MOORE

CIBERSEGURIDAD

Webinar Moore Colombia
Junio 2020 | V1.0

CONTENIDO

PANELISTAS

Conoce más sobre nuestros expertos.

Adriana Piñango
Gerente de Consultoría Empresarial y TI

MOORE COLOMBIA

Ingeniera de Sistemas
CISA – ITIL 4

Cuenta con más de 10 años de experiencia profesional enfocada en el diseño, ejecución y gestión de proyectos de auditoría de Tecnología de la Información bajo estándares NIA y PCAOB, y aseguramiento razonable bajo estándares ISAE3000 / ISAE3402. Ha desarrollado proyectos de consultoría para la mejora de procesos de negocio, tecnología, control interno de TI, cumplimiento regulatorio, gestión integral de riesgos, seguridad de la información e implementación SOX.

Los proyectos desarrollados le dan amplio conocimientos en diversos sectores económicos como financiero, educativo, alimentos y bebidas, farmacéutico, oil and gas, salud, retail, entre otros.

Cuenta con alta experiencia en sistemas de información complejos como SAP ECC - S/4HANA, Oracle, Dynamics y herramientas de administración de usuarios para la gestión de riesgos a nivel de accesos y segregación de funciones.

MOORE COLOMBIA

Ingeniero de Sistemas,
con Especialización en Gobierno Electrónico

Certificado en ISO27001 auditor líder e implementador (PCEB), CEH (En proceso) y curso CSX Cybersecurity Fundamentals (ISACA).

Con más de 7 años de experiencia en proyectos de auditoría interna de TI y consultoría, relacionados con controles generales de Tecnología, Controles SOX TI y Seguridad de la información y ciber riesgos; incluyendo evaluación y gestión de riesgos tecnológicos sobre sistemas críticos.

Ha desarrollado su trabajo en clientes del sector financiero, sector real, farmacéutico y educativo.
Se ha desempeñado como consultor senior en el área de Advisory en firmas Big4 y en el área de auditoría interna de TI en una entidad financiera.

Oscar Leandro Rodríguez
Supervisor de Consultoría Empresarial y TI

Webinar

CIBERSEGURIDAD

11 DE JUNIO DE 2020

- ✓ Ciberseguridad.
- ✓ Retos actuales para las empresas

Concepto de Ciberseguridad

La ciberseguridad se puede definir como la estrategia que desarrollan las compañías para la protección de los activos de información no tangibles, abordando las amenazas a la información procesada, almacenada y transportada por sistemas de información.

Es importante tener presente que actualmente tenemos un mundo hiperconectado y las dinámicas entre los sistemas, se apoyan en herramientas y recursos que están construidos por tecnologías de diferentes fabricantes.

¡Consigue la Presentación completa!

LEER MÁS

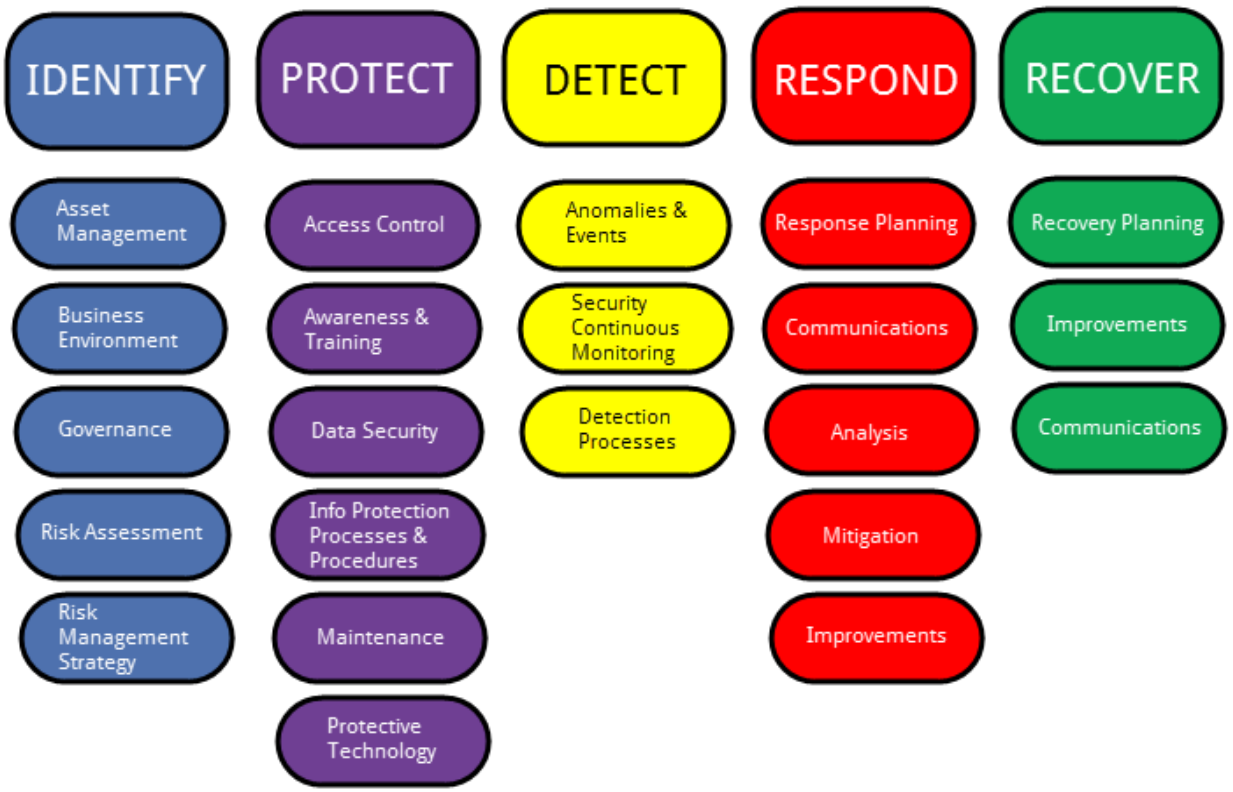
ASPECTOS TECNOLÓGICOS QUE AFECTAN LA SEGURIDAD DE LOS SISTEMAS

- Complejidad de los sistemas de TI tomando como referencia todo el conjunto de servicios, interfaces y tecnologías que están desplegadas en el ambiente tecnológico de la compañía.
- El esquema de conexión toma relevancia, cuando la operación se desarrolla en diferentes escenarios usando redes propias, redes de terceros e incluso redes públicas.
- Dispositivos especializados de la industria deben ser teniendo en cuenta al momento de definir lineamientos de seguridad debido a la particularidad de su funcionamiento.
- Sistemas en la nube y la tendencia de las compañías para migrar a servicios SaaS, Iaas y Paas.
- Tipos de usuarios y sus capacidades especificas quienes son un actor importante en la ejecución de los procesos
- Herramientas de seguridad las cuales se convierten en un recurso importante para desarrollar capacidades internas, con el fin de mantener un control tecnológico adecuado.

ASPECTOS EMPRESARIALES QUE AFECTAN LA SEGURIDAD DE LOS SISTEMAS

- Misión, visión y estrategia de seguridad de TI deben estar alineadas con la estrategia de la empresa, para garantizar el correcto aseguramiento de la infraestructura crítica de TI.
- Es importante entender la naturaleza del negocio como un elemento clave, para definir el esquema de protección de mi ambiente tecnológico.
- Apetito y tolerancia al riesgo se deben tener en cuenta al momento de gestionar riesgos, ya que permiten afinar las estrategias de mitigación para que sean más efectivas.
- Alinear mis prácticas de seguridad con la industria y tendencias tecnológicas.
- Requisitos de cumplimiento y regulaciones especificas se deben tener en cuenta, para no materializar impactos negativos relacionados con sanciones por parte de las entidades reguladores.
- Fusiones, adquisiciones y alianzas teniendo como premisa, que este tipo de dinámicas exige la integración de operaciones y procesos de una manera adecuada, para evitar alteraciones en la operación .
- Servicios de TI contratados con externos

Modelo de desarrollo de capacidades para la gestión de ciberseguridad tomando como referencia el marco NIST:



Fuente: NIST CIBERSECURITY FRAMEWORK

Identificar

La capacidad de Identificar está relacionada a la comprensión del contexto de la compañía, de los activos de TI que soportan los procesos críticos de las operaciones y los riesgos asociados a los mismos.

De esta manera la compañía define los recursos de acuerdo con la estrategia de gestión de riesgos y los procesos de mitigación de estos.

Esta capacidad incluye el desarrollo de: Gestión de Activos; Gestión de riesgos; Entity Level Control y definición de estrategias de mitigación.

Proteger

La capacidad de proteger está relacionada a la implementación de medidas de seguridad para asegurar los procesos y los activos de la compañía.

Esta capacidad incluye el desarrollo de: Definir el esquema de control de acceso; Concientización y formación; Seguridad de datos; Procesos y procedimientos para la protección de la información; Mantenimiento; Tecnología de protección.

Detectar

La capacidad de detectar está relacionada a la definición y ejecución de las actividades enfocadas a la identificación oportuna de los incidentes de seguridad.

Esta capacidad incluye el desarrollo de: Detección anomalías y Eventos; Monitoreo continuo de la seguridad y de manera general establecer procesos de detección.

Responder

La capacidad de responder está relacionada a la definición y ejecución de medidas de respuesta ante la de detección de un evento de seguridad. El objetivo principal es reducir el impacto del incidente.

Esta capacidad incluye el desarrollo de: Planificación de la respuesta; Comunicaciones; Análisis; Mitigación; Mejoras.

Recuperar

La capacidad de recuperar está relacionada a la definición y ejecución de las actividades dirigidas a la gestión de los planes y actividades para restaurar los procesos y servicios deficientes debido a un incidente de seguridad. El objetivo es asegurar la resistencia de los sistemas e instalaciones y, en caso de incidentes, para apoyar la recuperación oportuna de las operaciones.

Esta capacidad incluye el desarrollo de: Planificación de la estrategia de recuperación; Mejoras en el proceso de respuesta; Comunicación con las partes interesadas.

RETOS EMPRESARIALES POST COVID19

- Mantener un nivel de cultura de seguridad en nuestros colaboradores
- Si se hacen cambios significativos se deben identificar los nuevos activos críticos para incluir dentro del esquema de monitoreo
- Actualizar y ajustar el esquema de continuidad acorde a la emergencia de la pandemia

TENDENCIAS TECNOLOGICAS POST COVID19

- La adopción de esquemas mixtos de infraestructura locales – cloud, lo cual ha permitido fortalecer aspectos como continuidad y seguridad de las plataformas, sin embargo, hay que tener presente que los modelos de operación con tecnológica de computación en la nube requieren que se tenga en consideración temas como el control y propiedad de la información que se almacena en el tercero, el esquema de conectividad para garantizar el acceso y el proceso de gestión de vulnerabilidades.
- Aumentar el control de acceso en los dispositivos móviles, ya que pueden significar nuevos escenarios de riesgos no cubiertos
- Desarrollo de capacidades en BI y analítica para generar nuevas estrategias de trabajo y mejorar el proceso de gestión de seguridad, aprovechando los nuevos volúmenes de información que generan las herramientas
- El manejo efectivo de la información que está circulando de la marca en las redes sociales y medio digitales.

Enfocar el crecimiento estratégico de la compañía de manera para que incluya estrategias de crecimiento en la cultura de seguridad de la información

LECCIONES DEL CIBERATAQUE A TRAVELEX

Empresa dedicada al intercambio de divisas. Conozca los insights de uno de nuestros líderes mundiales en seguridad cibernética

Por: Patrick Rozario, Moore Hong Kong

Otro ciberataque de alto perfil se reportó durante el año nuevo, cuando Travelex, la red de oficinas de cambio más grande del mundo, con más de 1,000 tiendas y 1,000 cajeros automáticos en todo el mundo, anunció que algunos de sus servicios estaban comprometidos por un *ransomware* que buscaba secuestrar sus datos. Como medida de precaución, Travelex apagó inmediatamente todos sus sistemas para evitar una mayor propagación del virus informático a través de sus redes.

Un ransomware es un tipo de malware que impide o limita el acceso de los usuarios a sus sistemas, ya sea bloqueando el acceso al sistema o bloqueando los archivos de los usuarios a menos que se pague un rescate exigido por los delincuentes informáticos. Las iteraciones más avanzadas de ransomware incluyen cifrar ciertos tipos de archivos en sistemas infectados y obliga a los usuarios a pagar el rescate mediante criptomonedas.

El ataque de ransomware ha tenido un fuerte impacto en los servicios de cambio de divisas, afectando a bancos como Lloyds, Barclays, HSBC y RBS. Evaluando el impacto financiero después del ataque de ransomware en Travelex, la pérdida puede llegar a decenas de millones de dólares, o hasta cientos de millones.

En los últimos años, ha habido varias violaciones importantes de seguridad cibernética que involucran a grandes organizaciones. Uno de los elementos comunes entre estas organizaciones objetivo es que albergan cantidades considerables de información personal. El acceso no autorizado a la información personal podría generar ganancias financieras ilícitas, que es el factor más común de violación de datos.

El Informe de Investigaciones de Violación de Datos de Verizon (DBIR) de 2019 ofrece una perspectiva crucial sobre las amenazas cibernéticas que enfrentan las organizaciones hoy en día. La 12ª edición del DBIR se basa en datos del mundo real de incidentes de seguridad y violaciones de datos proporcionados por 73 fuentes de datos, tanto públicas como privadas, que abarcan 86 países de todo el mundo. Incidente se refiere a un evento de seguridad que compromete la integridad, confidencialidad o disponibilidad de un activo de información. Incumplimiento se refiere a un incidente que resulta en la divulgación confirmada (no solo exposición potencial) de datos a una parte no autorizada.

Para combatir esto, las organizaciones pueden implementar tecnología anti-ransomware como bloquear archivos ejecutables en su puerta de enlace de correo electrónico, deshabilitar documentos de oficina habilitados para macros, detener el inicio de JavaScript malicioso y mantener actualizado el software de todos los sistemas y aplicaciones para eliminar vulnerabilidades. Además, la sensibilización del personal y la capacitación en ciberseguridad también son cruciales. Sin embargo, la tarea más importante que cualquier organización podría hacer es asegurarse de hacer una copia de seguridad de los datos críticos de manera regular y consistente, al mismo tiempo que filtra los correos electrónicos y sitios web maliciosos. Si un ataque de ransomware es exitoso, estas organizaciones tendrían al menos sus datos importantes en otro lugar para la recuperación de manera rápida y efectiva.

Según el DBIR de Verizon 2019, el 52% de las infracciones incluyeron piratería informática en las que el 70% son ataques a aplicaciones web (cualquier incidente en el que una aplicación web fuera el curso del ataque, esto incluye explotaciones de vulnerabilidades de nivel de código en la aplicación, así como frustrar mecanismos de autenticación), el 33% incluía ataques sociales, el 28% involucraba malware, los errores varios representaban el 21% de las infracciones, el 15% eran mal uso por parte de usuarios autorizados, el robo físico y la pérdida eran el 4% de las infracciones. Muchas de estas acciones se superponen, por lo tanto, los porcentajes son superiores al 100%.

Algunas de las mejores prácticas para evitar infracciones son establecer una línea de base de activos y seguridad en torno a los activos orientados a Internet, como servidores web y servicios en la nube, estos pueden incluir:

- Segmentación de la red, muchas infracciones son el resultado de una seguridad deficiente y falta de atención a los detalles;
- Realizando análisis y pruebas de seguridad a las aplicaciones web para encontrar vulnerabilidades potenciales, los compromisos de las aplicaciones web ahora incluyen código que puede capturar los datos ingresados en los formularios web;
- Implementar MFA (autenticación Multifactor), lo cual complica considerablemente la posibilidad de robo de credenciales, no hay excusa para la falta de su implementación;

- Rastrear el comportamiento interno monitoreando y registrando el acceso a datos confidenciales;
- Proteger los sistemas de DoS-DDoS (ataque de denegación de servicio) que incluye protección contra interrupciones con monitoreo continuo y planificación de capacidad para tráfico anormal. Estos generalmente resultan en la degradación del rendimiento o la interrupción del servicio.

Al mantenerse socialmente expuestos, los ataques sociales son formas efectivas de capturar credenciales, monitorear el correo electrónico en busca de enlaces y archivos ejecutables, llevar a cabo una capacitación de concienciación para que su personal informe posibles suplantación de identidad o suplantación de identidad; Por último, pero no menos importante, aplicar parches oportunos a sus sistemas operativos y de aplicaciones es fundamental.

En relación con este ciberataque a Travelex, han surgido una serie de temas interrelacionados para discusiones y debates interesantes. Un tema es, ¿se debe pagar un rescate? Europol (Agencia de la Unión Europea para la Cooperación en materia de Aplicación de la Ley) ha declarado regularmente que pagar alimenta actividades criminales. Iniciativas como la "Campaña No Más Rescate" alientan a las víctimas a no ceder ante las demandas de los piratas informáticos. Sin embargo, las empresas podrían gastar mucho más en operaciones de recuperación que en pagar al pirata informático.

Es fundamental que cualquier organización implemente un marco de seguridad cibernética como el publicado por el NIST (Instituto Nacional de Tecnología de Estándares), ya que está destinado a ayudar a las organizaciones a gestionar y mitigar los riesgos de seguridad cibernética.

El NIST Cybersecurity Framework está organizado en 5 funciones:

1. Identificar: desarrollar el entendimiento organizacional para administrar el riesgo de ciberseguridad a los sistemas, activos, datos y capacidades;

2. Proteger: desarrollar e implementar las salvaguardas apropiadas para asegurar la entrega de servicios de infraestructura crítica;

3. Detectar: desarrollar e implementar las actividades apropiadas para identificar la ocurrencia de un evento de seguridad cibernética;

4. Responder: desarrollar e implementar las actividades apropiadas para tomar medidas con respecto a un evento de ciberseguridad detectado; y

5. Recuperar: desarrollar e implementar las actividades apropiadas para mantener los planes de resiliencia y restaurar las capacidades o servicios que se vieron afectados debido a un evento de seguridad cibernética.

Independientemente del tipo y la cantidad de datos que mantiene una organización, siempre hay alguien que está tratando de robarlos. Tener una buena comprensión de las vulnerabilidades y amenazas a las que se enfrentan una organización y sus pares, cómo han cambiado con el tiempo y qué tácticas de piratería se están empleando podría ayudar a preparar a la organización para gestionar estos riesgos de manera más efectiva y eficiente.

Para obtener asesoramiento sobre ciberseguridad en su negocio y operaciones, comuníquese con la oficina de Moore Colombia Edgar Perez en eperez@moore-colombia.co, Adriana Piñango en apinango@moore-colombia.co o Patrick Rozario en patrickrozario@moore.hk.

Por: Patrick Rozario, Moore Hong Kong

Si quieren saber mas sobre nuestras soluciones, herramientas y acompañamiento que podemos aportar a su empresa, no duden en contactarnos.

MOORE

ADRIANA PIÑANGO LATUFF
apinango@moore-colombia.co

OSCAR RODRÍGUEZ
orodriguez@moore-colombia.co

PAOLA SERRANO ROMERO
gestioncomercial@moore-colombia.co


MOORE