
DATA
BREACH
"A CYBERATTACK HAPPENS
EVERY 39 SECONDS"

QUE ES DATA BREACH?

UN DATA BREACH (O BRECHA DE DATOS) ES UN INCIDENTE DE SEGURIDAD EN EL QUE PERSONAS NO AUTORIZADAS ACCEDEN, ROBAN O EXPONEN INFORMACIÓN CONFIDENCIAL O PROTEGIDA. ESTOS DATOS SUELEN INCLUIR NOMBRES, CONTRASEÑAS, NÚMEROS DE TARJETAS DE CRÉDITO O REGISTROS MÉDICOS.

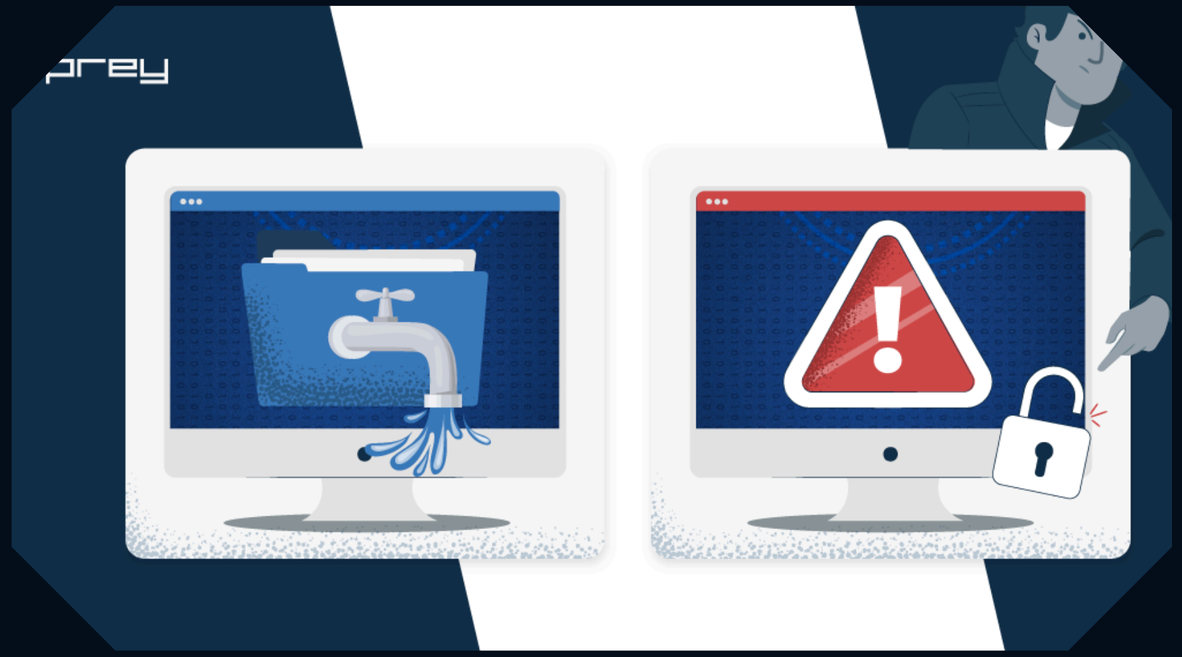
COMO OCURRE?

ATAQUES EXTERNOS: PIRATAS INFORMÁTICOS QUE USAN PHISHING (ENGAÑOS POR CORREO), MALWARE O EXPLOTAN FALLOS EN SISTEMAS DESACTUALIZADOS.

ERRORES HUMANOS: EMPLEADOS QUE ENVÍAN ARCHIVOS AL DESTINATARIO EQUIVOCADO O CONFIGURAN MAL UN SERVIDOR EN LA NUBE.

MALA CONFIGURACIÓN EN LA NUBE: OCURRE CUANDO UNA EMPRESA GUARDA INFORMACIÓN EN SERVIDORES DE INTERNET (COMO AMAZON S3 O GOOGLE CLOUD) PERO OLVIDA PONERLES UNA CONTRASEÑA O RESTRINGIR EL ACCESO

DATA BREACH Y DATA LEACK



DATA BREACH: OCURRE CUANDO UN ACTOR EXTERNO (O ALGUIEN CON MALAS INTENCIONES) LOGRA SALTARSE LAS BARRERAS DE SEGURIDAD PARA ENTRAR EN UN SISTEMA Y COPIAR INFORMACIÓN

DATA LEACK: OCURRE CUANDO LA INFORMACIÓN SE VUELVE ACCESIBLE PARA CUALQUIER PERSONA EN INTERNET SIN QUE NADIE TENGA QUE REALIZAR UN HACKEO. LOS DATOS SIMPLEMENTE "SE ESCAPAN" POR UNA GRIETA EN LA CONFIGURACIÓN.

FORMAS DE EVITARLO

SMART STEPS TO PREVENT ATTACKS

AUTENTICACIÓN MULTIFACTOR (MFA): ES LA BARRERA MÁS EFECTIVA. INCLUSO SI UN ATACANTE ROBA TU CONTRASEÑA, NO PODRÁ ACCEDER SIN EL SEGUNDO MÉTODO DE VERIFICACIÓN (COMO UN CÓDIGO EN TU CELULAR O UN ESCANEO BIOMÉTRICO).

GESTIÓN DE CONTRASEÑAS: USA CONTRASEÑAS LARGAS, COMPLEJAS Y ÚNICAS PARA CADA SERVICIO. UN GESTOR DE CONTRASEÑAS ES LA MEJOR HERRAMIENTA PARA MANEJAR ESTAS CLAVES DE FORMA SEGURA.

ACTUALIZACIONES INMEDIATAS: MANTÉN EL SISTEMA OPERATIVO Y TODAS LAS APLICACIONES AL DÍA. LAS ACTUALIZACIONES SUELEN INCLUIR "PARCHES" QUE CIERRAN AGUJEROS DE SEGURIDAD QUE LOS HACKERS YA CONOCEN Y EXPLOTAN.

CIFRADO DE DATOS: ASEGÚRATE DE QUE LA INFORMACIÓN SENSIBLE ESTÉ CIFRADA TANTO CUANDO SE ENVÍA COMO CUANDO ESTÁ ALMACENADA. ESTO GARANTIZA QUE, SI ALGUIEN LOGRA ROBAR LOS ARCHIVOS, NO PUEDA LEER SU CONTENIDO SIN LA CLAVE.

CASO DE ESTUDIO

CHANGE HEALTHCARE

EN FEBRERO DE 2024, EL GRUPO DE RANSOMWARE ALPHV/BLACKCAT LOGRÓ ENTRAR EN LOS SISTEMAS DE CHANGE HEALTHCARE, UNA EMPRESA QUE PROCESA PAGOS Y RECETAS MÉDICAS PARA MILES DE HOSPITALES Y FARMACIAS EN EE. UU

LOS ATACANTES ENTRARON USANDO UNA CUENTA DE ACCESO REMOTO QUE NO TENÍA ACTIVADA LA AUTENTICACIÓN MULTIFACTOR (MFA). ES DECIR, SOLO NECESITARON UNA CONTRASEÑA ROBADA PARA ACCEDER A LA RED DE UNA EMPRESA GIGANTE.

GRACIAS