Control de Acceso 2024-09-10 #1

Emsa S.A. - Av. Uruguay 370 - Posadas

Escenario

En la empresa de energía EMSA SA recientemente, se ha realizado un ingreso desde la empresa a una cuenta bancaria desconocida. El gerente de la sucursal afectada dice que no cometieron ningún error. Afortunadamente, pudieron detener el pago. El directorio le ha pedido que investigue lo sucedido para evitar futuros incidentes.

Para ello, se hará un poco de investigación sobre el incidente para comprender mejor lo sucedido.

\* Se revisará el registro de accesos del incidente.

\* Se tomarán notas que puedan ayudar a identificar a un posible actor de la amenaza.

\* Se detectará los problemas con los controles de acceso que fueron aprovechados por el usuario.

\* Por último, se recomendarán mitigaciones que puedan mejorar los controles de acceso de la empresa y reducir la probabilidad de que este incidente vuelva a producirse.

Revisar el registro de incidentes (Event Log)

Los registros de eventos contienen información relacionada con el funcionamiento y el uso de un sistema. Pueden utilizarse para identificar actividades sospechosas, detectar vulnerabilidades y rastrear usuarios.

Se guardó el registro del evento sospechoso en la hoja de cálculo. Se revisó cuidadosamente el registro de eventos de este incidente para comenzar su investigación:

El Evento tuvo lugar el 10/09/2024 a las 8:29:57 AM

El usuario es Contador. La dirección IP de la computadora utilizada para iniciar sesión es 152.207.255.255

Identificar los problemas de control de acceso que provocaron el Incidente

En esta empresa trabajan diferentes empleados. Actualmente, todos ellos gestionan los recursos de la empresa mediante una unidad de disco compartido en la nube.

Se comparó la información encontrada en la pestaña directorio de empleados con la información de la pestaña registro de eventos:

Roberto Daniel Gimenez. era un contador contratado con acceso de administrador

Su contrato finalizó en 2023, pero su cuenta accedió a los sistemas de nómina en 2024

Recomendar mitigaciones que puedan evitar una futura violación

Se ha finalizado la investigación del pago extraño y se ha descubierto fallos en la forma en que la empresa gestiona su Información:

Las cuentas de usuario deberían caducar a los 30 días

Los contratistas deberían tener un acceso limitado a los recursos de la empresa

Se debería habilitar la autenticación de múltiples factores (MFA)

Access Control Worksheet

|  | Nota(s) | Problema(s) | Recomendacion(es) |
| --- | --- | --- | --- |
| Autorización/ Autenticación | ¿Cuándo ocurrió?  El evento tuvo lugar el 10/09/2024  ¿Quién causó este incidente?  El usuario es Contador  ¿Qué dispositivo se utilizó?  La dirección IP de la computadora usada para acceder es 152.207.255.255 | ¿Qué nivel de acceso tenía el usuario?  Roberto Daniel Giménez es un Admin    ¿Su cuenta debería estar activa?  Su contrato terminó en 2023 pero su cuenta accedió a los sistemas de pago en 2024 | ¿Qué controles técnicos, operativos o de gestión podrían ayudar?  Las cuentas de usuario deberían expirar después de 30 días sin uso  Los contratados deberian tener accesos limitados a los recursos de negocios  Activar MFA (Autenticación de Múltiples Factores) |