ISMS Forum Spain
ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN

Juan Bravo, 3A
28006 Madrid
España

Tel. +34 91 436 74 13
Fax +34 91 436 73 65
comunicacion@ismsforum.es
www.ismsforum.es

nota de prensa

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

EL USO DE TABLETS, SMARTPHONES Y DISPOSITIVOS EXTERNOS QUE SE CONECTAN A LA RED DE LAS ORGANIZACIONES INCREMENTA LA NECESIDAD DE MONITORIZAR A LOS EMPLEADOS Y DE CONOCER LOS RIESGOS EN TIEMPO REAL

Madrid, 10 de mayo de 2011.- 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.

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 Cepsa, la Guardia Civil, Endesa, ONO y Telefónica España, junto a expertos de las empresas Arbor Networks Iberia, Blancco Iberia, Buguroo 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**.

"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 dejó claro que tanto los sistemas en línea como aquellos offline corren riesgos de filtración de los datos de una organización.

"**El 'trusted' ya no es válido. Hay 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.

Juan Bravo, 3A
28006 Madrid
España

Tel. +34 91 436 74 13
Fax +34 91 436 73 65
comunicacion@ismsforum.es
www.ismsforum.es

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. **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 cumplir con los objetivos de seguridad: Buguroo Boy Scout, que audita varios códigos a la vez, detecta más del 94% de sus vulnerabilidades y discrimina falsos positivos".

Se acabaron los usuarios de confianza

Alex Rocha, Country Manager de **Swivel Iberia,** explicó que "las contraseñas ya no son seguras: al menos el 50% de las personas usa contraseñas de menos de 7 caracteres, es decir poco seguras". 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.**

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 como el realizado por Blancco que certifica que se ha borrado a través de 16 estándares soportados por certificados y emite un informe con base legal.

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 han hecho que haya aún más riesgos de seguridad. Las soluciones comentadas van desde la prohibición de conexión a la red con dispositivos externos, hasta una adecuada gestión de la tecnología o mayor control de quién accede a la información.

¿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.

Juan Bravo, 3A
28006 Madrid
España

Tel. +34 91 436 74 13
Fax +34 91 436 73 65
comunicacion@ismsforum.es
www.ismsforum.es

Respecto a si la monitorización de los empleados es un tema técnico o jurídico, hay diversidad de opiniones. Para Carbayo "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: "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".

Sobre ISMS Forum Spain:
ISMS Forum Spain es una Asociación española sin ánimo de lucro, cuyo principal objetivo es fomentar la Seguridad de la Información. Se constituye como foro especializado para que todas las empresas, organismos públicos y privados y profesionales del sector colaboren, intercambien experiencias y conozcan los últimos avances y desarrollos en materia de Seguridad de la Información.
La Asociación está respaldada por algunas de las más representativas empresas y organizaciones comprometidas con la Seguridad de la Información. Los socios fundadores ejercen su labor en muy diversos ámbitos que van desde la enseñanza superior y la I+D hasta la Consultoría, pasando por los sectores de Banca, Seguros, Sanitario, Construcción, Servicios Jurídicos Tecnologías de la Información o Telecomunicaciones. Hoy en día cuenta con el respaldo de más de 100 empresas y más de 750 profesionales asociados, lo que la convierte en la mayor red activa española de Seguridad de la Información. Más información en www.ismsforum.es .