DIRIGENTES
MADRID
01/10/12
Prensa: Mensual
Tirada: Sin datos OJD
Difusión: Sin datos OJD
Cód: 62586192
Página: 61
Sección: OPINIÓN Valor: 6.083,00 € Área (cm2): 458,4 Ocupación: 100 % Documento: 1/1 Autor: Núm. Lectores: 0

tribuna

Un nuevo escenario de movilidad y seguridad

Olof Sandstrom
Director de Operaciones de Arsys

El nuevo modelo de consumo tecnológico masivo y multi-device nos plantea una nueva reflexión sobre cuestiones relacionadas con la gestión corporativa y el uso personal de los mismos, consideraciones legales o accesibilidad a la información.

Acostumbrados a un modelo en el que la empresa ejercía un extenso control sobre la propiedad y gestión de sus equipos es necesario comprender que ha llegado un nuevo escenario en el que los usuarios no solo llevan información personal o contactos de trabajo, sino que aproximadamente una de cada tres personas almacena en sus dispositivos móviles información confidencial relacionada con su trabajo.

El modelo de seguridad al que debemos aproximarnos tiene un enfoque nuevo. No tiene sentido seguir creyendo que somos capaces de controlar todo lo que entra y sale de la empresa, pues los límites son muy difusos.

Un ejemplo es que hasta hace muy poco nos parecía una locura plantearnos la posibilidad de acceder desde un cibercafé a alguna aplicación que manejara datos sensibles.

Ahora, nos conectamos al WiFi de cualquier cafetería y nos ponemos a trabajar desde nuestros dispositivos móviles.

Las ventajas de este nuevo contexto, en términos de accesibilidad y movilidad, son incuestionables.

Sin embargo, poder beneficiarnos de su potencial exige tener consciencia de la forma en la que debemos utilizar la tecnología para garantizar la seguridad de la información.

Para ello, tenemos que ser conscientes de las posibles amenazas que supone, los usuarios deben decidir qué herramientas de seguridad instalar en sus dispositivos, como por ejemplo una contraseña de calidad o una herramienta de cifrado para el correo, para que en caso de pérdida o robo del mismo cualquier usuario no pueda acceder a los datos almacenados ni al contenido al que dan acceso las aplicaciones.

En realidad, desde el punto de vista tecnológico, la seguridad de las infraestructuras en el entorno Cloud no se diferencia tanto de la seguridad que conocemos en entornos tradicionales.

Los servicios Cloud siguen teniendo las mismas necesidades de seguridad de toda la vida, con algún enfoque ligeramente distinto: corren en máquinas virtuales que están alojadas en servidores físicos, que almacenan la información en cabinas de discos, conectados a través de switches, cortafuegos y routers a la Red.

Con este panorama, tenemos que asumir la securización de estos dispositivos móviles, tal y como hacíamos con los ordenadores portátiles tradicionales, pues el número de aplicaciones maliciosas para dispositivos móviles se multiplica año tras año.

Antivirus, cortafuegos de puesto, cifrado, protección mediante contraseñas, localización y borrado remoto del contenido del terminal, etc. tienen estar cada vez más presentes en los dispositivos móviles.

Y, tal vez, lo más importante de todo: los usuarios tienen que conocer y entender las amenazas que están relacionadas con los dispositivos móviles y la información que se gestiona a través de ellos.