ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN

Principales conclusiones de la conferencia "Modelo de Seguridad Confianza Cero"

DEL "TRUST, BUT VERIFY" AL "VERIFIY AND NEVER TRUST"

La Asociación para el Fomento de la Seguridad de la Información, ISMS Forum, celebró la semana pasada un encuentro para discutir sobre el planteamiento defendido por Forrester Research y su "Zero Trust" o "Confianza Cero", según el cual, el tráfico generado por los empleados y colaboradores que se encuentran dentro de la organización, debe ser objeto del mismo nivel de desconfianza que el tráfico generado desde fuera del entorno corporativo.

Madrid, 28 de abril de 2011.- La desaparición progresiva del perímetro, la necesidad de centrar la seguridad en el dato, la importancia de conocer en tiempo real los riesgos y problemas de seguridad, la monitorización del tráfico y la concienciación sobre el uso de la red y todos los dispositivos que se conecten a ella, así como el conocimiento de las debilidades de cada organización desde el punto de vista de la seguridad, fueron las principales conclusiones de la jornada organizada por ISMS Forum.

El evento contó con la participación de 14 ponentes de primer nivel, responsables de la seguridad en organizaciones como Telefónica España, Cepsa, la Guardia Civil, ONO, Endesa, junto a expertos de las empresas Arbor Networks Iberia, Buguroo, Blancco Iberia y Swivel Iberia.

Gianluca D`Antonio, Presidente de **ISMS Forum Spain** y CISO del **Grupo FCC**, inauguró la conferencia con la explicación del *Modelo de Seguridad de Confianza Cero y su aplicación en grandes corporaciones*. Según D´Antonio, **se ha pasado del modelo "trust but verify" –una estrategia reactiva focalizada en la estructura de red- al "verify and never trust" o confianza cero**.

"Verificar siempre. Se trata de un modelo proactivo, centrado en el dato y focalizado en el usuario, ver qué puede hacer este usuario de la red y saber cuáles son sus privilegios".

D'Antonio explicó que cada vez es mayor el robo de datos por parte de "insiders" que no necesariamente son empleados de la organización sino identidades suplantadas. Según el "2010 Data Breach Investigations Report" de Verizon Business, el robo de datos por parte de insiders ha aumentado un 26% y ya alcanza el 48% de las incidencias relacionadas con este tipo de delitos.

"Necesitamos construir un Network Analysis & Visibility (NAV). Es decir, capacidad para proteger el acceso a la información, monitorizar toda la actividad, filtrar el contenido para que no sea accesible a todo el mundo. Tengo que ser capaz de saber: ¿Quién navega por mi red? ¿Por qué tiene acceso a mi red? ¿Cómo? ¿Cuándo? ¿Con qué dispositivo? ¿A qué información accede?".

Seguridad Vs. Wikileaks

Alberto Cita, Consulting Engineer de **Arbor Networks Iberia**, empleó el caso de Wikileaks para introducir su conferencia "*Los riesgos de seguridad de las organizaciones y la necesidad de mejorar el análisis y la visibilidad de lo que está pasando en la Red corporativa".*

Cita quiso dejar claro que tanto los sistemas en línea como aquellos offline corren riesgos de filtración de los datos de una organización. Un ejemplo son los llamados "Bots" que se instalan en el sistema sin conocimiento de su propietario y contactan con otro sistema para ponerse a su disposición. Es así como un *botmaster* envía instrucciones a los bots para realizar "tareas" como convertirse en un *site* de *phiishing*, envío de spam o proporcionar datos de cuentas bancarias, etc.

"**El 'trusted' ya no es válido tenemos que ir a un modelo de seguridad de confianza cero, ahora hay que monitorizar todo el tráfico. Este es el desafío** porque estas redes dan servicio a un centenar de

empleados". Cita presentó una solución que lo facilita: Peakflow X, de Arbor Networks. A través de la exportación de datos de flujos IP en los dispositivos de red se puede medir a distancia lo que está ocurriendo y hacer un "Network Behavioral Analysis". Esta solución provee de información de red a nivel transaccional más datos del plano del control de red. De esta manera se crean líneas base (estadísticas y relacionales) que permiten la identificación de anomalías en tiempo real.

Para Cita, la implementación de un modelo de Seguridad de Confianza Cero requiere "visibilidad y seguridad de red global para detectar la 'anormalidad'".

Seguridad desde el código fuente

Abel González Lanzarote, Business Development Manager de **Buguroo**, se centró en el Modelo de confianza cero aplicado a la estructura al código fuente. "Más del 90% de las vulnerabilidades están en el código. El problema es que no tenemos en cuenta la seguridad al desarrollar las aplicaciones, ya sea por tiempo o por coste. **La solución es implantar desde la base el desarrollo seguro: Gestionar la seguridad desde el origen: desde el código fuente**".

González propuso una tecnología para poder cumplir con los objetivos de seguridad: Buguroo Boy Scout, que audita simultáneamente varios códigos y detecta más del 94% de sus vulnerabilidades. Discrimina falsos positivos y facilita el acceso desde la nube para cualquier organización, grande o pequeña, con un coste adecuado a su nivel de uso". Para él la clave está en tener "acceso desde la nube con escalabilidad ilimitada y poder determinar por perfiles quién puede acceder a qué y no esperar a que el código esté terminado".

Se acabaron los usuarios de confianza

Alex Rocha, Country Manager de **Swivel Iberia,** explicó que "las contraseñas ya no son seguras: Sabemos que hay password muy sencillas como 12345…al menos el 50% de las personas usa contraseñas de menos de 7 caracteres; es decir poco seguras. Igual la seguridad corporativa es fuerte dentro de mi organización, pero la de mi gmail no…Entonces, si yo me envío el trabajo a mi gmail, ya no todo es seguro…". Con esta acción tan simple se puede debilitar la cadena de seguridad de la empresa.

Rocha también habló de la frecuencia con la que las contraseñas se dejan debajo del teclado o del monitor como otra evidencia de la debilidad de las contraseñas. Algo que tampoco puede solventarse con los datos de autenticación, pues no ofrecen una gran seguridad debido a su carácter estático y permanente.

Para evitar problemas Rocha **explicó el modelo PinSafe basado en cuatro dígitos que nunca cambian, pero que pueden ofrecer cuatro millones y medio de posibilidades y hacer nuestras contraseñas más seguras.**

"PinSafe es una solución de autenticación fuerte. La clave está en que nunca tenemos que teclear nuestro pin, pero tenemos un pin. Funciona con un protocolo patentado que asocia un pin a cada uno de los usuarios. Este pin va cambiando de posición según el uso de una cadena de seguridad. El pin no cambia, cambia la cadena de seguridad".

Destrucción de datos

La posibilidad de que los datos que han sido borrados de un disco duro puedan ser recuperados representa un riesgo para las organizaciones que deben buscar soluciones para garantizar la destrucción de esos datos pues "formatear no es borrar de manera definitiva" según explicó **Javier Carreras Amorós**, Managing Director de **Blancco Iberia** en su conferencia "*Retos en la gestión del ciclo de vida del dato: Control de dispositivos y borrado seguro".*

Carreras propuso el borrado de la información con un protocolo seguro. “Se necesita un software de sobrescritura que destruya toda la información y realice un informe de borrado que dice qué, quién, cuándo, cómo y por qué se ha borrado. Actualmente –añadió- la información está dispersa en múltiples dispositivos, proponemos una solución independiente del hardware. Para todas debe haber un informe de borrado”.

La clave, según Carreras, está en el “borrado”, es decir, la creación de un protocolo seguro para el borrado de la información; el “informe”, que consiste en la emisión de un reporte con todos los datos necesarios y con base legal; y la “auditoría”. Este último aspecto se refiere a que **el** proceso de borrado debe ser supervisado internamente **y todos los informes deben incluirse en** una base de datos unificada. De esta manera, si todos los datos están en una base común, se podrán realizar auditorías con mayor facilidad.

“Si no se ha hecho nada hasta ahora no es una cuestión de dinero, sino de concienciación”; añadió el representante de Blancco.

El fin de la perimetralidad interna y externa

En la mesa redonda “*Estrategias y claves para la implantación de los pilares de modelo*” participaron **Pedro Morcillo**, Comandante, Jefe área de Redes y Seguridad de la **Guardia Civil**; **Rafael Hernández**, Responsable de Seguridad DSI de **Cepsa**; **Tomás Gómez Pérez**, Subdirector de informática del **Sistema Público de Salud de la Rioja**; con la moderación de **Juan Miguel Velasco**, Director Asociado de Servicios de Seguridad y Proyectos de Seguridad de la Unidad de Grandes Clientes de **Telefónica España**.

En este debate quedó claro que han desaparecido los perímetros y que no hay diferencias por tipos de usuarios internos y externos. El uso de dispositivos móviles, *tablets*, *smartphones*, que se conectan a la red de una organización ha hecho que haya aún más riesgos de seguridad que deben gestionarse.

Velasco introdujo el debate analizando la situación de Sony tras el robo de datos y cómo afectó al valor de la compañía en bolsa y planteó la primera duda: “¿Tenemos un perímetro? ¿Hay usuarios buenos y usuarios malos?”. En el caso de Cepsa, Hernández comentó que la perimetralidad interna y externa se está acabando. “Cada vez usan más dispositivos móviles. El dispositivo personal-de empresa cada vez está más extendido. Hay herramientas que ayudan a hacer ese trabajo pero es muy es muy importante tener en cuenta la tecnología y la gestión de la tecnología”.

Para el subdirector de informática del Sistema Público de Salud de la Rioja, la dificultad de establecer un perímetro, principalmente por el uso de dispositivos que se conectan a la red, ha obligado a la organización a impedirlos. “De momento solo podemos gestionar los positivos que nosotros entregamos. Por lo que no damos acceso a los dispositivos que no controlamos”.

Pedro Morcillo de la Guardia Civil comentó que cuando se planteó un proyecto de seguridad perimetral se decidió que el primero que tenía que estar fuera del usuario. “En nuestro proyecto tenemos un ordenador de internet y otro de intranet”.

¿Se puede monitorizar al empleado?

En la mesa redonda “**Implicaciones legales de la monitorización de la actividad de los empleados”** que contó con la participación de **Javier Carbayo**, Asociado Senior del Área de Governance, Risk & Compliance, de **Ecija**; **Ana González Romo**, del departamento de Seguridad de la Información de **Endesa**, **Diego Bueno**, Senior Manager IPBR, IT Advisory en **KPMG**; **Javier Santos**, Gerente de Operaciones de Seguridad de **ONO**; y la moderación de **Antonio Ramos**, presidente de **ISACA Madrid**; se llegó a la conclusión de que la clave está en establecer una normativa de uso que sea conocida por el empleado. “La concienciación es necesaria pero tiene que ser de arriba abajo”, explicó Ramos en relación con el cumplimiento de los protocolos de seguridad por parte de todos los empleados.

Respecto a si la monitorización de los empleados es un tema técnico o jurídico, hay diversidad de opiniones. Para Carbayo, de Ecija, “es un tema legal que normalmente se articula a través de medidas

tecnológicas. Se busca tener una capacidad para cumplir una normativa y que en el cumplimiento de la misma no se viole otra". En el caso de Endesa, González considera que se trata de "un tema organizativo que pasa por las políticas y las normas que establece la empresa". Desde KPMG, Bueno explica que es un tema técnico que depende de la estrategia de seguridad: "Hay que analizar los riesgos a los que se está sometido y tomar las medidas adecuadas". Santos, de Ono, lo ve como jurídico-organizativo: "En nuestro caso tener más capacidad de monitorización nos hace tener que hacer menos esfuerzo tecnológico. Tiene que haber concienciación y que el usuario sepa que lo estamos monitorizando".

En cualquier caso como explicó Javier Carbayo "la normativa nos da unas ciertas fronteras. Que cada vez están más definidas y nuestro trabajo es identificar cuáles son las fronteras, según la actividad del empleado y saber que no tienen que superar ciertos límites".

Gianluca D`Antonio concluyó el evento haciendo énfasis sobre la importancia de permitir el uso privado y moderado de la red y los sistemas de la organización a cambio de poder monitorizar a los usuarios, pero sin correr el riesgo de que el CISO se tome más atribuciones. "El negocio es el que tiene que prohibir. El departamento de seguridad hace el análisis de riesgo, propone controles y aconseja al negocio sobre cómo controlar estos riesgos. Somos un asesor interno que facilita la toma de decisiones, pero no somos los propietarios de la información".

Gianluca D´Antonio, Presidente de ISMS Forum, durante su intervención.