AR Consulting

MA ESTRATEGIAS
Asesoría en Estrategias y Riesgos Legales

Lecciones que debemos aprender del incidente en CLARO

CENTROAMÉRICA

Miguel Argüello Oviedo
Derecho e Inversión

AJÁ... ¿QUÉ ES LO QUE ESTÁ PASANDO?

- Claro es una empresa de telecomunicaciones que está en varios países de América Latina.
- El día 25 de enero 2023, tuvo un incidente en sus sistemas de servicio para Centroamérica.
- El 25 de enero, solo hubo un comunicado al respecto.
- El día 02 de febrero 2023, emiten un comunicado vía facebook para explicar la situación

Claro

Estimado cliente

Le informamos que, presentamos algunos inconvenientes en nuestros canales de atención por lo que podrán estar percibiendo lentitud.

Ponemos a disposición nuestra línea de atención vía WhatsApp al: 7002-7002.

Estamos trabajando para resolver esta situación lo más pronto posible y continuar brindándoles el mejor servicio.

Atentamente, Claro Costa Rica

25 de enero de 2024

02 de febrero 2024

Claro

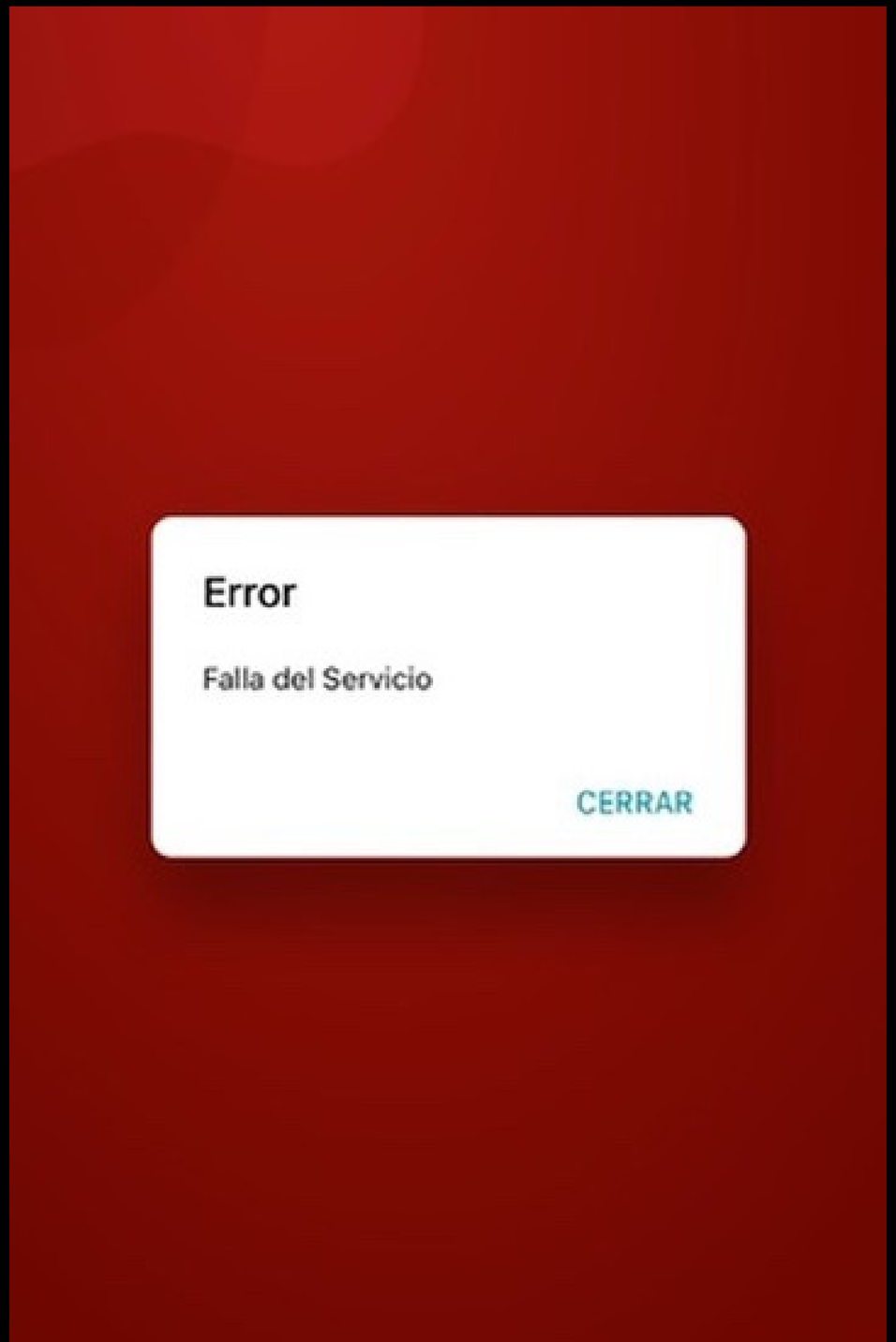
Estimado cliente:

El día 25 de enero de 2024, identificamos la existencia de una actividad anómala en algunos de nuestros sistemas, por lo que tomamos medidas inmediatas para investigar. Determinamos que se trataba de un incidente de ransomware en algunos equipos, por lo que como parte de nuestros protocolos, dichos equipos fueron aislados y decidimos apagar otros sistemas como medida precautoria.

Hemos logrado dar continuidad a nuestra operación utilizando mecanismos alternos y estamos en proceso de restauración de los equipos afectados para regresarlos a su operación normal. Esperamos que todos nuestros sistemas estén operando de forma regular en el corto plazo.

Agradecemos la comprensión y confianza de nuestros clientes

03 DE FEBRERO 2024 DESDE MI LÍNEA CLARO



QUÉ + ANALIZAMOS DE LO POCO QUE SE CONOCE?

- Las únicas 2 comunicaciones ***no hay detalles sobre el origen*** del incidente de *ransomware*.
- ***No sabemos*** cómo el malware ingresó al sistema es crucial para implementar medidas preventivas y evitar futuros ataques similares.
- ***No se menciona*** si han informado a las autoridades pertinentes, clientes o partes interesadas sobre el incidente.
- Solo ***dos comunicados*** emitieron en un lapso de 7 días.
- Desconocemos la evaluación del ***alcance*** que tiene el incidente.
- ¿Cuáles han sido los ***controles de seguridad*** aplicados?
- No se especifica si los ***datos personales están seguros*** y no fueron alcanzados.

QUÉ + ANALIZAMOS DE LO POCO QUE SE CONOCE?

- No se menciona ni se conoce información acerca de la restauración de equipos afectados. Falta de información sobre el daño ocasionado.
- No se especifica si había o no un backup actualizado. Mucho menos si se realizaron pruebas regulares de restauración.
- No establecen criterios investigativos que puedan determinar origen, nivel de afectación, situación de los activos informaticos afectados y no afectados.
- Consideramos que es muy posible que los datos personales hayan sido vulnerados al ver que no es posible el acceso a la app de Claro

Aprendamos que gestionar la seguridad de la información es un tema serio e importante para cualquier empresa

DATOS INTERESANTES

- El costo de las brechas de seguridad en Latinoamérica pasó de 2.69 millones dólares en el 2022 a 3.69 millones de dólares (IBM report)
- Las 10 principales industrias afectadas por brechas de seguridad son:
  - Salud
  - Financiero
  - Farmaceuticas
  - Energia
  - Industrial
  - Tecnología
  - Servicios profesionales
  - Transporte
  - Comunicación
  - Consumo

DATOS INTERESANTES

- El Panorama de Amenazas 2023 de Kaspersky revela un aumento del 50% en los ataques de troyanos bancarios en la región
- Empresas como Kaspersky registraron 286 millones bloqueos de intentos de *phishing* en 12 meses a agosto 2023. Representa un aumento del 617% en comparación con 2022 y un promedio de 544 ataques por minuto.
- Guatemala, Costa Rica, Panamá y El Salvador los países con más brechas de seguridad en los últimos años
- Algunos de los grupos de ransomware que más han atacado a la region LATAM son: Conti, Hive, LockBit o Vice Society

¿QUÉ PUDO PASAR?

FORMAS DE INFECTARSE

Descargas Automáticas
(Drive-By Downloads)

Páginas web infectadas

A través de spam
malicioso

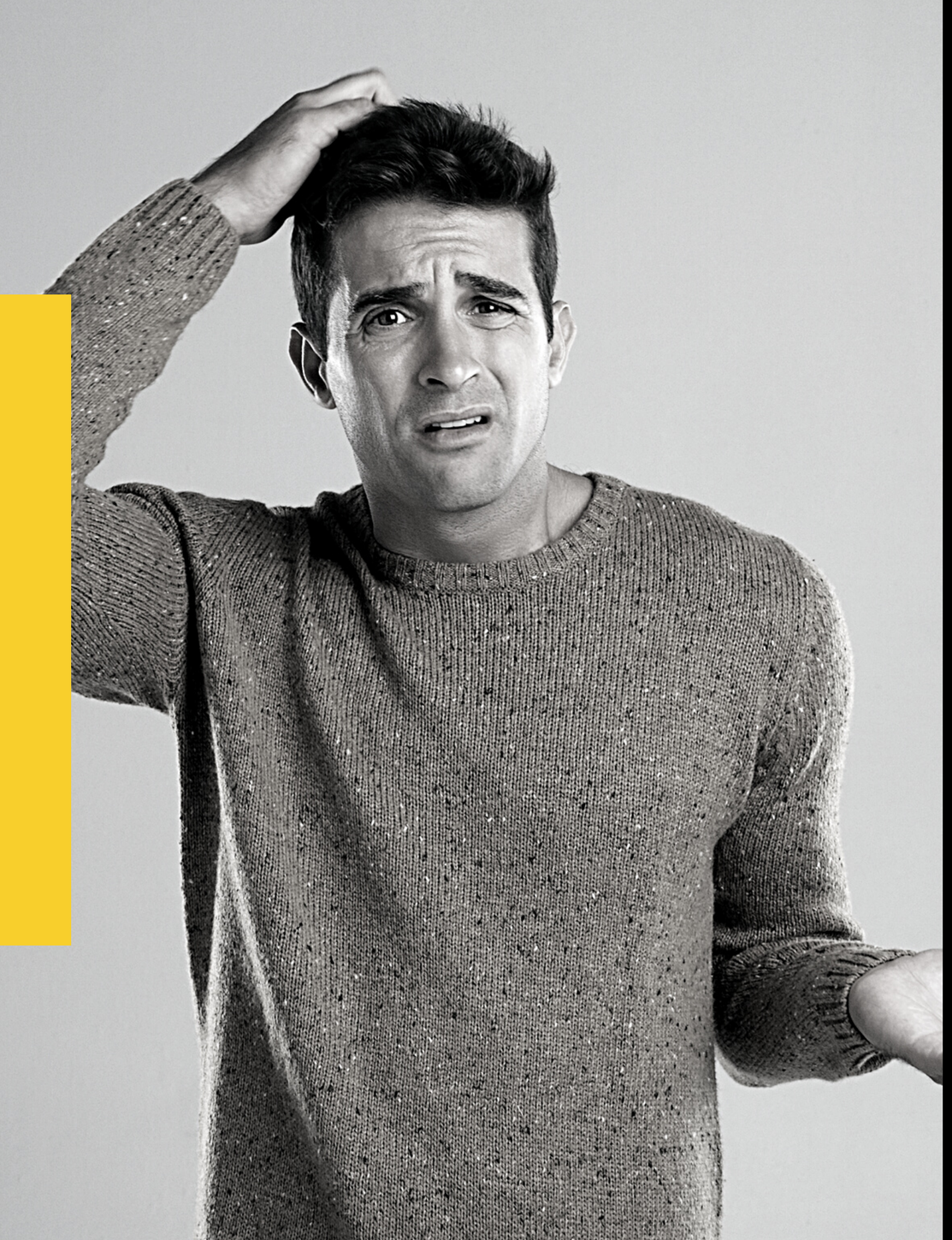
Explotación del protocolo
de escritorio remoto (RDP)

Explotación de
vulnerabilidades de
software

¿QUÉ LECCIONES HAY?

GESTIÓN DE LOS RIESGOS

- Todas las empresas están expuestas a ser atacadas. Ninguna es la excepción.
- La comunicación es esencial, importante y necesaria en momentos de enfrentar una brecha de seguridad. La empresa Claro no ha tenido la mejor comunicación e información.
- Tener un plan de Ciberseguridad es vital. Sin embargo, la manera de gestionar la continuidad del negocio es clave.
- Los datos son “oro”... la protección de los datos personales debe ser una prioridad en las empresas
- La buena reputación en el mundo que vivimos también depende de la buena gestión de riesgos digitales y tecnológicos.



PREGUNTAS QUE NOS HACEMOS

- ¿Qué sucedió realmente? La información no se muestra de la manera correcta. No hubo gestión y comunicación correcta a nuestro criterio.
- ¿Qué investigaciones post brecha se están llevando a cabo?
- ¿Cuáles son los sistemas que fueron realmente afectados? Esto es una evaluación de alcance.
- ¿Hubo o no vulnerabilidad a los ficheros de datos personales en los sitemas de Claro? ¿Están comprometidos los datos de los usuarios?
- ¿Qué tan efectiva ha sido la restauración de los equipos y sistemas?
- ¿Cuánto ha sido el costo para la empresa?

¿NECESITAS ASESORÍA ESPECIALIZADA?

AR CONSULTING

Te ayudamos a que conozcas tus riesgos estratégicos, digitales y legales

Te proporcionamos una asesoría regulatoria completa. Conocer la regulación es importante.

Guiamos a tu empresa por el proceso de implementar un Sistema de Gestión de la Seguridad de la Información

Colaboramos en la creación de políticas de seguridad de la información y continuidad del negocio

COMUNÍCATE CON NOSOTROS

MÁS INFORMACIÓN

ALCANCE CONSULTORIA

Regional

E-MAIL

consultoria@arguelloromero.com

WEBSITE

https://www.derechoeinversion.com/ar-consulting

LINKEDIN

/arguello-romero-consulting/