Objetivos para mejorar la seguridad en el uso de dispositivos móviles en entornos personales y corporativos

A partir del análisis realizado y los resultados obtenidos en la práctica, se plantean los siguientes objetivos fundamentales para mitigar los riesgos y mejorar la seguridad de los dispositivos móviles.

1. Aumentar la concienciación de los usuarios sobre los riesgos de seguridad en dispositivos móviles

Uno de los principales desafíos en seguridad móvil es la falta de conocimiento por parte de los usuarios. Muchas veces, se desconocen los riesgos que implican acciones como hacer jailbreak, rootear el dispositivo o instalar aplicaciones desde fuentes no oficiales. Este desconocimiento puede poner en peligro tanto la información personal como la corporativa.

Para alcanzar este objetivo, es fundamental llevar a cabo campañas de concienciación y formación específicas sobre buenas prácticas, riesgos más comunes y medidas preventivas. También se pueden realizar talleres prácticos o simulacros de ciberataques (por ejemplo, phishing móvil) para mostrar en la práctica los efectos de una mala decisión.

2. Establecer políticas de seguridad específicas para el uso de dispositivos personales (BYOD)

El uso de dispositivos personales en entornos corporativos es una práctica cada vez más común, pero si no se gestiona adecuadamente, puede convertirse en una amenaza directa para la seguridad de la información de la empresa. Es necesario establecer reglas claras que regulen este tipo de uso.

Para ello, se recomienda implementar una política de BYOD que defina requisitos mínimos de seguridad (como el uso de cifrado, bloqueo del dispositivo o antivirus), además de herramientas de gestión de dispositivos móviles (MDM) que permitan monitorear el acceso y aplicar restricciones en función del nivel de riesgo. También es recomendable que los empleados acepten un acuerdo de uso responsable antes de conectar sus dispositivos a la red corporativa.

3. Utilizar herramientas de seguimiento y monitoreo para detectar incidentes en dispositivos móviles

El uso de herramientas de seguimiento y monitoreo permite detectar de forma temprana cualquier comportamiento anómalo en los dispositivos, lo que facilita una respuesta rápida ante incidentes como robos, pérdidas o accesos no autorizados.

Este objetivo puede alcanzarse mediante la implementación de herramientas como "Encontrar mi dispositivo" de Google o iCloud de Apple en el entorno personal, y mediante soluciones más avanzadas de monitoreo en entornos empresariales (como Microsoft Intune o IBM MaaS360). Estas herramientas permiten geolocalizar, bloquear y borrar los datos del dispositivo en caso de compromiso.

4. Promover buenas prácticas de seguridad y definir protocolos de actuación ante el robo o compromiso del dispositivo

Además de la prevención, es fundamental que tanto usuarios como organizaciones tengan claro qué hacer ante el robo, pérdida o compromiso de un dispositivo. Una reacción rápida puede minimizar significativamente los daños.

Para lograrlo, se debe crear y difundir una guía de buenas prácticas (por ejemplo, uso de contraseñas fuertes, activación del cifrado, uso de VPN, etc.) y establecer protocolos de actuación claros ante incidentes. Estos protocolos deben incluir medidas como el bloqueo remoto del dispositivo, el cambio de contraseñas y la notificación inmediata al departamento de TI.

Referencias

-Agencia Española de Protección de Datos (AEPD). Catálogo de medidas preventivas y herramientas para proteger la privacidad en dispositivos móviles.

-OWASP Mobile Application Security Testing Guide (MASTG).

-NIST Special Publication 800-124 Revision 2: Guidelines for Managing the Security of Mobile Devices in the Enterprise.