Adiestramiento del Personal

Compilado por: Rodolfo Peña García, Director Técnico de Energywise, S. A. de C. V.

Más del 70% de las intrusiones y ataques a las redes y dispositivos computacionales de las empresas se deben al llamado “phishing,” es decir, el inducir a usuarios de la empresa a abrir o hacer clic en archivos que vienen adjuntos a algún correo electrónico proveniente del atacante o atacantes maliciosos.

1) Configuración de Firewalls

Las reglas de los firewalls deben restringir y examinar el tráfico que va entrando e igualmente el que va de salida de la red y de los servidores más importantes. Restringir el acceso a solamente aquellos servicios (puertos abiertos) que sean necesarios para conducir los negocios. Restringir el tráfico de salida a solamente los sitios web que sean de confianza o las direcciones IP reconocidas. Prohibir que los dispositivos y programas que se encarguen de transacciones comerciales puedan navegar por la Internet. Separar los sistemas que no sean parte de los procesos comerciales de la empresa o que se requieran para conducir el negocio y ponerlos en redes separadas. Llevar a cabo auditorías periódicas en todas las firewalls de la empresa, sus puertos y servicios mediante análisis de vulnerabilidades y pruebas de penetración. Asegúrese que todos los firewalls y analizadores de vulnerabilidades se basen en equipo (hardware) y no software y que provean análisis continuo las 24 horas y siete días de la semana, ofreciendo alarmas y reportes periódicos.

2) Adiestramiento respecto a contraseñas seguras (passwords) y políticas de uso por el personal para evitar el llamado “phishing.”

Adiestramiento cuyo objetivo es elevar la concientización de los usuarios respecto al uso de contraseñas más complejas, los peligros de abrir o hacer clic en archivos adjuntos de proveniencia desconocida o sospechosa.

Familiarizar a los usuarios con las prácticas de la ingeniería social (social engineering) y los peligros que existen al usar las redes sociales.

3) Configuración de sistemas y programación segura

Asegurar que se establezcan lineamientos para el endurecimiento de los sistemas y programas contra las vulnerabilidades y amenazas conocidas. Basar la configuración de los sistemas y programas el las mejores prácticas de la industria. Configurar los sistemas operativos para eliminar puntos de debilidad, sobre todo en ambientes Windows. Verificar que no haya modificaciones sin autorización a los ambientes de los sistemas, por ejemplo, almacenamiento externo vulnerable, software no autorizado o de proveedores autorizados. Implementación de procesos que registren todo cambio a los sistemas y al ambiente computacional.

4) Asegurar el acceso remoto

Establecer autentificación de dos factores para todos los ambientes de acceso remoto. Asegurar que el acceso de terceros se cierre automáticamente y los usuarios autorizador lo puedan utilizar cuando lo necesiten.

5) Administración de parches

Actualizar los equipos, sistemas operativos y programas tan pronto se reciban los parches o actualizaciones. Mantener las aplicaciones y “plug-ins” de browsers actualizados con las últimas versiones proveídas por las compañías que los venden.

6) Escaneo de vulnerabilidades internas y externas.

Escaneos frecuentes externos e internos para encontrar y remediar vulnerabilidades. Igualmente llevar a cabo pruebas de penetración por lo menos una vez al año y sobre todo después de cualquier actualización significativa a la infraestructura, aplicaciones o sistemas.

7) Registros (logs) y Monitoreo de Amenazas a la Ciberseguridad

Configuración de los logs de Windows para que capturen todo evento de seguridad, de las aplicaciones y los sistemas. Mantener los registros por lo menos 90 días en el sistemas y un año el archivos fuera de línea. Llevar a cabo regularmente revisiones de los registros de todos los dispositivos. Establecer procedimientos para responder a eventos críticos. Implementar sistemas de detección de intrusiones. Implementar monitores de la integridad de archivos.

8) Utilizar los anti-virus para eliminar todo virus y “malware” de TODOS los dispositivos

Asegurar que el software anti-virus esté actualizado en todos los sistemas y dispositivos. Y que esté configurado para actualizar las definiciones de virus. También, asegurar que la licencia del anti-virus sea válida para toda la empresa y que el software esté accediendo a la nuevas definiciones correctamente.

9) Adiestrar y abogar por un grupo especializado en las políticas y procedimientos de ciberseguridad. Llevar a cabo adiestramiento de los empleados respecto la ciberseguridad por lo menos una vez por semestre. Instruir al personal respecto la prohibición de utilizar software no autorizado o ir a visitar sitios del web peligrosos. Contratar expertos externos regularmente como medida proactiva para medir la dureza de los sistemas y mejorar los sistemas de detección de amenazas.