Ciberseguridad

Contents

Entrega de proyecto 4 diciembre

Libros

The Tao of network monitoring

Prevenir

Ahora mismo estamos hablando de la calse pasada, de cómo vimos que se podia vulnerar cualquier dispositivo, donde con un panel de control se pueden realizar acciones desde el exterior.

- MDM: Mobile Device Management

Entre las medidas para prevenir los ataques tenemos:
- Hacer uso de antivirus
- Utilizar un MDM para notificación de
- No estar descargando software que no es de fiar
- Dar platicas de conscientización a los que nos rodean
- Monitorear la actividad de los dispositivos para detectar anomalías
- No se puede confiar 100% en las aplicaciones de tiendas oficiales
  - Por esto es necesario checar los permisos que solicitan las aplicaciones
  - En caso de que requiere muchos permisos podemos buscar aplicaciones que usen menos permisos
  - Si somos los desarrolladores debemos verificar que estamos poniendo los permisos esenciales y ya

Fallo de Ciberseguridad

En teconologia existe tanto los fallos de ciberseguridad y la desigualdad digital son varios de los riezgos mas importantes que hay a nivel global, de la mano con el nivel de tecnología de los gobiernos.

Las fallas de seguridad que involucran las computadoras causan inestabilidad económica, perdidas económicas, intestabilidad social.

Los entes reguladores suelen aprender de los ataques, lo que implica que hasta que el daño esta hecho, creando las areas de seguridad después de perder. CISO: Chief Information Security Officer. Director de la ciberseguridad

Existe un gran deficit en las empresas y en los gobiernos en el tema de la ciberseguridad.

Terceros
No basta con contratar a terceros para gestionar servicios, pues la falta de estándares de seguridad y de confianza pueden resultar en que los mismos terceros de forma indirecta o directa posibiliten un flanco para ser vulnerados.

Muchas empresas se suelen inclinar del lado de los servicios de terceros debido al dinero y esfuerzo que requiere el mantener el hardware y software necesario para aumentar la seguridad.

Si se contratan terceros se debe de buscar auditar a los terceros, poniendo clausulas de contrato. El chiste es evitar a toda costa el filtrado de información.

Los fallos de ciberseguridad pueden crear cadenas de sucesos sociales negativos.

CIEM: Concentran todos los eventos. Si hay terceros entonces pueden observar todo lo que sucede.

Tambien existen riezgos a nivel fisico, como cuando respaldas información en discos y por lo tanto el robo de información no se nota.

Nube
Cuando se utilizan servicios en la nuve la responsabilidad sobre la seguridad es compartida.

Que el proveedor de servicios cumpla con sus certificaciones de seguridad no significa que la aplicación sea segura, como desarrolladores podemos vulnerar la serguridad de nuestro servicio como un todo al tener malas practicas a nivel de aplicación.

Seguridad
De *securitas*, que esta en un estado sin preocupaciones.

La seguridad es un proceso continuo, como decia el libro, en lugar de decir ‘estamos seguros’, la respuesta correcta es ‘déjame revisar’.

Ciclo de demming
- Plan
- Do

Seguridad
- Seguridad Informatica: Seguridad integral de los dispositivos
- Seguridad Información: Se encarga del ambiente digital y físico
- Ciberseguridad: Se encarga solo del ambiente digital

En estos puntos se busca:
- Integridad: La información se mantiene en un estado valido, confiable.
- Disponibilidad: Se encuentra disponible cuando se desea utilizar.
- Confidencialidad: Se encuentra solo expuesta a los entes autorizados.

*Se dice **ente** porque pueden ser personas, empresas, etc.*

Una cadena de custodia, al hacer una denuncia de un crimen en la cadena se registran los distintos dispositivos durante el proceso donde el perito extrae los indicios que se pueden convertir en evidencias. En esta custodia.

Seguridad de la Información
Se abarca la tecnologia, las personas y los procesos. Es decir, tanto lo

Ciberseguridad
Esta enfocada en el entorno digital, es el conjunto de herramientas, politicas,guias, análisis y acciones necesarios enfocados en lo digital.

Principios CIA y DAD

La confidencialidad, integridad y disponibilidad. Por sus siglas en ingles *Confidenciality*, *Integrity* y *Availability*.

Lo contrario a la CIA es la DAD, la alteración, destrucción o divulgación.

La ISC2 es un ente de no se que. Menciona que es bueno rotar actividades

Control de seguridad

Entre las distintas medidas que podemos tomar para proteger la información podemos tener politicas de:

- Integridad:
  - Permisos mínimos para los entes
    - Lo que implica controles de acceso.
  - Need to know: Que la persona solo sabe lo que *necesita* saber.
- Disponibilidad:
  - Tolerancia a fallas/redundancia
    - Ej. Dos fuentes de poder.
  - Clusters de alta habilidad (*HA Clusters*)
- Confidencialidad:
  - Segregación de privilegios
  - Rotación de actividades
  - Canales encubiertos
  - Análisis de tráfico
  - Cifrado
  - Controles de accesso

Tendencias de Gartner

Es una consultora que realiza estudios a nivel mundial que se toma como referencia para la seguridad.

- Se puede reducir en un 90% los impactos financieros si se adopta arquitectura segura.
- El 60% de empresas considerará la seguridad de terceros para realizar tratos.
- Preventivo no reactivo. Resiliencia, poder recuperarse de un efecto grave. No es un gasto, es solo medidas preventivas para prevenir más gastos/pérdidas.
- Hay provedoores y fabricantes especificos de seguridad que desarrollan hardware para bases de datos, etc.
- Se prevee que la coberseguridad tome mucha fuerza, se creen comites de seguridad.
- Desde 2020 se habla de la ciber-resilencia.
- Los que vulneran pueden tomar los artefactos vulnerado como arma.

Nota: Un solo provedor trae desventajas como que todos tengan las mismas vulnerabilidades, asi como que si el principal es atacado no tienes a donde moverte.

Certificaciones

Hay distintas certificaciones que van desde seguridad, inteligencia artificil, computo en la nube, seguridad. A nivel de persecpión económica un project manager ya no es tan valioso.

Entre las certificaciones más solicitadas esta:

- CISP: Para cargos altos, es para nivel diseño, es muy completo, incluye de todo. Es como una maestria
  - Necesita 5 años de experiencia
  - Estudios solo cuentan como un año en algunos casos
- CISA: Auditoria de sistemas
- OSCP, OSCE: Ofensivo
- CEH: Certified hacker
- EJPG: Pentester junior

Entidades certificadoras

- ISC2: Muy valorado, hay ahora mismo uno abierto
  - Certificado en Cibserseguridad: Básico, gratis (https://isc2.org/certifications/cc)
- EC-Council
  - Ethical Hacking Essentials
  - Y más (https://www.eccouncil.org/cybersecurity-exchange/cyber-novice/free-cybersecurity-courses-beginners/)
- ISACA
- Offensive Security
- Sans Institute

Los posgrados tienen más peso a largo plazo y en las oportunidades que se pueden tener pues aprendes a nivel profundo sobre los temas que se tratan.

En las certificaciones solo se evalua herramientas y puntos escpecificos, esta bien tenerlas pero mejor primero maestria.

No hay que quedarse en una sola herramienta.

Laboratorio: Hack-mex

Términos

- 0Day: Vulnerabilidad de reciente creación, por lo que no hay un parche

Desventajas de un solo proveedor