sedian

Seguridad Digital
de Andalucía

Ficha técnica

Configuración segura en Windows

Modalidad: presencial virtualizada

Fecha inicio: 23 de mayo de 2022

Fecha finalización: 6 de junio de 2022

Junta de Andalucía

Sumario

1 DATOS BÁSICOS DE LA ACCIÓN FORMATIVA

Nombre de la acción formativa: Configuración segura en Windows

Modalidad: Presencial virtualizada.

Fecha de Inicio: 23 de mayo de 2022 .

Fecha de Finalización: 6 de junio de 2022.

Sesiones en directo vía streaming:

- 23 de mayo: 11:00 a 13:30 A.M.
- 30 de mayo: 11:00 a 13:30 A.M.
- 6 de junio: 11:00 a 13:30 A.M.

Fechas para las tutorías:

- 25 de mayo de 05:30 a 06:30 P.M.
- 1 de junio de 05:30 a 06:30 P.M.

Dirigido a: Responsables de seguridad TIC y personal TIC de la Junta de Andalucía

Número máximo de personas participantes: 30.

2 DESCRIPCIÓN

Los administradores de sistemas siguen prácticas generales a la hora de proteger los sistemas Windows. Si bien esta actividad es necesaria, hoy en día se torna insuficiente porque la administración de equipos Windows se realiza de la misma forma que en versiones previas y no se aprovechan las novedades de seguridad presentes en las últimas ediciones. Por otro lado, se da la circunstancia de que el profesional de TI no suele disponer de tiempo para investigar por su cuenta las buenas prácticas de

seguridad de Windows, que se muchas y algunas complejas. Esta formación pretende ser muy concisa, concreta y avanzada, aportando los conocimientos que el profesional no tiene y cambiando prácticas tradicionales que o bien ya no tienen sentido o han sido sustituidas por configuraciones modernas.

3 OBJETIVOS

- Aprender a gestionar la sincronización de hora en Windows.
- Conocer cómo funcionan y qué aportan los protocolos de VPN, DirectAccess y RDS.
- Conocer las posibilidades del Firewall de Windows.
- Aprender cómo defender a Windows frente al Malware.
- Determinar los servicios esenciales que debe correr un sistema Windows y cerrar el resto (Bastionado por líneas base de seguridad)
- Gestión correcta de las cuentas de usuarios locales y su interacción con las de dominio.
- Determinar si están desplegados convenientemente las configuraciones recomendadas de seguridad de Active Directory para proteger el dominio.
- Entender qué ocurre en un sistema Windows atendiendo a los eventos y la auditoría.
- Conocer el uso de bitlocker para proteger los dispositivos.
- Configuraciones avanzadas de la red WiFi en los dispositivos Windows.

4 CONTENIDOS

- Sincronización de Hora:
  - Cómo funciona el Servicio de Hora de Windows.

    - La misión del maestro de operaciones de emulación del PDC respecto a la sincronización de hora de los equipos miembros de un dominio de Active Directory.
    - Sincronización de hora con las herramientas del servicio de hora de Windows (cliente NTP).
- Acceso remoto con Direct Access.
    - Opciones de despliegue del servidor Direct Access.
    - Protocolos de túnel del servidor Direct Access.
    - Configuración del servidor de Direct Access por GPO.
- Acceso remoto VPN tradicional.
    - Escenarios de uso de servidores VPN.
    - Protocolos de túnel.
    - Tipos de autenticación para VPN.
    - Reconexión automática VPN (IKEv2)
    - Creación de perfiles de conexión de cliente con CMAK.
- Acceso remoto por medio de Servicios de Escritorio Remoto (RDS)
    - Ventajas e inconvenientes.
    - Configuración del acceso local y por GPO.
    - Configuración del acceso RDS usando una puerta de enlace (protección SSL)
    - Monitorización de los accesos remoto.
- Windows Defender Firewall con seguridad avanzada.
    - Perfiles de reglas o creación de reglas locales.
    - Creación de reglas por GPO.
    - Reglas de seguridad de la conexión IPSec con Firewall de Windows.
- Protección frente a malware.
    - Vectors de ataques prominentes (Spear phishing, USB como plataforma de ataque).
    - Recuperación frente a ransomware (Historial de archivos de Windows).
    - Soluciones centralizadas de antivirus.
    - Función del sandbox en un antivirus.

- Defensa frente a malware de día cero.
- Detección de vulnerabilidades presentes en Windows.
- El reto de Windows como servicio (WaaS) el nuevo modelo de parcheo y actualización de Windows.
- Configurar la actualización de Windows localmente.
- Configurar la actualización de Windows por medio de WSUS/WaaS (Nuevas GPOs disponibles).

- Bastionado de sistemas Windows por medio de líneas base.
  - ¿Qué es Security Compliance Toolkit?
  - Minimizar la superficie de ataque con líneas base de seguridad.
  - El principio del menor privilegio.
  - Descargas de líneas base de configuración de seguridad recomendadas por Microsoft.
  - Análisis de las líneas base.
  - Creación de una GPO a partir de líneas base.
  - Aplicación masiva de las líneas base seguridad por medio de GPO.
- Protección de las cuentas locales.
  - Cuentas por defecto de usuario: La cuenta “Guest”, la cuenta “HelpAssistant”
  - Cuentas por defecto del sistema.
  - Cómo administrar las cuentas locales.
  - Restricción y protección de cuentas locales con derechos de administrador.
  - Pertenencia a grupos locales de identidades del dominio: Buenas prácticas.
  - La GPO de grupos restringidos.
  - Eliminar o cambiar contraseñas de cuentas locales que crean los servicios al instalarse o evitar ataques de movimiento lateral con cuentas locales.
  - Los grupos locales y los permisos para poder instalar programas en Windows.
  - Evitar que los usuarios cambien la configuración IP del dispositivo.
- Configuraciones de Active Directory para mejorar la seguridad.

- ¿Qué es el TGT (Ticket Granting Ticket)? La política de Kerberos: Cómo evitar ataques del tipo “Replay”.
- La política de contraseña del directorio.
- Conseguir diferentes esquemas de complejidad de contraseña por medio de objetos de ajuste de password (PSO objects).
- La problemática del uso de una cuenta de usuario de AD para instalar servicios.
- Minimizar la probabilidad del éxito de ataques de fuerza bruta a servicios por medio de Cuentas de Servicio Administradas de Grupo (GSMA).
- Activación de la Papelera de Reciclaje de Active Directory.
- Configurar mensaje de bienvenida (Disclaimer y política de acceso) al iniciar sesión en Active Directory.
- Windows Hello para la Empresa: El nuevo paradigma de la autenticación Kerberos que evita ataques del tipo Rainbow Table.
- Establecer MFA en Active Directory.
- Cómo un CAPTCHA puede evitar ataques de denegación de servicio en la autenticación de usuarios.

- El visor de eventos de Windows.
  - Filtrado de eventos.
  - Acceso a logs operacionales (Avanzados) de Windows.
  - Recopilar los eventos remotos en el ordenador del técnico mediante la suscripción a eventos.
- Mantenimiento preventivo de sistemas Windows.
  - El log de Sistema y de Aplicación.
  - El Monitor de rendimiento.
  - Confirmar el correcto funcionamiento del sistema operativo por medio de Conjuntos Recopiladores de Datos.
  - Observar el degradado de un sistema Windows en el tiempo por medio del Monitor de Fiabilidad de Windows.
- La auditoría de Windows.

  - Elementos del sistema que se pueden auditar (inicios de sesión, cambio de credenciales, …)
  - Habilitar la auditoría de acceso a objetos (archivos)
  - Configurar el registro circular del log de seguridad (auditoría)
  - Activar la auditoría en el sistema de archivos de Windows.
  - Consultar la auditoría. Herramientas de terceros que mejorar la comprensión y la consulta del log de auditoría.
- Cifrado del almacenamiento secundario.
  - ¿Qué es Bitlocker?
  - La misión del módulo TPM (Trusted Platform Module) respecto a las claves de Bitlocker.
  - Emulación del TPM.
  - Exigir PIN o lectura biométrica para desbloqueo de TPM.
  - Configuraciones de bitlocker/TPM por directiva local/grupo.
  - Cifrar unidades de sistema y de datos.
  - Almacenar las claves de Bitlocker en Active Directory.
  - Recuperación de unidad Bitlocker.
- Implementación del acceso inalámbrico en Windows.
  - Despliegue y configuración de APs: Buenas prácticas.
  - Creación de grupos de seguridad de usuarios WiFi.
  - Políticas de configuración 802.11 en Windows.
  - Control centralizado de la autenticación de AP por medio de NPS.
  - Consideraciones al unir al dominio un equipo desde la red WiFi.
  - Asignación de perfil de firewall para conexiones WiFi.
  - Configuración de redes de uso medido mediante directiva local.

5 TEMPORALIZACIÓN

Sesiones en directo vía streaming:

- 23 de mayo: 11:00 a 13:30 A.M.

- 30 de mayo: 11:00 a 13:30 A.M.
- 6 de junio: 11:00 a 13:30 A.M.

Fechas para las tutorías:

- 25 de mayo de 05:30 a 06:30 P.M.
- 1 de junio de 05:30 a 06:30 P.M.

6 METODOLOGÍA

Esta formación está concebida para desarrollar la parte teórica y conceptual en modalidad online mediante **sesiones por streaming**. De este modo, los participantes asistirán a tres sesiones online mediante la herramienta de videoconferencia "Gotomeeting". La duración total será de 6 horas de formación teórica, donde el docente expondrá y explicará los contenidos del curso. Para complementar dichas explicaciones teóricas se propondrán una serie de casos prácticos usando laboratorios virtuales que permitirán afianzar los conocimientos.

Por otro lado, se empleará una metodología activa basada en el "**Aula invertida**" (Flipped Classroom). Esta metodología trata de obtener el máximo provecho de las sesiones online en directo, dedicando el máximo tiempo a la aplicación y puesta en práctica de los contenidos teóricos. Dichos contenidos estarán accesibles en el campus virtual en todo momento para que los participantes puedan consultarlos fuera de las sesiones online.

Asimismo, durante las sesiones online se dedicará un tiempo inicial a presentar y exponer dudas por parte de los participantes que el docente resolverá y pondrá en común con el grupo.

7 DOCENTE

IMPARTIDO POR: Alejandro Cortés

Experto en Ciberseguridad. Perito Judicial Informático, con más de 15 años de experiencia en este sector.

Director del Máster Internacional de Ciberseguridad y profesor de Ciclo Formativo Grado Superior en EIG Business School. Profesor de Robótica en ESIC Business & Marketing School y profesor de Investigación en DeepWeb y DarkWeb, en el máster de ciberseguridad, en la Escuela Internacional de Posgrados.

Ha participado como ponente en distintos talleres y charlas sobre seguridad informática, como CyberInsuranceDay 2020 o Tapas&Hacks.

Acceso a su perfil LinkedIn

8 EVALUACIÓN

La evaluación se efectuará en base a las **evidencias de aprendizaje** obtenidas mediante actividades que los participantes deberán realizar durante el periodo lectivo. Estas actividades serán de dos tipos:

1. **Actividades prácticas.** Se trata de ejercicios que buscan que el participante ponga en práctica los conocimientos adquiridos en situaciones y escenarios cercanos a la realidad. Dichas actividades se solicitarán a los participantes al final de las tres sesiones online y se deben enviar a través de los buzones habilitados a tal efecto en la plataforma.

2. **Pruebas de autocomprobación.** Dichas pruebas permiten conocer tanto al usuario acerca de su propio progreso en cuanto al manejo de los conocimientos teóricos y prácticos del curso.

9 ATENCIÓN AL ALUMNADO

Para realizar un correcto seguimiento del curso y disponer de los medios necesarios para que los alumnos puedan elevar sus dudas al tutor, se dispondrán de los siguientes canales para tal fin:

1. Mail del tutor. Los alumnos podrán mantener contacto con el/la tutor/a del curso mediante la dirección de mail formacion.sedian@juntadeandalucia.es donde el/la tutor/a dispondrá de un plazo máximo de 48h para responder al alumnado.

2. Videoconferencia mediante GoToWebinar. En la Ficha técnica del curso y en la propia aula virtual el alumnado tiene disponible los días y horarios de las clases en directo, para que los participantes puedan mantener una videoconferencia con el/la tutor/a y así poder resolver las dudas o profundizar en contenidos que requieren una asistencia técnica.

3. Tutorías mediante GoToWebinar. En la Ficha técnica del curso y en la propia aula virtual el alumnado tiene disponible los días y horarios de las tutorías, para que los participantes puedan mantener una videoconferencia con el/la tutor/a y así poder resolver las dudas o profundizar en contenidos que requieren una asistencia técnica.

4. Foro de discusión. Los alumnos disponen de un foro de discusión donde mantendrán una relación colaborativa y podrán mantener contacto con el/la tutor/a.

10 OBSERVACIONES

Los participantes deben tener conocimientos previos en informática a nivel usuario.

Previa al inicio de la acción formativa se realizará un cuestionario de conocimientos previos de carácter voluntario que permita a la docente analizar los conocimientos en la materia del curso de presencia virtualizado.