it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Septiembre 2018 - nº 11

Black Cloud viene al rescate

BAS, simulación de ataques para aumentar la seguridad

Black Hat USA 2018 verano en Las Vegas

El hogar inteligente, el hogar conectado, ¿el hogar inseguro?

Los grandes retos de la seguridad cloud

Guarda esta revista en tu equipo y ábrela con Adobe Acrobat Reader para aprovechar al máximo sus opciones de interactividad

it Digital Security

Director	**Rosalía Arroyo** rosalia.arroyo@itdmgroup.es
Colaboradores	Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez
Diseño revistas digitales	Contracorriente
Producción audiovisual	Favorit Comunicación, Alberto Varet
Fotografía	Ania Lewandowska

it Digital MEDIA GROUP

Juan Ramón Melara	juanramon.melara@itdmgroup.es
Miguel Ángel Gómez	miguelangel.gomez@itdmgroup.es
Arancha Asenjo	arancha.asenjo@itdmgroup.es
Bárbara Madariaga	barbara.madariaga@itdmgroup.es

Clara del Rey, 36 1º A · 28002 Madrid · Tel. 91 601 52 92

¿Te avisamos del próximo IT Digital Security?

Black Cloud
viene al rescate

Perdidas las fronteras tradicionales, la seguridad evoluciona hacia el perímetro definido por software (SDP), que mantiene invisibles, en una Black Cloud, todos los recursos de la empresa salvo para usuarios y dispositivos autenticados. Se decide que nada es confiable mientras no se demuestre lo contrario, de forma que se restringe el acceso a la red a todo salvo a los elementos permitidos. En lugar de establecerse un perímetro alrededor de las aplicaciones y sistemas, el enfoque SDP establece un perímetro que sólo permite conectar al usuario autorizado y el dispositivo confiable a la aplicación protegida.

Se habla mucho del hogar inteligente, de ese hogar conectado a internet que nos hace más fácil el día a día. Pero además de las enormes posibilidades que ofrece, también genera problemas de seguridad. Clave en la interconexión de dispositivos para el control del hogar digital es Message Queuing Telemetry Transport (MQTT), un protocolo que es seguro en sí mismo, pero como ocurre en muchas ocasiones, si su implementación no se hace correctamente puede generar grandes problemas de seguridad.

Cada día nos despertamos con una brecha de seguridad, una empresa atacada con éxito, nuevos tipos de malware y ataques cada vez más complicados. Las propuestas de pentesting tradicionales, aplicadas un par de veces al año, se quedan cortas. Llega la era del BAS, o Breach and Attack Simulation, que permite a las organizaciones ejecutar simulaciones de ciberseguridad continuas y bajo demanda en cualquier momento sin afectar sus sistemas

La Seguridad Cloud centra otro de nuestros #DesayunosITDS, en el que hemos reunido a Ignacio Gilart, CEO de WhiteBearSolutions; Raúl Flores, Senior Systems Engineer de Infoblox y César Moro, Sales Consultant Quest Software para plantear algunas de las preocupaciones que plantea el uso de la nube.

Y por último os ofrecemos un resumen de algunos de los anuncios, investigaciones e informes más destacados que se han presentado en Black Hat USA, una de las conferencias de seguridad más importantes del mundo que se celebra cada verano en Las Vegas.

¿Te interesa la seguridad? Entonces seguro que te gusta este número de IT Digital Security.

DESCUBRE LAS **TENDENCIAS** QUE DEFINEN EL **FUTURO DIGITAL**

it TRENDS

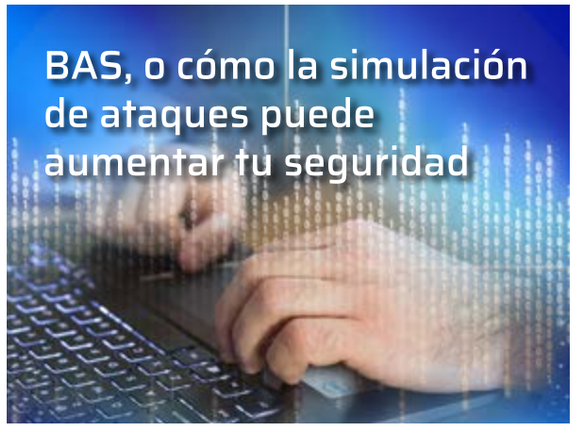
Sumario

En Portada

Black Cloud viene al rescate

Actualidad

El hogar inteligente,
el hogar conectado,
¿el hogar inseguro?



BAS, o cómo la simulación de ataques puede aumentar tu seguridad

Agosto en Las Vegas

No solo IT

Seguridad gestionada como bote salvavidas en el viaje digital de las organizaciones

Si la formación continuada ha sido siempre importante, hoy es imprescindible

¿Te avisamos del próximo IT Digital Security?

Desayunos ITDS

Los retos de la Seguridad Cloud

Índice de anunciantes

Ingecom

Trabajamos para Ti

Si te gusta la CiberSeguridad y quieres unirte a un equipo de profesionales de la misma, ponte en contacto con nosotros

www.ingecom.net info@ingecom.net

MADRID C/ Infanta Mercedes, 90 - 8ª Planta – 28020 Madrid – Tel.: +34 91 571 51 96 Fax: +34 94 441 05 39
BILBAO C/ Máximo Aguirre, 18 Bis - 8ª Pl. – 48011 Bilbao (Bizkaia) – Tel.: +34 94 439 56 78 Fax: +34 94 441 05 39
LISBOA Edificio Infante, Avenida D. João II, 35, 11ºA – 1990-083 Lisboa – Tel.: +351 21 012 65 65

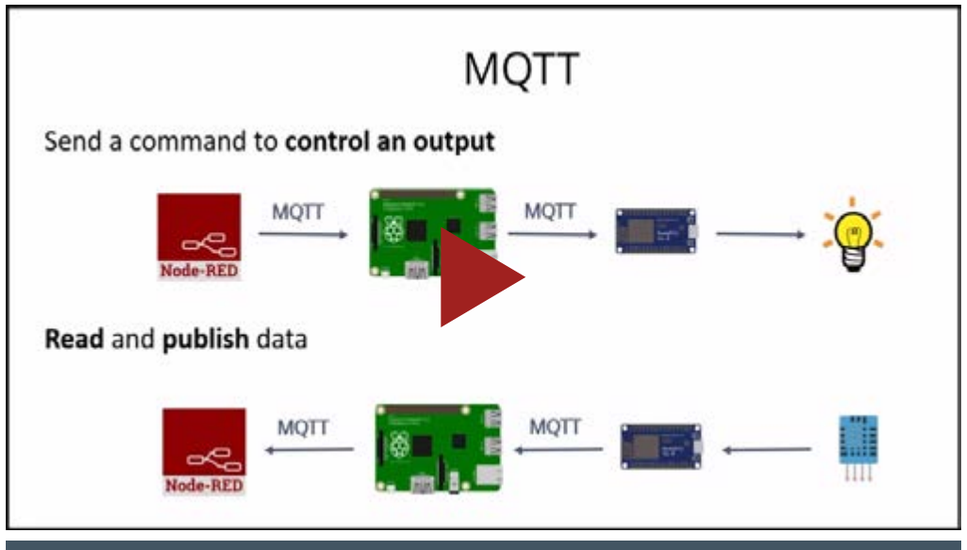
A10 · algosec · ALIEN VAULT · allot See. Control. Secure. · Array NETWORKS · Bitdefender · CYBONET · CYMULATE

FORCEPOINT · ForeScout · F-Secure · GARLAND TECHNOLOGY · Hdiv · McAfee Together is power. · MobileIron

mojo Networks · RAPID7 · sealpath · Terafence · thycotic · viewtinet · wbsgo

El hogar inteligente, el hogar conectado, ¿el hogar inseguro?

Mucho se habla del IoT, de ese internet de las cosas que se supone que hace más inteligente un simple sensor, una bombilla, un termostato. Quizá se hable tanto como se tema, porque si algo está trayendo ese Internet de las cosas además de enormes posibilidades, es un montón de problemas de seguridad. La mayoría llegan de base, en un firmware mal desarrollado y que además no se puede cambiar. En todo caso, a poco que sea el problema, cuando la cantidad de dispositivos afectados se suman en miles de millones, todo se multiplica.



¿QUÉ ES MQTT Y CÓMO FUNCIONA? CLICAR PARA VER EL VÍDEO

MQTT, los usuarios configuran un servidor que en el caso de los usuarios es un ordenador o incluso un mini ordenador como Raspberry Pi, con la cual los dispositivos pueden conectarse y comunicarse. Se trata de un protocolo seguro en sí mismo, pero como ocurre en muchas ocasiones, si su implementación no se hace correctamente puede generar grandes problemas de seguridad. Y eso es lo que pone de manifiesto un reciente informe de Avast.

La compañía de seguridad ha utilizados Shodan IoT y ha detectado más de 49.000 servidores MQTT visibles públicamente en Internet como consecuencia de una configuración incorrecta del protocolo. “Esto incluye más de 32.000 servidores que no tenían protección con contraseña, lo que pone a estas casas inteligentes y negocios que usan dichos servidores MQTT en riesgo de filtración de datos”, explica Martin Hron, investigador de seguridad de Avast, añadiendo que no sólo se podrían manipular los sistemas de entretenimiento, sino abrir una puerta. Es más, bajo ciertas condiciones, los ciberdelincuentes incluso pueden rastrear el paradero de un usuario, lo que puede ser una seria amenaza para la privacidad y la seguridad.

Los sistemas que te permiten controlar tu hogar conectado desde un dispositivo móvil y desde cualquier parte del mundo existen. La gran pregunta es: ¿Son seguros?

Poco a poco nuestros hogares se van llenando de cosas capaces de conectarse a internet. Si hace no mucho se contabilizaban el número de ordenadores, portátiles, tabletas, teléfonos e incluso televisores como elementos conectados, y se hablaba del número de pantallas que tenían los usuarios, ahora se suman relojes, pulseras de fitners, enchufes, bombillas, termostatos, alarmas. Está claro que es un paso inevitable, como lo es que podamos desarrollar algún tipo de control con ello.

La clave de la interconexión de dispositivos para el control del hogar digital es un protocolo: Message Queuing Telemetry Transport (MQTT). El protocolo MQTT es el que se utiliza para interconectar y controlar los dispositivos de un hogar inteligente a través de un hub. Al implementar el protocolo

Por qué es necesario el protocolo MQTT

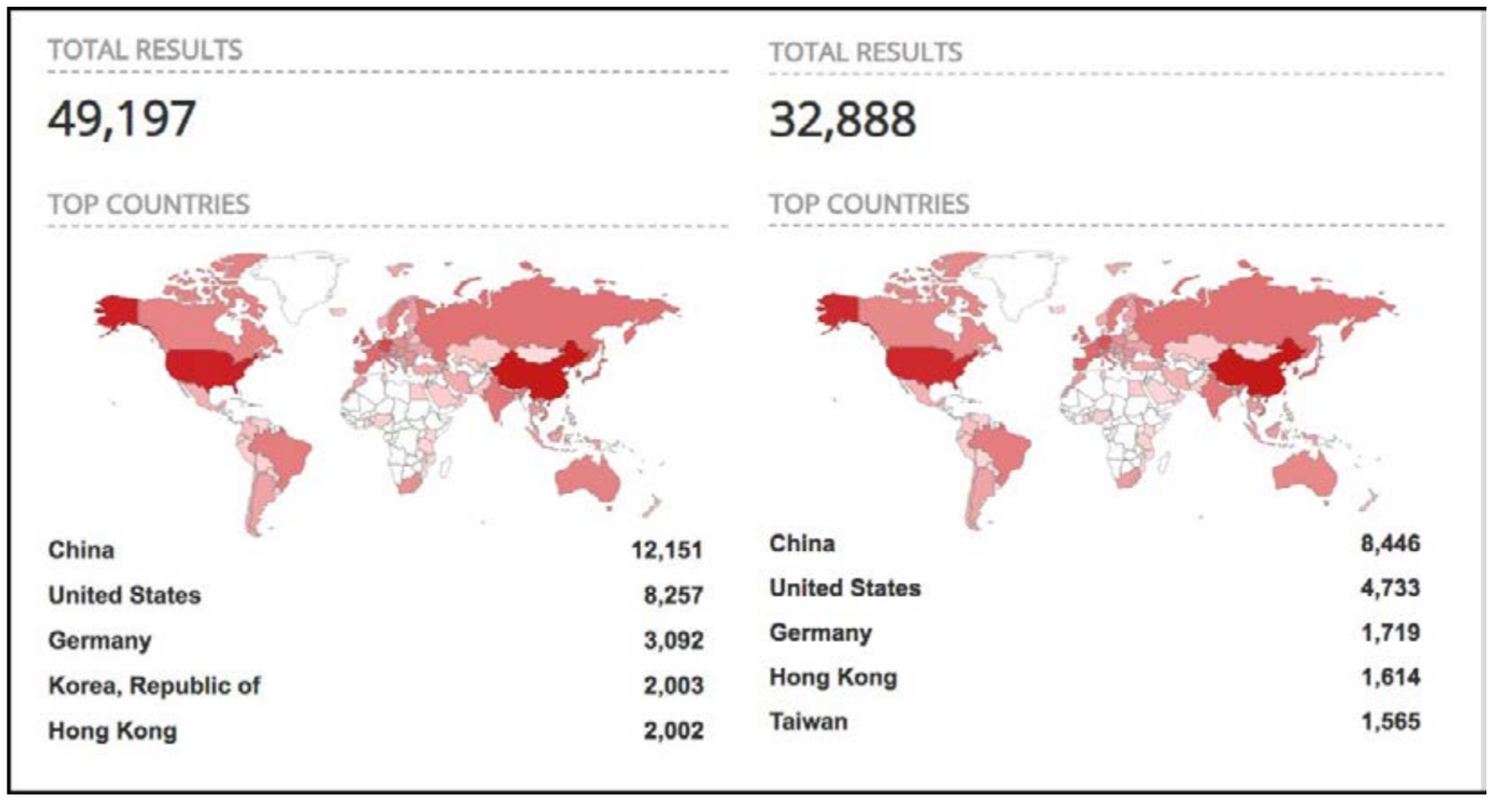
Controlar de manera manual un puñado de dispositivos no es problema, pero cuando la cifra crece puede convertirse en un imposible. Llega un momento en que sin automatización no puede haber gestión; ese momento en que los dispositivos inteligentes se conectan unos con otros y cooperan en la realización de tareas en las que no se requiere

interacción humana; ese momento en el que llegas a casa, la puerta del garaje se abre, las luces se encienden, la calefacción ha arrancado hace veinte minutos y la música suena en el salón.

En todo ello han participado sistemas de localización que determinan que el usuario está llegando a casa a una hora en la que se requiere de luz, a una temperatura que inicia el termostato y en el momento del día que necesitas desconectar escuchando algo de buena música. El entorno puede ser idílico mientras que un problema de seguridad no lo convierta en un infierno.

Es decir, los sistemas que te permiten controlar tu hogar conectado desde un dispositivo móvil y desde cualquier parte del mundo existen. La gran pregunta es: ¿Son seguros?

Message Queuing Telemetry Transport, O MQTT, fue desarrollado a finales de los años 90 como uno de los protocolos SCADA, y por tanto utilizado principalmente en entornos industriales para, como su nombre indica, transportar mensajes cortos de datos de telemetría. No existe un estándar relacionado con el formato de datos que transporta, de forma que puede llevar, virtualmente, cualquier carga. El



Según el motor de búsqueda Shodan, hay casi 49.000 servidores MQTT expuestos a Internet, de los que unos 32.000 no tienen protección de contraseña.

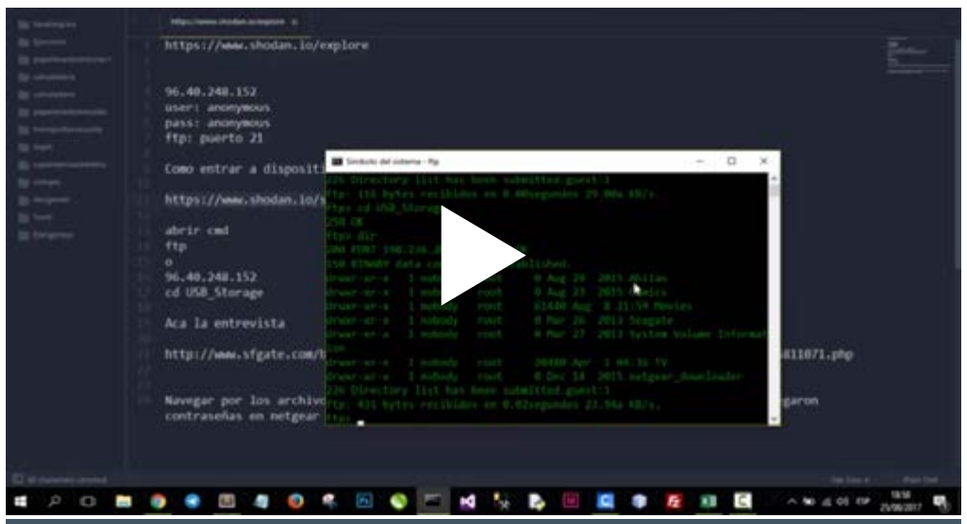
tto". De hecho, tanto MQTT como Mosquitto tienen amplias capacidades de seguridad, por ejemplo, para proporcionar un control de acceso detallado por usuario y tema. "Al igual que con muchas cosas, los problemas se crean en la implementación y configuración", dice el experto de seguridad de Avast, que en la investigación describe cinco maneras en las que los servidores MQTT mal configurados pueden ser explotados por los ciberdelincuentes.

En primer lugar, servidores MQTT abiertos y no protegidos que pueden encontrarse utilizando el motor de búsqueda Shodan. Cuando un ciberdelincuente se conecta a estos servidores pueden leer los mensajes transmitidos mediante este protocolo. En su estudio, Avast muestra que los chicos malos son capaces de leer el estado de los sensores inteligentes y saber cuándo se encienden y apagas

La clave de la interconexión de dispositivos para el control del hogar digital es el protocolo Message Queuing Telemetry Transport (MQTT)

protocolo se entiende como un modelo de suscriptor/editor; funciona como una fuente RSS: se suscribe a un tema, y una vez que alguien publica algo sobre el tema, la carga se entrega a todos los suscriptores.

Como asegura Martin Hron, "no existe un problema de seguridad con el protocolo MQTT ni con el software de servidor más común que implementa este protocolo (o broker como se lo conoce en el caso de MQTT), que se denomina Mosqui-



SHODAN

CLICAR PARA VER EL VÍDEO

¿Qué es Shodan?

Tan útil como polémico, Shodan es un motor de búsqueda para dispositivos conectados a Internet que cada mes analiza millones de dispositivos y servicios y los indexa en una base de datos.

El propio motor, en su página web, explica que tiene servidores localizados alrededor del mundo que rastrean Internet las 24 horas del día, los 7 días de la semana, para proporcionar la última inteligencia de Internet. "¿Quién compra televisores inteligentes? ¿Qué países están construyendo la mayor cantidad de parques eólicos? ¿Qué empresas se ven afectadas por Heartbleed? Shodan proporciona las herramientas para responder preguntas en la escala de Internet". El motor cuenta además con API públicas que permite a otras herramientas acceder a todos los datos de Shodan, de forma que permitiría saber si nuestros dispositivos conectados están correctamente protegidos o, de lo contrario, pueden estar al alcance de piratas informáticos.

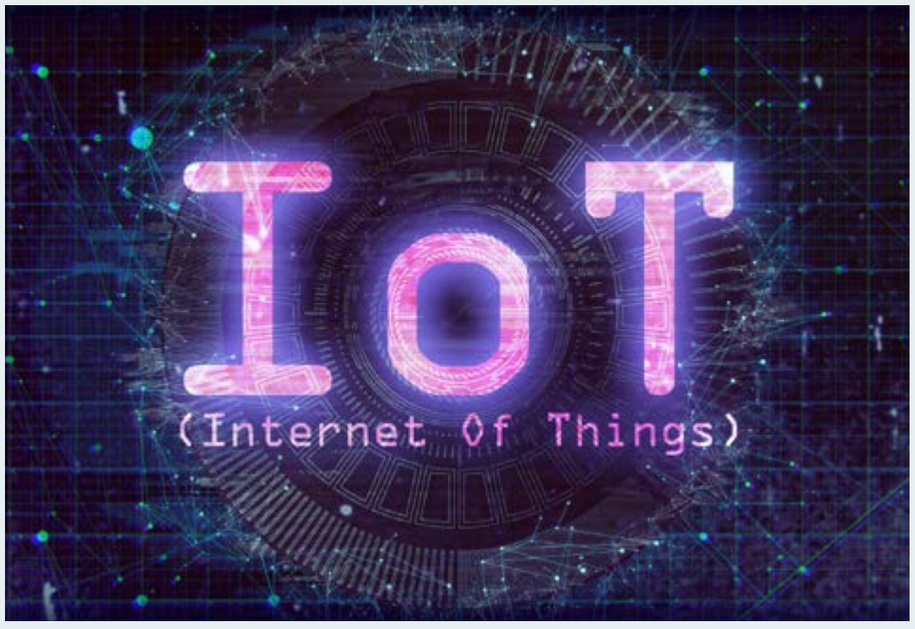
Shodan fue lanzado en 2009 por el programador informático John Matherly, quien, en 2003, concibió la idea de buscar dispositivos vinculados a Internet.

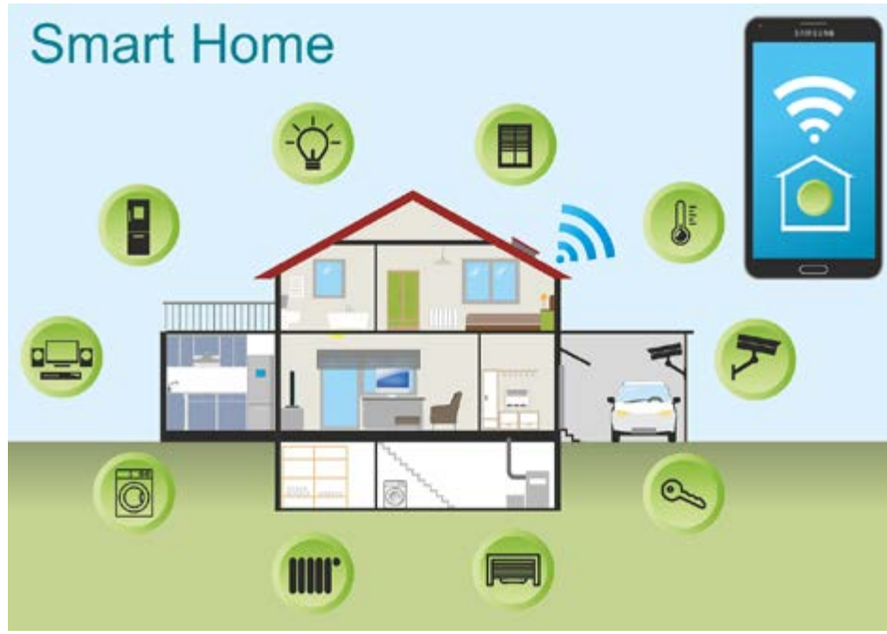
El nombre Shodan es una referencia a SHODAN, un personaje de la serie de videojuegos System Shock.

Los usuarios de Shodan pueden encontrar sistemas que incluyen semáforos, cámaras de seguridad, sistemas de calefacción para el hogar y sistemas de control para parques acuáticos, estaciones de servicio, plantas de agua, redes eléctricas, centrales nucleares y ciclotrones de aceleración de partículas....

En resumen, Shodan puede buscar, y localizar, cualquier dispositivo o servicio mediante reglas y filtros, pudiendo, por ejemplo, buscar versiones concretas de un servicio, servidores con un puerto determinado abierto o posibles vulnerabilidades, y en un país determinado.

Ya en septiembre de 2013 se hacía referencia al uso de Shodan para encontrar los fallos de seguridad en las cámaras de seguridad TRENDnet.





para abrir una puerta o encender la calefacción a deshora.

Hay un paso más: cuando un servidor MQTT está protegido, Avast descubrió que un hogar inteligente puede ser hackeado a través del panel de control. Explica la compañía que muchos usuarios utilizan configuraciones predeterminadas que vienen con su software Smart Home Hub y que a menudo no están protegidas con contraseña, lo que significa que un pirata informático puede obtener acceso completo al panel de control, lo que le permitía virtualmente controlar cualquier dispositivo conectado a través de ese panel.

Si tanto el servidor MQTT como el panel de control están convenientemente protegidos, en su estudio Avast descubrió que en el caso del software Home Assistant, las acciones SMB abiertas y no seguras son públicas y, por lo tanto, accesibles

> No existe un problema de seguridad con el protocolo MQTT, sino con su implementación y configuración

para los ciberdelincuentes. Explica la compañía en su estudio que SMB es un protocolo utilizado para compartir archivos en redes internas, principalmente en la plataforma de Windows. Avast encontró directorios compartidos públicamente con todos los archivos de Home Assistant, incluidos los archivos de configuración. En los archivos expuestos, Avast encontró un archivo que almacena contraseñas y claves en texto plano, lo que permitiría obtener el control completo de un hogar.

Los propietarios de la casa inteligente pueden usar herramientas y aplicaciones para crear un panel de control basado en MQTT y así poder controlar sus dispositivos conectados. Entre las herramientas está MQTT Dash con la que los usuarios tienen la opción de publicar la configuración que utilizan para poderla replicar fácilmente en tantos dispositivos como deseen. Según Avast, si el servidor MQTT utilizado no es seguro, un pirata puede acceder fácilmente al tablero del usuario, lo que le permite hackear fácilmente el hogar inteligente.

Finalmente, Avast descubrió que MQTT puede, en ciertas instancias, permitir a los ciberdelincuentes rastrear la ubicación de los usuarios, ya que los servidores MQTT normalmente se concentran en datos en tiempo real. Muchos servidores MQTT están conectados a una aplicación móvil llamada OwnTracks, que ofrece a los usuarios la posibilidad de compartir su ubicación con otras personas, pero también puede ser utilizado por propietarios inteligentes para que los dispositivos inteligentes del hogar puedan saber cuándo el usuario se acerca al hogar, para activar dispositivos inteligentes, como lámparas inteligentes. Para configurar la función de seguimiento, los usuarios deben configurar la aplicación conectándose a un servidor MQTT y exponiendo el servidor MQTT a Internet. Durante este proceso, los usuarios no están obligados a configurar las credenciales de inicio de sesión, lo que significa que cualquier persona puede conectarse al servidor MQTT. Los hackers pueden leer mensajes que incluyen el nivel de batería de un dispositivo, la ubicación que usa puntos de latitud, longitud y altitud, y la marca de tiempo para la posición.

Enlaces de interés...

- Are smart homes vulnerable to hacking?

Compartir en RRSS

¿Te avisamos del próximo IT Digital Security?

SOPHOS

INTERCEPT X

VER EL FUTURO ES EL FUTURO DE LA CIBERSEGURIDAD.

- Protección Anti-Ransomware
- Protección Anti-Exploit
- Protección Predictiva Deep Learning
- Remediación y Limpieza Avanzados

Más información y pruebas gratuitas en:
www.sophos.com/es-es

BAS, o cómo la simulación de ataques puede aumentar tu seguridad

Múltiples capas y controles preventivos son claves para conseguir una arquitectura de red segura. En ocasiones los controles fallan, y por eso es esencial que una arquitectura integral de defensa en profundidad incluya controles detectives diseñados para monitorizar y alertar sobre actividades anómalas. El establecimiento de un programa de ejercicio de simulación de brechas y ataques (BAS) bien definido permite evaluar la efectividad de los procedimientos de seguridad, la infraestructura, las vulnerabilidades y las técnicas mediante el uso de una plataforma de simulación de brechas y ataques.

Que los ciberdelincuentes son cada vez más agresivos no es un secreto, como tampoco lo es que los fabricantes de seguridad están respondiendo con nuevas tecnologías.

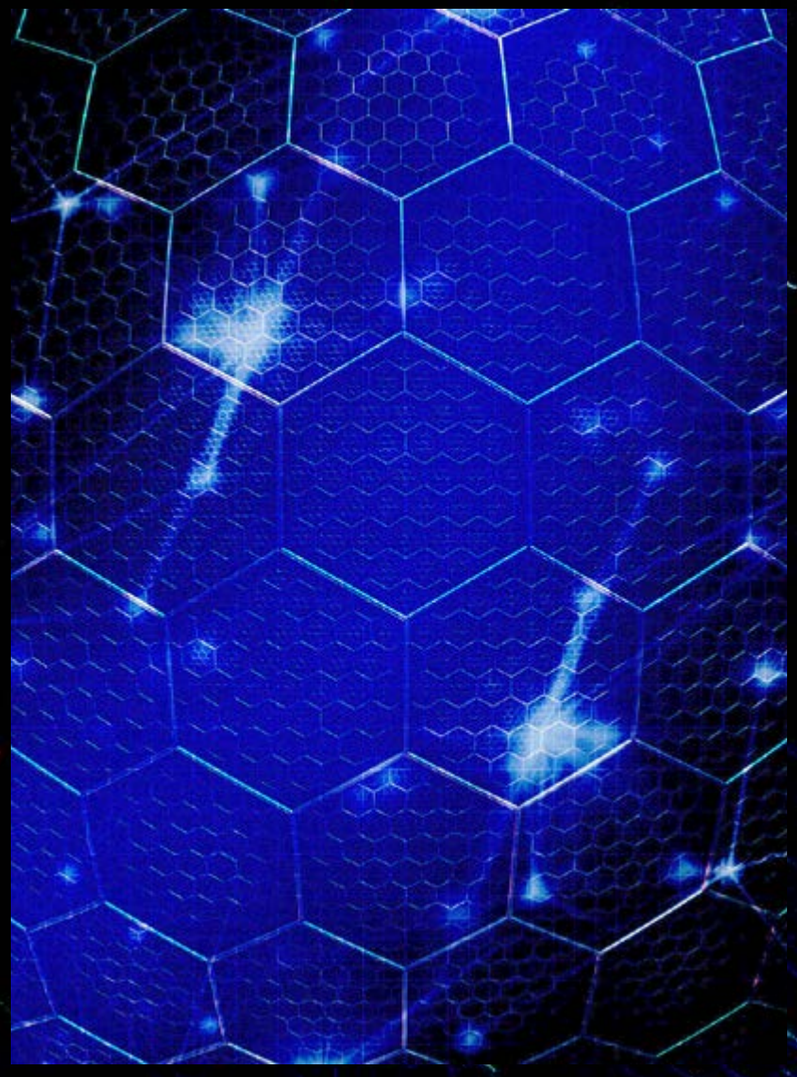
La situación actual del mercado de la ciberseguridad es la que sigue: crecerá un 8,5% este año hasta los 96.600 millones de dólares, estando el mayor incremento y ventas en las tecnologías empresariales, según Gartner. El mercado de consumo, valorado en unos 7.750 millones de dólares permanecerá plano. Los servicios son el mayor segmento, 57.720 millones de dólares, seguido de infraestructura con 17.540 millones de dólares, seguridad de red con 11.920 millones y gestión de identidades y accesos (4.720 millones). Las cifras son de Gartner, que asegura que las soluciones BAS (Breach and attack simulation) representan un nuevo y emergente mercado adyacente al mercado de Vulnerability Assessment; "realizan pruebas de seguridad automatizadas y modelan la cadena de ataque que identifica la ruta más probable que un atacante utilizaría para comprometer un entorno .... También ayudan a presentar una visión más real del mundo de las vulnerabilidades que conducirán a una brecha contra la cantidad total de vulnerabilidades presentes".

La Normativa europea sobre protección de datos, GDPR, están impulsando el gasto en seguridad. Datos de la misma consultora indican que las empresas de Europa están invirtiendo 1,4 millones de dólares en cumplimiento, cifra que en Estados Unidos es de un millón para cumplir con la nueva ley de seguridad. La lista de las inversiones en seguridad para los próximos dos años se inicia con productos de CASB (Cloud Access Security Manager), seguido de gestión de accesos con privilegio, monitorización y análisis de conducta de entidades y usuarios (UEBA), testing de seguridad de las aplicaciones, cifrado/tokenización, gestión de eventos y seguridad de la información (SIEM), endpoint detection and response (EDR), data loss prevention (DLP) y seguridad del Gateway.

CYMULATE BREACH & ATTACK SIMULATION PLATFORM **CLICAR PARA VER EL VÍDEO**

Todas estas herramientas y otras muchas que no aparecen porque son inversiones consolidadas en el tiempo, tienen como objetivo mantener las empresas a salvo. El número de herramientas y productos que se gestionan crece, de hecho, una organización de tamaño medio invierte en al menos 35 tecnologías de seguridad diferentes, y eso hace que el control sobre

Priorizar la inversión en seguridad es el desafío más grande de muchas organizaciones



BAS, o el fin del pentesting simple

El pentesting, como lo conocemos hoy, dejará de existir. La frase es de Augusto Barros, analista de Gartner, quien antes de generar un cisma, en el siguiente párrafo, añadía: "el pentesting simple, para fines de búsqueda de vulnerabilidades puras y sin la intención de replicar el comportamiento de amenaza, se desvanecerá". Una actividad muy diferente a otros ejercicios de calidad que replican el enfoque y los métodos de las amenazas y que están creciendo.

A través de un post, el analista de Gartner mete en el terreno de juego las herramientas BAS y explica que si son capaces de automatizar el pentester simple, realizar el ciclo básico de escanear/explotar/repetir con un simple clic, "¿por qué utilizar un humano para hacer eso? La herramienta puede garantizar la coherencia, proporcionar mejores informes y hacerlo más rápido. Sin mencionar que requieren menos habilidades (¡ni siquiera necesitas saber cómo usar Metasploit!)".

El hecho de que haya empresas que no se decidirán a comprar y desplegar herramientas BAS hace que, según Augusto Barros, queden opciones para los proveedores de servicios que venden pentesting básico, pero al mismo tiempo, el hecho de que BAS también se pueda ofrecer como SaaS, vuelve a poner una losa sobre el método tradicional del pentesting simple

Pero, puede argumentar, no todos comprarán y desplegarán esas herramientas, por lo que todavía hay espacio para los proveedores de servicios que venden pentesting básico. ¡Bueno no! BAS no se ofrecerá solo como algo que puede comprar e implementar en su entorno. También, como todas las demás herramientas de seguridad, se ofrecerá como SaaS. Con eso, ya no necesita comprarlo e implementarlo, puede "alquilarlo" para un solo ejercicio. Esto es más simple que contratar pentesters, y proporciona mejores resultados (una vez más, estoy empezando a sonar repetitivo, pero excluyendo los pentest realmente buenos ...). Entonces, ¿por qué contratarías gente para hacerlo?

"En el futuro, sus opciones para probar su seguridad serán escaneo de vulnerabilidades, BAS o equipo rojo. Cada uno con objetivos, ventajas y desventajas específicas, pero ya no es necesario que las personas sigan haciendo pentest básicos", concluye el analista.

los mismos sea cada vez más complicado. Priorizar la inversión en seguridad es el desafío más grande de muchas organizaciones porque los programas de evaluación de vulnerabilidad y las pruebas de penetración no pueden conectar los riesgos con las métricas de negocios.

Las plataformas basadas en tecnología BAS permiten a las organizaciones ejecutar simulaciones de ciberseguridad continuas y bajo demanda en cualquier momento sin afectar sus sistemas. Bajo un modelo de Software-as-a-Service (SaaS), simula ataques multivectoriales, internos o externos al enfocarse en las vulnerabilidades más recientes. Estos ataques simulados exponen brechas de vulnerabilidad que le permiten a la organización determinar si su arquitectura de seguridad brinda la protección adecuada y si sus configuraciones se implementan correctamente.

Pentesting, más de medio siglo de historia

Corría la década de los '60 cuando la popularidad de los sistemas informáticos de tiempo compartidos accesibles a través de líneas de comunicación telefónica crearon nuevas preocupaciones de se-

No existe el “milagro” israelí

Ocupada de liderar Cymulate, una empresa de origen israelí, desde el pasado mes de noviembre, Daniela Kominsky lleva dieciséis años en España. Desde hace seis trabaja con empresas de ciberseguridad en Israel, organizando viajes que permiten a bancos y grandes empresas españolas conocer la tecnología del país, y a las empresas de Israel poder mostrar sus innovaciones. No es de extrañar que forme parte de la Cámara de Comercio España-Israel, ni que le inviten a dar conferencias en universidades. “A veces se habla del milagro israelí, pero la verdad es que milagro hay bastante poco”, dice esta directiva. Lo que ocurre en Israel a nivel de tecnología es la suma de muchas decisiones estratégicas que se tomaron hace más de 20 años.

Explica Daniela Kominsky que Israel era un país con una economía basada fundamentalmente en la agricultura, y en un momento determinado dieron el salto hacia la tecnología, para lo cual el estado, junto con el sector privado, crearon y apoyaron aceleradoras, atrayendo a los que sí sabían cómo era el negocio de la tecnología, atrayendo capital extranjero y realzando la importancia de la Universidad.

“No hay que olvidar también que en Israel chicos y chicas tienen que pasar por el ejército, que es un espacio muy potente de formación y que cuenta con una unidad específica que se llama 8200 que es una unidad de élite donde se desarrolla mucha de esta tecnología”, y estos chicos y chicas salen del ejército con mucho conocimiento, con mucha experiencia en la tecnología que han desarrollado. Todo eso lo aplican luego en el sector civil y por eso, dice Daniela Kominsky, “es un ecosistema muy potente”.

Otras las empresas de seguridad de Israel son Check Point Software, que además es la mayor empresas de tecnología del país; CyberArk, que ofrece soluciones de seguridad para cuentas con privilegios; Imperva, que fundada por Shlomo Kramer, co-fundador de

Check Point, se dedica a ofrecer seguridad para los centros de datos; fundada en 2009, Votiro desarrolló su Spear-Phishing Protection Service para desinfectar todos los archivos adjuntos a los mensajes de correo electrónico; Argus Cyber Security fue fundado por veteranos de la Unidad de Inteligencia israelí 8200 para mantener a los automóviles del futuro a salvo de los piratas informáticos; Covertix ha ganado varios premios por su sistema SmartCipher, que asigna políticas y derechos a los archivos de datos, bloqueando virtualmente a usuarios no autorizados.

guridad. En 1965, en una de las primeras conferencias de seguridad organizada por la System Development Corporation (SDC), se detectó que uno de sus empleados había evadido las protecciones añadidas al sistema informático de tiempo compartido AN/FSQ-32 de la SDC. Que el otro único modelo fabricado estuviera en manos de la Agencia Central de Inteligencia de los Estados Unidos motivó que se propusiera una de las primeras peticiones formales para usar la penetración de computadoras como una herramienta para el estudio de la seguridad de sistemas. Según recoge Wikipedia, fue durante esa conferencia donde “los expertos en seguridad informática Willis Ware, Harold Petersen y Rein Tern, todos de la Corporación RAND, y Bernard Peters de la Agencia de Seguridad Nacional (NSA), utilizaron la frase ‘penetración’ para describir un ataque contra un sistema informático”.

En años sucesivos, el uso del pentesting como una herramienta para la evaluación de seguridad se volvería más refinada y sofisticada. Por cierto, ¿qué es

Desde su aparición en los '60, el uso del pentesting como una herramienta para la evaluación de seguridad se volvería más refinada y sofisticada

el pentesting? Es la práctica de atacar diversos entornos con la intención de descubrir vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas.

Lo que impulsa este mercado de pruebas de penetración no es otra cosa que la necesidad de protección contra diversos ciberataques y el aumento del número de usuarios y aplicaciones móviles. El mercado de pruebas de penetración está creciendo rápidamente debido a las crecientes necesidades de seguridad de las tendencias de Internet de las cosas (IoT) y Bring Your Own Device (BYOD) y una mayor implementación de aplicaciones empresariales basadas en la web y en la nube. Se espera que este mercado crezca desde los 594,7 millones de dólares de 2016 hasta los 1.724,3 para 2021, según MarketsandMarkets.

Lo habitual es que las empresas realicen una o dos acciones de pentesting al año para conocer el estado de su seguridad. Y a la sombra de este mercado nace BAS. En un post publicado en el blog de Gartner dos ejecutivos de la consultora hablan de ir "más allá del pentesting, teaming rojo, pruebas

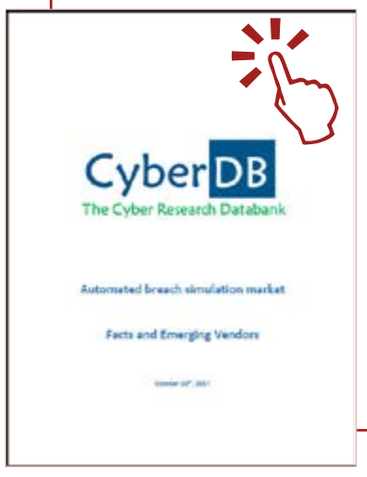
> Según Gartner, las soluciones BAS (Breach and attack simulation) representan un nuevo y emergente mercado adyacente al mercado de Vulnerability Assessment

de aplicaciones, evaluaciones de madurez [bueno, el último elemento no es realmente una prueba per se], etc. al meta-desafío de probar su seguridad general. ¿No será divertido?", para a continuación anunciar que quieren ver más de cerca las tecnologías llamadas Breach and Attack Simulation (BAS), enumerar algunos fabricantes de los que han oído hablar, como Cymulate, SafeBreach o Verodin; "Tal y como lo entendemos, estas herramientas pretender realizar cosas similares a lo que harán los atacantes (como movimiento lateral, exfiltración, abuso de privilegios, quizás explotación, etc.) para probar cómo funcionan sus controles de seguridad (prevención, detección, respuesta)".

De forma que, evolución del pentesting, BAS es un concepto relativamente nuevo. Sin tener un cuadrante dedicado, Gartner ya ha acuñado el término y enumera algunas empresas relevantes, una de las cuales de Cymulate, a la que la nombrado 'cool vendor' y sobre la que dice que "ofrece beneficios

MERCADO DE SIMULACIÓN DE BRECHAS Y ATAQUES (BAS)

Este documento elaborado por CyberDB, que es una plataforma de investigación que proporciona datos y análisis sobre proveedores y soluciones de TI, se centra en los factores clave para este mercado de BAS, qué son las tecnologías de simulación de brechas y ataque, las técnicas de prueba de seguridad, las herramientas y la oferta de servicios de los proveedores emergentes, y la visión general del mercado.



Las soluciones BAS realizan acciones similares a lo que harán los atacantes para probar cómo funcionan sus controles de seguridad (prevención, detección, respuesta)

inmediatos mediante la automatización de procesos que los usuarios pueden programar fácilmente y comenzar una evaluación con cualquiera de los vectores de amenaza obteniendo resultados y recomendaciones para mitigar en el momento".

Con menos de dos años de vida y más de cien clientes en todo el mundo, la plataforma de simulación de brechas y ataque de Cymulate, basada en la nube, evalúa la postura de seguridad de los clientes utilizando métodos de ataque reales. Al exponer las vulnerabilidades ocultas y ofrecer información procesable, Cymulate ayuda a identificar y resolver las brechas de seguridad antes de que sea demasiado tarde.

Daniela Kominsky es la responsable de Cymulate en España, una compañía israelí que trabaja a través de Ingecom. "Nosotros no venimos a evaluar el pentesting, sino a evolucionarlo", asegura Daniela. Explica la directiva que uno de los fundadores de la compañía, experto en pentesting, se dio cuenta que la necesidad que tenían las empresas de poder evaluar de manera continua el nivel de seguridad real de las organizaciones. Porque la "evaluación continua" es la principal diferencia entre BAS y el pentesting tradicional.

Cuando se realiza un pentesting, el cliente recibe un informe que, en un mercado como el de la seguridad, cuando se crean malware y se detectan vulnerabilidades a diario, queda desactualizado en muy poco tiempo. Por supuesto que los pentesting sí que sirven, asegura Daniela Kominsky, "pero cada día nos levantamos con una nueva amenaza o alguna noticia de empresas que han sido comprometidas", por eso, "lo que tiene realmente de potente esta tecnología es la evaluación y simulación continua; es probar de manera continua todos los controles y todos los productos que protegen a nuestra organización".

Y eso es lo que hace Cymulate, que ha desarrollado una plataforma de simulación de ataques, automatizada y multivector que responde de manera continua a la pregunta: ¿cuán seguro estoy en estos momentos? Esto es lo que te permite la tecnología BAS.

"Nosotros lo que hacemos es simular ataques para poner a prueba, por ejemplo, el correo electrónico, la navegación, las aplicaciones web, campañas de phishing… Después de la simulación de los ataques lo que hacemos es un reporte con el detalle de las

diferentes vulnerabilidades y recomendaciones de mitigación", nos cuenta Daniela Kominsky, a quien preguntamos si en esas pruebas de cómo están funcionando las diferentes herramientas y soluciones de seguridad se han encontrado con alguna que no funcione como se espera. Asegurando que las empresas están invirtiendo mucho dinero en seguridad dice la responsable de Cymulate para España, Portugal y Latinoamérica que "nosotros no cuestionamos los productos", reconoce en todo caso, que muchas empresas no aprovechan el 100% de las capacidades que les ofrecen estos productos o soluciones. Según datos que maneja la compañía, las empresas sólo utilizan entre el 20% y el 30% de las capacidades de los productos y en ocasiones las brechas o problemas de seguridad surgen por problemas de configuración. "La idea es que utilizando nuestra tecnología pueden incrementar el ROI de las inversiones. Nosotros tenemos más de cien clientes a nivel mundial y lo que nos dicen es que utilizando Cymulate pueden incrementar entre un 20-30% el nivel de seguridad de la compañía sin más inversiones, lo que es muy interesante".

Sobre el tipo de empresas que están adoptando la tecnología BAS, los verticales van desde la banca y aseguradoras, pero también con empresas de infraestructuras críticas, retail. incluso se acaba de cerrar un acuerdo con las fuerzas y cuerpos de seguridad del estado. "En general es más fácil para las grandes corporaciones, pero también para las empresas de entre 400 y 500 empleados", dice Daniela Kominsky.

En todo caso el camino de Cymulate es largo. Trabajan a través de canal de distribución y cuentan con dos perfiles, por un lado, el partner que vende la solución y el que la ofrece como un servicio, que es cuando se puede llegar a más empresas, o de menor tamaño.

No es el momento de dar cifras, salvo los más de cien clientes que tienen en España y las dos personas que actualmente se encargan de la actividad de Cymulate en España, Portugal y Latinoamérica, pero el futuro, dice Daniela, es prometedor. "Sí te puedo decir que cada vez estamos teniendo más clientes, y el pronóstico para fin de año será muy bueno porque se suman muchas empresas que no puedo mencionar. Acabamos de cerrar un acuerdo con los cuerpos de seguridad del estado y en las próximas semanas se irán anunciando novedades". it

Compartir en RRSS

Enlaces de interés...

- Cymulate abre oficina en España
- Ingecom factura un 41% más en el segundo trimestre
- W Mercado de simulación de brechas y ataques
- La ingeniería social sigue estando detrás de demasiados ataques

smartLogin

wbsgo

Trabajamos para hacer de la tecnología un bien más accesible, democratizando su uso

Soluciones globales para la seguridad del dato **esté donde esté**

WBSAirback
Storage &
Backup
Appliance

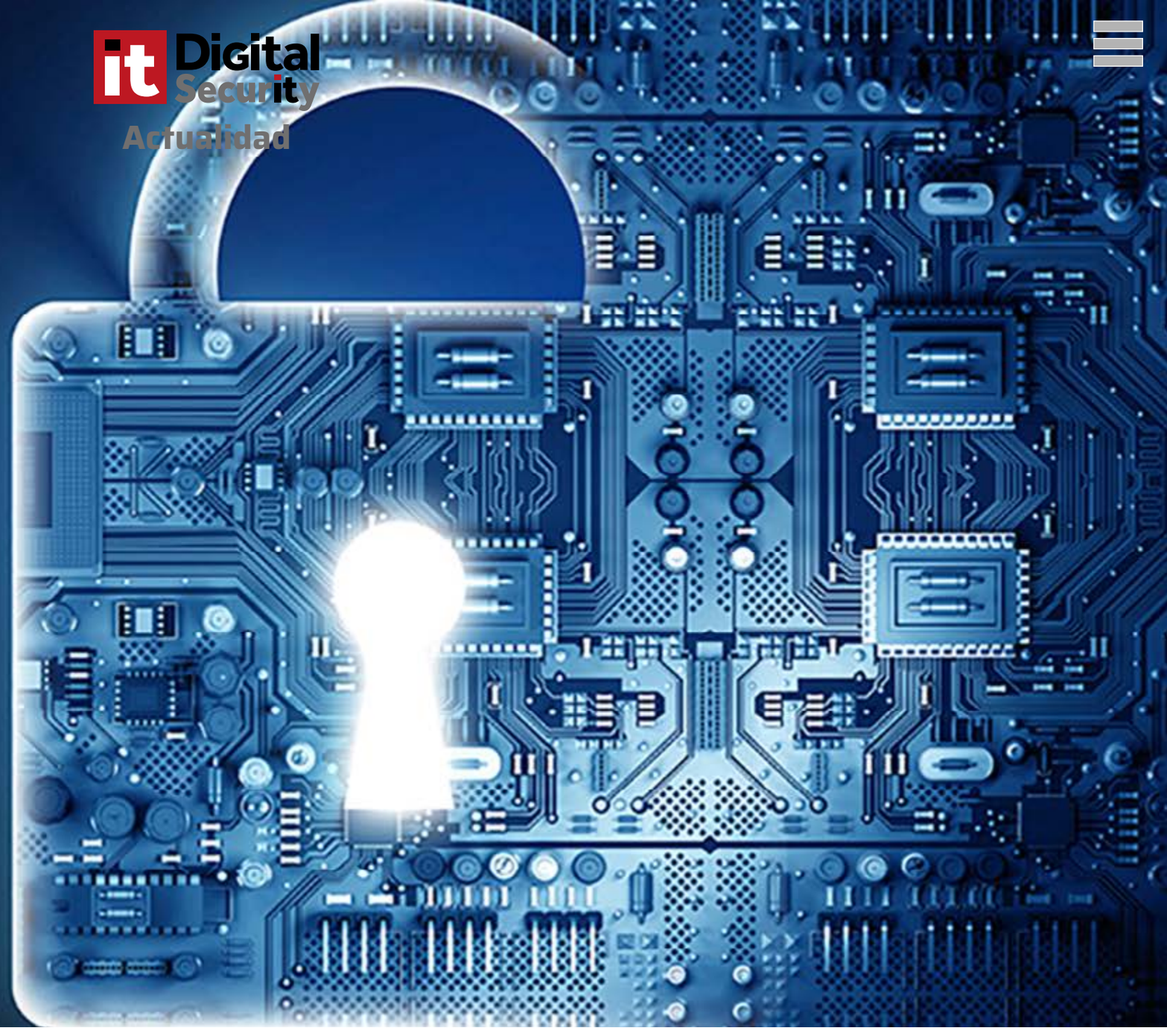
WBSVision &
SmartLogin
Identity and
Access
Management
Appliance

Tecnología basada en open source y estándares

www.wbsgo.com | **info@wbsgo.com**

Agosto en **Las Vegas**

Ir al desierto en una de las épocas más calurosas del año no es algo que se haga si no es por una buena razón. Y precisamente hay dos buenas razones para ir a Las Vegas en Agosto: Black Hat USA y DefCon, dos grandes eventos de seguridad que reúnen a miles de expertos que tienen la oportunidad de demostrar, año tras año, que el de la ciberseguridad es un mercado en expansión y que el gran problema sigue siendo cómo hacer frente a multitud de amenazas, de diferentes actores haciendo uso de las últimas tecnologías.



El mes de agosto de 2018 no ha sido diferente. Se demostró que, a pesar de haber mejorado, aún se puede hacer más para hacer frente a los ciberataques; que la inteligencia artificial y el machine learning también se utilizan para mejorar un ciberataque; que el internet de las cosas es un vector de ataque cada vez más atractivo; que el cryptojacking es muy rentable, casi más que el ransomware… y que los aviones, los coches, las webs, los cajeros o las impresoras son relativamente fáciles de hackear.

Este tipo de eventos no sólo sirven como centros de formación y de certificación, sino de información. Allí se conocen las últimas herramientas, los últimos lanzamientos, investigaciones que ponen los pelos de punta y las pruebas de concepto que hacer realidad lo impensable.

Entre las novedades, cuatro herramientas de seguridad que ayudarán a los profesionales a resolver problemas difíciles e investigar de una manera diferente. Security Boulevard se encargaba de enumerarlas en un artículo: ChipWhisperer-Lint, NLP Social Engineering Analysis Tool, Deserialization Toolkit y Kernel Exploit Framework

Sobre la primera, es un desarrollo de Colin O'Flynn, un hacker que busca vulnerabilidades en hardware y que lanzaba la herramienta, de código abierto, para detectar de una manera automatizada ataques de canal lateral, más populares desde la aparición de Spectre y Meltdown a primeros de año.

NLP (Natural Languaje Processing) propone utilizar el procesamiento del lenguaje natural para ayudar a detectar interacciones maliciosas y ataques basados en ingeniería social

En el pasado, la explotación de fallos de deserialización ha sido principalmente manual, pero un ingeniero de seguridad de Netflix, Ian Haken, propone nueva herramienta y método, Deserialization Toolkit, que automatiza los descubrimientos de deserialización y brinde a los equipos defensivos una manera más fácil de priorizar errores de deserialización basados en la capacidad de explotación.

El proceso de descubrir las vulnerabilidades del kernel se ha automatizado, pero hasta ahora la explotación todavía ha necesitado una gran cantidad de trabajo manual. Tres investigadores está a punto de cambiarlo con Kernel Exploit Framework, que presentaron en el evento junto con una serie de exploits descubiertos con la herramienta centrados en defectos de kernel que no habían ha sido confirmados como explotables en el pasado.

En Black Hat se conocen las últimas herramientas, lanzamientos, investigaciones y pruebas de concepto que hacer realidad lo impensable

Estudios

Entre las muchas funciones del evento está el presentar estudios que puedan aportar luz a lo que ocurre en el mercado, o simplemente ponga cifras a los que se sabe que ocurre. Entre lo que estudios que se presentaron el pasado mes de agosto destacamos el que recoge que el 65% de los responsables tecnológicos dicen que no tienen suficiente personal cualificado para afrontar las amenazas. Además, un 34% citan la falta de skills como una de las razones principales por las que las estrategias de seguridad de las empresas fallan.

También conocido como Dark Tangent, Jeff Moss es el fundador de Black Hat y DefCon, dos de las conferencias de seguridad más importantes del mundo.

Algo más curioso resultó el elaborado a raíz de una encuesta y cuya principal conclusión fue que el crimen organizado juega un papel mucho menos importante en el mundo del cibercrimen de lo que la gente se espera

Durante un período de siete años, Jonathan Lusthaus, director del proyecto de ciberdelincuencia humana en el departamento de sociología de la Universidad de Oxford, estudió el papel de la mafia/organizaciones en los ciberdelitos para concluir que, si bien el crimen organizado brinda ayuda u orientación a las bandas del cibercrimen en algunos casos, la mayor parte de estas actividades son realizadas por una nueva clase de delincuentes.

Según Lusthaus, está claro que están usando tecnología para mejorar sus otras operaciones criminales, aunque esto no es un cibercrimen per se. Y asegura también el investigador que hay cuatro actividades en donde las organizaciones del crimen organizado se cruzan con el cibercrimen: brindar protección a los ciberdelincuentes, invertir en operaciones de ciberdelincuencia, actuar como “proveedores de servicios” para un esquema de cibercrimen y ayudar a guiar a los ciberdelincuentes en sus actividades.

Como no podía ser de otra manera, el IoT también es objeto de estudio, y llamó la atención la encuesta realizada por la empresa Armis entre más de 130 profesionales que atendieron a la conferencia y que recogió que el 93% veían el futuro del IoT no como algo necesariamente más inteligente, sino más peligroso, pronosticando que las naciones

Parisa Tabriz, la Security Princess

“Hay que ser buen jugador de equipo”


Parisa Tabriz, Google

Entre las responsabilidades de Parisa Tabriz, directora de ingeniería de Google, el que Chrome sea más seguro, además de liderar el equipo de investigación de seguridad Project Zero de la compañía. Entre los mensajes de la que se conoce como la Security Princess en una de las conferencias más comentadas del evento, que el enfoque actual de la industria con respecto a la seguridad cibernética es insuficiente. “En esta sala se encuentran los mejores expertos del mundo en seguridad informática, que se está convirtiendo en la seguridad del mundo. Tenemos que hacer más para resolver los problemas”, aseguraba añadiendo que, aunque se han realizado grandes progresos durante la década, “hay más trabajo por hacer en un panorama cada vez más complejo”.

Según Tabriz, la forma de mejorar las cosas se divide en tres grandes pasos: abordar las causas raíz, elegir hitos y celebrar los logros, y construir una coalición fuera de la seguridad.

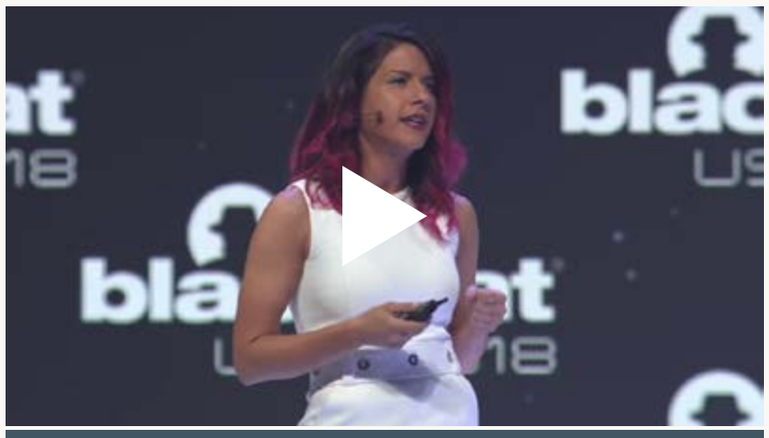
Comparaba la directiva la actual metodología de la industria con un juego de arcade, Whack-A-Mole, en el que las amenazas individuales son simplemente derrotadas una vez que se conocen o se ignoran hasta que se convierten en un verdadero problema, y aseguraba que debe atajarse el problema de raíz, para lo que deben plantearse cinco interrogantes, o cinco ‘¿Por qué?’ y ponía como ejemplo: ¿Por qué este error llevó a la ejecución remota de código?; ¿Por qué no lo descubrimos antes?; ¿Por qué nadie escribe pruebas o usa fuzzers?; ¿Por qué llevó tanto tiempo actualizar?; ¿Por qué se tardan cinco semanas en probar una solución?

Entre las cosas estratégicas que su equipo pudo hacer al abordar las causas raíz se encontraba mejorar la respuesta y los tiempos de parcheo para las vulnerabilidades. “Descubrimos que el tiempo de respuesta de los proveedores para arreglar las cosas variaba ampliamente”, dijo, “porque no siempre tenían incentivos para mejorar la seguridad”.

El paso fue que Project Zero estableciera una política de divulgación de 90 días: la cantidad de tiempo que dan a una empresa para corregir una vulnerabilidad antes de que se haga pública.

Otra de las iniciativas fue la adopción de HTTPS por defecto. Los resultados muestran que la adopción de HTTPS en Chrome aumentó de 45% a 87% y en Android de 29% a 77%.

Aseguró Parisa Tabriz que parte del éxito que ha conseguido Google procede de saber mantener a los equipos motivados durante proyectos a largo plazo de forma que incluso esos hitos actuaran como un faro para otros equipos fuera de la seguridad e incluso con otros proveedores que los cambios estaban en proceso. “Parte de mi trabajo es asegurarme de que mi equipo crea que el cambio es posible y se mantenga optimista a largo plazo”, dijo Tabriz y describió el proceso de cambio de las insignias de HTTPS en Chrome. “Celebramos muchas de las transiciones en público. Los hitos, cada uno de ellos, resultaron en retrocesos y también en ocasionales mensajes de odio. Pero cumplieron un propósito realmente importante: fueron un recordatorio para el mundo de que esto venía y ponga una fecha límite muy clara para que la gente trabaje hacia ella”.



La tercera propuesta de Tabriz para mejora la seguridad mundial es buscar coaliciones. Asegurando que los beneficios de todos los proyectos podrían no ser inmediatos, señaló que el trabajo para mejorar la arquitectura de Chrome que comenzó en 2012 e implicó el aislamiento del site “nos dio una gran ventaja en Spectre”, que los proveedores de hardware descubrieron a mediados de 2017. Spectre es una vulnerabilidad en las CPU que permite ataques de canal lateral con variantes que también afectan a los navegadores, pero pueden mitigarse con el aislamiento del sitio. “Para hacer que un proyecto como este funcione a gran escala, se necesitan muchos participantes”, y agregó que, si las coaliciones van a funcionar, “hay que ser un buen jugador de equipo”.

estado explotarán los dispositivos conectados en masa durante el próximo año.

Además, un 23% de los encuestados citaron a las compañías de energía y servicios públicos como las entidades más expuestas al riesgo de ataques futuros al IoT; un 17% dijo que el cuidado de la salud estaba en grave riesgo, y el 15% que creía cree que el sector financiero será el más afectado por las futuras ciberamenazas basadas en IoT.

Investigaciones

Además de resultados de estudios, el Black Hat también es el entorno ideal para presentar investigaciones. Se cuentan por decenas, y entre ellas cabe mencionar unas pocas, como la realizada por la empresa Duo Security, que asegura que cada vez se falsifican más cuentas de grandes personalidades en Twitter y que las bots de esta red social se están haciendo cada vez más sofisticados.

Para su investigación Duo Security se propuso crear una metodología de código abierto para buscar impostores. Los bots se identificaron primero con una marca que incluía las horas promedio tuiteadas por día, la cantidad promedio de usuarios mencionados en un tweet y la cantidad de tweets con el mismo contenido por día. Haciendo uso del machine learning para identificar a los usuarios que tenían una alta probabilidad de ser cuentas automáticas, los investigadores asignaron sus conexiones. El resultado fue una intrincada web bots de Twitter en la que se descubrieron que algunas cuentas automatizadas de Twitter existen con el único propósito de mejorar la reputación de otras cuentas. Los bots imitaban a las organizaciones de noticias, creaban cuentas de celebridades falsas y pirateaban cuentas verificadas de usuarios reales.

> Durante Black Hat USA se han presentado cuatro herramientas que ayudarán a resolver problemas de seguridad e investigar de una manera diferente

IOActive dejaba al descubierto que los sistemas de comunicación por satélite, utilizado por barcos aviones y unidades militares, están en riesgo gracias a una serie de vulnerabilidades que se hicieron públicas tanto en Black Hat como en DefCon.

Además del riesgo de que los atacantes modifiquen o deshabiliten las comunicaciones satélites, o deshabilitar la Wi-Fi durante el vuelo, los dispositivos con GPS incorporado podrían filtrar la ubicación de las unidades militares. Se plantean los "ataques ciberfísicos" según lo cual si, por ejemplo, se manda suficiente energía a través de una antena de satélite, puede irradiar energía lo suficientemente potente como para afectar el tejido biológico y los sistemas eléctricos. El mismo principio general que un horno de microondas.

El ransomware SamSam fue objeto de una cuidadosa investigación por parte de Sophos, que presentó un informe de 47 páginas sobre una amenaza que, según la compañía, ataca a las víctimas de forma diferente a cualquier otro ataque anterior de ransomware. El informe analiza cómo defenderse contra SamSam, que parece seleccionar los objetivos con cuidado. El informe revela que el atacante de SamSam usa una variedad de herramientas integradas de Windows para escalar sus propios privilegios administrativos. Escanean la red en busca de objetivos valiosos. Su objetivo es obtener

Una de las cosas que pone de manifiesto Black Hat es que aviones, coches, webs, cajeros o impresoras son relativamente fáciles de hackear

credenciales cuyos privilegios les permitan copiar su carga ransomware en cada máquina. Estos incluyen servidores y puntos finales.

A diferencia de otras amenazas de ransomware, SamSam cifra no solo los archivos de documentos y datos de trabajo, sino también los archivos de configuración y datos necesarios para ejecutar aplicaciones como Microsoft Office. Esta estrategia presenta un desafío difícil en términos de continuidad del negocio. Las víctimas que solo respalden documentos y datos tendrán que volver a crear imágenes de las máquinas para recuperarlas.

Y no en Black Hat sino en DefCon, investigadores de Check Point demostraron cómo comprometer toda la red empresarial a través de un fax, máquinas casi ignoradas pero conectadas a la red y que se convierten en el Gateway perfecto para un ciberdelincuente. La firma de seguridad detectó vulnerabilidades críticas en varias impresoras todo-en-uno. En su demostración utilizaron lo que llamaron un Faxploit para enviar un archivo de imagen al número de fax de una impresora HP, ocultando líneas de código malicioso. Una vez almacenado en la memoria de la máquina, los investigadores pudieron utilizar la máquina de fax como un punto de partida utilizando “movimiento lateral” para infiltrarse en una red completa y en los ordenadores conectadas a ella. Check Point trabajó directamente con HP para corregir la vulnerabilidad, que lanzó un parche antes de que se publicara la investigación.

Pero sin duda una de las investigaciones más relevantes es la relacionada con las máquinas utilizadas en las votaciones. Durante una charla titulada “Lessons from Virginia - Un análisis forense comparativo de las máquinas de votación de WinVote” durante la conferencia Black Hat 2018, Schuermann, profesor asociado en la Universidad de Copenhague, presentó datos que mostraban irregularidades en las máquinas de votación en los sistemas WinVote utilizados en una variedad de elecciones estatales y federales de 2004 a 2014.

El investigador de seguridad encontró máquinas con puertos abiertos que usan una versión de Windows XP de 2002 que no se habían actualizado, junto con unidades del sistema accesibles con la

contraseña “abcde”. Incluso llegó a descubrir archivos MP3 descargados que reproducían canciones chinas en una máquina y más de sesenta archivos modificados durante un período de una hora en otra. Ambas máquinas de votación fueron utilizadas para las elecciones de gobernador en Virginia.

Anuncios

Estudios, investigaciones y anuncios. Las empresas participantes en eventos y congresos no dejan pasar la oportunidad de lanzar sus grandes anuncios delante de decenas de miles de colegas y clientes.

Por la relevancia que tiene el ransomware, identificada por los grandes expertos de seguridad como una de las principales amenazas, destacamos el anuncio de Blackberry, que asegura poder reversar los efectos de la amenaza si se infiltra en una o más cuentas. Se trata de una nueva capacidad de su Blackberry Workspaces Collaborate and Secure Plus, sin coste extra y que permite a los administradores congelar una cuenta cuando se detecta la infección para después retrotraer dicha cuenta a un punto justo antes de que ocurriera la infección. Según la compañía no se pierden datos y no se debe pagar ningún rescate; la infección simplemente se borra como si nunca hubiera sucedido.

Tan relevante como el ransomware es la Inteligencia Artificial. Asociada la mayoría de las veces a temas de Big Data, también toma protagonismo en otras áreas, entre ellas la de la seguridad; y no sólo para hacer mejor seguridad, sino para perfeccionar los ciberataques. Consciente de esta dualidad, IBM presentaba DeepLocker, una prueba de concepto cuyo objetivo es, según la compañía, “comprender cómo varias técnicas de IA y malware que ya se pueden ver en la naturaleza podrían combinarse para crear una nueva clase altamente evasiva de malware, que oculta su intención maliciosa hasta que alcanzara un nivel específico víctima”.

Enlaces de interés...

- Presentaciones Black Hat USA 2018
- DeepLocker, la nueva ciberamenaza animada por IA
- Mejora la seguridad cloud con una solución de gestión de claves virtuales

Compartir en RRSS

¿Te avisamos del próximo IT Digital Security?

GDPR is coming.

Not sure where to start?

Get Our Checklist ›

Quest

Los grandes retos de la seguridad cloud

Hoy en día lo queremos todo: sencillez, disponibilidad, accesibilidad... ¿La respuesta? El cloud, al que se puede acceder desde cualquier dispositivo, que está siempre disponible y que ha mostrado la flexibilidad que es capaz de ofrecer en el despliegue y forma de consumo. Por encima un reto, transversal a cualquier tecnología: la seguridad.

Los entornos cloud, ¿son seguros? ¿y el acceso a los mismos? ¿cómo está viajando la información? ¿están mis datos y aplicaciones aisladas de las de los demás? ¿quién tiene la responsabilidad de asegurar el cloud? Algunos de las preocupaciones que plantea el uso de la nube es si en estos entornos se protege adecuadamente la confidencialidad, se puede garantizar el cumplimiento normativo o si se puede controlar el acceso.

Lo que está claro es que los enormes beneficios que ofrece la nube se pierden desde el momento

en que no se convierte en un entorno seguro para la información sensible. Algo que hemos tratado en un desayuno que bajo el título Los grandes retos de la seguridad cloud reunió a Ignacio Gilart, CEO de WhiteBearSolutions; Raúl Flores, Senior Systems Engineer de Infoblox y César Moro, Sales Consultant Quest Software.

Arrancamos el debate planteando si la seguridad ha pasado de ser una barrera para la adopción del cloud a un habilitador. Para Ignacio Gilart no es tanto un habilitador como una necesidad “porque el cloud que no sea seguro no tiene futuro” porque todo lo que ponemos en la nube son nuestras aplicaciones y el activo más valioso de las empresas, que es la información. Y concluye el directivo asegurando que el cloud “es esencial para muchos proyectos de transformación digital, pero tiene que están garantizado”.

LOS GRANDES RETOS DE LA SEGURIDAD CLOUD — CLICAR PARA VER EL VÍDEO

Raúl Flores se refiere a la seguridad del cloud como un parámetro más que hay que gestionar, y añade que hay que tener claro que “hay que extender las políticas de seguridad de las empresas al cloud”.

Para César Moro la seguridad sí es un habilitador “en cuanto que es mucho más fácil al estar implementada una seguridad per se”. Añade el ejecutivo que en la seguridad lo que hay que mirar es todo, que es eslabón más débil es el que nos indica dónde va a estar nuestra seguridad, y si está en el on-premise el cloud va a estar comprometido”.

Sobre si las empresas están adoptando la seguridad en la nube de una manera consciente o todavía están lejos de ello, asegura Ignacio Gilart que más que adoptando la seguridad “están utilizando las facilidades de seguridad que aporta la nube”.

Incide el responsable de WhiteBearSolutions que nube cuenta con mecanismos nativos para que sea una herramienta segura, “y por tanto las empresas tienen que aprovecharse de esos mecanismos, de esos estándares, de esos protocolos para facilitar la integración”.

La experiencia de Raúl Flores es que las grandes empresas sí que están muy involucradas en la seguridad; “están utilizando mucha cloud pública desde hace bastante tiempo y las ventajas es que pueden estandarizar su seguridad, pero también

"El cloud es esencial para muchos proyectos de transformación digital, pero tiene que están garantizado"

Ignacio Gilart, CEO de WhiteBearSolutions

¿Te avisamos del próximo IT Digital Security?

"Si no implantas la misma seguridad en un entorno on-premise que en uno cloud tendrás una brecha"

César Moro,

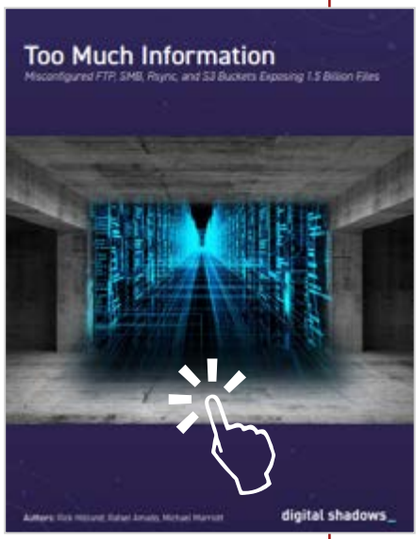
Sales Consultant Quest Software

tener un control y detectar, por ejemplo, el shadow IT. Les permite tener un único panel de control de todos sus recursos y saber en todo momento lo que tienen y lo que no, porque además de la seguridad, la visibilidad y el control también son importantes".

César. Todas las empresas se están yendo a la nube, todas, y uno de los puntos interesantes es la flexibilidad que están dando respecto a la tecnología; unos van con IaaS, otros con IaaS y SaaS… y al final depende de las necesidades de las compañías en cuanto al modelo.

César Moro tiene claro que se adopta con seguridad "porque al final si no implantas la misma seguridad en un entorno on-premise que en uno cloud tendrás una brecha. De forma que como mínimo están aportando la misma seguridad que tienen on-premise". Comenta el ejecutivo de Quest que el cloud ha facilitado mucho la adopción de autenticación de doble factor, una tecnología que inicialmente compraban unas pocas empresas y que en año

DEMASIADA INFORMACIÓN



Más de 1.500 millones de archivos confidenciales corporativos y de otro tipo son visibles en internet debido a errores humanos. En este estudio de Digital Shadows podrás conocer el alcance de la exposición de datos en todo el mundo sólo en los tres primeros meses de 2018; las geografías más afectadas; la fuente de estos datos expuestos; ¿Qué porcentaje de esta información era información personal del empleado o del cliente?; cómo los adversarios pueden usar estos datos para explotar tu negocio y tus clientes; qué pueden hacer las organizaciones para identificar qué información está expuesta y cómo mitigar el riesgo.

y medio “tienen implementado muchísimas empresas, y eso es gracias al cloud”.

En todo caso, y aunque se esté adoptando la seguridad en entornos cloud, preguntamos a nuestros expertos quién tiene la responsabilidad última de la seguridad, la empresa o el proveedor. “Yo creo que la responsabilidad de tu activo más valioso es tuya, eso siempre es así”, asegura Ignacio Gilart, quien añade que, obviamente, como en cualquier relación contractual, se tienen que tener todos los aspectos que puedan afectar al negocio tratados con tus proveedores y la nube no es una excepción.

Para el ejecutivo de Infoblox “la clave está en definir una estrategia de adopción de cloud a nivel de seguridad”, mientras que César Moro diferencia entre IaaS, SaaS o PaaS, porque “aunque la seguridad es global, no es lo mismo cómo se gestiona en unas situaciones u otras”. Dice el representante de Quest Software los proveedores también “somos responsables de la información que nos deja el cliente. Si internamente tenemos un ataque o tenemos una brecha, contractualmente estamos ligados, esos SLA está ahí y han de cumplirse. Pero no es lo mismo que haya un ataque de suplantación de una identidad que accede y tienen permisos en nuestra plataforma, ahí no podemos ser los responsables, de forma que tiene que estar muy clara dónde está la línea entre una responsabilidad y otra”.

Cómo proteger el cloud

Durante el debate ya se planteó cómo el cloud está acelerando la adopción de tecnologías de seguridad como el doble factor de autenticación. ¿Prestan las empresas atención a la gestión de identidades? En general, ¿qué tecnologías se están utilizando para proteger el cloud?

Ignacio Gilart tiene claro que hay que garantizar de manera inequívoca la identidad de quién accede al cloud y si tiene los permisos adecuados en tiempo y forma, así como auditar toda esa asignación de permisos y garantizar la información que estamos guardando. “Los que nos dedicamos a la gestión de identidad y de accesos estamos viviendo una segunda juventud de este tipo de herramien-

"La clave está en definir una estrategia de adopción de cloud a nivel de seguridad"

Raúl Flores,

Senior Systems Engineer de Infoblox

¿Te avisamos del próximo IT Digital Security?

tas, porque, aunque están funcionando desde hace muchísimos años, ahora se ha convertido en una necesidad", asegura el directivo.

Raúl Flores se muestra de acuerdo en que es muy importante controlar quién está accediendo a la aplicación por temas de seguridad, y menciona el servicio Active Trust Cloud de Infoblox, centrado en ofrecer seguridad al protocolos DNS a nivel recursivo.

Coincidiendo con sus compañeros, César Moro diferencia entre el control de accesos y por parta parte cómo se explota esa información, "y ahí es donde las empresas se basan en herramientas de terceros para gestionar la cantidad ingente de información de autenticaciones que se recibe. Es decir: "la información te la da el proveedor y tú lo que tienes es que, con las herramientas que tengas trabajar para controlar ese entono cloud".

¿Te avisamos del próximo IT Digital Security?

Frente a grandes retos, grandes soluciones

Al finalizar el debate y como es habitual en los #DesayunosITDS, pedimos a nuestros invitados que expongan las soluciones de sus compañías para aportar seguridad al cloud.

Ignacio Gilart, CEO de **WhiteBearSolutions.** Nosotros desde hace quince años venimos trabajando en dos líneas de negocio: Una es el almacenamiento y backup, que a veces se convierte en la última línea de fuego; y por otro lado en la parte de gestión de identidad y acceso, que está viviendo una segunda juventud y apuestas que se hicieron en su día, como los protocolos de federación o algún tipo de creación de API cuando no estaba tan de moda, pues resulta que cuando ha eclosionado esto del cloud nos da una ventaja competitiva que nos permite integrar la realidad de nuestros clientes que tienen on-premise con el cloud. Por diferenciarnos un poco de otras empresas, lo que nosotros intentamos es que la tecnología se democratice un poco; por filosofía de producto y de implantación intentamos que llegue a mucha más gente.

Raúl Flores, Senior Systems Engineer de **Infoblox.** En mi empresa la tecnología es híbrida por diseño y lo que hacemos es ayudar a los clientes a extender sus servicios de core a la nube de una forma fácil y consolidado, que con una sola consola puedan ver sus recursos on-premise, como en la cloud. Una puntualización a nivel de seguridad tiene que ver con exfiltración de datos; muchos malware lo que hacen es utilizar el protocolo DNS para después hacer un tunelling y así poder infiltrar o exfiltrar datos, y es importante poder identificar estas malas praxis; son túneles que los firewalls tradicionales, o que incluso los DLP no son capaces de detectar porque no son especialistas en el servicio DNS.

César Moro, Sales Consultant **Quest.** Dentro de Quest tenemos un portfolio muy amplio de soluciones. Con más de 24 años de vida hemos nacido on-premise pero la adopción a la nube, al mundo híbrido fue rapidísima. Desde el primero momento lo que quisimos es que todas las funcionalidades que tienen las empresas con nuestras soluciones implantadas on-premise las tengan para gestionar, administrar y controlar el entorno cloud, y eso ha sido muy provechoso. Y esto es porque lo que se han encontrado la mayoría de las empresas es que el mismo número de personas que llevaban el entorno on-premise tenían que llevar más entornos, y les hemos facilitado toda la gestión de una forma transparente.

Los enormes beneficios que ofrece la nube se pierden desde el momento en que no se convierte en un entorno seguro para la información sensible

¿Cómo escoger el proveedor cloud más adecuado? La pregunta no es fácil, y por eso se la planteamos a nuestros invitados. Para Ignacio Gilart la clave es la solvencia. Dice el responsable de WhiteBearSolutions que con el cloud han aparecido todo tipo de proveedores, “pero hay buscar la solvencia”, además de la facilidad de gestión, “porque yo creo que el cloud se vende como algo muy sencillo y al final no lo es tanto porque cambiar el perímetro de seguridad, cambia el control de recursos, cambian las herramientas, no es fácil y todo eso hay que tenerlo muy en cuenta”. Y finalmente recomienda adoptar pequeños servicios de muestra para ver en la realidad cómo funciona ese cloud, cómo se despliega, cómo se securiza…

Raúl Flores recomienda leerse la letra pequeña, firmar los SLA a nivel legal y si se tiene oportunidad hablar con clientes que han consolidado con ese proveedor y pueden hablar de su experiencia de cómo les ha ido. “Al final yo creo que lo más importante es definir una estrategia de adopción del cloud a nivel de seguridad y que se pueda aplicar en todo”.

Secundando las recomendaciones de sus compañeros, César Moro comenta que “el decidirte por un proveedor cloud u otro no es tanto por la seguridad que te ofrece sino por la estrategia tecnológico, porque los grandes ofrecen unos estándares de seguridad muy similares”.

Enlaces de interés...

- Seguridad y Cloud, ¿qué nos queda por aprender?
- ¿Qué es una solución EFFS?
- Por qué necesitas Smart Login
- Seguridad sin fronteras para una infraestructura híbrida
- 20 casos de uso de CASB
- Diez consejos sobre la gestión de bots
- La cloud pública sigue imparable pese a las reticencias de seguridad

Próximos #ITWebinars

Resolviendo los retos de IoT

SEPTIEMBRE

Registro

Inteligencia de amenazas, ¿a qué esperas?

SEPTIEMBRE

Registro

Dando forma al Big Data para la toma de decisiones

Registro

OCTUBRE

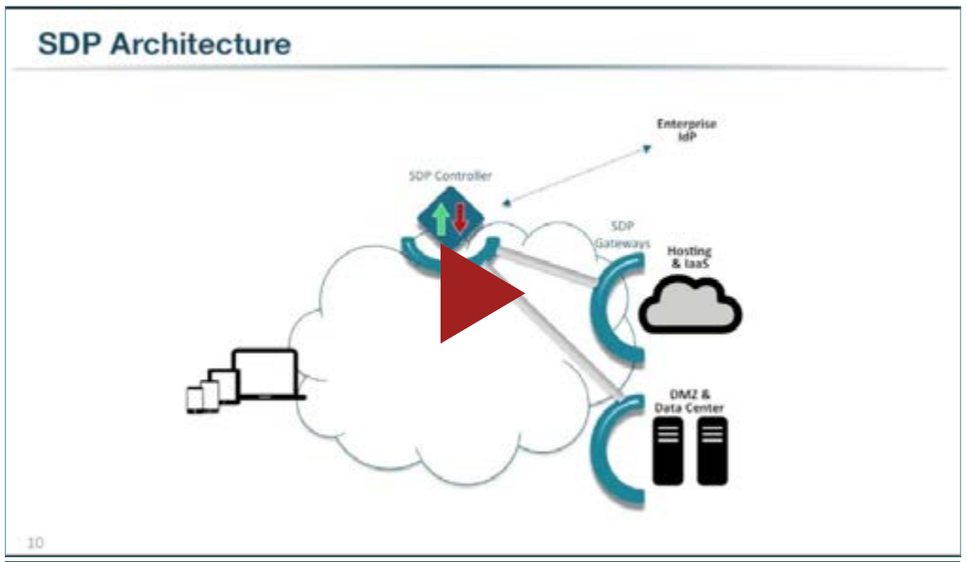
www.ittelevision.es

it televisión

Black Cloud viene al rescate

¿Te avisamos del próximo IT Digital Security?

La adopción del cloud y la movilidad ha hecho que el perímetro de seguridad tradicional, que una vez protegiera a los usuarios y servicios internos dentro de la red corporativa, haya dejado de tener sentido. Ha llegado el momento de que la seguridad evolucione, y una de las propuestas es SDP, o perímetro definido por software, que solo permite a los dispositivos autenticados individualmente acceder a los recursos de la red, incluso los dispositivos internos en la red. Toda conexión entre un objeto y una máquina debe ser reconocida de manera expresa, y monitorizada



SOFTWARE DEFINED PERIMETER **CLICAR PARA VER EL VÍDEO**

La decisión de adoptar servicios en la nube y tecnologías móviles ha mejorado la experiencia de usuario, ha simplificado el acceso a los recursos, ha democratizado el uso de la tecnología, pero también ha tenido un impacto en lo que a seguridad se refiere.

La premisa de la arquitectura de red tradicional es crear una red interna separada del mundo externo por un perímetro fijo formado por una serie de funciones de firewall que bloquean el acceso de usuarios externos, pero permiten la salida de los usuarios internos. Durante años los perímetros fijos tradicionales han permitido que los servicios internos permanecieran seguros ante las amenazas externas gracias a una característica simple: bloquear la visibilidad y la accesibilidad desde fuera del perímetro a las aplicaciones internas y la infraestructura. El modelo, no obstante, quedó obsoleto con la llegada de la movilidad, del Bring Your Own Device (BYOD), de amenazas como los ataques de phishing, que proporcionaban acceso no

confiable dentro del perímetro, y propuestas como el SaaS y el IaaS, que cambiaban la localización del perímetro.

El Perímetro Definido por Software (Software Defined Perimeter – SDP) es una arquitectura de seguridad que restringe el acceso a la red y las conexiones a determinados elementos permitidos. SDP sirve para identificar el origen y el destino de una conexión de red; la tecnología asume que no hay confianza entre los potenciales participantes y que una conexión segura solo se concede cuando se permite de manera explícita.

(DISA). El objetivo inicial de SDP era proporcionar un método de seguridad de red para proporcionar acceso a servicios de misión crítica sobre una base de confianza cero utilizando Internet y software, y no tecnologías de hardware alojadas en el centro de datos. Es decir, se restringen las conexiones sólo a las que son absolutamente confiables. El perímetro definido por software se popularizó a raíz del SDP Working Group de la Cloud Security Alliance, que buscaba la manera de crear redes que fueran muy confiables de extremo a extremo para uso empresarial.

El protocolo SDP está diseñado para proporcionar funcionalidad perimetral, aprovisionada dinámicamente cuando sea necesario para aislar servicios de redes no seguras

SDP aísla una aplicación para que sea invisible para todos en la red, verifica la confiabilidad del usuario y del dispositivo, y solo entonces conecta el usuario autorizado y el dispositivo confiable a la aplicación protegida. La arquitectura consta del controlador, la puerta de enlace y el cliente. Los tres componentes trabajan juntos para vencer los ataques más devastadores que se utilizan en las amenazas avanzadas.

El concepto de perímetro definido por software no es, ni mucho menos, un concepto nuevo. Desarrollado en 2007, se basa en el trabajo realizado por la Agencia de Sistemas de Información de Defensa

Conocido también como Dark Cloud, con SDP las organizaciones pueden mantener los recursos de la nube completamente oscuros para usuarios no autorizados, lo que elimina por completo muchos vectores de ataque, incluidos los ataques de fuerza bruta, inundaciones de red, así como vulnerabilidades de TLS como Heartbleed y Poodle.

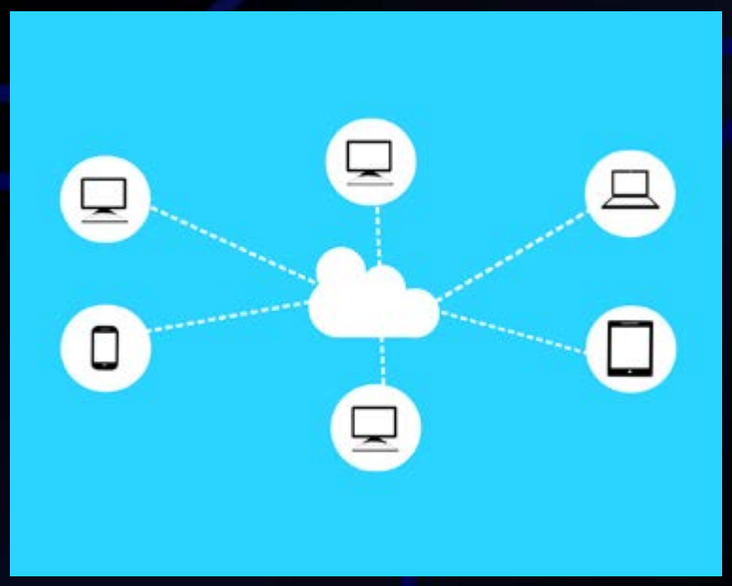
Definido por software

Como en otras propuestas “software defined”, lo que hace el perímetro definido por software es dar a los responsables de las aplicaciones la capacidad para desplegar la funcionalidad del perímetro

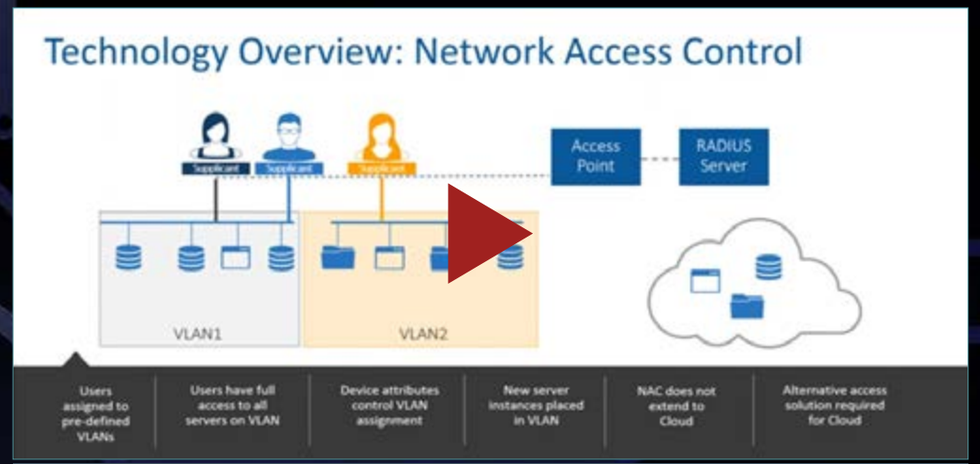
SDP, el nuevo NAC

Network Access Control, o NAC, es una tecnología que permite controlar qué dispositivos pueden acceder a la red. Las soluciones NAC permiten establecer políticas a cumplir por todos los dispositivos antes de conectarse a la red corporativa; si los dispositivos no cumplen la política establecida, no podrán interactuar con los demás elementos de red hasta que no se resuelva el incumplimiento.

La adopción de NAC se vio impulsada por la expansión de las redes WiFi en los entornos empresariales hace más de una década. Cuando se combinaban con la autenticación del Directorio Activo, los productos NAC comprobaban si determinados empleados deberían tener acceso al centro de datos. Pero en diez años las cosas han cambiado mucho. Las primeras soluciones NAC llegaron al mercado en 2005, en una época en la que los empleados desenchufaron los portátiles de la red, se los llevaron fuera de la oficina y los traían de nuevo a la red corporativa infectados con malware. NAC fue diseñado para verificar el estado de salud de los portátiles que se conectaban a la red, así como los derechos de identidad y acceso del usuario, antes de permitir el acceso total a la red. Si hay un problema, el acceso puede denegarse o minimizarse hasta que pueda realizarse una reparación.



La situación actual es distinta. Ahora, los endpoints no son sólo ordenadores portátiles corporativos, sino también una variedad de ordenadores, smartphones y tabletas, todo tipo de cosas conectadas a Internet e incluso servidores virtualizados. Las personas que se conectan a la red no son solo los empleados habituales, sino proveedores de servicios, socios e invitados. Y para algunos, como Jon Oltsik, de CSOnline, los NAC han dejado de cumplir con las expectativas.



NETWORK ACCESS CONTROL VS SOFTWARE DEFINED PERIMETER

CLICAR PARA VER EL VÍDEO

De manera similar a los NAC, SDP funciona como una puerta de enlace entre el usuario y los recursos de la aplicación. Sin embargo, el diseño distribuido de SDP permite su implementación dentro de la empresa y en nubes públicas. La conectividad de las provisiones SDP se realizan en tiempo real, lo que garantiza que el acceso coincida con la política. Y lo más importante, el canal de control SDP se puede combinar con un software avanzado de detección de malware, una memoria RAM inviolable y tecnologías de micro-virtualización para garantizar que el punto final sea verdaderamente confiable.

donde sea necesario. SDP reemplaza los appliances físicos con componentes lógicos que operan bajo el control del propietario de la aplicación y, llegado el momento, sólo proporciona acceso a la infraestructura de la aplicación después de la certificación del dispositivo y la verificación de la identidad.

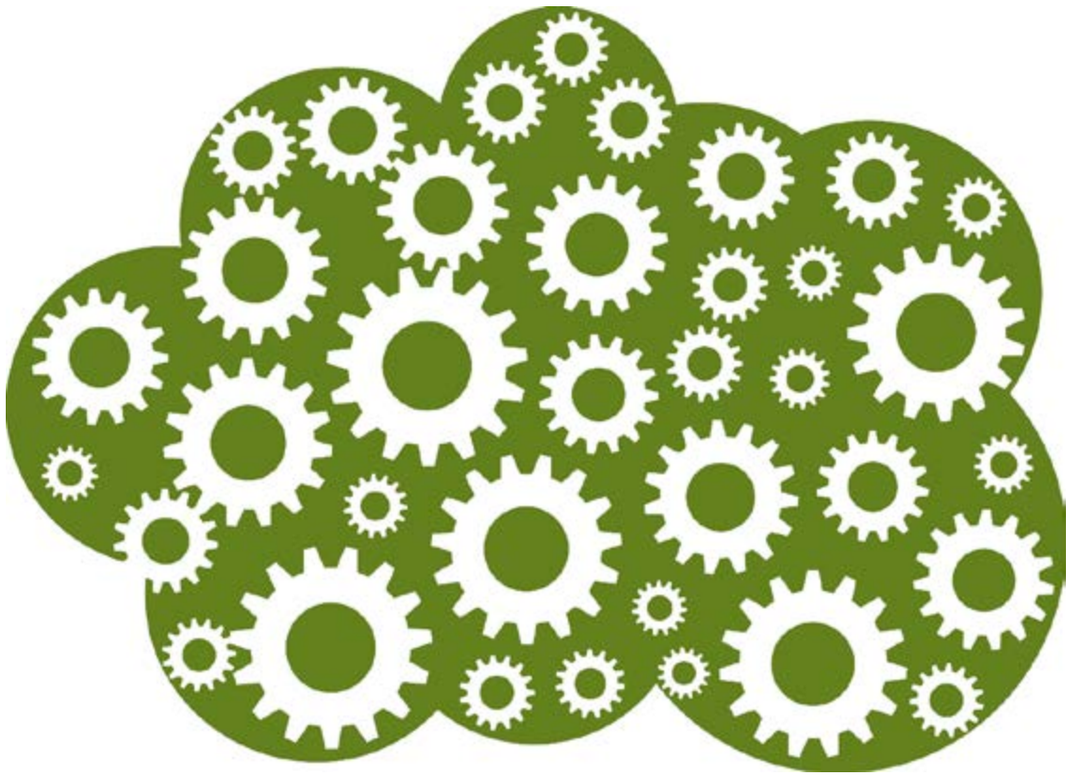
Los SDP mantienen los beneficios de un modelo que necesita conocer antes de permitir, pero eliminando las desventajas de necesitar un dispositivo de puerta de enlace de acceso remoto. Los SDP requieren que los puntos finales se autentiquen y sean autorizados primero antes de obtener acceso a la red a los servidores protegidos, y luego, las conexiones cifradas se crean en tiempo real entre los sistemas solicitantes y la infraestructura de la aplicación.

En su forma más simple, el perímetro definido por software consiste en dos componentes: SDP Hosts y SDP Controllers. El primero puede iniciar conexiones y aceptarlas; estas acciones son gestionadas por los SDP Controllers a través de un canal de control seguro. De esta forma, y según la Cloud Security Alliance, en los perímetros definidos por software el plano de control está separado del plano del dato para crear un sistema completamente escalable. Además, todos los componentes pueden ser redundantes para propósitos de escala o tiempo de actividad.

PERÍMETRO DEFINIDO POR SOFTWARE, GUÍA PARA CIOS

El perímetro definido por software (SDP) es un nuevo enfoque de seguridad que mitiga los ataques basados en red. Protege tanto los activos de TI heredados como los servicios en la nube de todos los niveles de clasificación. Funciona ocultando los activos críticos de TI dentro de una nube invisible e indetectable.

Este documento proporciona información valiosa a los responsables de TI sobre el funcionamiento del perímetro definido por el software (SDP), mapeará el diseño técnico y el flujo de trabajo, describirá todas sus características, identificará las protecciones obtenidas e introducirá puntos de referencia y monitorización.



El Perímetro Definido por Software (SDP) es una arquitectura de seguridad que restringe el acceso y las conexiones a la red sólo a los elementos permitidos

Software Defined Perimeter Working Group

Una vez claro que las técnicas de defensa perimetrales tradicionales no podían proteger a las empresas en un entorno de adopción del cloud y la movilidad se crea, en 2013 y dentro de la Cloud Security Alliance, el Software Defined Perimeter Working Group, con el objetivo de desarrollar una solución para detener los ataques a la red contra la infraestructura de la aplicación.

Para lograr su objetivo, el equipo consideró que tres elementos de diseño eran clave. Primero, un modelo de seguridad que verifique la identidad del usuario, sus dispositivos y su rol antes de otorgar acceso a los sistemas protegidos. En segundo lugar, la verificación criptográfica para garantizar el cumplimiento del modelo de seguridad. Y tercero, que los protocolos para lograr los elementos uno y dos sean controles de seguridad de dominio público probados.

Explica este grupo de trabajo que una vez identificadas las claves decidieron que una arquitectura basada en canales de control que utilizara componentes estándar como SAML, PKI y TLS mutuo proporcionaría el enfoque ideal. Publicaron un documento en diciembre de 2013 para determinar si había interés en el concepto y lo llamaron SDP.

Comprobado el interés por la nueva propuesta, se publicó la especificación SDP Versión 1 en abril de 2014. El diseño inicial consistió en un Initiating Host que transmitiría la identidad del dispositivo y del usuario a un Controlador a través de una conexión TLS mutua. El Controlador a su vez se conectaría a una CA expedidora para verificar la identidad del hardware y a un Proveedor de Identidad para verificar la identidad del usuario. Una vez verificado, el Controlador proporcionará una o más conexiones mutuas TLS entre el Anfitrión Iniciador y los Anfitriones Aceptantes correspondientes.

Los productos SDP comerciales iniciales implementaron este concepto como una red superpuesta para aplicaciones empresariales. El Initiating Host del SDP se convirtió en un cliente y el host aceptado se convirtió en una puerta de enlace, o Gateway. Trabajando juntos, los tres componentes de la

Al SDP también se le conoce como Dark Cloud porque la infraestructura que protege es "oscura" o invisible ya que las direcciones IP sólo se revelan a los dispositivos autorizados

arquitectura proporcionan una serie de propiedades de seguridad únicas:

- **1) La información está oculta.** No hay información de DNS ni puertos visibles de la infraestructura de aplicaciones protegidas. Los activos protegidos SDP se consideran “darks”, ya que es imposible escanear los puertos para detectar su presencia.
- **2) Pre-autenticación.** La identidad del dispositivo (del host solicitante) se verifica antes de que se otorgue la conectividad. La identidad del dispositivo se determina a través de un token MFA que está incrustado en la configuración de TCP o TLS.
- **3) Pre-autorización.** Los usuarios reciben acceso de aprovisionamiento solo a los servidores de aplicaciones que son apropiados para su función. El sistema de identidad utiliza una aserción SAML para informar al controlador SDP de los privilegios de los hosts.
- **4) Acceso a la capa de aplicación.** Los usuarios solo tienen acceso en una capa de aplicación (no en la red). Además, SDP suele incluir en la lista

blanca las aplicaciones en el dispositivo del usuario, por lo que las conexiones aprovisionadas son de aplicación a aplicación.

- **5) Extensibilidad.** SDP se basa en componentes probados y basados en estándares, como los certificados mutuos TLS, SAML y X.509. La tecnología basada en estándares garantiza que SDP se pueda integrar con otros sistemas de seguridad, como el cifrado de datos o los sistemas de certificación remota.

Los SDP reducen el éxito de ataques DDOS, man-in-the-middle, o de movimientos laterales como inyecciones SQL

Casos de uso

Ya hemos comentado que el perímetro definido por software mejora la seguridad de las empresas, reduciendo las brechas de seguridad que buscan acceder a propiedad intelectual, información financiera o cualquier otro dato sensible que esté disponible dentro de la red empresarial. Los ciberdelincuentes podrían acceder a la red interna comprometiendo alguno de los ordenadores de la red para después moverse en busca de la información. Se podría

SDP como solución Zero Trust

En 2010, Forrester Research publicó un documento sirvió para popularizar el concepto Zero Trust, o Confianza Cero. La consultora planteaba la idea de que las empresas no deberían confiar inherentemente en ningún usuario o red, y que cualquier intento de acceder a un sistema o aplicación comercial debe verificarse siempre antes de conceder cualquier nivel de acceso.

De manera que bajo un modelo Zero Trust no se confía en todo el tráfico de red y, por lo tanto, los responsables de seguridad "deben verificar y proteger todos los recursos, limitar y hacer cumplir estrictamente el control de acceso e inspeccionar y registrar todo el tráfico de la red". Que son los conceptos de que plantean en la tecnología de perímetro definido por software.

El modelo Zero Trust ha llevado a la popularización del nuevo enfoque de seguridad de red dentro de las empresas del que trata este reportaje: el perímetro definido por software (SDP).

En el documento, los analistas de Forrester aseguraban que Zero Trust "es una oportunidad para reinventar la red y crear redes más seguras", y enumeran una serie de beneficios implícitos en una red Zero Trust:

- **Es una plataforma agnóstica,** capaz de soportar cualquier tipo de recurso.
- **Reduce el coste de cumplimiento** y otras evaluaciones de seguridad.
- **Permite una virtualización segura**
- **Escala con tu empresa** y las nuevas formas de hacer negocio
- **Es la base de un entorno multiusuario seguro**
- **Permite balancear las cargas de trabajo fácilmente**

Por cierto, que Google fue una de las primeras compañías en adoptar este nuevo enfoque, inicialmente como una forma de conectar a los empleados de Google con sus aplicaciones internas. El servicio Google BeyondCorp nació de este desarrollo.

desplegar un SDP dentro del centro de datos para aislar las aplicaciones de alto valor del resto de aplicaciones y de los usuarios no autorizados en toda la red. Con SDP los usuarios no autorizados ni siquiera serían capaces de detectar la aplicación protegida.

Por otra parte, la naturaleza de superposición de software del SDP le permite integrarse fácilmente en nubes privadas para aprovechar la flexibilidad y elasticidad de dichos entornos. Y, además, los SDP pueden utilizarse para ocultar y proteger las instancias de nube pública en forma aislada, o como un sistema unificado que incluye instancias de nube privada y pública y/o clústeres de nubes cruzadas.

Explica también la Cloud Security Alliance que si bien la ubicación ideal para la infraestructura de escritorio virtual (VDI) se encuentre en una nube elástica en la que el uso del VDI se paga por hora a veces, si el usuario de VDI necesita acceder a servidores dentro de la red corporativa, VDI puede ser un uso difícil y puede abrir agujeros de seguridad. Sin embargo, VDI junto con un SDP resuelve estos dos problemas a través de una interacción del usuario más simple y acceso granular.

> Mientras que el perímetro de seguridad tradicional busca establecer un perímetro alrededor de las aplicaciones y sistemas, el enfoque SDP es establecer un perímetro alrededor del usuario

Otro de los casos de uso del perímetro definido por software tiene que ver con el internet de las cosas. Las aplicaciones back-end que gestionan este tipo de dispositivos y extraen la información de estos a menudo actúan como custodios para los datos sensibles o privados. En estos casos se puede hacer uso del SDP para esconder estos servidores y sus interacciones en Internet.

SDP, más que una VPN

Una VPN, o red privada virtual, es una tecnología que permite que un ordenador en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Para ello se establece una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

Hace años que las empresas utilizan VPN para mantener seguros los datos y dispositivos corporativos de los empleados remotos, proveedores y otras personas autorizadas a acceder a las redes de las

empresas. Quizá las VPN se han visto superadas desde el momento en que el teletrabajo es cada vez más habitual, y ya no sólo se utiliza un portátil, sino que también conectamos a las redes empresas nuestras tabletas y smartphones. Más dispositivos, más conexiones, más superficies de ataque.

En un informe publicado en noviembre de 2017 Gartner pronosticó que para 2021 el 60% de las empresas dejarán de utiliza VPNs a favor de los perímetros definidos por software. Hay quien habla del fin de las VPN, aunque esto parece exagerado.

Como solución Zero Trust, el perímetro definido por software trabaja con dos criterios clave: permitir que un dispositivo se conecte, y saber si el usuario en particular está autorizado. Como hemos dicho: SDP cierra el acceso a la red externa para usuarios y dispositivos no autorizados y lo

> Como en otras propuestas "software defined", el SDP da a los responsables de TI la capacidad para desplegar la funcionalidad del perímetro donde sea necesario

abre a petición y para aquellos que solo han sido autorizados.

De esta manera, elimina la presencia visible en Internet de una organización; no requiere administración de certificados de usuario final; no requiere acceso físico a aplicaciones y redes, solo señala el acceso a la aplicación; no hay puertos abiertos en el firewall desde los segmentos que no son de confianza a los de confianza, lo que reduce las posibilidades de errores.

Mercado al alza

El crecimiento del mercado del perímetro definido por software está impulsado por la creciente necesidad de un sistema de seguridad capaz de proteger aplicaciones empresariales dispersas, aumentar los servicios basados en la nube y, en general, hacer frente a la transformación digital. En este escenario, las soluciones SDP permiten que la infraestructura de seguridad se configure, administre y controle

fácilmente utilizando un marco de seguridad escalable, programable y basado en políticas, sin ninguna experiencia externa de alto nivel.

Otros factores, como el desarrollo económico, la rápida urbanización y la tasa de empleo junto con la rápida industrialización, también están impulsando el mercado de perímetro definido por software global. Los vendedores en el espacio perimetral definido por software tienen importantes oportunidades de crecimiento en regiones como Asia Pacífico, América Latina, y Medio Oriente y África atribuidas a su economía industrial en ascenso significativo.

Un informe de Transparency Market Research publicado en agosto asegura que el mercado de SDP es competitivo debido a la alta concentración de proveedores de servicio, y para ser competitivos recomienda a los fabricantes adoptar planes de crecimiento, tanto orgánico como inorgánico, así como nuevos lanzamientos de productos.

La consultora prevé crecimientos del 30,9% medio anual hasta 2025, pasando de los 1.129 millones de dólares de 2016 a 12.247 e la fecha indicada.

Hay que destacar también que en 2016 el vertical de banca, servicios financieros y aseguradoras fue el segmento con más porcentaje de mercado, un 24,8%, y que en términos geográficos mientras que América del Norte domina el mercado de perímetro definido por software, se espera que Asia Pacífico muestre una mayor tasa de crecimiento sobre otras regiones durante el período previsto.

Algunos retos

Aseguran que SDP es una solución atractiva para la seguridad cloud porque no requiere de grandes in-

La iniciativa de investigar el concepto de SDP fue lanzada en 2013, por CSA Cloud Security Alliance, para encontrar una manera eficaz bloquear los ataques de red a la infraestructura de aplicaciones

En su forma más simple, el perímetro definido por software consiste en dos componentes: SDP Hosts y SDP Controllers

versiones. Básicamente, combina la autenticación de dispositivo existente, el acceso basado en identidad y la conectividad aprovisionada dinámicamente que la mayoría de las organizaciones deberían tener bajo una superposición de software. Y según la Cloud Security Alliance, el modelo SDP ha demostrado que detiene todas las formas de ataques a la red, incluida la denegación de servicio distribuida (DDoS), man-in-the-middle, inyección SQL y amenaza persistente avanzada. No por ello su adopción deja de plantear algunos retos.

No se puede implementar una solución SDP completa en una infraestructura existente sin algunas interrupciones en la red y la infraestructura de software. Las aplicaciones y las configuraciones del sistema operativo deben conocer el SDP para acceder al flujo de trabajo SDP y a los túneles seguros. La presencia de un controlador significa que hay otro elemento en el que las redes pueden confiar, y necesita ser asegurado y estar altamente disponible.

Como explica el IEEE no son retos que no se puedan superar, y añade que los SDP utilizan redes IP convencionales y no cambian la arquitectura fundamental de las redes de capa 2 a 7; y que las herramientas y los procedimientos operativos existentes de gestión y supervisión de la red y de seguridad pueden necesitar cambios si SDP reemplaza los métodos de seguridad convencionales.

En todo caso, SDP promete resolver muchos desafíos de seguridad. La arquitectura se basa en tecnologías existentes, como los túneles VPN, y los combina con conceptos modernos de SDN y microsegmentación para proporcionar una arquitectura más segura. Ha demostrado tener éxito en la seguridad militar y puede ampliarse para despliegues comerciales y empresariales. Se muestra prometedor en aplicaciones basadas en la nube que exhiben fundamentalmente modelos de implementación distribuidos y no se ajustan a un modelo de seguridad perimetral tradicional.

Enlaces de interés...

- W Seguridad en tu red: The Zero Trust Network Architecture
- W Zero Trust Networks
- W Perímetro Definido por Software, por la Cloud Security Alliance
- W Perímetro Definido por Software, guía para CIOs
- W Por qué debería tenerse en cuenta el Perímetro Definido por Software
- W Perímetro Definido por Software - Glosario

Compartir en RRSS

¿Te avisamos del próximo IT Digital Security?

AYÚDANOS A CONOCER LAS

itTRENDS

QUE PREDOMINAN EN LA EMPRESA

PARTICIPA

JOSÉ CANO

DIRECTOR DE ANÁLISIS Y CONSULTORÍA DE IDC ESPAÑA

Director de Análisis y Consultoría en IDC Research España. Anteriormente, Director de Consultoría Técnica y Desarrollo de Negocio en GAC Grupo (España) y Director Académico del EMBA Blended (Madrid). Ha trabajado en consultoría de estrategia y operaciones en Avantia XXI S.L Global, y asesor ejecutivo para entidades públicas y privadas en el ámbito de la innovación y desarrollo de negocio (Deusto Business School, ICARUM ANS S.L, etc.). También ha sido socio fundador y director de consultoría de estrategia y operaciones en ACL Strategy S.L, y Senior Manager de Innovación en consultoría de sector público (E&O) en Deloitte.

Seguridad gestionada como bote salvavidas en el viaje digital de las organizaciones

Decir que el mercado de la seguridad es complejo y desafiante es una opinión, dada la cantidad de partes móviles que participan en la defensa de una empresa de ciberataques. El mercado de servicios de seguridad gestionada es fundamental para el éxito de las organizaciones que están luchando por mantenerse al día con el aumento de la frecuencia y la complejidad de los ataques que estamos sufriendo en la actualidad.

La capacidad de una empresa para mantener el nivel necesario de inteligencia de amenazas y capacidades avanzadas de análisis junto con las habilidades para interpretar y actuar sobre los hallazgos puede ser un esfuerzo desalentador.

las soluciones de seguridad son caras y los talentos de seguridad son escasos. Como resultado,

LOS RIESGOS DE BLOCKCHAIN

Casi todas las industrias han invertido, adquirido o implementado blockchain en alguna capacidad. Sin embargo, McAfee prevé un enorme potencial de riesgos de ciberseguridad que podría amenazar el rápido crecimiento de esta tecnología revolucionaria. Según este informe, los ciberdelincuentes buscan aprovechar la rápida adopción de las criptomonedas y los primeros usuarios que las usan a través de cuatro vectores clave de ataque: esquemas de fraude o phishing, malware, exploits de implementación y vulnerabilidades tecnológicas. Muchos ataques que abarcan estas categorías aplican técnicas antiguas y nuevas de cibercrimen y han demostrado ser altamente lucrativas para los ciberdelincuentes.

Será necesario que los proveedores entiendan perfectamente al cliente, sus necesidades y su estadio en el viaje digital

las organizaciones debaten “construir versus comprar “ y muchos se están volviendo a la figura del proveedor de servicios de seguridad gestionada. Este tipo de proveedor permite a las organizaciones cumplir varios objetivos:

- Reducir el coste total de propiedad y apalancar el modelo de gastos para ofrecer precios y presupuestos predecibles.
- Ofrecer una postura de seguridad holística que sea más proactiva y predictiva versus reactiva.
- Proporcionar una profundidad y amplitud de habilidades de seguridad en un mercado donde el talento de seguridad es escaso.
- Habilitar capacidades avanzadas como inteligencia de amenazas, análisis de datos grandes, métodos avanzados de detección y respuesta a incidentes y análisis forense.
- Implementar las mejores prácticas que están evolucionando con un entorno de amenaza que cambia rápidamente.
- Mejorar la eficiencia de los costos racionalizando el presupuesto de seguridad con soluciones de seguridad más eficaces.

Según datos de IDC, el mercado de servicios de seguridad gestionad presenta una tasa de crecimiento anual compuesta (CAGR) 10,3% para el periodo 2017-2021. Dada esta previsión de crecimiento, hay una oportunidad significativa para los vendedores y empresas de todos los tamaños, fundamentalmente debido a que la complejidad y la frecuencia de las amenazas de seguridad han aumentado, impulsando la necesidad de una postura de seguridad más holística que sea proactiva y predictiva en lugar de reactiva. En este sentido, hay una necesidad de características de seguridad avanzadas que permitan que las soluciones de seguridad más eficaces incluyan capacidades sofisticadas de inteligencia de amenazas, correlación avanzada de datos y análisis, experiencia para interpretar y actuar sobre los hallazgos, capacidades de respuesta a incidentes y exámenes forenses

que son reseñables. Según datos de IDC, en 2019 el 60% de las empresas dispondrá de una estructura de liderazgo digital. Esto es relevante porque que va a poner en marcha nuevos nuevos KPIs, nuevos modos de monetizar los datos y por tanto generar nuevos ingresos digitales, y en 2020 el 50% del gasto de TI empresarial estará asociado a datos. Por ello, dado que existe una demanda muy significativa de soluciones que permitan a las empresas extraer valor del activo de mayor potencial que poseen hoy que son los datos, la autenticación y confianza aparecen como palancas clave que toda empresa debe gestionar (más allá de disponer de servicios de seguridad gestionada o no), ya que el 80% de los usuarios que vean comprometidos sus datos no confiará de nuevo en la empresa. De hecho, según los datos que manejamos en IDC, en 2019 el 75% de los CIOs reenfocarán la ciberseguridad en torno a la autenticación y confianza, y en 2020 cualquier servicio o activo digital incorporará la seguridad desde el diseño. Sin embargo, donde se producirá un verdadero hito será en la adopción de enfoques de plataformas de gestión integrada de ciberseguridad, de forma que se eliminen los silos de las organizaciones y se disponga de una visión global de la seguridad. Para el 30% de las empresas esta última plataforma será una prioridad en el año 2020.

En este contexto, la correlación y el análisis de datos que provienen de fuentes variadas requieren para apoyar la legalidad, así como requisitos de cumplimiento.

La Transformación Digital está transformando no sólo la forma en la que las empresas están gestionando su relación con los clientes reales, sino que también está transformando la forma en que ofrecemos servicios y aplicaciones. Este viaje digital de las empresas tiene diferentes hitos que van a condicionar sobremanera la perspectiva de la gestión de la seguridad de las empresas. Entre ellos, existen dos

Enlaces de interés...

- Seguridad gestionada: ventajas e inconvenientes
- Hacia servicios de detección y respuesta gestionada cada vez más inteligentes
- La seguridad gestionada se convierte en oportunidad para las operadoras

grandes capacidades de datos para maximizar la visibilidad en diversas amenazas a nivel global, por lo que se requiere una reestructuración de los gastos de seguridad del modelo de CAPEX al gasto.

Es necesario disponer de soluciones de inteligencia de amenazas y capacidades avanzadas de big data, ya que los ciberataques aumentarán en frecuencia e intensidad (severidad). En este contexto actual, las organizaciones no pueden permitirse una estrategia de seguridad "hacer lo mínimo", ya que no es suficiente. Por ello, será necesario adquirir y usar inteligencia "predictiva" confiable que resulta de una combinación robusta de tecnología y experiencia. En este escenario, la agregación y correlación avanzada de datos, el comportamiento del usuario y la detección basada en heurística, el análisis forense y las capacidades de detección y respuesta aparecen como características necesarias en cualquier proveedor de servicios de seguridad gestionada. Así mismo, disponer de capacidades avanzadas de detección y respuesta de amenazas es un factor diferenciador entre los proveedores.

Así mismo, dado que según datos de IDC las vulnerabilidades de sistema operativo de código abierto dejarán hasta un 10% de la nube PaaS/IaaS, será necesario determinar el modelo de entrega de servicio por parte de los proveedores, así como apoyarse en una red de proveedores que puedan proporcionar una amplia gama de servicios que cubran las brechas de seguridad que otros proveedores no pueden.

A menudo, los proveedores de servicios de seguridad gestionada fallan en la alineación de sus soluciones con los objetivos de negocio y las prioridades de negocio de sus clientes. Por ello, para poder competir en este mercado, será necesario que los proveedores entiendan perfectamente al cliente, sus necesidades y su estadio en el viaje digital, de manera que faciliten la transición y progresión del viaje digital de su cliente.

Según datos de IDC, el mercado de servicios de seguridad gestionada presenta una tasa de crecimiento anual compuesta (CAGR) 10,3% para el periodo 2017-2021

¿Te avisamos del próximo IT Digital Security?

¿CUÁLES SON LAS **VENTAJAS** DEL SOFTWARE DE GESTIÓN EMPRESARIAL EN CLOUD?

Descarga este **documento ejecutivo** de it User RESEARCH

MAYTE RUIZ DE VELASCO

DIRECTORA DEL DIGITAL INNOVATION CENTER

Licenciada en filología inglesa y experta en marketing y comunicación, ha pasado por diferentes consultoras de comunicación, como Marketingcom y Ogilvy. Tras su paso por el mundo de la comunicación, dio el saltó a otras áreas de la empresa, alcanzando puestos de dirección, siendo directora de Servicios Ruiz Nicoli Lineas, directora general en RMG Connect y directora general de Wunderman. El pasado año da un giro a su carrera profesional, entrando en el sector de la educación como directora del Digital Innovation Center, donde se encarga de desarrollar el plan de negocio.

Si la formación continuada ha sido siempre importante, hoy es imprescindible

No es nada nuevo afirmar que los profesionales más demandados son los que están relacionados con la tecnología y la digitalización: ingenieros, informáticos y expertos en datos son profesiones que vez están más en voga. Sin embargo, no nos cansamos de leer que no llegamos a generar los suficientes perfiles tecnológicos cualificados como para cubrir la demanda del mercado laboral. Sin duda, esto tiene que tener un porqué.

La tecnología es un área que se está desarrollando a una velocidad que hace difícil estar al día sin un empeño personal. No obstante, la evolución en ramas como la biotecnología, el manejo de datos y la comunicación hacen que su avance sea imparable. La tecnología está aquí para quedarse y está contribuyendo a un cambio de paradigma laboral y social. Es curioso que estas tecnologías que hoy vemos como novedosas se empezaran a desarrollar hace más de 50 años y haya sido sólo de unos años a esta parte cuando hayan cuajado definitivamente.

Las nuevas tecnologías son una revolución como lo fue la electricidad. El tiempo real, la capacidad de los procesadores, la rapidez de los canales de comunicación y un acceso al alcance de muchos, han conseguido que florezcan, lleguen al consumidor y cambien la forma en la que vivimos, nos relacionamos y compramos.

Igual que ocurrió durante la Revolución Industrial, la Revolución Tecnológica trae consigo el cambio de los perfiles laborales que las empresas demandan. La automatización de procesos va a eliminar puestos de trabajo, pero en paralelo va a crear otros nuevos. Todas las revoluciones que afectan a la producción y a la estructura social obligan a pasar por un cambio en la cualificación de la mano de obra para adaptarse a demandas que antes no existían. De hecho, la Unión Europea anunciaba en 2016 que para 2020 serán necesarios 900.000 puestos de trabajo nuevos vinculados con la Ciencia y Tecnología.

Hoy en día, las empresas demandan perfiles que no existen todavía o que son escasos. Como pasa con el efecto dominó, cada nuevo avance tecnológico desarrolla una serie de nuevos perfiles necesarios para desarrollarlos, supervisarlos, gestionarlos...

Por ejemplo, los datos: arquitectos de big data, científicos de datos, auditores de datos, ingenieros de calidad de datos o especialistas en inteligencia

Hoy en día, las empresas demandan perfiles que no existen todavía o que son escasos. Como pasa con el efecto dominó, cada nuevo avance tecnológico desarrolla una serie de nuevos perfiles necesarios para desarrollarlos, supervisarlos y gestionarlos

del consumidor. Somos capaces de producir más datos de los que podemos analizar para actuar de forma más eficiente, amigable, adaptándonos a necesidades o demandas del consumidor, cliente, ciudadano. Por ejemplo, las herramientas de análisis pueden cambiar la forma en la que trabajan los departamentos de recursos humanos. Analizar cómo se comportan los recursos humanos de una compañía puede mejorar la situación de los trabajadores y que se acabe la elección por intuición. Y este es un perfil de analista especializado, orientado a recursos humanos, perfil inexistente hasta ahora.

Al mismo tiempo, todos esos datos y las transacciones que ya no hacemos de persona a persona sino a través de un medio digital hacen necesario

REALIDAD VIRTUAL PARA ATRAER A LOS EXPERTOS EN SEGURIDAD

Siguen haciendo falta expertos en ciberseguridad. Pero un estudio parece haber encontrado la manera de atraer talento: la adopción de nuevas tecnologías. ProtectWise, una empresa de seguridad experta en visibilidad, detección automatizada de amenazas y exploración forense, ha realizado un estudio en el que el 74% de los encuestados aseguran que la presencia de herramientas de Realidad Virtual incrementaría las posibilidades de que escogieran estudios relacionados con la ciberseguridad.

Enlaces de interés...

- La experiencia del empleado mueve el negocio
- Digital Innovation Center

vida que construía muebles hoy tiene que aprender a trabajar con maquinaria de control numérico.

Y estos son solo algunos ejemplos.

Entendiendo que toda revolución es un cambio y todo cambio es traumático, creo que la revolución tecnológica traerá consigo nuevos puestos de trabajo más cualificados y un cambio de mentalidad hacia el aprendizaje, la absorción de nuevas competencias. Abrazar este cambio solo puede hacernos crecer como profesionales y como país. Acceder a los nuevos puestos tecnológicos nos obliga a actualizarnos permanentemente para ser competitivos. Cada día se va a demandar una mano de obra más formada y que tenga la actitud de seguir formándose. El aprendizaje ya no acaba en la escuela o la universidad.

Somos capaces de producir más datos de los que podemos analizar para actuar de forma más eficiente, amigable, adaptándonos a necesidades o demandas del consumidor, cliente, ciudadano

que existan expertos en seguridad, muchos más de los que había hasta ahora. Y, además, expertos en malware o badware por el crecimiento de las amenazas informáticas a través de software intencionadamente malo: según Panda Security, durante los doce meses del 2011 se crearon 73.000 nuevos badwares por día, 10.000 más de la media registrada en todo 2010.

La autonomía y libertad del usuario a la hora de elegir dónde y qué comprar hacen que necesitemos expertos en análisis del consumidor actual (que pasa muchas horas en entornos digitales), diseñadores de UX que faciliten la compra, expertos en rediseñar las experiencias en espacios físicos, no digitales. Expertos en marca, porque en un mundo donde la libertad de elección es casi infinita, lo único que puede frenar la comparación es la elección por marca, por la seguridad que te dé o por las garantías que te ofrezca.

Todas las profesiones tradicionales del tejido productivo y la industria de nuestro país se están tecnificando, así que las empresas buscan perfiles tradicionales con competencias digitales para desempeñarlos. Por ejemplo, el carpintero de toda la

Compartir en RRSS

¿Te avisamos del próximo IT Digital Security?

Blockchain: la tecnología con mayor potencial para redefinir el entorno digital

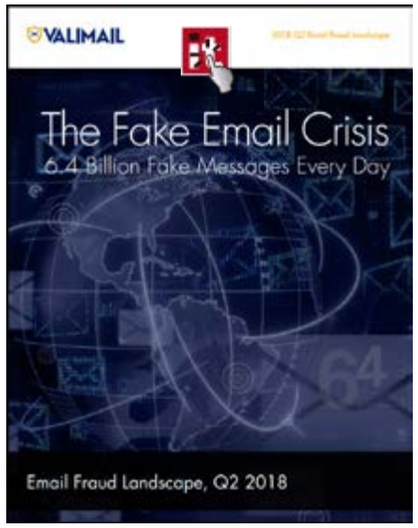
La historia es cíclica. La industria también. Vamos adoptando modas, ideas y tecnologías que aseguramos son nuevas pero que en realidad giran sobre sí mismas. Si hace unas cuantas décadas la centralización movió la industria y la economía hacia una nueva era de prosperidad, ahora es la descentralización quien tira del carro.

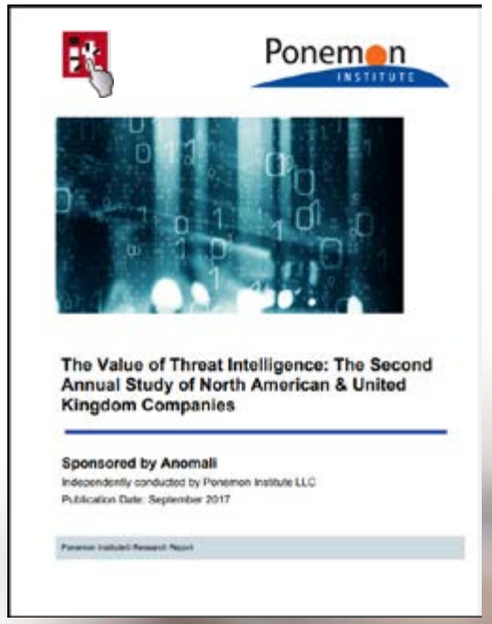
La cambiante cara de los ciberataques

Ataques cada vez más complejos continúan amenazando a las empresas en todo el mundo. La rápida evolución del panorama de las ciberamenazas ha dado lugar a una serie de ciberataques inesperados de alto perfil.
Este documento le ayudará a entender los diferentes tipos de amenazas que se están propagando actualmente. Un ataque DDoS, por ejemplo, puede ser sólo una cortina de humo para un ataque más grave, un ataque de ransomware puede ser utilizado para exfiltrar datos y un ataque IPv6 para acceder a IPv4.

La crisis del email falso

El correo electrónico sigue siendo un medio eficaz para las comunicaciones en todo el mundo, pero cada día se envían 6.400 millones de email falsos. Lejos de ser simplemente un problema de “ingeniería social”, el correo electrónico falso es el resultado directo de problemas técnicos con la forma en que se implementa el correo electrónico: carece de un mecanismo de autenticación incorporado que hace que sea muy fácil fallar a los remitentes. Sin embargo, este problema también es susceptible de solución técnica, comenzando con los estándares de autenticación de correo electrónico DMARC, SPF y DKIM.





El valor de la Inteligencia de Amenazas

Los resultados de este estudio muestran que las organizaciones están incorporando rápidamente la inteligencia de amenazas en sus programas de seguridad.
Algunos de los datos que aporta este informe: Un 84% dice que la inteligencia de amenaza es esencial para una fuerte postura de seguridad; un 80% ya usa inteligencia de amenazas en su propia organización (en comparación con 65% en 2016); un 68% dice que la inteligencia de amenaza es demasiado voluminosa y compleja.

La Seguridad TIC a un solo clic