Desafío técnicas de redacción concisas

José Miguel Rivera

Uso indebido de credenciales en Empresa TechSecure

Se ha realizado una denuncia por mal uso de credenciales en la sección de ventas, siendo revisado por el equipo de seguridad informática y confirmada la actividad inusual del usuario, poniendo en riesgo información de tipo confidencial que puede afectar la relación de cliente con la empresa y más aún puede comprometer la reputación de la misma, comprometiendo la evaluación y evolución favorable de la empresa en estos últimos años.

Esta filtración de información se realizó mediante un intento de phishing, realizado por el atacante por una falla en el sistema de correo electrónico de la empresa, logrando enviar un correo que convenció al usuario de descargar y ejecutar un archivo adjunto, el cual sirvió para obtener los datos de usuario y dirección IP que permitió concretar el robo de información.

Esta acción es un golpe duro para la empresa, la cual deja en evidencia un problema en la autenticación de los usuarios y no se logró detectar a tiempo los intentos que se estaban realizando para acceder a la red. La información filtrada ha provocado molestias en los clientes afectados y pueden desencadenar en la pérdida de negocios concretos y un daño en la imagen corporativa de esta, la confianza de los clientes se verá afectada al saber de los problemas informáticos que están sucediendo en TechSecure.

Las causas investigadas apuntan a la poca preparación del equipo de seguridad informática, la falta de aplicación de firewalls en el servidor de correos, además de falta de capacitación a los usuarios en la utilización y revisión de sus correos electrónicos.

Se sugiere revisar las mejoras propuestas en los sistemas informáticos en un corto plazo a fin de recuperar la confianza de los clientes y evitar otras posibles fugas de información en el equipo de trabajo. Se sugiere además revisar la tabla de permisos para los usuarios y posibles vacíos en la segmentación de la red para evitar comunicaciones que no correspondan.

TechSecure deberá enviar un comunicado a las empresas afectadas solicitando las disculpas pertinentes y manteniendo las excelentes relaciones que hasta la fecha han sido un pilar fundamental en el avance de los negocios establecidos.

Causa del incidente	Descripción	Consecuencias
Falta de autenticación	No se realizaron comprobaciones de los usuarios que sufrieron robo de credenciales	Se produjeron accesos no autorizados por parte de usuarios a datos e información clasificada
Exfiltración de datos	Se realizó un ataque hacia una dirección IP definida	Se determinó que este ataque produjo lentitud y falla en el acceso a sistemas
Phishing	Robo de información mediante un keylogger enviado por correo electrónico.	Robo de credenciales y direcciones IP con las cuales se accedió a información clasificada y privada.

El informe ha evidenciado que existe una falta de control y gestión en los accesos a sistemas, además que el personal debe ser capacitado e informado de buenas prácticas y políticas correspondientes en la empresa.

Se deben aplicar mecanismos mas fuertes y reforzar el uso de contraseñas seguras, mejorar el monitoreo de procesos y continuamente realizar chequeos. Estas acciones deberían reducir riesgos y evitar incidentes que afecten la información y activos de la empresa.