**6/10/2024 Historia de la ciberseguridad – modulo2 – Google**

**Términos**

* **Virus informático**: código malicioso escrito para interferir en las operaciones de un ordenador y causar daños en los datos y el software.
* **Programa maligno (Malware):** que es software diseñado para dañar dispositivos o redes.
* **CERTs®:** Acrónimo de Equipo de Respuesta ante emergencias informáticas.
* **La ingeniería social:** es una técnica de manipulación que explota el error humano para obtener información privada, acceso u objetos de valor.
* **El phishing:** es el uso de las comunicaciones digitales para engañar a las personas para que revelen datos sensibles o implementen software malicioso.
* **Firewall:** dispositivo que se usa para monitorear y filtrar el tráfico entrante y saliente de la red de computadoras.

Veamos como se formo la ciberseguridad tal y como la conocemos hoy en día, unos de los primeros ataques de software conocidos son el “*virus brain* “(1986) y el “*gusano Moris* “ (1988). Fueron creados por desarrolladores de malware para llevar a cabo tareas específicas. Sin embargo, los desarrolladores subestimaron el Impacto que tendría su software malicioso y la cantidad de computadoras infectadas que habría.

En 1986, los hermanos Alvi crearon el virus Brain, aunque la intención del virus era rastrear copias ilegales de software médico e impedir las licencias piratas, lo que el virus hizo en realidad fue inesperado. Una vez que una persona utilizaba una copia pirata del software, el virus infectaba esa computadora. A continuación, cualquier disco que se insertara en la computadora también quedaba infectado. A continuación, cualquier disco que se insertara en la computadora también quedaba infectado. El virus se propagaba a una nueva computadora cada vez que alguien utilizaba uno de los discos infectados. Sin ser detectado, el virus se propagó por todo el mundo en un par de meses. Aunque la intención no era destruir datos o hardware, el virus ralentizó la productividad e impactó significativamente en las operaciones empresariales.

El virus del cerebro alteró fundamentalmente la industria informática, enfatizando la necesidad de un plan para mantener la seguridad y la productividad.

En 1988, Robert Morris desarrolló un programa para evaluar el tamaño de Internet. El programa rastreaba la web y se instalaba en otras computadoras para contar el número de computadoras que estaban conectadas a Internet. Suena sencillo, ¿verdad? El programa, sin embargo, no supo llevar la cuenta de las computadoras que ya había comprometido y continuó reinstalándose hasta que las computadoras se quedaron sin memoria y se bloquearon.

Este ataque costó millones de dólares en daños debido a las interrupciones del negocio y a los esfuerzos requeridos para eliminar el gusano. Después del gusano Morris, Los Equipos de Respuesta a Emergencias Informáticas, conocidos como CERTs®, se establecieron para responder a incidentes de seguridad informática.

Para comprender mejor los ataques en la era digital, hablaremos de dos ataques notables que se basaron en Internet: el ataque LoveLetter y la brecha de Equifax.

En el año 2000, Onel De Guzman creó el software malicioso LoveLetter para robar credenciales de inicio de sesión en Internet. Este ataque se propagó rápidamente y se aprovechó de personas que no habían desarrollado una sana desconfianza hacia los correos electrónicos no solicitados. Cada correo electrónico contenía un archivo adjunto con la etiqueta "Love Letter For You." Cuando se abría el archivo adjunto, el software malicioso escaneaba la libreta de direcciones del usuario. A continuación, se enviaba automáticamente a cada persona de la lista e instalaba un programa para recopilar información del usuario y contraseñas.

En 2017, los atacantes se infiltraron con éxito en la agencia de información crediticia, Equifax. Esto dio lugar a una de las mayores filtraciones de datos conocidas de información confidencial. Se robaron más de 143 millones de registros de clientes, y la filtración afectó aproximadamente al 40% de todos los estadounidenses.

Los registros incluían información de identificación personal, como números de la seguridad social, fechas de nacimiento, números de carné de conducir, direcciones particulares y números de tarjetas de crédito. Desde el punto de vista de la seguridad, la filtración se produjo debido a múltiples fallos por parte de Equifax. No fue sólo una vulnerabilidad la que aprovecharon los atacantes, fueron varias.

**Retro alimentación**

En primer lugar, hemos hablado de los virus, incluidos el virus Brain y el gusano Morris, y hemos analizado cómo estas primeras formas de software malicioso dieron forma a la industria de la Seguridad. También hemos hablado de cómo muchos ataques actuales son variantes de estos primeros ejemplos. Comprender los ataques anteriores es fundamental para los profesionales de la seguridad que trabajan para proteger a las organizaciones y a las personas de posibles variantes futuras. También hemos hablado de la ingeniería social y de los motivos de los agentes de amenaza al conocer el ataque LoveLetter y la filtración de datos de Equifax. Estos incidentes mostraron los amplios Impactos y Costos asociados de las violaciones de seguridad más recientes en la era digital. Por último, presentamos los ocho dominios de seguridad de CISSP y cómo pueden utilizarse para categorizar diferentes áreas de enfoque dentro de la profesión de la seguridad. ¡Espero que se sienta seguro de sus conocimientos básicos sobre seguridad! Aprender la historia de la seguridad puede permitirle comprender mejor la industria actual. Los ocho dominios de seguridad del CISSP proporcionan una forma de organizar el trabajo de los profesionales de la seguridad.