PRÁCTICA 1.1: PLAN DE CONCIENCIACIÓN

Crea una empresa ficticia

Daniel García Acevedo y Eric Serrano Marín

Contenido

1. INTRODUCCIÓN

GameForge Entertainment es una empresa que trabaja en la industria de los videojuegos. Se especializa en el desarrollo y publicación de videojuegos para varias plataformas, incluyendo PC, consolas y dispositivos móviles.

2. DEFINICIÓN EMPRESA

A continuación, definiremos con más detalles cómo funciona nuestra empresa:

2.1 DEPARTAMENTOS

Departamento de desarrollo de Juegos:

- Ingenieros de software y programadores.
- Diseñadores de juegos y gráficos.
- Escritores de historias y guionistas.
- Testers y control de calidad.

Departamento de Publicación y Marketing:

- Gerente de publicación y marketing.
- Especialistas en marketing digital y redes sociales.
- Personal de relaciones públicas.
- Analista de mercado y estrategia.

2.2 NÚMERO DE EMPLEADOS

GameForge Entertainment cuenta con más de 100 personas en total. El departamento de Desarrollo de Juegos cuenta con 70 empleados, mientras que el departamento de Publicación y Marketing emplea alrededor de 30 personas.

2.3 ACTIVOS CRÍTICOS

- Propiedad Intelectual: Derechos de autor y propiedad intelectual de los juegos son activos críticos para la empresa.

- Servidores y Plataformas: La infraestructura de servidores para alojar los juegos en línea, plataformas de distribución y tiendas en línea.

- Datos de Usuarios: Información de los jugadores, como perfiles, compras en el juego y datos de pago.

- Equipos de Desarrollo: Hardware y software utilizados por los equipos de desarrollo de juegos.

- Contratos de Distribución: Acuerdos de distribución con plataformas de juegos y socios comerciales.

2.4 CULTURA DE CIBERSEGURIDAD

GameForge Entertainment sabe de la importancia de la ciberseguridad, por su protección a sus juegos y a los datos de sus usuarios. La empresa trabaja en su seguridad de la siguiente manera:

- Formación en ciberseguridad: Se da formación regular a los empleados sobre prácticas de ciberseguridad

- Protección de datos: Se implementan políticas y procedimientos para proteger la información de los jugadores, incluyendo medidas de seguridad en servidores y sistemas de autenticación segura.

- Protección de Propiedad Intelectual: Nos aseguramos de que se respeten y protejan los derechos de autor y propiedad intelectual en sus juegos.

- Monitoreo de Seguridad: GameForge Entertainment establece sistemas de monitoreo para detectar y responder posibles amenazas cibernéticas y vulnerabilidades en los juegos en línea.

2.5 POSIBLES RIESGOS

Los posibles riesgos incluyen la **piratería de juegos**, **ataques cibernéticos** dirigidos a servidores, **robo de propiedad intelectual**, **infracciones de datos** de usuarios y la **pérdida de confianza** de los jugadores.

3 DOCUMENTACIÓN

A continuación, definiremos la documentación de GameForge Entertainment.

3.1 PLANIFICACIÓN

3.1.1 IDENTIFICAR NECESIDADES

Objetivo: Formar a todos los empleados de la empresa en la importancia de la ciberseguridad.

Razón: La seguridad de la información y la protección de nuestros activos críticos son fundamentales para el éxito de GameForge Entertainment. Y más con la creciente amenaza de ataques. Es esencial para nosotros que todos los empleados estén preparados para identificar y mitigar posibles riesgos.

3.1.2 DESTACAR DEBILIDADES

Puntos débiles detectados:

- **Contraseñas débiles:** Falta de conciencia sobre prácticas seguras en el uso de contraseñas y dispositivos personales en el lugar de trabajo.
- **Inseguridad:** Riesgo de caer en estafas de ingeniería social, como el phishing.
- **Mantenerse actualizado:** Falta de actualización de software y sistemas de seguridad en dispositivos personales y de trabajo.

3.1.3 ADAPTACIONES NECESARIAS DEL PROGRAMA DE CONCIENCIACIÓN

Peculiaridades de GameForge Entertainment:

- La empresa tiene empleados en varias ubicaciones, incluyendo trabajadores remotos y en sedes físicas.
- Trabajamos en un entorno donde utilizan sistemas de juego en línea, lo que puede aumentar la exposición a amenazas específicas de la industria de los videojuegos.
- Variedad de plataformas y dispositivos utilizados en el desarrollo y pruebas de juegos.

Adaptaciones necesarias:

- El programa de concienciación se adaptará para cubrir a todos los empleados, independientemente de su ubicación o método de trabajo (presencial, remoto o híbrido).
- Se dará importancia a la ciberseguridad en la industria de los videojuegos, con ejemplos

específicos de amenazas comunes.
- Se proporcionará orientación sobre las mejores prácticas para la protección de dispositivos utilizados en el desarrollo de juegos.

3.1.4 METODOLOGÍA

Metodología para Desarrollar la Concienciación en Ciberseguridad:

- **Formación en línea**: Utilizaremos recursos en línea interactivos y vídeos educativos que los empleados podrán completar a su propio ritmo.
- **Sesiones de formación en vivo**: Organizaremos sesiones de formación en línea periódicas con ayuda de expertos en ciberseguridad.
- **Recursos y material de referencia**: Proporcionaremos guías, infografías y documentos de referencia para reforzar la formación.
- **Simulacros de ataques**: Realizaremos ejercicios de simulacros de ataques de phishing para que los empleados practiquen la identificación de correos electrónicos fraudulentos.

3.2 IMPLEMENTACIÓN DEL PLAN DE CONCIENCIACIÓN

3.2.1 ALCANCE Y OBJETIVOS:

Alcance: El programa de concienciación en ciberseguridad se extiende a todos los empleados de GameForge Entertainment, incluyendo el personal de desarrollo de juegos, publicación y marketing, así como aquellos que trabajan en oficinas centrales.

Objetivos:

- Aumentar la concienciación de las amenazas cibernéticas y las mejores prácticas de seguridad en toda la empresa.
- Reducir el riesgo de caer víctima de ataques de phishing y otros ataques de ingeniería social.
- Mejorar la seguridad de los dispositivos utilizados en el desarrollo y pruebas de juegos.

3.2.2 INVOLUCRAMIENTO DE TODO EL PERSONAL

- Cada empleado recibirá formación personalizada según su rol y responsabilidades en la empresa.
- El departamento de Recursos Humanos coordinará la formación y asignará a los empleados a las sesiones que les corresponda.
- Expertos en ciberseguridad y personal de TI se encargará de la creación de contenido y la impartición de sesiones de formación en vivo.

El programa se llevará a cabo de manera continua, con actualizaciones regulares para abordar las amenazas emergentes.

4 ORGANIZACIÓN Y MANTENIMIENTO DE LA CONCIENCIACIÓN

Para organizar la concienciación en ciberseguridad y mantenerla a lo largo del tiempo en GameForge Entertainment, implementaremos una serie de actividades educativas y recordatorios prácticos. A continuación, veremos el conjunto de actividades que se llevarán a cabo.

Organización de la concienciación:

- **Sesiones de formación inicial:** Estas sesiones se llevarán a cabo al comienzo de la contratación de cada empleado, será una charla de orientación sobre la importancia de la ciberseguridad en nuestra empresa y se proporcionará una introducción a las políticas y prácticas clave.
- **Cursos en línea personalizados:** Todos los empleados completarán cursos en línea, que abordarán amenazas específicas a las que pueden enfrentarse en su trabajo diario.
- **Sesiones de formación en vivo:** Se realizan en vivo periódicamente, dadas por expertos en ciberseguridad, que cubrirán temas actuales y nuevas amenazas. Estas sesiones se grabarán para que los empleados puedan acceder a ellas en cualquier momento.

Mantenimiento y Reforzamiento de la Concienciación:

- **Simulacros de Ataques Phishing:** Realizaremos ejercicios de simulacros de ataques phishing de forma regular para evaluar la capacidad de los empleados para identificar correos electrónicos fraudulentos.
- **Boletines de seguridad:** Enviaremos boletines de seguridad mensual a todos los empleados, que destacarán amenazas actuales, ofrecerán consejos y mejores prácticas.
- **Carteles de Recordatorio:** Colocaremos carteles en la empresa que recuerden a los empleados

las prácticas seguras, como la importancia de no dejar documentos impresos en las impresoras o la necesidad de proteger las contraseñas.

- **Ejercicios de Seguridad Informática:** Realizaremos ejercicios prácticos donde los empleados deberán identificar posibles amenazas en situaciones cotidianas.
- **Premios y Reconocimientos:** Reconoceremos y recompensamos a los empleados que demuestren un alto nivel de concienciación en ciberseguridad o que reporten posibles amenazas.
- **Actualización Continua:** La formación y la información sobre ciberseguridad se mantendrá actualizada para abordar las amenazas emergentes y cambios en las políticas de seguridad.
- **Canal de Comunicación Abierto:** Fomentaremos un canal de comunicación abierto donde los empleados puedan plantear preguntas, preocupaciones o informar sobre posibles amenazas.

La concienciación en ciberseguridad se convertirá en una parte integral de la cultura de GameForge Entertainment. La combinación de formación, práctica y recordatorios regulares ayudará a garantizar que todos los empleados estén conscientes de las amenazas y estén preparados para proteger nuestros activos críticos.

5 MONITORIZACIÓN Y EVALUACIÓN DEL GRADO DE CONSECUCIÓN

5.1 MÉTRICAS DEL FUNCIONAMIENTO

Para monitorizar y evaluar el grado de consecución de la concienciación en ciberseguridad en GameForge Entertainment, utilizaremos una serie de métricas y métodos de comprobación.

Métrica de Éxito: Se considera que la plantilla está concienciada si, en días de control de impresoras aleatorios, menos del 10% de los empleados abandonan sus documentos impresos en la bandeja de salida durante más de 5 minutos.

Método de Comprobación:

Revisión de Bandejas de Impresión:

- En días aleatorios, el personal de seguridad o TI revisará las bandejas de impresión para verificar si los documentos impresos se han recogido en un plazo razonable.
- Registrarán el número de empleados que abandonaron sus documentos durante más de 5 minutos y cuántos lo hicieron dentro de ese período.

Frecuencia de Comprobación:

- Se llevarán a cabo revisiones aleatorias en un ciclo de, al menos, una vez al mes.

Si la métrica de éxito se cumple de manera consistente (es decir, menos del 10% de los empleados abandonan sus documentos durante más de 5 minutos en las revisiones aleatorias), se considerará que la concienciación en ciberseguridad ha funcionado en este aspecto.

Además de este ejemplo, aplicaremos otras métricas para evaluar la concienciación en ciberseguridad en diferentes áreas, como la tasa de éxito en ejercicios de simulacros de ataques de phishing, el número de informes de posibles amenazas cibernéticas por parte de los empleados y la disminución de incidentes de seguridad. Si observamos mejoras en estas métricas a lo largo del tiempo, consideraremos que el programa de concienciación en ciberseguridad ha sido un éxito. En caso contrario, se realizarán ajustes en el programa y se ofrecerá formación adicional para abordar las áreas problemáticas.

6 CONCLUSIÓN

En conclusión, el programa de concienciación en ciberseguridad que hemos implementado en GameForge Entertainment ha demostrado ser esencial para la protección de nuestra empresa y la seguridad de nuestros activos críticos. A lo largo de este trabajo, hemos identificado la importancia de sensibilizar a todos los empleados sobre las amenazas cibernéticas y las mejores prácticas de seguridad.

En resumen, la ciberseguridad es responsabilidad de todos en GameForge Entertainment, y nuestra empresa está comprometida en continuar mejorando y manteniendo una cultura de concienciación en ciberseguridad sólida y eficaz.

7 REFERENCIAS

Kit de concienciación de INCIBE: https://www.incibe.es/empresas/formacion/kit-concienciacion

Cómo promover la concienciación sobre la ciberseguridad en su organización: https://www.metacompliance.com/es/blog/cyber-security-awareness/how-to-promote-cyber-security-awareness-in-your-organisation