energywise
s.a. de c.v.

Pruebas de Vulnerabilidad y de Penetración

Cuando y como son relevantes

energywise
s.a. de c.v.

¿Qué son las pruebas de vulnerabilidad y penetración?

- Las pruebas de vulnerabilidad examinan las redes, dispositivos y programas de una empresa para detectar los aspectos vulnerables de las redes, dispositivos y programas que puedan dar oportunidad a agentes maliciosos de atacar y penetrar la seguridad de una empresa o institución.

- Las pruebas de penetración buscan explotar vulnerabilidades encontradas para verificar hasta donde puede penetrar un agente malicioso dado el estado de dichas vulnerabilidades.

energywise
s.a. de c.v.

¿Qué diferencia hay entre una prueba de vulnerabilidad y una de penetración?

- Las pruebas de vulnerabilidad se llevan a cabo con programas que intentan identificar si existe una vulnerabilidad en un servicio dado.
  - Esta información se utiliza para ayudar a automatizar el parcheo
  - Esto ayuda a los administradores de sistemas a establecer prioridades de parcheo
  - Esto permite endurecer los servicios y bienes de la organización.
  - Pero, no ayuda a proveer información respecto lo que un agente malicioso pudiera hacer u obtener si explota con éxito una vulnerabilidad

energywise
s.a. de c.v.

¿Qué diferencia hay entre una prueba de vulnerabilidad y una de penetración?

- Las pruebas de penetración se llevan a cabo con programas que intentan identificar explotar las vulnerabilidades en un servicio dado.
  - Esta información se utiliza para ver que nivel de acceso se puede obtener en los sistemas y redes de una organización
  - La prueba de penetración utiliza varias vulnerabilidades para crear un camino de explotación y así llegar a robar información u obtener múltiples niveles de acceso a los bienes físicos e intelectuales de la organización.
  - Estas pruebas dan a la organización una imagen más clara de lo que podría hacer un agente malicioso que atacara a la organización.
  - También mostrará lo expuesto que puede estar la información más importante de la organización si un agente malicioso explota con éxito una vulnerabilidad.

energywise
s.a. de c.v.

Si no tengo un plan de ciberseguridad, ¿qué debe ser mi primer paso?

- Las pruebas de vulnerabilidad se deben de llevar a cabo para determinar el grado de riesgo con que corre la organización.
- Si su organización jamás ha llevado a cabo un diagnóstico del estado de su ciberseguridad, debe hacer lo siguiente:
  - Hacer una prueba o diagnostico de la vulnerabilidades existentes.
  - Permitir al personal de sistemas remediar las vulnerabilidades.
  - Llevar a cabo una prueba de penetración para medir el nivel de acceso que se le permitiría a un agente malicioso dado el estado de las redes y sistemas.
  - Repetir estos tres pasos con cierta regularidad.

energywise
s.a. de c.v.

Mi organización es relativamente pequeña, ¿vale la pena hacer estas pruebas?

- Las pruebas de vulnerabilidad y penetración valen la pena sin importar el tamaño de su organización.
- Nuevas vulnerabilidades y técnicas de penetración aparecen cada día.
- Lo que era cierto ayer, ya no es válido hoy en día.
- Estas pruebas ayudan a asegurar que su organización está consciente de su ciberseguridad y que está al día en las actualizaciones de seguridad.
- Para las organizaciones pequeñas, contratar a terceros para llevar a cabo estas pruebas es benéfico pues normalmente el departamento de sistemas tiene recursos limitados y no puede llevar a cabo estas pruebas con prontitud o detalladamente.

energywise
s.a. de c.v.

¿Qué diferencia hay entre una prueba de vulnerabilidad y una de penetración?

- Las pruebas de vulnerabilidad se llevan a cabo con programas que intentan identificar si existe una vulnerabilidad en un servicio dado.
  - Esta información se utiliza para ayudar a automatizar las actualizaciones.
  - Esto ayuda a los administradores de sistemas a establecer prioridades de actualización.
  - Esto permite endurecer los servicios y bienes de la organización.
  - Pero, no ayuda a proveer información respecto lo que un agente malicioso pudiera hacer u obtener si explota con éxito una vulnerabilidad.

energywise
s.a. de c.v.

¿Qué diferencia hay entre una prueba de vulnerabilidad y una de penetración?

- Las pruebas de penetración se llevan a cabo con programas que intentan atacar un servicio dado.
  - Estas nos permiten evaluar que tan penetrables son las defensas cibernéticas de la organización.
  - Esto ayuda a los administradores de sistemas a buscar elementos para endurecer las defensas.
  - También permite endurecer los servicios y bienes de la organización.
  - Y ayuda a proveer información respecto lo que un agente malicioso pudiera hacer u obtener si explota con éxito una vulnerabilidad.

energywise
s.a. de c.v.

¿Qué verá el personal de sistemas durante una prueba de vulnerabilidades o penetración?

- Las pruebas de vulnerabilidades o penetración se pueden llevar a cabo abiertamente o con sutileza.
  - Dependiendo de los recursos del departamento de sistemas, puede ser que les den seguimiento a las pruebas o quizás ni las detecten.
  - Si se cuenta con las herramientas adecuadas, el personal de sistemas notaría múltiples intentos de entrar en cuenta, salidas no autorizadas de información, correos electrónicos apócrifos dirigidos al personal de la organización (phishing).
  - Intentos de entrar en cuentas apócrifas fuera de horas de oficina.
  - Y otras señales más que indican un ataque o intento de penetración.
  - En el caso de la prueba de vulnerabilidades, esta es muy difícil de detectar, pero no imposible, si se tienen las herramientas adecuadas.

energywise
s.a. de c.v.

¿Qué límites tienen las pruebas?

- Las pruebas de penetración se llevan a cabo con sigilo a menos que la dirección pida que sean abiertas.
- Las pruebas de vulnerabilidades se llevan a cabo abiertamente avisando al personal con tiempo y preferiblemente fuera de horas hábiles.
- Se evita interrumpir el servicio o hacer que se interrumpa el buen funcionamiento de sistemas o dispositivos.
- No se generarán reportes negativos; se generarán reportes de cómo mejorar la ciberseguridad de la organización.
- Se intentarán llevar a cabo las pruebas en un ambiente no crítico para la organización para evitar posibles interrupciones del servicio.

energywise
s.a. de c.v.

¿Qué determina si las pruebas tuvieron éxito?

- ¿Qué significa para la organización tener éxito?
- Las pruebas de vulnerabilidades tendrá éxito si la organización actúa para remediar las vulnerabilidades.
- Las pruebas de penetración tendrán éxito si ayudan a la organización a buscar herramientas que eviten o hagan más difícil el camino de la penetración.
- Para una organización, estas pruebas tendrán éxito si le ayudan a comprender que puede hacer para mejorar su seguridad.
- Si se determina correctamente el estado actual de la seguridad de la organización y los que conducimos las pruebas entregamos recomendaciones útiles basadas en los resultados de las pruebas, entonces estas tuvieron éxito.

energywise
s.a. de c.v.

Gracias por su atención a esta presentación.