puede aplicar son muchas, pero consideramos que ya hemos visto algunas señales de esto. La pila IPv6 en Windows 7 y Windows 8 es vulnerable a un fallo de agotamiento de recursos que permite a un atacante enviar anuncios de router aleatorios continuos y consumir el 100 % de la CPU del sistema (hasta que Microsoft puso a disposición un parche parcial, este problema era capaz de bloquear el sistema completamente) y la mayoría de la gente sigue ajena a este fallo, a pesar de que sigue efectivo todavía hoy en día.

En un sentido más amplio, IPv6 vuelve a implementar algunos de los fallos antiguos de IPv4, p. ej., mecanismos para poder hacer de «hombre en el medio» como en los ataques ARP en IPv4. Aunque de forma estándar hay medidas para atajar esto, todavía no han llegado al mundo real de implementaciones y políticas.

También se deben considerar cambios de hardware a nivel inferior como el cambio a UEFI. UEFI proporciona un entorno de arranque rico significativamente más fácil de programar que con un BIOS tradicional. Este entorno de arranque rico proporciona capacidades interesantes para rootkits y bots que pueden proporcionar nuevos vectores de ataque o versiones más potentes de los ataques vistos hasta ahora.

En general, parece que estamos predestinados a repetir muchos de los errores que cometimos la primera vez al desplegar estas tecnologías y estamos a punto de vivir cambios masivos importantes con respecto a las anteriores tecnologías. En definitiva, en esta área se pueden reabrir viejas heridas o revelar nuevas categorías de fallos de seguridad importantes.

Ventas en el Reino Unido e internacionales:
Teléfono: +44 8447 671131
Correo electrónico: sales@sophos.com

Ventas en España:
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en Norteamérica:
Teléfono: +1 866 866 2802
Correo electrónico: nasales@sophos.com

Oxford (Reino Unido) | Boston (EE. UU.)

SOPHOS