MEJORAS DE SEGURIDAD DEL DESARROLLO DE APLICACIONES EN UNA EMPRESA NACIONAL DE RETAIL

Adán Navarrete Mora

Guía: Roque Hernández

Presentado como parte de los requisitos para el Título de Magíster en Ciberseguridad. CES: RPC-SE-19-NO.151-2020. Cohorte 2022 - 2023.

Correo electrónico del autor: adanavarrete15@gmail.com Guayaquil, 06/04/2023.

Introducción

En la actualidad, muchas empresas han ampliado sus canales de venta a través del comercio electrónico, pero no todas son conscientes de los riesgos cibernéticos que esto conlleva, como por ejemplo el robo de información, la pérdida de reputación, e incluso la posibilidad de perder la empresa son algunas de las consecuencias de un ataque cibernético.

Este proyecto hace referencia a una empresa de retail, la cual, para expandir sus ventas, ha optado por comprar software a terceros, pero más ha invertido en el desarrollo de software internamente, llegando a tener cuatro tipos de canales de venta: físico, web, aplicación móvil y chatbot Whatsapp. Cumpliendo con las funciones de un desarrollador full stack, se ha podido identificar ciertas vulnerabilidades en el proceso del desarrollo o del despliegue de aplicaciones, la falta de un plan de continuidad del negocio, entre otras. Para mejorar la seguridad, se han enfocado en materias como Seguridad de Bases de Datos, Estrategias y Políticas Multilaterales de Ciberseguridad, Continuidad del Negocio y Ciberseguridad Ubicua.

Desarrollo

A continuación, se describen las materias mencionadas anteriormente con una breve descripción de lo aprendido en cada una de ellas y la forma en la que se aplicó en la empresa:

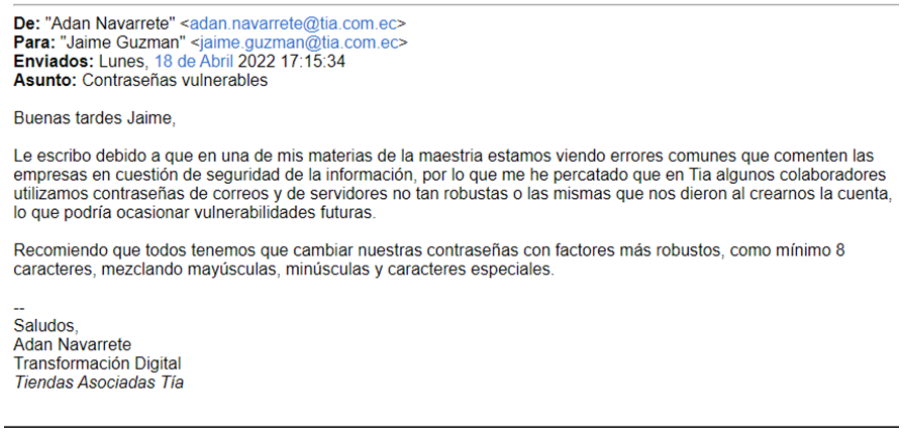
Estrategias y políticas multilaterales para la ciberseguridad

Es común que en las empresas existan vulnerabilidades en las contraseñas de las cuentas o correos de los colaboradores (Jiménez, M. M., 2022), lo cual es una de las vulnerabilidades que se presentó en esta empresa. Esta vulnerabilidad podría ser perjudicial,

debido a que por defecto, la clave de los colaboradores era “nombre2021”, además, la misma clave se usaba para establecer la conexión VPN además de otros accesos.

En esta asignatura se realizó un taller, donde se hizo una campaña de concientización a los colaboradores de los diversos departamentos en la cual se les comunicó las consecuencias que ocasionaría que una persona externa descifre una contraseña de algún colaborador y pueda acceder al sistema. En consecuencia, después de hablar con los encargados del área, se consiguió cambiar de proveedor de correo electrónico, el cual exige que por defecto se ingrese una contraseña más robusta.

Figura 1



De: "Adan Navarrete" <adan.navarrete@tia.com.ec>
Para: "Jaime Guzman" <jaime.guzman@tia.com.ec>
Enviados: Lunes, 18 de Abril 2022 17:15:34
Asunto: Contraseñas vulnerables

Buenas tardes Jaime,

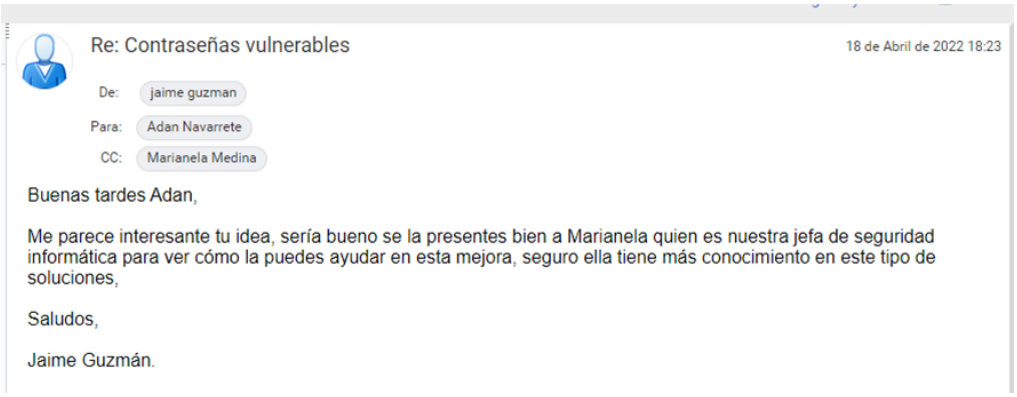
Le escribo debido a que en una de mis materias de la maestria estamos viendo errores comunes que comenten las empresas en cuestión de seguridad de la información, por lo que me he percatado que en Tia algunos colaboradores utilizamos contraseñas de correos y de servidores no tan robustas o las mismas que nos dieron al crearnos la cuenta, lo que podría ocasionar vulnerabilidades futuras.

Recomiendo que todos tenemos que cambiar nuestras contraseñas con factores más robustos, como mínimo 8 caracteres, mezclando mayúsculas, minúsculas y caracteres especiales.

--
Saludos,
Adan Navarrete
Transformación Digital
Tiendas Asociadas Tía

Navarrete, A. (2023). Correo electrónico enviado al jefe del departamento de TD. Empresa Retail S.A, Ecuador.

Figura 2



Navarrete, A. (2023). Respuesta del jefe del departamento de TD. Empresa Retail S.A, Ecuador.

Ciberseguridad ubicua

En la actualidad la ciberseguridad es un tema cada vez más importante en nuestra vida cotidiana, y no solo se limita a un ataque a nuestra computadora personal, sino cualquier dispositivo que esté conectado a una red puede ser vulnerable a los ataques cibernéticos. Por ejemplo, nuestros teléfonos móviles, tablets, sistemas de domótica, entre otros (Enciso, J., 2021). En esta materia, aprendimos que es importante tomar medidas de seguridad adecuadas en todos nuestros dispositivos, como por ejemplo, mantenerlos actualizados con las últimas versiones de software y de los sistemas operativos.

En esta asignatura, se realizaron varios talleres, uno de ellos fue "¿Quién está en tu casa?", el cual fue muy útil para tomar conciencia de todos los dispositivos que estuvieron conectados en la red local y poder identificar a sus propietarios, ya que algunos de ellos pudieron ser vulnerables a los ataques cibernéticos. Al identificar a cada propietario, pudimos asegurarnos de que no había una persona ajena a la empresa conectada a la misma red local. Debido a que uno de los canales de venta de esta empresa es a través de una

aplicación móvil, es importante concientizar a los usuarios sobre la importancia de mantener sus dispositivos móviles actualizados, ya que existen vulnerabilidades en los sistemas operativos de dichos dispositivos que pueden ser explotadas por los ciberdelincuentes para comprometer la seguridad de la aplicación y de los sistemas de la empresa (Norton, 2019).

Continuidad del negocio

Esta materia fue de gran importancia para comprender que una empresa no solo debe estar preparada para enfrentar riesgos relacionados con la ciberseguridad, sino también para factores externos como protestas, incendios y otros sucesos impredecibles que pueden ocasionar pérdidas económicas y, en los peores casos, incluso pérdidas humanas. Es fundamental contar con un plan de acción y un plan de continuidad del negocio para mitigar los riesgos y garantizar la continuidad de la empresa ante cualquier suceso o evento (Torchio, A., Cabai, D., & Astorga, R., 2020).

Una de las primeras acciones que se llevaron a cabo fue la identificación de los procesos críticos de la empresa. Para lograrlo, se realizó una concientización a los diversos departamentos de la empresa acerca de la importancia de contar con un plan de continuidad del negocio, lo que permitió una mejor identificación de los procesos críticos en cada área. Después de identificar los procesos críticos, se trabajó en conjunto con compañeros de otros departamentos para desarrollar la matriz BIA y proponer un plan de continuidad del negocio. Los directivos de la empresa se mostraron muy interesados en este proceso colaborativo y en las soluciones propuestas para garantizar la continuidad del negocio en situaciones adversas.

Figura 3

Navarrete, A. (2023). Reunión con colaboradores de otras áreas. Empresa Retail S.A, Ecuador.

Figura 4

Navarrete, A. (2023). Reunión con el jefe del departamento de datos maestros. Empresa Retail S.A, Ecuador.

Tecnología, modelos y técnicas de ciberseguridad

Durante esta asignatura, se aprendió el uso de varias herramientas y tecnologías útiles para la implementación de medidas de protección de la información en la empresa. Entre ellas se incluyen soluciones de seguridad de red como firewalls, VPN y autenticación de usuarios. También repasamos los principales modelos para proteger una red de la empresa, cuyos conocimientos nos permitieron comprender mejor cómo proteger las redes y la información de la empresa de manera efectiva. Una de las herramientas que más llamó la atención fue el uso de honeypots, que se utiliza como una especie de trampa para los ciber atacantes. La cual simula sistemas vulnerables para atraer a los atacantes y así poder identificar sus técnicas y patrones de ataque (Espinosa, O., 2019). De esta manera, se pueden tomar medidas preventivas y mejorar la seguridad del sistema en general, cuya herramienta fue propuesta para futura implementación con el jefe del departamento, sin embargo, aún está en trámites debido a cambios de directivos en el departamento.

Seguridad de Aplicaciones y Bases de Datos

En la empresa, se llevan a cabo proyectos y desarrollos internos que son utilizados por los usuarios para llevar a cabo compras en línea o para registrar sus datos personales. Con el rol de desarrollador de software, durante la realización de esta materia se ha aprendido acerca de las diversas formas en que los ciberdelincuentes pueden infiltrarse o atacar páginas web y servicios en línea, y se ha adquirido conocimiento sobre herramientas y metodologías para prevenir dichos ataques. Entre estas herramientas se encuentra la metodología de seguridad OWASP, la cual es fundamental para garantizar el desarrollo seguro del software. Gracias a lo aprendido en esta materia, se han implementado mejores medidas de seguridad en las aplicaciones desarrolladas, disminuyendo el riesgo de vulnerabilidades y ataques cibernéticos.

Una de las medidas adoptadas consistió en realizar pruebas utilizando el analizador de código SonarQube antes de la puesta en producción, con el fin de identificar posibles vulnerabilidades en el código desarrollado. Otra mejora que se implementó en el desarrollo del backend fue el uso de archivos .env para manejar las credenciales y las rutas de navegación de los programas desarrollados. Además, se ha adquirido una mayor conciencia sobre la importancia de la seguridad en el desarrollo de software en la empresa.

Implementación

Durante el proceso de la maestría, se ha logrado implementar mejoras significativas en la seguridad de la empresa. Se cambió a una plataforma de correo electrónico que exige contraseñas más robustas por defecto, después de una campaña de concientización sobre los riesgos de tener una contraseña vulnerable. También implementé el uso de un analizador de código, SonarQube, para minimizar las vulnerabilidades y desarrollar software más seguro antes de desplegarlo en producción. Aunque se han logrado avances, todavía existen oportunidades para fortalecer la seguridad y continuidad del negocio. Por ejemplo, sería beneficioso implementar un plan de seguridad que contemple normas y prácticas de seguridad para mejorar la protección en las transacciones comerciales, aprovechando la matriz BIA que ya se ha propuesto. Se sugiere realizar pruebas de hacking ético periódicas en todas las áreas de la empresa para detectar posibles infiltraciones o fugas de información. También se podría establecer una matriz de responsabilidades que establezca roles y responsabilidades claras en la gestión de información para reducir el riesgo de acceso no autorizado o fuga de información. Además, se podría implementar un proceso de análisis de código previo al despliegue de los desarrollos a producción para reducir el riesgo de fallos de seguridad y mejorar la calidad del software utilizado internamente o por los clientes de la empresa.

Conclusiones

Se concluye que es importante tomar medidas para mejorar los niveles de seguridad en la empresa, tales como llevar un control de acceso a la información crítica para rastrear posibles fugas de información, motivar a los colaboradores a usar contraseñas robustas para acceder a sus correos electrónicos y sistemas internos, instalar antivirus y WAF (Web Application Firewall) en la empresa para prevenir ataques cibernéticos. No tomar estas medidas puede poner en riesgo la continuidad del negocio y su reputación

Además, se concluye que es importante llevar a cabo una evaluación periódica de las medidas de seguridad implementadas en la empresa, con el fin de detectar posibles debilidades o brechas en la seguridad y tomar acciones preventivas para corregirlas. Asimismo, se sugiere la implementación de capacitaciones y entrenamientos para los colaboradores en cuanto a buenas prácticas de seguridad informática y concientización sobre los riesgos asociados a la falta de seguridad en el desarrollo de software y la gestión de información crítica en la empresa. De esta manera, se puede fomentar una cultura de seguridad en la organización y minimizar los riesgos de posibles amenazas.

Recomendaciones

Se recomienda que se lleve a cabo una campaña de concientización sobre la importancia de contar con un plan de continuidad del negocio. Esta campaña podría incluir la presentación de ejemplos reales de ataques o incidentes que han ocurrido en otras empresas y la forma en que han manejado la situación. Debería estar presente un representante de cada área para que brinde información sobre los procesos críticos del negocio y se pueda elaborar una matriz de riesgos detallada y un mejor plan de continuidad del negocio. De esta manera,

se podrán identificar posibles vulnerabilidades y estar preparados ante situaciones inesperadas y disminuir los riesgos o pérdidas que se puedan presentar.

Otra recomendación sería, que, además de proponer aumentar el presupuesto para la compra de herramientas como honeypots y WAF, se debería presentar un análisis de los beneficios de cómo estas herramientas pueden ayudar a reducir los riesgos de seguridad cibernética y los costos asociados con los ataques cibernéticos. También sería importante destacar la necesidad de mantener estas herramientas actualizadas y monitoreadas para asegurar su efectividad y eficiencia en la protección de la información y los activos de la empresa.

Limitaciones

La principal limitación que se presentó en el desarrollo del planteamiento del proyecto fue el recorte de personal en la empresa, lo que imposibilita cumplir con las propuestas de implementación para mejorar la seguridad de la información de los diferentes departamentos de la empresa, tal como se esperaba.

Otra de las limitaciones que se encontró en el proceso de implementar un plan de continuidad del negocio fue el cambio de directivos en el departamento de sistemas, por lo que se tuvo que volver a presentar la idea a los nuevos directivos, y, de esta manera, esperar la aprobación y sugerencias de los mismos.

Por último, otra dificultad que se presentó a lo largo del proceso de la maestría, fue la falta de presupuesto para contratar los diversos servicios o herramientas para mejorar la seguridad de la información de la empresa, debido a que muchas de estas herramientas son nuevas o desconocidas para los directivos de la empresa.

Referencias

Jiménez, M. M. (2022). *Vulnerabilidades que afectan la seguridad de la información.* Piranirisk.com. Recuperado de https://www.piranirisk.com/es/blog/vulnerabilidades-en-seguridad-de-la-informacion

Enciso, J. (2021). *Ubicuidad: riesgos de ciberseguridad*. Grupomicronet.com. Recuperado de https://blog.grupomicronet.com/ubicuidad-riesgos-de-ciberseguridad

Norton. (2019). *Mobile security threats to your iPhone & android devices* Norton.com. Recuperado de https://us.norton.com/blog/mobile/mobile-security-101

Torchio, A., Cabai, D., & Astorga, R. (2020). *La importancia del Plan de Continuidad de Negocio*. CUATROi. https://www.cuatroi.com/la-importancia-del-bcp/

Espinosa, O. (2019). *Qué es y para qué sirve un Honeypot*. RedesZone. https://www.redeszone.net/tutoriales/seguridad/que-es-honeypot/

Glosario

Sistema de domótica: Un sistema de domótica es un conjunto de tecnologías y dispositivos diseñados para controlar y automatizar diversos aspectos del hogar o edificio, como la iluminación, la climatización, los sistemas de seguridad, entre otros. La domótica permite a los usuarios gestionar y monitorear los diferentes sistemas de su hogar o edificio de manera centralizada, ya sea a través de un dispositivo móvil o una computadora.

VPN: Son las siglas de "Virtual Private Network" (Red Privada Virtual en español). Se trata de una tecnología de red que permite establecer una conexión segura y cifrada entre dos dispositivos a través de Internet o una red pública.

WAF: son las siglas de "Web Application Firewall" o Firewall de Aplicaciones Web en español. Es un tipo de cortafuegos o firewall diseñado específicamente para proteger aplicaciones web de ataques malintencionados.

Anexos

Anexo 1 (Evidencia de aprendizaje): https://n9.cl/q2l3c

Anexo 2 (Propuesta de implementación): https://n9.cl/7bq87