Manejo de la seguridad en un mundo móvil

Julio A. Omaña G.
Gte de Seguridad de Información
PwC

Agenda:

- Introducción
- Riesgos de los dispositivos móviles
- Factores de riesgo concurrentes
- Como establecer un modelo de seguridad
- Conclusiones

Introducción:

El uso de dispositivos móviles es una tendencia irreversible y avasallante. Las personas prefieren acceder a su información de trabajo a través del mismo dispositivo con que cambian su estatus de Facebook, revisan el twitter y se comunican con sus familiares y amigos……..¿Esto es razonable?

.

.

.

Con un manejo adecuado de los riesgos, la productividad de los empleados puede ser 25% superior si se establece una estrategia de movilidad efectiva.

¿Qué hacemos?

Riesgos de los dispositivos móviles:

- Mayor participación del mercado, mayor exposición a malwares y virus (Android 45%, iOS 27%)-(Rooted-Jailbreak)
- Robo de identidad
- Servicios premium y spoofing
- Facilidad para compartir información por canales inseguros
- Dependencia y confianza en redes públicas o controlada por terceros
- Geotaging y seguridad personal
- Dificultad para la identificación del canal utilizado en la comunicación
- Control de la información muy relacionado con el control físico
- Los dispositivos no son propiedad de la empresa
- Heterogeneidad de plataformas
- Velocidad de cambios
- Dificultad de reforzamiento de los controles

Factores de riesgo concurrentes:

- BYOD – “Bring Your Own Device” – 2011:28% y 2013:35%
- Almacenamiento limitado y uso de Cloud Services
- Trust Among Friends en Redes Sociales
- Excepciones en los controles para los ejecutivos C-level

Como establecer un modelo de seguridad:

Framework de Seguridad

- Definición de políticas de seguridad para los dispositivos
- Realizar un inventario de todos los dispositivos móviles de la organización
- Analizar el riesgo asociado al uso de los dispositivos en las diferentes áreas de la organización
- Definir un estándar de seguridad
- Establecer controles para evitar dispositivos no autorizados
- Definir las características de almacenamiento permitida para la diferente información (red, cloud, disp, etc)
- Definir un esquema de aprobación de APPs o desarrollo interno
- Desarrollar políticas de uso de los dispositivos y su relación con las redes sociales
- Capacitar y concientizar a los usuarios

Finanzas, Marketing, Unidades de Negocio, TI, Riesgo, Legal, Cumplimiento, Auditoría, etc…

Conclusiones:

Entonces…..¿Que hacemos?