Su empresa es el blanco de un

ataque ransomware

¿Qué hace?

Sarah es la Gerente de TI de Buy More, un minorista líder en Oriente Medio y África.
El día antes del Black Friday, Sarah comienza a recibir llamadas preocupantes de sus colegas.

El equipo de atención al cliente llama para decir que los productos están desapareciendo de los carritos de compras en línea de los clientes.

Los gerentes de las tiendas informan que los clientes en las tiendas tienen problemas para usar sus tarjetas de crédito.

Sarah informa del problema al CTO de la empresa. **¿Qué debe hacer el CTO?**

A Continuar tratando de resolver el problema

B Escalar el problema al CEO

El CTO escala la situación al CEO, quien pide que lo mantengan al tanto, pero ahora a solo 13 horas del Black Friday la situación va de mal en peor.

A medida que Buy More se convierte en un tema de moda en Twitter, los líderes de la compañía se dan cuenta de que han sido golpeados por un ataque de ransomware.

En tan solo 30 minutos el número de sucursales afectadas pasa de 12 a 25. Cada hora que pasa sin ventas es dinero perdido.

Mientras que el CEO pide los informes sobre las pérdidas financieras, el equipo recibe una nota de ransomware de un hacker conocido.

El área legal de la compañía aconseja no ponerse en contacto con el hacker, pero el equipo está preocupado por una mayor pérdida financiera.

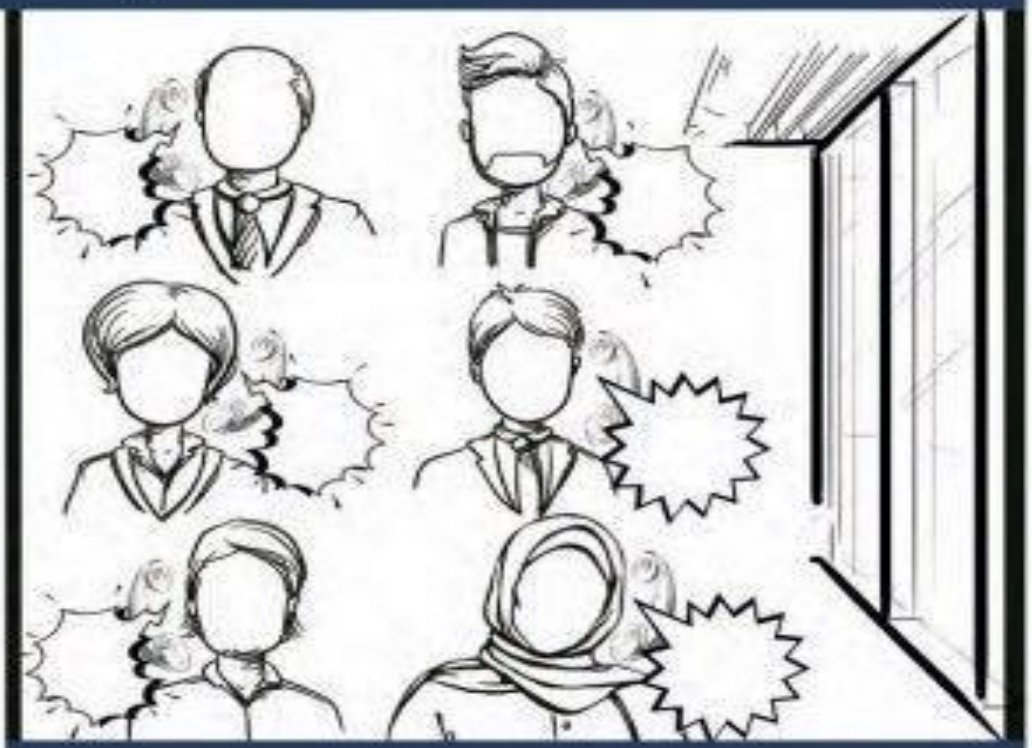
¿Qué deben hacer?

A Contactar al hacker usando el enlace

B Ignorar el mensaje e intentar mitigar el ataque

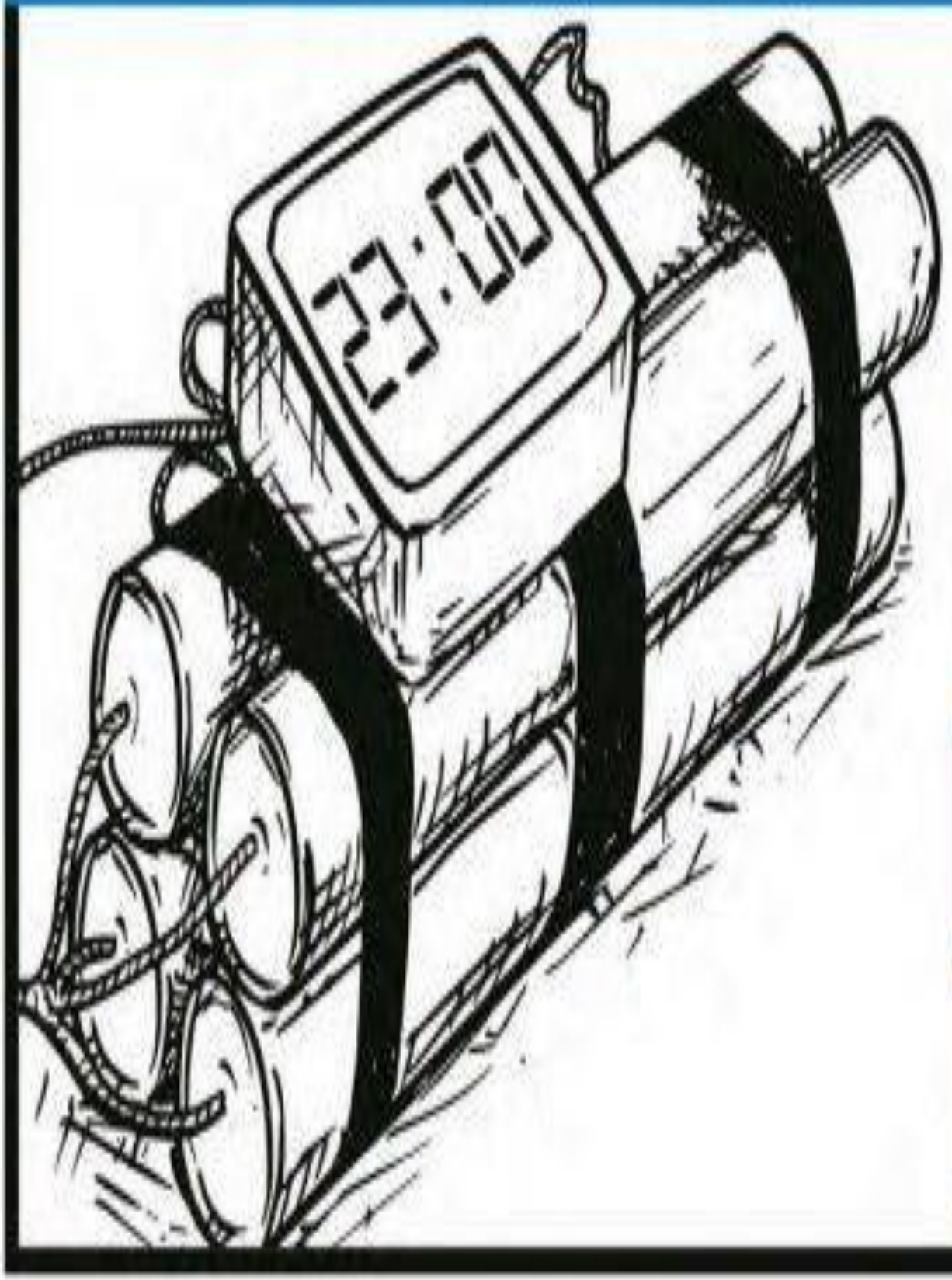
Al ingresar al enlace, el equipo se encuentra con una voz robótica distorsionada que les informa que el hacker tiene todos los datos de sus clientes: nombres, direcciones e identificación y números de tarjetas de crédito.

A menos que Buy More pague 10 millones de dólares en bitcoin, el hacker amenaza con el caos en el Black Friday.



Con el sitio web ahora completamente sin funcionar, los periodistas piden algún comunicado de la empresa. Ahora la reputación de la empresa está en juego.

Una hora antes del Black Friday, el director financiero sugiere pagar el rescate para asegurar las ventas del Black Friday y compensar el daño.



Las pérdidas financieras podrían ser devastadoras si no se paga el rescate. Pero no hay garantía de que el hacker devuelva los datos robados si se paga el rescate.

¿Qué debe hacer el CEO?

A Pagar el rescate

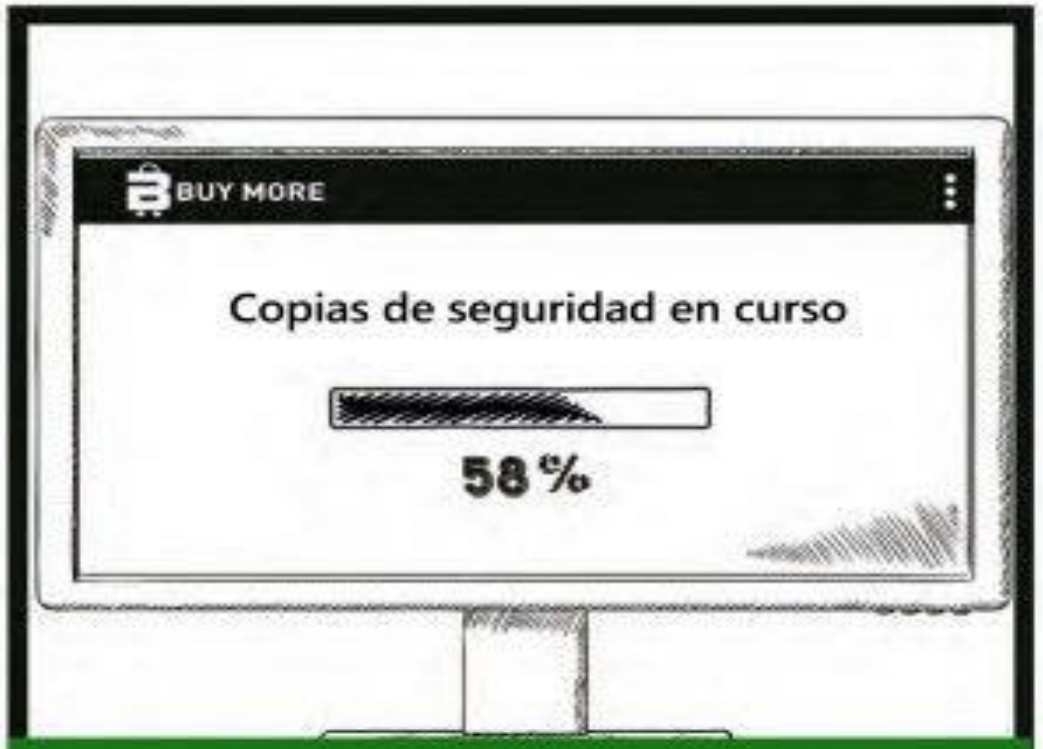
B No pagar el rescate

Cómo la historia debería haber comenzado...

Faltan seis meses para el Black Friday. Después de observar el creciente número de ataques de ransomware en las empresas de la región, el gerente de TI de Buy More, Sarah, reúne a los equipos de TI, seguridad y negocios de la compañía...

Discuten qué sistemas críticos para el negocio son los más importantes e inmediatamente comienzan las copias de seguridad periódicas de esos sistemas.

Al comprender que los atacantes se dirigirán deliberadamente a las copias de seguridad, Sarah sugiere que trasladen sus datos a la nube para beneficiarse de las copias de seguridad automáticas.



Ella sabe que los proveedores de la nube como Microsoft Azure tienen herramientas para ayudar a las empresas a restaurar las copias de seguridad más rápido y pueden proteger los sistemas necesarios para la recuperación.

Como precaución adicional, el equipo de seguridad garantiza que las copias de seguridad en línea solo se puedan modificar o borrar mediante autenticación de múltiples factores.

En los meses siguientes, el equipo simula cómo responderían en el caso de un ataque, asegurando que puedan llevar rápidamente las operaciones comerciales críticas en línea desde la funcionalidad cero.

Finalmente, es una vez más la mañana antes del Black Friday y Sarah está disfrutando tranquilamente de su taza de café por la mañana.

El equipo de atención al cliente llama para decir que los productos están desapareciendo de los carritos de compras en línea de los clientes.

Luego vienen los gerentes de la tienda con informes de que los clientes en la tienda están teniendo problemas para usar sus tarjetas de crédito.

Pero Sarah ejecuta con calma un análisis antivirus completo en todos los equipos y dispositivos que ahora sospecha que han sido afectados por ransomware. Ella sugiere que los gerentes ofrezcan a los clientes algunos cupones de descuento mientras esperan...

Una vez que ha detectada y eliminada la carga útil asociada, comienza a restaurar todos los sistemas críticos para el negocio.

Afortunadamente, ahora la única persona que tiene una Black Friday triste es el hacker.

Microsoft Security