Aliaga_unidad1.md - Grip

Módulo 3 - Unidad 1

Ejercicio 1

En Javascript (y al parecer en casi todos los lenguajes de programación) es muy común usar distintas librerías. Estas librerías hacen que el desarrollo sea más rápido y eficiente: en vez de tener que programar todo desde cero, las librerias permiten moldear las aplicaciones sobre código que ya escribió alguien y modificarlo a nuestro antojo.

Sin embargo, una simple búsqueda en algunas de estas librerías, como React, Node, Angular... arroja miles de páginas web que describen las vulnerabilidades existentes en el lenguaje de programación por defecto de todas las páginas/aplicaciones web. Recordemos que Brendan Eigh (el creador de JS) escribió el código de JS en 10 días.

Algunas de estas vulnerabilidades aparecen mencionadas en https://snyk.io/learn/javascript-security/.

Ejercicio 2

En el texto de la unidad 1 del módulo 3 se habla de un puesto: Director de seguridad. Además de cumplir su rol de controlar que las medidas de seguridad se cumplan y sean las adecuadas, para mí, las personas que ocupan ese pueston deben responder siempre que NO a la pregunta: `¿las medidas que están implementadas son las suficientes?`

En el momento en el que el Director de Seguridad de una empresa (comúnmente conocido como *CISO*) baja la guardia y se conforma con lo que ha creado, podemos decir que la empresa está en problemas. Estas son las medidas mencionadas en el texto:

- que haya un responsable de seguridad
- protección de los dispositivos
- protección de la red
- protección de los servidores
- existencia de copias de seguridad y seguridad de la mismas
- protección de los recursos

Si bien estas medidas son necesarias e indispensables, agregaría a esta lista:

- capacitación constante de todo el personal. Si bien esto fue mencionado como una de las responsabilidades del CISO, es fundamental que no solo se concientice a los usuarios, si no que también se tiene que actualizar esa capacitación a través de charlas sobre las amenazas que enfrentó la empresa y cómo se solucionaron. Particularmente, el equipo de seguridad (equipo azul) debe estar pendiente de lo que ocurre en el espacio cibernético mundial para saber qué tecnologías están usando los atacantes y cómo reaccionar a ellas.

- pruebas constantes de que los recursos están informados y atentos. Esta sería una prueba de que la capacitación funciona de manera esperada. Por ejemplo, enviar a los usuarios emails internos con campañas de phising (organizadas por el equipo de seguridad de la empresa) para ver cuántas personas reportan ese ataque phising y cuántas hacen clic en los links del email de phising. Esto nos dará una muestra de dónde hay que mejorar, a qué recursos volver a capacitar, entre otras.

- contratación de empresas dedicadas a hacer pen-testing. Estas empresas se dedican a

probar cuán resiliente es nuestra organización ante múltiples escenarios, tanto vulnerabilidades en nuestra infraestructura física como virtual. A través de la realización del informe que nos presente la empresa de pen-testing, podremos ver en qué áreas está fallando la seguridad de la emprsea.

- además de la contratación de una empresa externa, realizar contstantemente auditorías internas de seguridad.

- preparación de un equipo de respuesta ante ataques y realización de simulacros de vulneración y pérdida de servicio. Este es un punto clave para determinar si la empresa es capaz de resistir un ataque a su infraestructura. Además de identificar a las personas claves que hay que contactar en caso de que se detecte un ciberataque, se debe establecer un procedimiento adecuado para cómo responder a ese ataque, a qué personas contactar, qué acciones tomar, qué prioridades se deben tener, entre otras.