Ciberseguridad en la nube: Defensa contra el Ransomware

Germán Ruiz

AWS | Partner Solutions Architect

Nuestra misión:

Ayudarlo a configurar la capacidad de ponerse en marcha después de un evento operativo o de seguridad.

Qué es Ransomware

¿Qué es Ransomware?

Obtención de acceso privilegiado y no autorizado a sistemas y datos cifrando esos datos para bloquear el acceso de usuarios legítimos y exigir el pago de un rescate.

Las organizaciones corren el riesgo de perder permanentemente sus datos, incluso si se paga el rescate

El Ransomware también puede filtrar los datos de la víctima como una oportunidad de rescate secundaria.

¿Por qué el Ransomware es efectivo?

- Muchas organizaciones no parchan o tardan demasiado en parchar sus sistemas
- Muchas organizaciones luchan con la administración de acceso privilegiado, lo que resulta en credenciales demasiado permisivas, credenciales heredadas y credenciales comprometidas.
- Muchas organizaciones tienen un modelo de confianza abierta, que permite que el malware se propague
- La concientización sobre seguridad entre los empleados es baja
- Algunas organizaciones no realizan copias de seguridad de los datos o no prueban sus procesos de copia de seguridad y restauración.
- El Ransomware y los servicios de eventos se han mercantilizado
- Confiar en procesos manuales que consumen mucho tiempo
- Se están empleando múltiples vectores de eventos.

Proteger y recuperar los datos de los clientes

Comprender la resiliencia en la nube

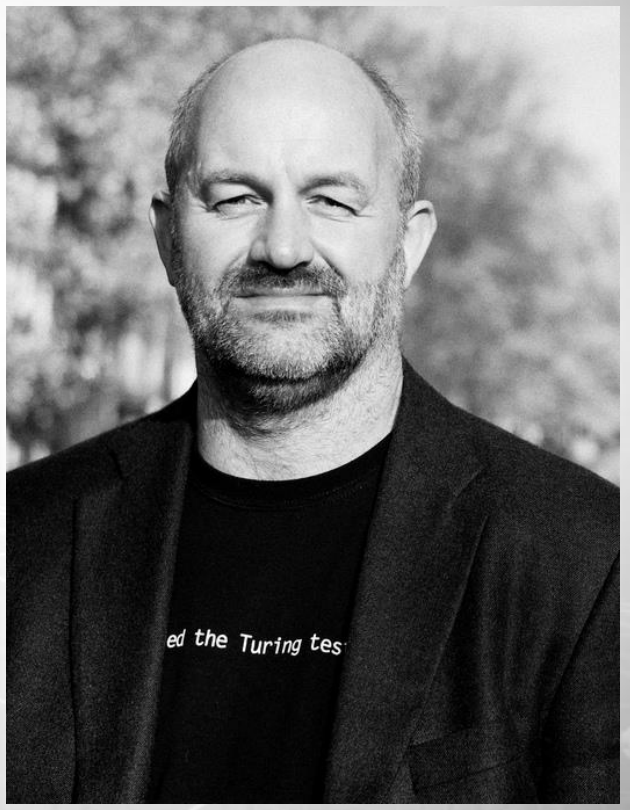
La resiliencia es una medida de cómo una infraestructura, carga de trabajo o plataforma puede protegerse contra la interrupción causada por eventos y condiciones adversas.

La resiliencia se mide en una escala. No se mide como una característica binaria (en otras palabras, resistente vs. no resistente).

Baila como si nadie te estuviera viendo…

Cifra como si todo el mundo lo hiciera…

– Werner Vogels, CTO, Amazon



Proteger y recuperar los datos de los clientes

Identificar

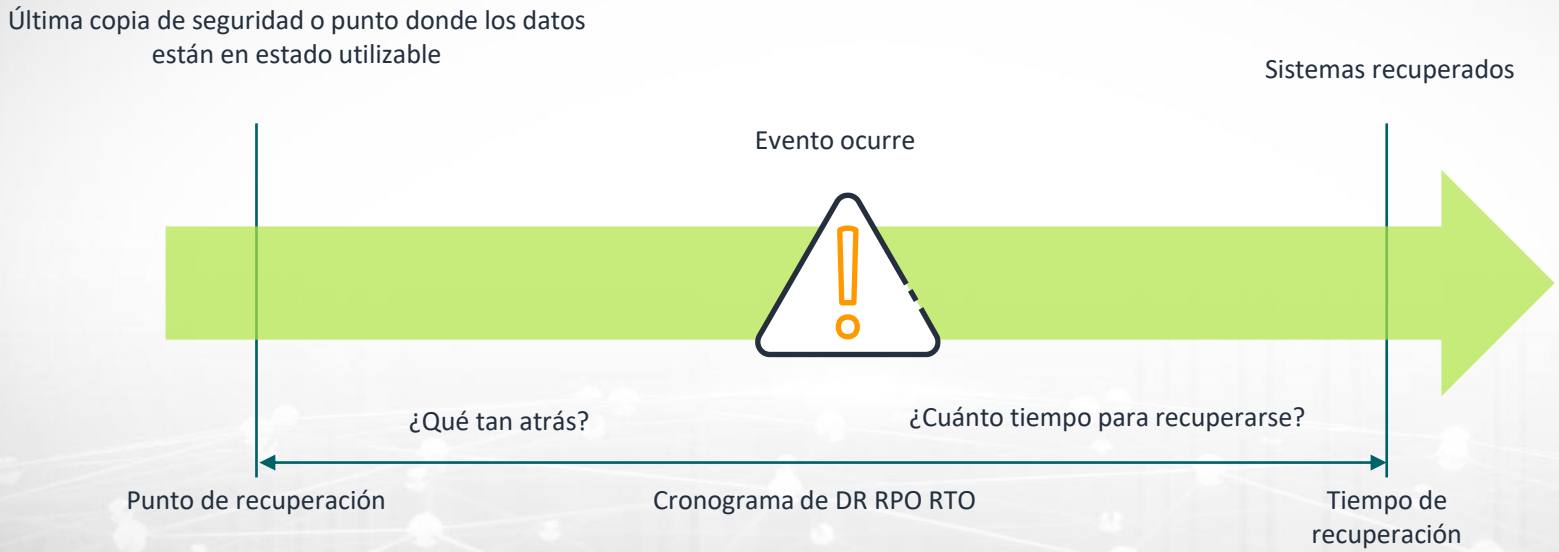
¿Qué cargas de trabajo son críticas para la recuperación?

Recuperar

Configure su capacidad de recuperación

Grupos de protección

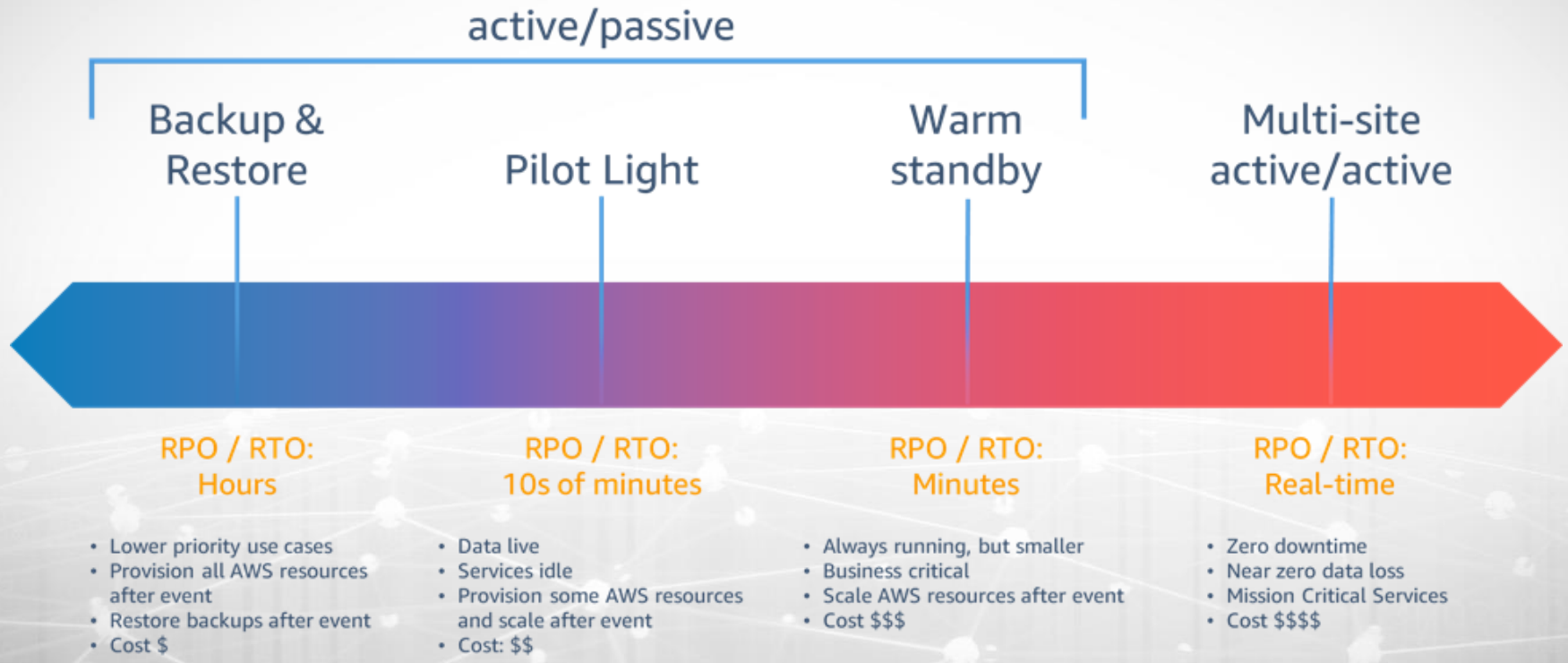
- Equilibre el tiempo de inactividad, la pérdida de datos y el presupuesto para cada aplicación



- Objetivo de punto de recuperación (RPO): cantidad de pérdida de datos aceptable
- Objetivo de tiempo de recuperación (RTO): cantidad de tiempo de inactividad de los sistemas definido por el tiempo total hasta que la empresa pueda reanudar las operaciones

Estrategias de recuperación ante desastres

Estrategias de recuperación ante desastres



Una recuperación ante desastres bien hecha

- Aísle completamente las copias de seguridad del entorno de producción. Almacénelas fuera del sitio y ocúltelas tanto como sea posible de un atacante potencial
- La recuperación se realiza a partir de una copia de seguridad estática de un punto en el tiempo conocido.
- La copia necesita estar aislada
- Muy costoso de hacer en las instalaciones; DRaas más rentable

Una recuperación ante desastres bien hecha

- **Operaciones robustas**
  Logre una confiabilidad y disponibilidad constantes basadas en objetivos de recuperación de primer nivel

- **Eficiencia operativa**
  Obtenga ahorros sustanciales de costos al reducir la necesidad de licencias e infraestructura duplicada

- **Tranquilidad en la continuidad de la empresa**
  Minimice el tiempo de inactividad y la pérdida de datos mediante la realización de pruebas de recuperación ante desastres no disruptivas y fáciles de iniciar.

AWS Elastic Disaster Recovery Service (DRS)

Flexible

Replicar desde cualquier fuente

Admite una amplia gama de sistemas operativos, aplicaciones y bases de datos

Elimine los recursos inactivos del sitio de recuperación y pague solo por lo que necesita

Seguro

Replicación continua robusta y sin interrupciones

RPO: Segundos
RTO: Minutos

Recuperarse de ransomware, corrupciones y errores humanos

Automatizado

Conjunto mínimo de habilidades requeridas para operar

Ejercicios sencillos y sin interrupciones

Proceso unificado para probar, recuperar y conmutar por recuperación

Estrategia de protección - Implementar en días

Gracias!!

Germán Ruiz

AWS | Partner Solutions Architect