INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE COMPUTO

"ACTIVIDAD DE APRENDIZAJE 5: SEGURIDAD Y DELITOS INFORMÁTICOS"

PROFESORA:
Jessie Paulina Guzmán Flores

ALUMNO:
Martínez Coronel Brayan Yosafat

GRUPO:
3CM20

FECHA DE ENTREGA:
1/Abril/2022

ÍNDICE

Contenido

INTRODUCCIÓN

La seguridad de la información es más que protección de datos y su implementación es la necesidad básica de cualquier organización. Uno de los pasos muy importantes hacia la seguridad de la información es hacking ético. Los hackers éticos pueden ayudar a las empresas en la búsqueda de los puntos débiles dentro de la infraestructura de TI, que algún hacker puede explotar y causar una brecha de información.

Es por eso que debes estar informado para tomar decisiones informadas sobre la exposición de la organización a las amenazas, hacer programación segura e implementación de seguridad.

OBJETIVOS

- Investigar sobre troyanos y backdoors
- Realizar una infografía con la información obtenida
- Documentar lo siguiente:
    - ¿Qué es?
    - ¿Cómo afecta?
    - ¿Cómo se previene?
    - ¿Cuál es el manejo y respuesta en caso de contingencia?
    - ¿Qué herramientas/ técnicas/metodologías se utiliza para monitoreo?
    - ¿Qué perfiles se necesitan para atender
    - ¿Qué costo tiene?
    - Dos ejemplos aplicados (Noticias)

INVESTIGACIÓN

Mediante una breve charla con un ingeniero en seguridad de aplicaciones, nos pudo comentar lo siguiente:

Pregunta: Disculpe, en la universidad me solicitaron investigar sobre estos temas, backdoors y troyanos, ¿cree que pudiera compartirme algo sobre esto?

Mira, la mayoría de las empresas no invierten en seguridad, porque realmente no lo ven como una inversión, lo ven como un gasto, y que muchas veces es un gasto que no quieren hacer y solo lo hacen cuando pasan algunos factores, por ejemplo

- Una empresa más grande los quiere comprar, por ejemplo, Santander quiere comprar una fintech, pero les pide que hagan un análisis de vulnerabilidades, porque no quieren comprar problemas.

- Se quieren certificar (iso 27001, 27002, pci, ley fintech, etc), y dentro de la certificación les piden que hagan análisis de vulnerabilidades, y esto lo hacen para abrir mercado, por ejemplo, si una fintech quiere establecerse en México, si o si, tiene que cumplir la ley fintech.

Son muy pocas empresas las que invierten en seguridad así porque sí. Ahora, ya entrando como a el sector empresarial, es miles de veces más barato pagar un servicio de hacking ético, que asumir el pago de un ransomware por ejemplo. Pero de verdad mucho más barato.

Por ejemplo, a Twitter recientemente lo hackearon, y accedieron a cuentas de personas tipo Bill Gates, Barack Obama, etc. Y les pidieron bitcoins, y si se los enviabas, te lo regresaban al doble, que pues obvio, era una estafa y robaron bastante.

Y ya en los troyanos y backdors, aparte del problema de que pues, se pueden robar información, y obviamente tienes que invertir en infraestructura tanto para reparar el problema, como para "indemnizar" a las personas, tipo que cambien sus claves, enviar correos, etc... Otro problema es el detectarlos. Si no invertiste en seguridad, pues vas a tardar muchísimo tiempo en detectarlos.

Igual el proceso más o menos es: Un atacante logra ejecutar comandos en un servidor y pues de ahí, trata de moverse a otros servidores, eso se llama pivoting, pero si lo descubren pues lo van a sacar. Entonces lo que hacen, es instalar un backdoor en el sistema, para que, si lo descubren y lo sacan, pueda volver a entrar y tener más tiempo para explotar las cosas. Por ejemplo, si sale que se filtró el código de Facebook, por decir algo, y lo sacaron de esa forma, pues puede que incluso hayan tenido acceso a los servidores muchísimo tiempo antes. Y cuando según ellos lo sacan, puede que aún tenga acceso al sistema, porque puede que se haya movido entre servidores.

Y los troyanos, básicamente son programas disfrazados de otros, entonces, lo que hacen es mandar un correo con un programa que en realidad es otra cosa, al final el factor más vulnerable de una empresa, son los empleados, y se recomienda tener súper bien seccionada la empresa, porque si a todos les dan acceso a todo, puede que algún empleado tenga intenciones de lucrar o por estar simplemente enojado, que ni siquiera sea de desarrollo. Muchas veces los atacantes no son genios malvados, solo son niños ricos, le pagan a esas personas y el resto es historia.

Por ejemplo, a Fedelobo, en su canal de YouTube, le mandaron un correo diciendo “Oye, mira mi juego, somos de una nueva desarrolladora, y queremos que lo pruebes, creemos que es un gran juego, no nos respondas, confiamos mucho en nuestro juego, pruébalo, y luego nos dices, no importa si nos rechazar, pero pruébalo”. Lo instaló y le robaron las cookies de su sesión de YouTube.

Pregunta: En todos los lugares que he visto la seguridad no es prioridad. Entonces, cuando se detecta un problema de estos dos, ¿cómo se procede? Y, aparte, en el mundo ideal de que sí le importe la seguridad, ¿cómo podrían prevenir ambos?

Primero pues, es tratar de, o desconectar todo de la red, o de sacar a los atacantes mientras sigues online, pero pues, es bastante difícil, es un proceso que no dura unas horas o un día, puede durar meses. Porque pues, un atacante puede tener un backdoor en múltiples sistemas.

Y para la otra pregunta, realizando pentesting periódicos, y haciendo seguridad defensiva, pero, a pesar de eso, es imposible cuidarte al 100%, entonces, debes tener también un plan de respuesta a incidentes.

Pregunta: ¿Y de costo?, ¿nos puede decir algo sobre eso?

Ahí no te puedo decir algo definitivo, no es lo mismo realizar un análisis pequeño en una empresa nueva, a hacerlo con miles de páginas, miles de empleados, de hecho, varían mucho los costos de este tipo de audiciones, no solo por el tamaño, sino por la complejidad, o lo que se pretender cubrir.

Los troyanos son virus de computadora que tienen el fin de crear una backdoor* para que así el atacante tenga acceso de manera remota a una computadora, con el objetivo de obtener información valiosa. Los permisos que el atacante obtiene dependen de los privilegios del usuario al que esté atacando y de las características del troyano.

Los troyanos están compuestos por dos archivos: un cliente que es el que envía las órdenes y un servidor que recibe las órdenes del cliente, las ejecuta y devuelve resultados.

Estos ataques pueden ejecutarse y durar mucho tiempo viviendo en tu computadora sin que puedas darte cuenta que está ahí, lo que hace su detección y eliminación manual muy difícil, pero afortunadamente, existen patrones que podrían darte un indicio que hay algo maligno:

- Si hay programas desconocidos iniciándose al momento de prender la computadora.
- Se crean y destruyen archivos de manera “automática”.
- Si la computadora corre más lento o hay errores en el sistema operativo.

Backdoor. En español puerta trasera, en informática se usa este término para referirse a un método para obtener acceso sin permiso. Pueden instalarse en tu sistema escondiéndose en un programa fidedigno o conocido, una actualización o en un código.

Las recomendaciones que se deben tener en cuenta para evitar anidar un caballo de Troya en nuestro equipo son:

- Contar con un software antivirus actualizado.
- Contar con un software antispyware.
- Aplicar constantemente actualizaciones de seguridad a nuestro equipo.

- No descargar archivos adjuntos de correos electrónicos sospechosos ni de remitentes desconocidos.
- No descargar archivos de sitios Web no confiables.

CONCLUSIONES

Es indiscutible que la seguridad no suele ser una prioridad en muchas de las empresas nacionales, pero, concientizarnos de ello es importante, nuestra carrera debe ser integral y debemos conocer al menos la forma de combatir o reducir este tipo de ataques, es importante dar a conocer el valor a largo plazo que se obtiene al implementar este tipo de medidas, que, si bien, no requiere tanto esfuerzo como el de reducir los accesos, es tedioso, pero, no suele llevarse a cabo porque hay mucha confianza.

REFERENCIAS

- UNAM. Seguridad en Cómputo: Troyanos y backdoors. Disponible en: http://blogs.acatlan.unam.mx/lasc/2016/02/11/troyanos-y-backdoors/
- UNAM. Usuario Casero: Troyano. Disponible en: https://www.seguridad.unam.mx/historico/usuario-casero/eduteca/main.dsc-id=167.html