Costo: $	Impacto: MEDIO	Complejidad: BAJA

2.M: ¿Usa el WWS controles de seguridad de correo electrónico para reducir las amenazas de correo electrónico habituales, como la suplantación de identidad, el robo de identidad y la intercepción?

Recomendación: Asegúrese de que los controles de seguridad de correo electrónico estén habilitados en toda la infraestructura de correo electrónico corporativo.

¿Por qué es importante este control?

Este control es importante porque el uso de controles de seguridad puede reducir el riesgo de ataques a través de correo electrónico a las operaciones del WWS al filtrar los correos electrónicos maliciosos antes de que lleguen a los empleados.

Los métodos más comunes y exitosos para que los atacantes ingresen a una red son a través de ataques relacionados con el correo electrónico, como el robo de identidad, la suplantación de identidad y la intercepción. El robo de identidad es un método de ataque en el que se envía a los empleados un correo electrónico con un archivo, un enlace o una solicitud maliciosos. Una vez que el empleado abre el enlace, un archivo malicioso puede cargar programas maliciosos en la red de su WWS, lo que puede llevar al robo de credenciales de empleados o a engañar a un empleado para que proporcione credenciales o fondos del WWS.

ORIENTACIÓN ADICIONAL

- Los WWS deben realizar campañas de capacitación y concientización para los empleados a fin de complementar estos controles técnicos recomendados y reducir el riesgo general de ataques basados en correo electrónico a la red del WWS.
- Si bien el WWS debe evitar todas las conexiones entre TO y el Internet público, si es posible (consulte la hoja informativa 2.X), el WWS no debe configurar ningún activo de TO para recibir correo electrónico, ya que los ataques por correo electrónico son comunes y, a menudo, efectivos.

La suplantación de identidad es un método que los atacantes suelen utilizar junto con el robo de identidad, en el que un atacante diseña un correo electrónico malicioso para que parezca que proviene de una fuente confiable, generalmente copiando el estilo y la dirección de correo electrónico de una empresa conocida.

La intercepción es un método en el que un atacante puede colocarse entre el remitente y el receptor de un correo electrónico, lo que le da la oportunidad de robar el correo electrónico y su contenido.

Consejos de implementación

Habilite STARTTLS (seguridad de la capa de transporte de inicio), SPF (marco de políticas del remitente) y DKIM (correo identificado por claves de dominio) en toda la infraestructura de correo electrónico de su WWS. La CISA recomienda que también habilite la autenticación de mensajes basada en dominios, informes y conformidad (DMARC) y lo configure en “rechazar”.

Recursos

Directiva Operacional Vinculante (BOD) 18-01 de la CISA del DHS: Consulte este recurso para obtener más información sobre cómo configurar varios controles de seguridad de correo electrónico. *https://www.cisa.gov/binding-operational-directive-18-01*

Estándar 800-177 (revisión 1) del NIST, Correo electrónico confiable: Consulte las secciones 2.3.1, 5.2.4, 5.2.5 y 7.3.1 para obtener más información sobre el protocolo simple de transferencia de correo (SMTP) (sección "Simple Mail Transfer Protocol (SMTP)"). *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf*

Estándar 800-53 (revisión 5) del NIST, Controles de seguridad y privacidad para sistemas de información y organizaciones: Consulte el control SI-8 (página 348) y SC-18 (página 311) para obtener más información sobre la protección contra correo basura (sección "Spam Protegerion") y la gestión de macros, denominadas como "Mobile Code" (código móvil). *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*