14 DE MAYO DE 2024

NOTIFICACIÓN A AUTORIDADES COMPETENTES

INCIDENTES DE CIBERSEGURIDAD

ERIC SERRANO MARIN
I.E.S MARTINEZ MONTAÑES
CETI

Contenido

1. Infección por ransomware:..... 2
2. Phishing en página web:..... 2
3. Ataque de denegación de servicios: 3
4. Brecha de datos personales: 3
5. Ataque de ingeniería social:..... 3

De los tipos de incidentes que has incluido en la tabla de la actividad anterior, indica por cada uno de ellos a cuáles de los siguientes actores de tu negocio (elige el tipo de empresa que quieras) crees que es necesario comunicarlo y por qué o por qué no:

- **Empleados**
- **Clientes**
- **Proveedores**

He decidido que la empresa va a ser una compañía de servicios financieros.

1. **Infección por ransomware:**
   - **Empleados:** Sí, es importante informar a los empleados sobre la infección por ransomware para que estén alerta y tomen medidas preventivas. Como por ejemplo no abrir correos electrónicos sospechosos o no hacer clic en enlaces desconocidos.
   - **Clientes:** No es del todo necesario, a menos que la infección afecta directamente a los servicios ofrecidos a los clientes. Sin embargo, si creemos que la seguridad de los datos de los clientes podría haber sido comprometida, podría ser una buena práctica informarles.
   - **Proveedores:** Sí, sobre todo si la infección puede afectar a las operaciones comerciales con los proveedores, ya que podría afectar a la red de proveedores.
2. **Phishing en página web:**
   - **Empleados:** Sí, los empleados deben estar informados sobre el phishing en la página web, para que así puedan identificar posibles intentos de fraude.
   - **Clientes:** Obviamente sí, ya que los clientes usando nuestra página web, y tienen que saberlo, para que no caigan en posibles estafas.
   - **Proveedores:** Sí, ya que el phishing en la página web podría afectar a la comunicación con los proveedores, aparte es importante informarles para prevenir posibles impactos en transacciones comerciales.

3. **Ataque de denegación de servicios:**
    - **Empleados:** Sí, ya que les afecta directamente, deben saber que puede haber interrupciones en los sistemas y servicios de la empresa.
    - **Clientes:** También es fundamental informar, ya que tienen que saber que puede verse comprometida la disponibilidad de los servicios, y también por transparencia.
    - **Proveedores:** Sí, ya que un ataque de denegación de servicio puede afectar a la comunicación, así que es necesario informarles para mitigar cualquier impacto en la cadena de suministro.
4. **Brecha de datos personales:**
    - **Empleados:** Sí, ya que los empleados deben estar al tanto de cualquier posible exposición de su información personal y así puedan tomar medidas para proteger su privacidad.
    - **Clientes:** Sí, por el mismo motivo que los empleados, para que estén alerta y puedan tomar medidas para proteger su información y estar alerta ante posibles intentos de fraude o robo de identidad.
    - **Proveedores:** Más de lo mismo, si es necesario, para que estén al tanto de cualquier impacto en la seguridad de sus datos y tomen medidas para proteger su información confidencial.
5. **Ataque de ingeniería social:**
    - **Empleados:** Sí, ya que es importante para que puedan reconocer posibles intentos de manipulación o fraude y proteger la seguridad de la empresa.
    - **Clientes:** Sí, para que puedan estar alerta ante posibles intentos de manipulación o estafas que podrían comprometer su seguridad financiera.
    - **Proveedores:** Sí, porque el ataque de ingeniería social puede afectar a la comunicación y la interacción en línea con los proveedores, por ello es importante informarles para prevenir posibles impactos en transacciones comerciales.