GRUPO DRAGON

INFORME MODELAMIENTO DE AMENAZAS CIBERNÉTICAS EN EL SISTEMA DE GESTIÓN EMPRESARIAL DE LA EMPRESA CREM HELADO

1. Introducción

Meals es una empresa colombiana que lidera el negocio de Helados de Grupo Nutresa. En Meals se fabrica y comercializa las marcas Crem Helado y Country Hill., tienen tres plantas de Producción ubicadas Armenia, Bogotá y Manizales. Segmentando mejor el análisis se estudiara la parte de Crem Helado con el fin de poder efectuar análisis eviten problemas y mejoren las condiciones de seguridad digital. Este informe aplica el modelo STRIDE para identificar y clasificar las amenazas cibernéticas en el sistema de información o gestión empresarial de Crem Helado. Esta empresa presenta sistemas obsoletos y no se evidencia deseos de innovación, se puede acceder a los sistemas desde un ordenador en las instalaciones de la empresa y desde los dispositivos personales de los empleados lo cual se configura como un sistema hibrido, por ende se requiere un análisis de modelado de amenazas que puede establecer una mejora continua potenciando la empresa para hacerla más rentable , segura y más competitiva en el ámbito de la convergencia digital donde se presentan últimamente muchos actores y riesgos para la seguridad. El siguiente análisis incluye amenazas, matriz de riesgos, diagramas de arquitectura de seguridad y políticas de mitigación.

2. Descripción del Escenario

Crem Helado utiliza un sistema de gestión de información empresarial el cual se encarga de manejar todos los sistemas de la empresa como el control de pedidos, distribución, gestión del talento humano, bodegas e inventarios, clientes, entre otros, el sistema de acuerdo a lo analizado presenta una estructura simple y con pocas capas de seguridad, ultimamemten se han tenido indicios de personas que han intentado de acdercarse a los empleados de la empresa de diferentes maneras lo cual genera alarmas para los directivos. Este sistema o plataforma está compuesto de la siguiente manera:

- Servidor central físico ubicado en las instalaciones principales, bases de datos en el sistema empresarial, sistema de acceso tanto en empresa como desde dispositivos personales
- Infraestructura: Cuenta con un servidor central, servidores en cada punto de distribución o ventas general, routers, cables, equipo de computación
- Usuarios: Administradores, personal de ventas y logística, distribuidores, clientes

3. Análisis de Riesgos aplicando STRIDE

3.1 Spoofing

- **Amenaza:** Ingeniería social permite que un atacante puede efectuar la suplantacion la identidad de un empleado para acceder al sistema de gestión de pedidos al obtener sus credenciales después de un análisis de inteligencia.
- **Mitigación:** Autenticación multifactor (MFA), certificados digitales, y monitoreo de accesos sospechosos, uso de firewall, segmentación de la red, uso de un buen antivirus tanto para el equipo como para el correo y navegador de internet.

3.2 Tampering

- **Amenaza:** La manipulación de los datos de pedidos o lo registrado en el inventario afecta disponibilidad y suministro de pedidos suministro de productos.
- **Mitigación:** Control de integridad de datos efectuando un monitoreo del tráfico, utilizar cifrado de datos, monitorear cambios sospechosos en los sistemas, inventarios y pedidos, revisar los permisos que tiene cada empleado y establecer los necesarios, emplear un sistema de control de versiones.

3.3 Repudiation

- **Amenaza:** El actor malicioso y malintencionado puede modificar datos sin dejar evidencia de la accion, esto evita que se identifique la responsabilidad.
- **Mitigación:** Registros con modelo de control de versiones, firma digital en transacciones y definir políticas de auditoría de los sistemas estrictas, autenticación biométrica para acceso a los sistemas.

3.4 Information Disclosure

- **Amenaza:** Filtración de información sensible de clientes, pedidos o rutas de distribución.
- **Mitigación:** Cifrado de los datos, monitoreo de los accesos, establecer políticas de confidencialidad, y monitorear el tráfico de datos para identificar información confidencial o sospechosa, capacitación y concientización del personal.

3.5 Denial of Service

- **Amenaza:** Un ataque de denegación del servicio podría inhabilitar el sistema de pedidos que salen y llegan, esto genera pérdidas monetarias y de fiabilidad del cliente
- **Mitigación:** Uso de firewalls, monitoreo en tiempo real, red fragmentada para que el ataque no afecte toda sino un segmento, acceso con dirección MAC evitando IP sospechosas

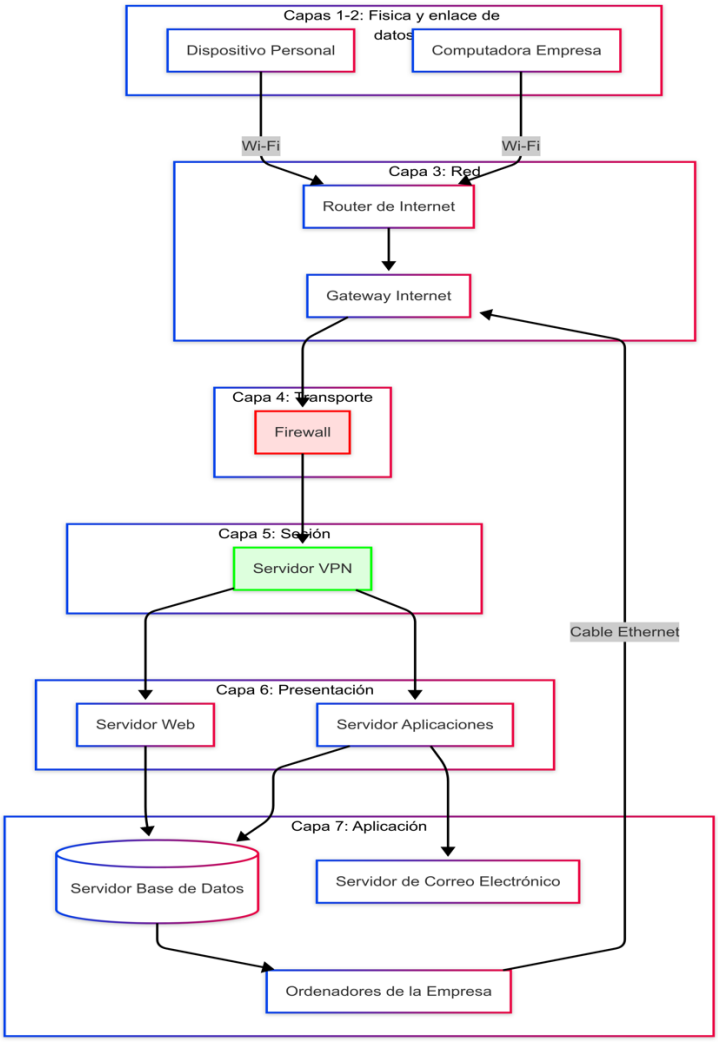
3.6 Elevation of Privilege

- **Amenaza:** El atacante puede ingresar y obtener privilegios mayores que le darian el control de los sistemas
- **Mitigación:** Cada usuario debe tener solo los privilegios necesarios, autenticación de doble factor, Parches de seguridad frecuentes, realizar auditoria de los sistemas, cambio de claves con periodicidad, actualizar aplicaciones y sistemas, alertas en tiempo real de intentos de accesos no autorizados o en horas no programadas.

Matriz de Riesgos

Tipo Amenaza	Probabilidad	Impacto	Mitigación
Spoofing	Alta	Alto	MFA, segmentación de red, firewalls, antivirus
Tampering	Media	Alto	monitoreo, auditoría del sistema, permisos necexarios
Repudiation	Baja	Medio	Control versiones, firma digital
Information Disclosure	Alta	Muy Alto	Cifrado de datos, monitoreo de datos, políticas de confidencialidad
Denial of Service	Media	Alto	Firewalls, red por fragmentos, monitoreo
Elevation of Privilege	Alta	Crítico	Privilegios mínimos por usuario, autenticar doble factor, auditoria de los sistemas, actualización de sistemas, alertas

Diagrama de Arquitectura de Seguridad



Políticas de Seguridad Propuestas

1. **Autenticación y Control de Accesos:** Implementar mejoras con la autenticación de doble factor, autenticación biométrica para empleados y distribuidores. Además restringir el acceso a plataformas de las empresa en equipos personales, solo se puede ingresar desde un ordenador de la empresa
2. **Cifrado de Datos:** Utilizar AES-256 para cifrar la bases de datos, como recomienda Schneier (2015).
3. **Monitoreo y Detección de actividades o tráfico inusual:** Implementar sistemas o aplicaciones que permitan la detección de amenazas o conductas anormales del sistema como el SIEM alineado con ISO 27001 (ISO/IEC 27001, 2022).
4. **Actualizaciones y Parches de Seguridad:** Mantener los sistemas actualizados y aplicar parches de seguridad con una periodicidad mínimo mensual, especialmente, priorizar parches críticos identificados en modelos STRIDE (Shostack, 2014).
5. **Capacitación del Personal:** Entrenar y concientizar a los empleados en temas de ciberseguridad y prevención de estafas, tipos de amenazas y como pueden llegar a ellos.

4. Conclusiones y Recomendaciones

- ⇒ El debido y adecuado análisis con STRIDE permitió identificar amenazas críticas en el los sistemas de gestión empresarial de Crem Helado lo cual permite actuar de manera rápida y oportuna antes de ocasionar un daño significativo tanto como para los sistemas, sus empleados y los clientes.
- ⇒ Se recomienda aplicar los protocolos y políticas de seguridad propuestas con el fin de evitar pérdidas o contingencias que se pueden presentar en un corto plazo
- ⇒ Incrementar la cultura de protección, confidencialidad y uso adecuado de la información de la empresa.
- ⇒ Aplicar el modelo PHVA en todos los procesos con el fin de identificar opciones de mejora y prevención o mitigación de riesgos identificados.

Referencias

Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking*. John Wiley & Sons.

ISO/IEC 27001. (2022). *Information security management systems — Requirements*. International Organization for Standardization.

Microsoft. (2021). *The STRIDE Threat Model: A Practical Approach*. Microsoft Security. https://docs.microsoft.com/en-us/security/engineering/threat-modeling-stride

NIST. (2020). *NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Schneier, B. (2015). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons.

Shostack, A. (2014). *Threat Modeling: Designing for Security*. Wiley.