CYBERSECURITY
by itwarelatam.com

Edición - N°14

La revista de Cloud Security

NOTA DE TAPA

La protección de los datos es urgente

INFORME ESPECIAL

Tendencias que preocupan a la industria de la salud

MÁS TEMAS

Todo sobre Segurinfo 2022

Mejores prácticas para evaluar riesgos

Los aportes de Blockchain a la nube

Qué es SSLDC

Edición N°14

NOTA DE TAPA

ES URGENTE PROTEGER LOS DATOS

Sumario

La importancia de proteger los datos

Si los datos han pasado a tener una importancia suprema para los negocios —y, porqué no, la vida—, si están siendo el principal insumo, se han convertido en uno de los más importantes activos a proteger. Y de eso se trata el tema de tapa de este número: de cómo protegemos los datos de cualquier evento que los amenace. Y esta vez, además, tratamos el tema desde dos visiones: la de los CISOs y la de los vendors.

Además, la información de salud es un tipo que almacena datos sensibles de la población y, por eso, hay que redoblar los esfuerzos que hay que hacer para protegerlos. De hecho, junto con gobierno y banca, salud ha pasado a ser uno de los principales objetivos de los criminales. Y de eso trata el informe especial de este número.

También le dedicamos varias páginas a Segurinfo, uno de los congresos de Ciberseguridad más importantes de la región que, este año, se llevó a cabo en formato mixto: presencial y virtual lo que, viendo el lado bueno del asunto, permitió que se presentaran referentes de ciberseguridad de varios países del continente.

Más allá de esos temas, abordamos las mejores prácticas en la evaluación de riesgos, veremos qué aportes le ha hecho Blockchain a la protección de la nube y tenemos la segunda parte de la nota sobre Principales riesgos de seguridad de IAM.

Hasta la próxima.

Matías Perazzo
Director Editorial
mperazzo@mediaware.org

Ricardo Goldberger
Contenidos
rgoldberger@mediaware.org

Leonardo Devia
Cybersecurity
Consultant - **CSA**

Suscripciones:
info@itwarelatam.com

Para publicar en este medio:
ventas@mediaware.org
www.itwarelatam.com

Consultar por suscripción anual

Puede leer y descargar la versión digital de esta revista en www.itwarelatam.com.com

Edita, diseña, comercializa y distribuye Mediaware Marketing

Microsoft

¿Ya formas parte de la Academia Genuino?

La ciberseguridad está al alcance de todos, aprende como hacer frente al Ransomware más sofisticado

Muchas empresas siguen eligiendo el software no autentico en lugar del genuino debido al menor costo y a la poca diferencia percibida entre ambos. **El software no genuino carece de las medidas de seguridad** necesarias ante el creciente número de ataques, aquí algunos de sus riesgos más comunes:

- Ciberataques de Malware con Ransomware
- Robo de tarjeta de crédito o datos bancarios
- Daños materiales o de reputación
- Robo de identidad
- Interrupción o continuidad del negocio
- Pérdida de datos importante

Vuélvete experto en licenciamiento de software genuino y protege a tus clientes de los ciberataques con potentes soluciones al alcance de todos.

68% de las PCs sin Sistema Operativo se entregan con una versión no genuina de Windows Pro*

4,000 millones de dólares es el costo estimado de la lucha contra el Malware en las PCs de la empresa*

$663 dólares es el costo medio durante la vida de una PC sin el sistema operativo previsto, en comparación con menos de $100 dólares con el sistema operativo genuino*.

Regístrate aquí

Para ayudarte a proteger los datos de tus clientes con el licenciamiento preferido por la mayoría de las empresas **Fortune 500**

#YoSoyGenuino ¿y tú?

*Informe de IDC, patrocinado por Microsoft. Pague ahora y ahorre después: El argumento para comprar sólo un PC con una versión auténtica de Windows Pro. Documento de IDC #US48882321, agosto de 2021.

ES URGENTE PROTEGER LOS DATOS

Por Ricardo Goldberger

En un mundo tan convulsionado como éste, en el que se desata una guerra que amenaza expandirse por el resto del planeta, sin haber salido completamente de una pandemia, conservar y, sobre todo, proteger nuestros datos —y aquellos de los que somos responsables— se vuelve extremadamente importante.

Desde el punto de vista individual, la privacidad es primordial: se trata de proteger nuestros datos particulares. Pero en cuanto a los negocios, la responsabilidad es doble. Por un lado, la información que pertenece a las empresas y, por el otro, la que pertenece a sus clientes. De ahí que la tecnología, los procesos y políticas y, sobre todo, el usuario, sean los componentes indiscutibles a la hora de proteger los datos.

Hablan los CISOs

Prácticamente todas las compañías conservan, en distintos grados, datos de los clientes, más o menos sensibles según la industria o el segmento en el que se mueven. Y uno de los principales garantes de esta doble responsabilidad son los CISOs o como quiera que se llamen los responsables de la ciberseguridad en una empresa. Por eso, lo primero que les preguntamos es si es distinto proteger sus datos y los de sus clientes.

Proteger a la organización sólo no basta

Andrés Gil, Líder de Servicios de Cyber Risk para Spanish Latin America y miembro del ExCo Global de Cyber Risk de Deloitte responde primero: "Técnicamente la protección se realiza con las mismas tecnologías y procesos, lo que varía es que en función al tipo de dato de clientes que se manejen puede haber requisitos adicionales de seguridad. Por ejemplo, si se manejan datos sensibles de aspectos médicos, se pueden requerir controles y esquemas de seguridad adicionales. Estos requisitos pueden emanar de necesidades de negocio y riesgo, o también de requisitos regulatorios."

Andres Gil

Fabian Muñoz

Por su parte, Fabián Muñoz, CISO de Banco Hipotecario, detalla: "Dejame aclarar que es una frontera muchas veces difusa, en nuestro caso la mayoría de los datos son de nuestros clientes, esos datos son nuestra razón de ser y existir. Ahora bien, puertas adentro de la empresa existe todo tipo de información que debe ser severamente resguardada, que es en muchos casos el candado que protege esa puerta de entrada a los datos del cliente. Allí todo es realmente distinto, porque todo se maneja por escala de atribuciones y segregación funcional, no teniendo nunca ningún colaborador el poder total de acceder a los datos. Para el caso de los datos de los clientes es igual de restrictivo, ya que solo se puede visualizar parcialmente a través de los aplicativos de la entidad y solo ser modificados por los mismos clientes a fin de evitar fraudes internos o modificaciones no validadas."

"Técnicamente la protección se realiza con las mismas tecnologías y procesos, lo que varía es que en función al tipo de dato de clientes que se manejen puede haber requisitos adicionales de seguridad" - Andrés Gil

Andres Felipe Mejia Sanchez

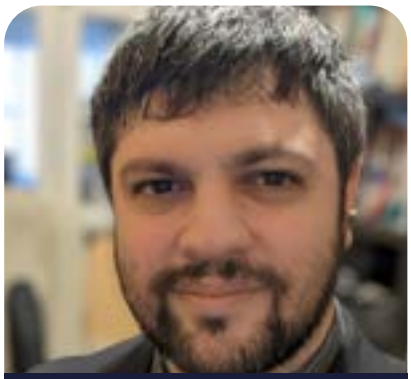
Alain Karioty

Andres Felipe Mejía Sánchez, CISO de Payválida amplía: "Eso lo determina el tipo de dato y el riesgo al que está sujeto, sumándole a esto los requerimientos legales o regulatorios que puedan existir que, para nuestro caso, cobra mucha relevancia la certificación PCI DSS y el cumplimiento de las Leyes de Protección de Datos Personales en cada país donde tenemos presencia. En última instancia los controles pudieran ser los mismos en muchos casos, sin embargo, dependiendo de lo que determine la evaluación de riesgos de dichos datos, se tendrá mayor foco (o inversión) en controles, monitoreo, y reacción frente a unos datos que otros."

Por su parte, Arturo Busleiman, responsable de Ciberseguridad del Ministerio de Relaciones Exteriores, Comercio Internacional y Culto de la República Argentina, sostiene: "Tenemos información vinculada al funcionamiento del estado, pero la más valiosa es la de nuestros 'clientes': los ciudadanos argentinos, así como extranjeros. Si se falla en proteger uno, se falla en proteger otro." Y aclara la diferencia entre el Estado y los privados: "las 'grandes empresas' tienen mayor preocupación por el 'qué dirán', y por eso suelen ni hacer denuncias (que, dicho sea de paso, la ausencia de denuncias es lo que imposibilita que la justicia y las fuerzas de la ley puedan demandar crecimiento en esta materia). Calculo que esta pregunta tiene sentido para aquellos que tienen un mayor interés en las ganancias o en cuidar sus propios... intereses, por usar un término educado."

Amenazas que penden

Gil de Deloitte, observa que "las organizaciones están expuestas a distintas amenazas, incluyendo actores internos (ej. Usuarios maliciosos) y actores externos. En cuanto a volumetrías, los ataques externos son la mayoría e incluyen muy variadas fuentes y características. Ej. Robo de credenciales (casi siempre el primer paso para un ataque), acceso no autorizado, Robo de información, ejecución de malware y/o ransomware, entre otros."



Arturo Busleiman

Para el CISO de Payválida, "en nuestro entorno (Fintech) suele usarse mucha ingeniería social a través de correos de spam que contienen enlaces a sitios de phishing o de descarga de archivos maliciosos que buscan suplantar la identidad de un usuario (comprador). También solemos detectar casi que a diario ataques fuerza bruta y DDoS, algu-

Elias Vucinovich

Para el CISO de Payválida, “en nuestro entorno (Fintech) suele usarse mucha ingeniería social a través de correos de spam que contienen enlaces a sitios de phishing o de descarga de archivos maliciosos que buscan suplantar la identidad de un usuario (comprador). También solemos detectar casi que a diario ataques fuerza bruta y DDoS, algunas de ellas desde Botnets, dada la exposición de nuestros servicios en internet y su funcionamiento 7X24.”

Muñoz, del Banco Hipotecario, también hace hincapié en el phishing, el ransomware, DOS y DDOS. “En la actualidad todos los profesionales en esta materia sabemos que en alguna parte del ciclo vamos a ser atacados —señala—, es por ello que hoy resuena entre nosotros una palabra clave ‘RESILIENCIA’. Ya nos es sólo cómo prevenir o mitigar, sino que lo más importante es cómo vamos a salir victoriosos de este tipo de ataques. Hoy toda la organización está comprometida en este proceso, desde cómo comunicar, cuándo y hasta qué medidas específicas tomar, para estar lo más rápido posible nuevamente online.

En el Estado, Busleiman es tajante: “Se ha hablado mucho de los tipos de amenazas, pero creo que es conveniente hablar de los tipos de problemas que pueden surgir: masivas pérdidas económicas, de confianza, o incluso la manipulación por parte de terceros de las actividades del organismo. La prevención se logra en múltiples capas, y no es deber absoluto de ningún área en particular. La gerencia, ante todo, debe sacar la cabeza de... sus intereses (para volver a usar el mismo término educado), y darse cuenta de que la seguridad NO SE CONSTRUYE con mentiras, u ocultamiento. Lógicamente, postergar cierta información durante una investigación es estratégico, pero ocultarla no hace más que transformarlos en un objetivo más “jugoso” a la vista de los atacantes, ni hablar que es imposible ocultar algo 100%. Pero el miedo los controla. La vergüenza. La mayor inseguridad siempre es por errores humanos.”

Más inteligencia que artificial

El Estado suele ser blanco de ataques muy dañinos, especialmente cuando el eslabón más débil es, justamente, el ser humano, el operador, el usuario. Por eso querríamos saber qué lugar ocupan la capacitación y las políticas de seguridad y la respuesta de Busleiman es precisa: “Top #1 y #2 respectivamente. Pero las políticas también pueden ser usadas en contra de la seguridad. A tal efecto, la revisión, discusión y actualización periódicas son los principales aliados. En la Argentina, el Estado Nacional ha puesto a más de una persona equivocada a cargo de los temas de ciberseguridad. La política y, por lo tanto, los ciudadanos son las principales víctimas. Demasiada burocracia, mucho interés en ‘reescribir’ y tachar lo que se ha logrado. De todas formas, es necesario recordar que la gente que efectivamente trabaja, como decimos, en las trincheras de la ciberseguridad en el Estado Nacional, se comunican y generan comunidad, con sólido intercambio de experiencia, y reduciendo la vergüenza y el ego a aquello que solo los políticos puros, partidarios, no han logrado desterrar.”

Victoria Martinez

No tan distinto es en el ámbito privado. Muñoz explica: "Las Políticas dentro de todas las compañías ocupan un lugar fundamental, son el marco que ordena y da sentido. Ninguna compañía que se precie de tal podría subsistir sin ellas, es importante decir que deben ser cumplidas y cumplibles, a mi entender son dos condiciones indispensables para que surtan el efecto deseado. Ya ahora en el terreno de la capacitación, podemos decir que aquellas compañías que no apuesten fuerte a un modelo de capacitación continua que permita a su personal estar permanente actualizado estarán destinadas a desaparecer o a perder su capacidad de atraer nuevos clientes.

Mejia Sanchez, por su parte, advierte que "las Políticas son uno de los puntos de partida en los modelos de seguridad, pero no dejan de ser un documento de buenas intenciones si no definimos estrategias para aplicarlas. La estrategia más importante es el fomento de la cultura en seguridad a través de las capacitaciones, marketing, foros, blogs, entre otras. Debemos propender a que las políticas y/o prácticas de seguridad se vendan como un beneficio y no como una imposición; como un habilitador para hacer negocios y no como una restricción."

Gil agrega: "[las políticas] son el marco normativo y modelo de gobierno de ciberseguridad; es el paraguas central donde se montan todas las capacidades de una organización. La capacitación en sentido amplio, técnica y de concientización es clave ya que muchas de las debilidades se generan por los propios equipos técnicos y por los usuarios finales por desconocimiento (derivado de la complejidad de los temas de ciberseguridad hoy) o limitada conciencia en temas de ciberseguridad."

La IA al rescate (y qué hacemos después)

¿Es la Inteligencia Artificial tan útil como la quieren mostrar?
Si la IA sirve para algo, será cuestión de que los especialistas nos lo digan.
Gil enfatiza: "Inteligencia artificial, machine Learning y modelos de datos son claves para la detección y respuesta. También se comienzan a utilizar para la definición de priorización de vulnerabilidades, es decir, para establecer qué prioridad se le da a la remediación y mitigación de una vulnerabilidad cuando compite con otras acciones y tareas colisionando con la disponibilidad de recursos"

> "En la actualidad todos los profesionales en esta materia sabemos que en alguna parte del ciclo vamos a ser atacados. Por eso es que hoy resuena entre nosotros una palabra clave: 'RESILIENCIA'" - Fabián Muñoz

Muñoz es más explícito: "La ciberseguridad y la inteligencia artificial están íntimamente ligadas. Hoy por hoy, las tecnologías de IA son altamente utilizadas en la ciberseguridad de todas las empresas, éstas ofrecen como mencionamos en las respuestas anteriores una gran capacidad de hacer posible un escenario de la denominada Resiliencia. En segundo término, la IA también está tendiendo a ser utilizada por ciberatacantes, por lo que claramente para poder tener contramedidas efectivas se hace necesario también utilizarla fuertemente en las empresas. Por último y para concluir, decir tam-

bién que los sistemas de IA no son impenetrables, pueden sufrir ataques, por ello es que también debemos asegurarnos que sean además de efectivos, seguros."

Y Mejía Sánchez aporta al debate al decir que "la IA se ha convertido en la protagonista. Los ataques son cada vez más sofisticados y rápidos de forma que es casi imposible para el ser humano poder gestionar todo oportunamente, o bien costaría mucho esfuerzo y dinero tener un equipo de personas pensando en todos los posibles casos de uso que se pudieran presentar y con precisión. Sin embargo, no es algo que funcione por sí mismo, por lo cual detrás siempre deberá estar ese equipo que ayude y mantenga este tipo de tecnologías y la calidad de los datos que esta utiliza para su óptimo funcionamiento."

Y hablando de equipo, ¿qué hacemos al respecto?

Para Muñoz "no está nada dicho aún, permanentemente surgen ideas y proyectos superadores que contemplan ambos frentes (Hard y Soft) y sin dejar de lado nuestra querida y a veces polémica nube (Cloud Computing) que si bien es cierto también está compuesta de Hard y Soft, incorpora una componente nueva que es la geolocalización de nuestros datos y su correspondiente confidencialidad, integridad y disponibilidad. Creo que el Soft está cumpliendo un papel destacado en esta pelea y que evidencia de ello son los cada vez más sofisticados WAF de BD o APP que se despliegan en las diferentes infraestructuras corporativas. Para prevenir los ataques, Mejía Sánchez propone: "Cultura y esfuerzo mancomunado: Debemos continuar generando mucha cultura tanto en los usuarios internos como en los clientes y participar de la mano de los diferentes sectores (Fintech en nuestro caso) y gobierno, a fin de generar sinergias para combatir el crimen cibernético. Monitoreo de controles: monitoreo proactivo y reactivo a través de nuestro SOC (Security Operation Center),

Hernan Conosciuto

al igual que garantizar el efectivo funcionamiento de los controles tecnológicos a través de testing continuo de seguridad, revisiones y auditorías periódicas. Constante monitoreo del riesgo: Si bien nuestro negocio y mercado evoluciona a una gran velocidad, al mismo ritmo aparecen vulnerabilidades día cero y nuevos vectores de ataque. Aquí juega primordial importancia la relación con la industria, el testing continuo de seguridad en la tecnología que desarrollamos, y la gestión de terceros al tener toda la infraestructura desplegada en la nube.

Busleiman es terminante: "El hardware y software propietarios son los mayores enemigos de la seguridad. Pero el lobby es muy fuerte contra las tecnologías abiertas y libres. No deja de ser, después de todo, una industria."

¿Qué pasa con los vendors?

Identificar riesgos y amenazas

"Existe un riesgo porque hay vulnerabilidades que son atacadas a través de ciertas técnicas de ataque y tienen un impacto que es el resultado" asegura Juan Marino, Regional Sales Manager de Ciberseguridad de Cisco. "Ese impacto en términos de afectación al negocio puede ser mayor o me-

> “El hardware y software propietarios son los mayores enemigos de la seguridad. Pero el lobby es muy fuerte contra las tecnologías abiertas y libres” - Arturo Busleiman

nor y hasta lo podemos cuantificar en algo económico y eso también configura al riesgo.”

“Hay que hacer un diagnóstico bastante profundo de mi ambiente de negocios, de cuáles son mis datos críticos, identificarlos y tener tecnologías y procesos para proteger ese ambiente de las vulnerabilidades que siempre van a existir. Entonces, hay que tener una buena gestión de vulnerabilidades, emparchar todo lo que se pueda y con el riesgo de que siempre van a existir. Tener tecnologías de seguridad que, con los procesos, nos permiten detectar y responder ante las amenazas cuando ocurran” siguió Marino.

Otro enfoque es el de Alain Karioty, VP Latam en Netskope: “Para identificar los riesgos y amenazas que asolan a los datos, lo primero es entender que, en estos momentos, hay más datos y usuarios fuera de la empresa que dentro, por lo que el perímetro ya no es un lugar, sino que se ha diluido. Por lo tanto, se hace necesario un nuevo perímetro que integre la nube, que haga un seguimiento de los datos y que los proteja, allá donde vayan.”

“Hay muchas maneras de detectar estos riesgos de seguridad —afirma Victoria Martínez, Business Development Manager en AI Projects de Red Hat— pero antes de entrar en ese detalle siempre tratamos de buscar la manera de mitigar estos puntos, por eso es la importancia de mantener actualizadas todas las versiones de middleware y software, en sus versiones estables. Ahora bien, considerando que este aspecto está mitigado, hay muchos modelos que se están usando para detectar preventivamente cuándo te podrían estar atacando, no tan sólo cuando está sucediendo sino de manera preventiva, entendiendo patrones y comportamientos. Es decir, uno entrena estos guardianes específicos de acuerdo a la frontera que estemos cuidando, en base a logs de red, y el entendimiento de estas trazas. Todo depende en que capa estemos parados.”

Marino continúa haciendo foco en el negocio: “Si tengo una vulnerabilidad y es atacada pero me cuesta muy poco, el riesgo es bajo, si en cambio me cuesta mucho dinero entonces el riesgo es muy alto.”

Y Karioty añade, más genéricamente, que “es importante comprender los flujos de datos, esto es, saber dónde residen, conocer sus distintas categorías y entender el perfil de la aplicación en la nube para decidir qué controles son necesarios. Las organizaciones deben realizar evaluaciones de seguridad continuas en torno a sus flujos de datos.”

Martínez, a su vez, usa la analogía: "También hay un aspecto muy importante que complementa a estos ataques y tiene que ver con conductas que son identificables, y que dependen de nosotros mismos. Por ejemplo: Podemos hacer la relación con la seguridad de una casa, si yo dejo las puertas abiertas ventanas y todo lo que tiene valor a la vista, en una zona donde no es segura, es muy probable que incremente los riesgos y sea atacado. Entender y aplicar con consciencia estas prácticas realmente mitigan muchos ataques que son simples, cómo dónde uno deja las contraseñas, hacer uso de los dobles y triples factores de autenticación que se usan para que puedan dar garantías que es la persona autorizada la que está operando. Incrementar medidas, con tecnología mitiga, pero no elimina el riesgo."

De adentro y de afuera

Las amenazas a los datos pueden venir tanto de afuera de la compañía como de adentro, accidental o intencionadamente y la problemática es, entonces, si hay alguna diferencia en protegerse de las amenazas internas o externas.

Para Marino "es diferente y en sí mismo podríamos abrir categorías, ya que hay distintos tipos de amenazas internas y externas también. Para cada tipo de amenazas hay distintas maneras de protegerse, de detectar y de responder."

Karioty, en un punto, disiente: "De entrada, no tendría por qué ser distinto, aunque es cierto que muchas empresas están mejor preparadas, tecnológica y mentalmente, para repudiar una amenaza externa que una interna."

Hernán Conosciuto, Arquitecto Principal de Soluciones en Red Hat sostiene que "en general la principal diferencia es que las empresas tienen el 100% intentando detectar amenazas externas y mucho menos foco sobre las internas. Esto sumado a la cantidad de fuentes que existen hoy día (celulares, tablets, notebooks, etc.) que se conectan a la red y, debido a la pandemia, el trabajo remoto con muchas veces máquinas que no cuentan con un compliance en seguridad, hace que sea mucho más factible este tipo de amenazas internas."

Vuelve Marino a explicar con más detalle: "La exfiltración de datos se puede dar por distintos motivos inclusive puede ser interno sin quererlo hacer, por accidente de un usuario que no haya sabido que estaba mal para las políticas de la empresa… ahí no tenés un ataque externo, tenés a alguien que se llevó información confidencial a un servicio online de almacenamiento de datos. Por otro lado un atacante puede ingresar con algún vector de ataque con el que logran penetrar, por ejemplo un phising, pero eso es solo el comienzo para comenzar un ataque a la organización, desde ahí el atacante puede hacerle un trabajo de exfiltrar datos, es entonces un usuario externo el que logró un control de la infraestructura y que, tomando provecho de las vulnerabilidades o la falta de protección que tiene esa infraestructura, es capaz de llevar información hacia afuera cuando eso no debería estar permitido."

"Ambos tipos de amenazas, tanto internas como externas —declara, tajante, Elías Vucinovich, Arquitecto de Soluciones de Seguridad de Logicalis Argentina,—, deben protegerse con la misma intensidad. Es correcto que un tipo de amenaza externa debe seguir ciertos pasos adicionales para poder obtener más información que una amenaza interna. Seguir esquemas de seguridad basados en Zero Trust, robustecer el perímetro, microsegmentación y visibilidad son fundamentales para protegernos tanto de amenazas externas como internas.

Karioty advierte: "Una vez más, es imperativo que las empresas se replanteen su estrategia de control orientada a amenazas internas y que no sigan basando su seguridad en herramientas tradicionales, como proxies y firewalls, que no son capaces de decodificar el lenguaje de las aplicaciones cloud que utilizan los empleados, y que no permiten cubrirles en movilidad. Es el momento de renovar los gateways de acceso a Internet con una verdadera plataforma unificada SASE, disponible cerca de los usuarios, siempre."

De los dos lados

Casi todas las empresas —por no decir todas, como dijimos antes— tienen una doble responsabilidad: proteger sus propios datos y los de sus clientes. Para algunos, es lo mismo, para otros hay diferencias.
Vucinovich es tajante: "No considero que sea distinto o diferente. Las técnicas de seguridad sobre la protección de los datos son aplicables tanto para datos de la empresa como para datos de los clientes. El impacto negativo derivado de una falta de protección de datos, tanto datos de la empresa como datos de los clientes, es grande."

Karioty concuerda: "Son datos sensibles ambos, por lo que la protección debe ser igual, sobre todo ahora, que están en movimiento. En este sentido, las investigaciones de Netskope Threat Labs revelan que los datos sensibles se mueven cada vez más lateralmente a través de las aplicaciones en la nube, como por ejemplo desde Microsoft Teams a OneDrive o SharePoint, por lo que los departamentos de seguridad de TI necesitan una mayor visibilidad y, posteriormente, un mayor control sobre los datos entre las aplicaciones e instancias en la nube, independientemente del método de acceso que empleen los usuarios."

Marino también coincide: "Los principios para la protección son similares. Es imposible proteger todo por igual, entonces una de las premisas en una estrategia de ciberseguridad es justamente identificar cuáles son los datos sensibles y poner los esfuerzos donde está el mayor riesgo" pero, además, aclara: "no es lo mismo proteger un archivo de trabajo que no tiene información confidencial que proteger información de mi cliente donde hay información sensible en cuanto a su identidad, transacciones, etc. Son dos tipos de información diferentes que primero hay que poder clasificarlas y luego implementar controles diferentes.

> "No tendría por qué ser distinto, aunque es cierto que muchas empresas están mejor preparadas, tecnológica y mentalmente, para repudiar una amenaza externa que una interna."
> - Alain Karioty

También habría que preguntarse hasta qué punto las regulaciones (GDPR, CCPA) facilitan o complican la prevención, defensa y/o remediación. Vucinovich es terminante: "Son regulaciones que ayudan a la prevención y, sobre todo, a la defensa de los datos. Son una excelente y reconocida guía a seguir para poder estable-

cer arquitecturas seguras y mejores métodos de prevención, defensa y remediación."

Karioty desarrolla: "El objetivo principal de regulaciones como GDPR o CCPA es proteger los datos sensibles y la información personal, aumentar la responsabilidad y simplificar el entorno normativo para las empresas, entre otras. Por lo tanto, desde el punto de vista de la seguridad, considero que ambas leyes suponen un elemento positivo, ya que las empresas dispuestas a aceptar la regulación mejorarán sus estrategias de protección de datos. Iniciativas como GDPR o CCPA proporcionarán un impulso adicional a las organizaciones para que no solo controlen sus estándares de protección de datos, sino que busquen la innovación en protección de datos."

Hay cuestiones que son muy importantes y que, al decir de Marino, implican que las empresas "pongan sus esfuerzos en donde más se sienten urgidos y uno de los motivos por los cuales van a decidir invertir e implementar esfuerzos de seguridad es porque tienen alguna exigencia que ante el no cumplimiento implica una pena, una multa por no cumplir." Y desarrolla: "El hecho de seguir una serie de requerimientos para poder cumplir con una regulación implica que se hicieron los deberes, uno por lo menos cumple esto y, por consecuencia, desde la óptica de la ciberseguridad, esto te debería facilitar la situación. Ahora, desde la óptica de la empresa u organización no deja de ser una complicación porque tienen que ver de qué manera adaptan su infraestructura, sus arquitecturas, sus procesos para poder cumplir y deben hacerlo pero como a veces las regulaciones son las mismas para todos pero las empresas no son iguales es posible que a alguna empresa le resulte más complejo y disruptivo implementar ciertos controles que son iguales para todos y que no necesariamente significa que la manera en se están protegiendo no es la correcta."

Martínez, por su parte, hace foco en el usuario: "Como usuaria si desconozco mis derechos en el mundo digital es muy probable que "regale" lo que tiene mucho valor "mis datos" y no entienda el poder de la privacidad. Lo que entra en internet no se borra más, por eso la educación, la conciencia las buenas prácticas son el "talón de Aquiles" en los fraudes y amenazas que se viven en el mundo digital. Siempre hay que trabajar fuertemente en este aspecto."

> "Hay un cambio cultural, ya que el área de sistemas dejó de ser responsable de la ciberseguridad y pasamos a serlo todos los usuarios de la empresa." - Hernán Conosciuto

Capacitación, políticas y el recurso humano

Marino comienza respondiendo acerca del papel de la capacitación y las políticas: "No todo se resuelve con tecnología y por eso hay que entender que la empresa son usuarios y ellos son un eslabón clave dentro de la ciberseguridad, porque si alguien hace algo indebido está comprometiendo a la empresa, entonces hay que educar al usuario en qué es lo que puede hacer y qué es lo que no, qué representa un riesgo, cómo detectar ciertas amenazas que generalmente llegan por correo (hoy en día estamos bastante familiarizados con las campañas anti phishing). Pero bueno, es algo que es constante, el usuario no aprende de un día para el otro y suele cometer errores entonces

tiene que ser parte de una estrategia y un plan en donde yo tengo que ir midiendo el nivel de consciencia y educación de los usuarios para ir haciendo correcciones y eso es clave para minimizar el riesgo. Y bueno, las políticas van de la mano de esto."
Conosciuto destaca que el tema de la ciberseguridad implica "un cambio cultural que se viene gestando desde hace unos años, ya que dejó de ser responsable el área de sistemas en cuanto a la ciberseguridad y pasamos a serlo todos los usuarios de la empresa. Para esto y que el usuario conozca los riesgos a los que puede exponer los datos, es sumamente necesaria una educación periódica. Hay vastos ejemplos de bloqueos de páginas para evitar problemas de ciberseguridad que terminaron ocasionando problemas reales en ese aspecto. Por eso, los usuarios deben conocer las políticas y normas de seguridad, qué implica el no cumplirlas, pero por sobre todo, ser educados regularmente para que ellos tengan un rol activo en lo que es la ciberseguridad."

Vucinovich sostiene que "la capacitación, de la mano de la concientización y la aplicación de políticas claras y estrictas" es un pilar fundamental y que "la Inteligencia Artificial ayuda a los especialistas de seguridad a prevenir las amenazas. Tecnologías de Inteligencia Artificial analizan y correlacionan archivos maliciosos, direcciones IP sospechosas o atacantes en segundos o minutos. Con estos datos previamente analizados, los especialistas de seguridad pueden tomar las decisiones adecuadas para poder mitigar las diferentes amenazas." Karioty, a su vez, da a entender que "además de implementar políticas y establecer planes de formación y de capacitación, es fundamental replantearse la estrategia de seguridad. Tanto si la nube entra en la empresa a través de grandes proyectos de transformación empresarial, como si lo hace a través de una aplicación descargada en un dispositivo no gestionado, no es algo que los equipos de seguridad puedan ignorar. Una estrategia SASE —con sólidos principios de confianza cero— puede detectar lagunas de seguridad y automatizar una corrección, o instruir a los empleados cuando se identifican comportamientos inadecuados de alto riesgo, haciendo que el papel de los responsables de seguridad sea menos reactivo y más proactivo."
"La IA puede ser utilizada para la búsqueda proactiva de bugs y "agujeros" en el software —define Conosciuto—. Además, la IA aplicada con la automatización puede eliminar la variable del tiempo ante una reacción provocada por un evento de ciberseguridad (que hoy día muchas veces sigue siendo una acción humana y manual) y de esta manera actuar evitando o reduciendo el riesgo que la amenaza representa."

"La Inteligencia Artificial es, sin duda, importante —remarca el ejecutivo de Netskope—. Por ejemplo, la eficacia de las herramientas de prevención de fuga de datos (DLP) puede mejorarse aún más con capacidades avanzadas como la coincidencia exacta de datos, el fingerprinting y

el reconocimiento óptico de caracteres (OCR) para detectar datos sensibles en imágenes. Aplicar DLP después de emplear controles de identidad y de aplicaciones, disminuye drásticamente su tasa de falsos positivos y libera ciclos para otras iniciativas de seguridad y protección de datos. Además, en esta fase se pueden aplicar técnicas innovadoras de escaneo y clasificación mediante capacidades de aprendizaje automático (ML). Los datos sensibles se ocultan cada vez más en las imágenes y se filtran a través de ellas, por lo que el escaneo mejorado por ML puede detectar y clasificar de forma fiable las imágenes que pueden contener datos confidenciales, como capturas de pantalla, diagramas de pizarra y documentos oficiales como por ejemplo pasaportes. En última instancia, también aumenta la precisión de la detección y reduce los falsos positivos para su motor global de DLP.

Juan Marino

" Pero Marino puntualiza que la Inteligencia Artificial "más que un término es un concepto, una capacidad de la que ya se viene hablando hace muchos años. A mí me da la sensación de que son de esas cosas que se las toma como muy a la ligera o como algo mágico. La realidad es que hoy por hoy, mirando el nivel de madurez de las empresas, estamos lejos de ver que haya una IA que resuelva todo, o sea, que detecte y responda. Hay un componente clave que es el humano y los procesos que, si no están bien implementados, la tecnología sola no va a impedir que me ataquen y que logren su objetivo de robar información o lo que sea. Sí hay una evolución muy favorable en las distintas tecnologías de ciberseguridad incorporando capacidades de lo que podemos llamar IA que, valga la redundancia, hacen que estas tecnologías sean más inteligentes y que requieran cada vez menos de procesos manuales por parte de un operador". Y concluye: "Cuanta más inteligencia me traiga la tecnología, mejor. pero aún estamos lejos de pensar que compro una solución tecnológica y que reemplazará al ser humano. No sé si llegará algún día, pero hoy al menos no estamos en ese lugar."

"Tenemos la responsabilidad de proteger los datos de los clientes"

Por Mauro Graziosi - CEO - SMARTFENSE

Mauro Graziosi
CEO - SMARTFENSE

¿Es distinto proteger las amenazas externas de las internas, por ejemplo, la exfiltración?
Sí, porque a las amenazas internas las tenemos mucho más controladas y podemos además producir cambios. Se puede tanto trabajar tanto en el control como en la prevención de una manera mucho más directa.

¿Es distinto proteger los datos de la empresa que los datos de los clientes?
Sí, porque el rol que tomamos es diferente entre encargado y responsable, además porque saben llevar distintos flujos de información.
Por otro lado, mientras que tenemos una responsabilidad de proteger los datos de los clientes por cumplimiento, los datos de la propia empresa son los que permiten alcanzar los objetivos de negocio (aunque una fuga de datos de clientes también puede hacer que los objetivos no se alcancen).

¿Qué lugar ocuparían la capacitación y las políticas?
Deberían estar en primer lugar, pero no lo están aún.
Las organizaciones en muchos casos aún tienen líderes técnicos en la protección de la información, por lo que los controles se terminan sesgando hacia aspectos tecnológicos. Sin embargo, se empieza a ver un balance entre controles técnicos, de gestión, legales y sobre los usuarios finales (concientización). En tiempos donde el personal está muy distribuido, deberían estar en el core de la estrategia la concientización y las políticas claramente comunicadas y aceptadas.

¿Hasta qué punto las regulaciones (GDPR, CCPA) facilitan o complican la prevención, defensa y/o remediación?
Yo creo que ayudan porque cada organización pone foco en algún punto de su mayor interés, pero estas normativas ayudan a tener una visión diferente sobre la protección que termina siendo complementaria.
Además implica poner en su lugar procesos específicos que fortalecen otras medidas.

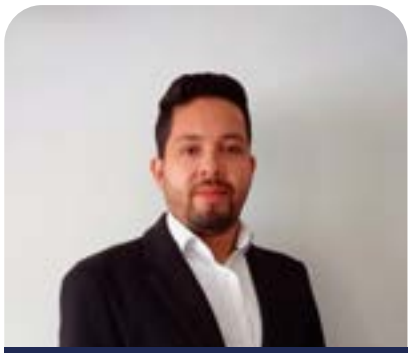
¿Qué lugar ocupa u ocupará la Inteligencia Artificial en prevención, defensa y/o remediación?
Si bien creo que es útil, es una tecnología que está teniendo más relevancia de la que en realidad ha demostrado aportar. Siendo útil para aliviar trabajo operativo en el análisis de logs por ejemplo, pero que no debe considerarse necesariamente mejor en todas las fases de la protección. Hay muchos casos donde una organización pequeña o mediana puede sentirse demasiado generalizada por ejemplo, más que todo si no tiene el volumen de información necesario para generar patrones de comportamiento.
¿Qué nueva tecnología o herramienta proponen para prevención, defensa y/o remediación?
Tecnologías vinculadas a la detección temprana de OSINT (Open Source INTelligence) contra la empresa y a la respuesta rápida ante ataques de ingeniería social.

Nueva imagen, Misma esencia.

Gestiona el riesgo
más relevante
con un proceso de
Hardening de usuarios

Una ciberdefensa corporativa exitosa

Por Diego Andrés Cepeda Jiménez, Presales Specialist, Softline



Diego Andres Cepeda
Presales Specialist - Softline

En 2021, el 41% de las organizaciones no pudo resguardar adecuadamente los datos de sus trabajadores. Si bien las empresas se enfrentan constantemente a la filtración de datos, no es un secreto que muchos de estos incidentes jamás se publican, ya sea por un tema de reputación o de protección hacia los mismos cibercriminales, que se enterarían de que la compañía se encuentra vulnerable.

Una ciberdefensa corporativa exitosa sólo se logra —de acuerdo con los especialistas de Softline, un proveedor global de soluciones y servicios de transformación digital y ciberseguridad, con sede en Londres— con una identificación previa de los riesgos y amenazas a los que se puedan enfrentar, ya sea con los datos que manejan internamente o con los que comparten con externos; además, hay que saber quiénes deben tener acceso a estos datos que se comparten necesariamente.Para comenzar con el análisis de cuáles son las principales vulnerabilidades en una empresa, que permitan una pérdida de datos, se debe empezar por una revisión de las aplicaciones que manejan los empleados. En un 60% el área de tecnología no tiene control de estas aplicaciones, de ahí que se generen un número considerable de riesgos. Estas aplicaciones no controladas solicitan a los usuarios información confidencial, credenciales y demás datos que, en muchas ocasiones, se utilizan para vulnerar los sistemas empresariales. Por eso se recomienda identificar estas aplicaciones que generan riesgo para posteriormente aplicar un CASB, y luego ejecutar una revisión de las identidades de los usuarios, como ingresan, que tipo de caracteres se les solicita, cada cuanto cambian las contraseñas, desde que dispositivos normalmente ingresan los usuarios, etc. Todo lo anterior nos facilita identificar si realmente los usuarios que se autentican son los correctos, si los datos a los que acceden están permitidos e incluso saber desde qué ubicación geográfica están consultando estos datos.

empresa y a la respuesta rápida ante ataques de ingeniería social.

Las contraseñas son un sistema de protección, pero en muchas ocasiones los criminales se las ingenian para averiguarlas. Para evitar esto Softline —compañía con 8200 empleados en casi 60 países— recomienda utilizar métodos de doble factor de autenticación e identificación de identidades. Otro proceso para reconocer las fallas de seguridad hacia nuestros datos es saber con quiénes se comparten, qué contienen los documentos, archivos, imágenes y demás. Si una empresa no aplica una política de prevención/fuga de pérdida de información no tiene control sobre ella. Debe quedar bien claro qué se comparte al interior de la empresa o al exterior. Incluso considerar que no todas las áreas de las organizaciones deben consultar estos datos; es importante aplicar una segmentación rigurosa y un etiquetado correcto para evitar que personas no autorizadas manipulen datos sensibles para la compañía.

mediaware MARKETING

Servicio 360
MARKETING Y VENTAS

Especializado en Tecnología y Consumo

- **MEDIOS DE COMUNICACIÓN**
- **DISEÑO INTEGRAL**
- **MARKETING DIRECTO Y SOLUCIONES DIGITALES**

Desarrolle su **PLAN** con **NOSOTROS**

mediaware.org

CIBERSEGURIDAD: LAS TENDENCIAS QUE PREOCUPAN A LA INDUSTRIA DE LA SALUD

Por Rocío Bravo

El sector de la salud es uno de los que más han debido apostar a la digitalización. El aumento en la inversión da cuenta de ello. Y en línea con eso, también los riesgos que eso implica desde el punto de vista de ciberseguridad han crecido. De hecho, junto con gobierno y banca, salud ha pasado a ser uno de los principales objetivos de los criminales. ¿Cómo abordar esta problemática?

"El de la salud es un sector que está cada vez más en la mira de los ciberdelincuentes por la sensibilidad de la información que maneja, el crecimiento del uso de herramientas de IoT y aplicaciones como Telemedicina con una fuerte dependencia tecnológica lo que aumenta considerablemente el espectro de ataque", analiza Herman Maseberg, Gerente de Seguridad Informática de Swiss Medical. Desde DigiCert comparten lo siguiente:

Los ataques de ciberseguridad pueden interrumpir la prestación de servicios sanitarios, afectando a la seguridad de los pacientes. Hoy, la pregunta ya no es si una instalación determinada será atacada, sino cuándo. Las consecuencias pueden incluir la reprogramación de citas y cirugías, el desvío de vehículos de emergencia o el cierre de unidades de atención e incluso de organizaciones enteras. Por lo que responder a estos riesgos requiere no solo un programa de seguridad sólido para evitar que los ataques lleguen a dispositivos y sistemas críticos, sino también un plan para mantener la atención al paciente cuando lo hacen.

Más de cinco años después de conocer el ransomware Wannacry, quien paralizó las infraestructuras médicas y otras organizaciones en todo el mundo, el sector salud parece estar aprendiendo su lección, ya que la cantidad de dispositivos médicos atacados (computadoras, servidores y equipos médicos) en 2022 disminuyó en todo el mundo.

Sin embargo, dice Diego Andres Cepeda Jimene, Presales Specialist de Softline, esto no significa que los incidentes en ciberseguridad no se sigan presentando en las entidades de este sector. "Por

ejemplo, en el 2020, mientras los sistemas de salud de todo el mundo cedían ante la tensión de la pandemia de COVID-19, también tuvieron que sufrir las acciones de los atacantes.
Una de las amenazas más significativas para las instituciones médicas durante el año pasado fueron los ataques de ransomware, en los que los cibercriminales cifraban los datos o extorsionaban a los directivos con la amenaza de publicar los archivos robados.

Bruno Toldo

Se estima que el número de ataques contra dispositivos de entidades médicas en regiones donde hasta ahora se implementan procesos de digitalización de la infraestructura aumentará significativamente en los próximos años. Al igual que la investigación médica es supremamente costosa y algunos grupos criminales de APT (Amenaza persistente avanzada) especializados se encargarán de arremeter contra estas instituciones con mucha frecuencia en los próximos años.

Bruno Toldo, Chief Medical Information Officer de Infor Latin America, plantea: “Los principales riesgos de ataques son: ransomware, malware, phishing y los DDoS, que son los ataques de negación de los servicios distribuidos. Las principales acciones que vuelven a las empresas más vulnerables son: uso de contraseñas débiles, softwares desactualizados, uso de softwares sin licencia (piratas), uso de redes inseguras, invasión de malwares y falta de patrones en el intercambio de información”.

En este sentido, “los principales riesgos para las empresas son: daños financieros, pérdida de credibilidad en el mercado con riesgo de pérdida de imagen de la marca, exposición de información confidencial de la empresa y de sus clientes, pago de multas por violaciones de la ley general de protección de datos en el área de salud y, en el peor escenario, riesgo para el paciente. Es por eso, que la atención de toda la estructura tecnológica y de las personas es fundamental en el sector de salud”.

“En una industria que se está digitalizando rápidamente con la cantidad de información personal almacenada y transferida electrónicamente, esto está abriendo nuevos canales de ataque para los

Emerson Machado

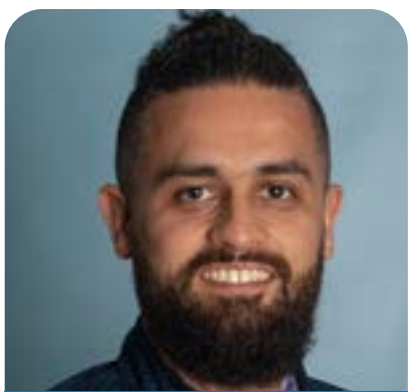
ciberdelincuentes que buscan nuevos puntos débiles para explotar”, dice Stephen Fallas, Cybersecurity Architect Strategist LATAM Territory de Trellix. “Y es probable que un ataque cibernético al sector salud ocurra por una de dos razones: para acceder a las historias clínicas electrónicas para vender en el mercado negro o para secuestrar sistemas e impedir el acceso hasta que se pague un rescate”.

A partir de ello, sigue, “el desafío es claro: el sector de la salud debe desarrollar estrategias cibernéticas más sólidas y dinámicas si quiere mantenerse a la vanguardia del panorama de amenazas globales en rápida expansión”.

Según Emerson Machado, Security Sales Executive for Latin America en Dell, “estamos en un momento en el que cualquier compañía puede pasar por un ataque cibernético con un impacto en sus operaciones. Los cibercriminales tienen la capacidad de atacar, infiltrarse silenciosamente y planear un ataque destructivo, generando un impacto financiero gigante. Los sectores de salud están entre los top 3 segmentos objetivo de los criminales que utilizan principalmente la “capacidad de pago” para enfocar los ataques”. Por eso mismo, sigue, “ para los líderes de seguridad en salud es clave aumentar considerablemente las inversiones en tecnologías para protección y prevención”.

“La creciente cantidad de datos que se tiene de los pacientes sumado a las posibilidades de mejorar la experiencia de las personas a través de un adecuado uso de los mismos, genera un mayor valor para las empresas del sector salud y por lo tanto más interés por parte de atacantes”, agrega Camilo Gutiérrez Amaya, Jefe del Laboratorio de Investigación de ESET Latinoamérica. “Por esta razón, es necesario pensar la operación desde la seguridad para garantizar la privacidad e integridad de los datos”.

Según el experto, poder reaccionar a un incidente de seguridad es uno de los mayores desafíos para cualquier empresa, sobre todo cuando se trata de un ataque para extraer información sensible. “Contar con tecnologías que permitan un monitoreo de la infraestructura para tener una respuesta proactiva es la mejor opción para detectar las señales que pueden



Camilo Gutiérrez

Pablo Rodríguez Romeo

llevar a detectar una intrusión. Pero además de tecnología es necesario conocer cómo operan este tipo de ataques, ya que cuando los ciberdelincuentes logran acceder a la red de una empresa y robar datos sensibles de los pacientes, es usual que además de vender o publicar los datos sensibles ejecuten algún otro componente malicioso, como un ransomware, buscando un mayor impacto y generando una necesidad más grande para pagar y restablecer las operación normal”.

¿Por dónde empezar?

“Sin ninguna duda, toda estrategia de ciberseguridad debe empezar por la prevención, y para esto la capacitación/ concientización es fundamental”, destaca el Ing. Pablo Rodríguez Romeo, Perito

Informático Forense, especialista en Seguridad, Socio del Estudio CySI de Informática Forense. “Podemos tener el mejor equipamiento instalado y en funcionamiento, el mejor hardware, pero si no tenemos capacitación/concientización tanto de quienes administran esos equipos, los especialistas en Seguridad, como del personal en general, cualquier estrategia de prevención se vuelve débil. La capacitación y concientización del personal es el punto de partida de cualquier estrategia que se piense de manera exitosa, considerando a todos los colaboradores, desde el más básico hasta el más especializado”.

“El punto de partida para establecer una estrategia de seguridad es contar con un equipo que conozca el funcionamiento del negocio, la infraestructura tecnológica que soporta la operación y su visión de crecimiento”, complementa el vocero de ESET. “Este trabajo articulado permitirá implementar los mecanismos de gestión más adecuados para cada empresa y las tecnologías que habiliten la operación. Cualquier estrategia de ciberseguridad se debe pensar como dinamizadora del negocio y no como un obstáculo; ya que pensar en seguridad desde el diseño va a permitir evitar incidentes futuros y garantizar la continuidad del negocio en caso de un incidente”.

Sumado a ello, dice el ejecutivo de Infor, “es necesario crear un plan de respuesta con una lista de escenarios y acciones probables que se tomarán, con división de las funciones de los equipos, una metodología clara para la colecta de pruebas legales y un plan de comunicación detallada para las partes relevantes tanto público interno como externo, con el objetivo de tener control sobre las informaciones y disminuir daños”.

Stephen Fallas

“El sector salud puede proteger mejor su infraestructura cibernética de ciberataques al adoptar un enfoque holístico”, asegura el ejecutivo de Trellix. “Esto inicia a través de un proceso arquitectónico unificado que considere todos los elementos tecnológicos de manera integral contra todas las amenazas potenciales es el primer paso para crear una infraestructura cibernética más resistente. Invertir en estrategias proactivas de detección y respuesta extendida permite protegerse contra la creciente ola de amenazas dirigidas”.

Con el fin de proteger la información de los pacientes y su negocio, es necesario combinar herramientas de seguridad rentables y altamente efectivas con las mejores prácticas de ciberseguridad tanto a nivel de TI como de los empleados. Un personal bien informado junto con un programa robusto y automatizado de ciberseguridad y control de amenazas, reducirá el impacto de los ciberataques a partir de la prevención y la detección temprana, aún estamos a tiempo de construir una cultura que nos permita prevenir cualquier inconveniente en materia de seguridad digital.

¿Cómo contrarrestar la evolución de los ciberataques en salud?

Por Diego Andres Cepeda Jimenez, Presales Specialist de Softline

Más de cinco años después de conocer el ransomware Wannacry, quien paralizó las infraestructuras médicas y otras organizaciones en todo el mundo, el sector salud parece estar aprendiendo su lección, ya que la cantidad de dispositivos médicos atacados (computadoras, servidores y equipos médicos) en 2022 disminuyó en todo el mundo.

Esto no significa que los incidentes en ciberseguridad no se sigan presentando en las entidades de este sector. Por el contrario, se estima que el número de ataques contra dispositivos de entidades médicas aumentará significativamente en los próximos años.

En el sector de la salud los ataques son más dañinos que en las demás industrias, el costo promedio de un ciberataque en el sector a nivel de pérdida de negocio, gastos de prevención, detección y recuperación pueden estar alrededor de los 7.13 millones de dólares en comparación a los 3.86 millones que, en promedio, cuestan los ciberataques en cualquier otra industria. A esto podemos agregar que los datos que maneja el sector son confidenciales y extremadamente sensibles. Por lo tanto, el impacto no material es demasiado grave.

A medida que la tecnología se vuelve más sofisticada y compleja, los ciberdelincuentes están en búsqueda del personal como puntos de entrada a su infraestructura, por lo tanto, es indispensable formar el capital humano de las entidades de salud y esto no solamente recae para el área de tecnología o ciberseguridad, se debe aplicar a todos los colaboradores de estas entidades desde la persona de la portería, recepcionistas, contadores, médicos, enfermeras, gerentes etc.

Diego Andres Cepeda

Presales Specialist Softline

Para iniciar con una buena asesoría es pertinente desarrollar una estrategia de preventa y de consultoría con el fin de tener la información necesaria de la organización en cuanto a infraestructura de centro de datos ya sea en nube o física, modalidad de trabajo de los empleados, herramientas o aplicaciones que utiliza la entidad, nivel de respuesta frente a un incidente, sistemas de backups, entre otras preguntas, son necesarias para dimensionar de manera eficiente las necesidades de la empresa. Todo esto se garantiza con el grupo de especialistas en redes, aplicaciones y ciberseguridad de Softline.

Después de recolectar esta información se procede a desarrollar diferentes escenarios donde se recomendarán las soluciones y servicios acorde con las necesidades que nuestros expertos identifiquen. Las soluciones que se presentan son plataformas de protección endpoint (EPP), seguridad de red (NGFW, IPS, ATP), seguridad en la nube (CASB), canales de comunicación seguros (VPN), movilidad segura (MDM, EMM), seguridad del correo electrónico y del tráfico web, entrenamiento/auditoría del personal (awareness), protección de datos (DLP), control de acceso (IDM, PAM, PIM, 2FA), encriptación de datos, seguridad de las aplicaciones, seguridad de las aplicaciones (WAF) y gestión de incidentes (SIEM, IRP). Los servicios disponibles incluyen security operation Center (SOC), estándares industriales, gestión de riesgos, cumplimiento de las leyes (152FZ, GDPR,STOBR, 382P. 683-684P. 187FZ), ethical Hacking, análisis de vulnerabilidades, hardening de Infraestructura, análisis de código, servicio administrados de seguridad, Auditoría de cambios, control de integridad, comprobación del código, gestión de configuraciones, pruebas de penetración (pentest).

En resumen, contamos con todos los recursos técnicos y experiencia para garantizar una infraestructura de confianza cero, que requieren las entidades de salud para garantizar la protección de sus datos.

> “No confíe en nadie, compruébalo todo. Para que esto ocurra, todos deben hacer parte de la creación de un ambiente ciberseguro”

Cómo preparar a las organizaciones ante el auge de la telemedicina

Por Miguel Llerena, Vicepresidente de Tanium para Latinoamérica

La atención médica siempre ha estado en la lista de los atacantes cibernéticos ya que los proveedores del sector administran datos de pacientes muy confidenciales que valen mucho dinero en la Dark Web, lo que significa que existe un gran incentivo económico para robar datos relacionados con la salud.

Otro factor altamente crítico de las redes hospitalarias, es que los atacantes saben muy bien que muchas instituciones de salud pagarán rescates porque no pueden permitirse el tiempo de inactividad de la red, ya que podría tener consecuencias de vida o muerte. Sumado a esto, la pandemia contribuyó a que la atención médica sea un objetivo aún mayor con muchas organizaciones de atención médica todavía al límite como resultado de un aumento en los pacientes. Frente a esto, es comprensible que la TI y la ciberseguridad pasen a un segundo plano frente a la atención al paciente.

La telesalud despegó y su uso se multiplicó enormemente en el primer año de COVID-19. Esto implica aún más peligro, principalmente porque todavía es relativamente nueva. Y si bien las organizaciones y los proveedores de atención están tratando rápidamente de formalizar las mejores prácticas, existe una curva de aprendizaje pronunciada. De hecho, el 30 por ciento de los proveedores de telesalud admitieron que algunos de sus médicos han visto comprometidos los datos de los pacientes al realizar sesiones remotas. A medida que se desarrolla este proceso, es muy posible que los atacantes vean una oportunidad para explotar las debilidades potenciales.

El mayor desafío es que descentraliza la red hospitalaria. Asegurar un entorno hospitalario único y centralizado ya era una tarea difícil, pero ahora el hospital se ha movido a los hogares de las personas. La superficie de ataque pasa a ser mucho más extensa con los nuevos dispositivos y aplicaciones que se utilizan en la sede del hospital, la nube y ahora en los hogares, hay muchos más puntos de entrada potenciales para los atacantes.

De acuerdo a cifras del Instituto Ponemon, 60% de las organizaciones del sector señalaron que fueron violadas como resultado de una vulnerabilidad sin parchear, situación que tarda alrededor de 12 días coordinando parches entre equipos para enfrentar las vulnerabilidades, lo cual evidencia que mantener los datos seguros, abordar los mandatos de cumplimiento y mantener los estándares de higiene de TI, es difícil con las herramientas actuales.

Miguel Llerena
Vicepresidente para Latinoamérica

En este escenario, lo ideal sería:

· Alcanzar los estándares de cumplimiento: ayudando a descubrir activos administrados y no administrados, consultando datos en tiempo real en los endpoints para garantizar el cumplimiento y se detecten vulnerabilidades antes de que se conviertan en amenazas graves, todo desde una única plataforma.

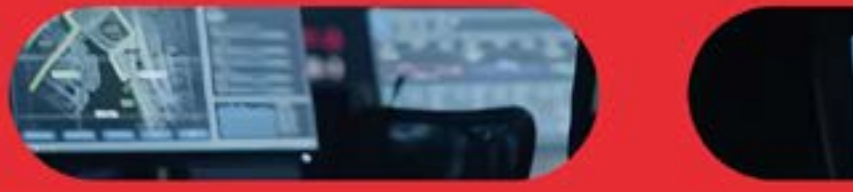
· Optimizar las TI: utilizando una plataforma única en todas las operaciones de TI y seguridad para automatizar la detección y la reparación, implementar parches y actualizaciones a escala y reducir la complejidad de TI al eliminar las soluciones puntuales y las licencias no utilizadas.

TANIUM

¡Vea y controle todos los puntos finales dondequiera que esté!

Administre, asegure y proteja su red con la única plataforma que ofrece datos de terminales de calidad, precisos y completos en los que confían las empresas más complejas y exigentes del mundo.

Tanium: el poder de la certeza



Prueba Tanium gratis

Inteligencia de datos para proteger la información crítica

"En salud, toda la información es propensa a ser atacada por los delincuentes digitales, pidiendo rescate por la misma"

Por Hector Alcazar, Territory Account Manager México

Hector Alcazar
Territory Account Manager México
Commvault

Pensemos por un momento en la información que se encuentra en las entidades de salud, podríamos comenzar con un expediente clínico de un paciente que contiene además de datos personales antecedentes de enfermedades previas y estudios que se le hayan practicado durante el tiempo.

Esta información la multiplicamos por la cantidad de pacientes, podríamos estar en los niveles de miles de expedientes que están alojados en el centro de datos del hospital.
Si un día reciben un ataque de tipo Ransonmware, el cual no es otra cosa más que el secuestro de esa información y liberación bajo un pago usualmente hecho en bitcoins, el hospital tendrá dos opciones: pagar la cantidad solicitada para que se libere la base de datos o, que por medio de nuestra tecnología, contar con la copia de la información libre de este ataque y lista para operar.

Lo que sucedería del lado del paciente es que llegaría al hospital y no podrían atenderlo ya que toda su información no se encuentra disponible. La pandemia, más que nunca. nos dejó la enseñanza de que la salud es lo más importante de nosotros como personas.
Si bien muchas organizaciones no están preparadas para abordar un escenario cada vez más marcado por los ciberataques, hay varios clientes que toman las acciones de prevención de forma muy seria y utilizan nuestra tecnología de base para toda esa información que es crítica para un hospital.

¿Por dónde comenzar?

Como primer punto y recomendación, se requiere de un análisis de cuál sería la información con la cual el hospital se vería comprometido ante un ataque. A partir de eso, habrá que establecer el perímetro de defensa de la misma, y posteriormente definir la estrategia de preguntarnos ¿Qué pasaría si al final de toda la tecnología de defensa falla? Ahí es justo donde entra la tecnología de Commvault para hacer las estrategias de protección de datos adecuadas ya sea en el mismo centro de datos del hospital o fuera de él, en algún otro sitio o inclusive en la nube.

La propuesta de inteligencia de datos de commvault es entender mejor qué es lo que tenemos en nuestros almacenamientos, cuáles se están utilizando y cuáles no. Con eso en mente, podemos definir la estrategia de respaldos adecuada pensando principalmente en caso de un ataque que tanto tiempo nos costará recuperarnos y si este tiempo es el adecuado con lo que el hospital requiere.

En este sentido, una implementación de commvault tiene que arrancar desde el análisis de qué vamos a proteger, cada cuánto tenemos que realizar el respaldo y, en ese caso, que se requiera que el tiempo de recuperación cumpla con las necesidades.

Una vez que se definen estos puntos simplemente la herramienta, de forma automática, generará las copias requeridas, sin necesidad de que haya un operador haciéndolo, por lo que liberamos estos recursos técnicos para otras actividades.


SitioSimple
Crear tu página web es tan rápido como leer esta publicidad
Hoy podés tener tu página web o tienda online ¡sin programar y en menos de una hora!
Más de 200 plantillas pre-diseñadas
0% comisiones por venta
Lista para celulares
Optimizada para Google
Múltiples opciones de pago y envíos
En pesos argentinos
ESCANEÁ
Y EMPEZÁ GRATIS
DonWeb.com

Por qué invertir en una estrategia sólida de gestión de datos en la nube

Por Dmitri Zaroubine, Presales Manager para Latam en Veeam Software

El sistema sanitario viene incorporando el uso de tecnología hace años, sin embargo, esto se expandió en el último tiempo, a la luz de la transformación digital que avanzó en todas las industrias. Estos cambios se reflejaron en la proliferación de la telemedicina, y la automatización de procesos. Pero a medida que aumentan los datos sensibles que maneja la industria, también el de la cantidad de ciberamenazas, especialmente peligrosas para este sector.

En nuestro Reporte de Tendencias en Protección de Datos 2022 elaboramos una edición especial sobre el sector Healthcare, con 399 encuestados de 28 países. En principio, el informe arrojó que el 76% de las organizaciones sufrieron un ataque de ransomware en el último año. A pesar de esto, lo más llamativo, fue que la brecha entre lo que las organizaciones de la salud esperan sobre la protección de sus datos y la capacidad real de sus equipos IT para responder a esto, sigue aumentando. El 93% de los responsables IT del sector creen que sus organizaciones tienen una "brecha de protección" entre la cantidad de datos que pueden permitirse perder y la frecuencia con la que se protegen los datos. El desafío está en poder garantizar que las inversiones en equipamiento, prestación y tecnología funcionen sobre la base de una infraestructura de comunicaciones acorde desde el punto de vista de la seguridad.

Los datos sanitarios son críticos y deben estar respaldados y replicados, garantizando su recuperación lo más rápido posible. La implementación de una estrategia sólida de gestión de datos en la nube se convierte en una necesidad para el sector, para garantizar que la infraestructura digital y las aplicaciones no se conviertan en un punto débil, con el fin de evitar la interrupción de los servicios que brinda un centro de salud o el secuestro de datos sensibles de pacientes.

Desde Veeam proponemos invertir en una Estrategia Moderna de Protección de Datos, que pueda dar una mayor y más ágil capacidad de respuesta a cualquier desastre (ciberataques, borrados accidentales, ransomware), y garantizar un backup de los datos para el funcionamiento de los establecimientos, el cuidado de los datos de los pacientes y así, una mejor atención para ellos. En este sentido,

Dmitri Zaroubine
Presales Manager para Latam en Veeam Software

a comienzos del año 2021, presentamos la nueva versión de Veeam Backup Replication™ v11, que, con más de 200 nuevas características y mejoras, como la protección de datos continua y protección confiable contra ransomware, es una solución única para la gestión integral de la información.

Hoy las ciberamenazas, lejos de ser una posibilidad, son una certeza. Esta solución es lo suficientemente poderosa y flexible como para proteger cada fase del ciclo de vida de los datos, mientras maneja todas las complejidades de un entorno multi-nube. Combina backup, replicación, snapshots de almacenamiento y protección de datos continua, algo que la industria sanitaria demuestra necesitar de manera urgente para cuidar sus datos, los de sus pacientes, sus proveedores, y colaboradores, de los ciberataques.

Santiago Rosenblatt agradece la distinción en el Ciclo de Emprendedores

Todo sobre Segurinfo 2022

Por Rubén Borlenghi

Inició en 2005 y ya van 105. Es Segurinfo, el Congreso Iberoamericano de Seguridad de la Información, uno de los más importantes de la región, declarado de interés por el Senado de la Nación y que ya se ha celebrado en 12 países. El evento de Seguridad más importante de USUARIA se llevó a cabo en abril pasado en formato híbrido y congregó a más de mil participantes. Ésta es la reseña del Congreso de este año.

El centésimo quinto Congreso Iberoamericano de Seguridad de la Información Segurinfo se llevó a cabo en salones del Hotel Four Seasons de Buenos Aires, el 19 de abril pasado. Fue una reunión en modo híbrido, con asistentes en la sala y transmisión por video, que llegó a más de 1000 participantes de Latinoamérica y España.

Las palabras iniciales estuvieron a cargo, como siempre, del presidente del congreso, Juan José Dell'Acqua, quien indicó que en la fecha se cumplían 18 años de la realización del primer Segurinfo. Señaló los cambios del rol de la seguridad de la información, gracias a la tecnología, pero también gracias a los profesionales y señaló el gran trabajo del comité académico en el momento de elegir las ponencias.

Luego convocó a Pedro Maidana, presidente de USUARIA (Asociación de usuarios de tecnología y telecomunicaciones), quien recordó que USUARIA como ONG cumple 40 años. También señaló que la seguridad informática se transformó en ciberseguridad, luego en ciberguerra, y ahora "se está inmerso en una problemática que a diario está socavando las garantías que teníamos de ofrecer servicios a nuestros usuarios, y esos usuarios pueden ser los de una empresa o los de un país", indicando que esa es la gran importancia que ha adquirido Segurinfo para la comunidad durante los 105 eventos presentados en Latinoamérica. Finalmente indicó que este año regresaran con eventos casi todos presenciales

Santiago Fernández, CISO de NaranjaX, presidente del comité académico y elegido como el anterior CISO del año, dio la bienvenida a los asistentes, auguró que la concurrencia lleve nuevos amigos, conozca nuevos profesionales y conocimientos en un espacio propicio para compartir vivencias, para que el colega, el compañero no tropiece con las mismas piedras, mejorando continuamente.

Abrió la jornada Gustavo Sain, Director Nacional de Ciberseguridad en la Jefatura de Gabinete de Ministros, de la Presidencia de la Nación quien mencionó que para su Dirección el 2022 es un año clave; indicó que Argentina tiene una norma de la cual están orgullosos, los Requisitos Mínimos de Seguridad de la Información para el Sector Público Nacional, que desde el año pasado

es una decisión administrativa de cumplimiento obligatorio para todo organismo centralizado o descentralizado, para estandarizar los niveles de seg
uridad del estado, dado que el estado no solo brinda servicios al ciudadano, sino que administra bases de datos personales de todos, en procesos auditados por la SIGEN.

Continuó señalando que esa reglamentación ha tenido una sorprendente cantidad de adherentes, como el Consejo Universitario nacional, o la junta de cortes supremas de justicia provinciales, que recomienda al poder judicial que adhiera al empleo de la norma.

De acuerdo con el programa nacional de protección de las infraestructuras críticas de información, creado en 2011, en 2022 trabajarán no solamente con infraestructuras críticas del sector público sino también del privado. Aprovechó la oportunidad para que, una vez aprobada la norma, se trabaje juntamente con los entes reguladores.

- La primera presentación, "Tendencias Globales, Ransomware protection" estuvo a cargo de Marcos Cavinato, Lead Security & Compliance @ Google Cloud quien, desde un video, explicó la estrategia de protección contra ataques de ransomware.

Panel de CISOs. Felipe Ernesto Roel Montellanos, Perú – Sergi Carmona, AGBAR - Claudio Colace, Banco Patagonia (en el sentido del reloj)

- Definió el tipo de amenaza e identificó cuatro modalidades: el cifrado de datos, el robo de datos que posiblemente se publiquen, un DDoS contra la infraestructura, y la amenaza de filtrar información a socios de negocio, periodistas y clientes.

- La siguiente estuvo a cargo de Marcelo Feldman, Director de Ciberseguridad en Microsoft Latinoamérica y Caribe y tuvo como título "La seguridad como prioridad en un mundo híbrido".

- Feldman adelantó que quería mencionar los desafíos que ahora trae aparejado estar nuevamente en actividad, en un mundo presencial mientras se convive con un mundo digital y otro híbrido. Un primer paso en un enfoque moderno de seguridad es Zero Trust: nunca confiar, siempre verificar, apoyado en tres conceptos: verificar explícitamente, usar el menor privilegio, asumir brechas.

Panel Ciberseguridad en la región. Primera fila (izq. a der.) Abel Decaroli, Argentina - Marushka Chocobar Reyes, Perú - José Callero, Uruguay. Segunda fila (izq. a der.) David Moreno, OEA - Juan Ramón Anria, Panamá.

Luego llegó el momento de escuchar a Gerardo (Gery) Coronel, Country Manager, South of LatAm, Check Point, con "Mereces la mejor seguridad".
Mencionó los ataques a las cadenas de suministros, el factor de prevención, a veces más importante que la detección y mostró la evolución del ransomware, desde lo clásico hasta la doble extorsión. Luego del ransomware as a service pasó a la descripción de ataques dentro del universo "mobile" y el tema BYOD.

"Ordenando la seguridad Multinube", estuvo a cargo de Ariel Santa Cruz, Sr. Solutions Engineer, de F5. Comenzó por mostrar que hubo un cambio fundamental en cómo las apps son diseñadas y como se despliegan, e importa observar la conectividad de las aplicaciones en diferentes ambientes.
A continuación, Camilo Gutiérrez Amaya, Head of Awareness & Research de ESET Latinoamérica presentó "¿Cómo funcionan los grupos de cibercrimen latinoamericano?" Relató una experiencia de trabajo con un cliente local. Luego habló de las APT, una de las cuales se conoce como Machete, usado para ciberespionaje. Otro tipo de amenaza que encontraron es crimeware, entre ellos los troyanos bancarios empleados en Latinoamérica. Otro grupo es la financial APT, en el que hay una que apunta a usuarios corporativos del sector bancario.
La siguiente disertación contó con la presencia de Jorge Pairó, Country Manager, Hernán Conosciuto, Principal Specialist Solution Architect, y Roberto Calva, Cloud Management and Automation Senior Specialist, todos de Red Hat en "La Importancia de la Ciberseguridad en la Transformación Digital."

Durante la presentación dialogaron sobre las amenazas informáticas que afloran, sobre todo en tiempo de pandemia. Dispositivos IoT, cámaras de seguridad, relojes digitales. Sugirieron que la automatización tiene que ser adaptativa, para ejecutar acciones de mitigación o ejecutar reglas. Daniel Sepúlveda, Cyber Security Account Executive de Darktrace, presentó "Defendiendo las organizaciones en medio de una crisis".
Inició recordando que "ya no es si voy a ser atacado o no, sino cuándo". La táctica de entender, identificar y elaborar estrategia no ha sido muy efectiva, "estamos intentado utilizar información del pasado para predecir el futuro".

Mejor sería utilizar Machine Learning para acelerar el proceso de detección, y cómo reaccionar de forma efectiva frente a ese tipo de ataque, por medio del análisis de comportamiento.

La siguiente actividad fue el primer panel de la jornada: “Transferencias 3.0 & Fintech”
Los integrantes fueron Mara Misto Macías, CISO en BCRA; Karen Collante, CISO, RappiPay; Lorenzo Aracena, Cybersecurity Director de Kavak Capital; Lucas Paus, CISO, Modo, y Marcelo Dalceggio, CISO de Cencosud.

Se conversó acerca de varios temas, entre ellos, qué son las (mal llamadas) transferencias 3.0 —pagos por medios digitales y la necesidad de su estandarización—; el rol del CISO relacionado con el directorio —y las diferencias entre una startup y una compañía ya establecida— y el aumento de la rotación de talentos.

Algunas opiniones:
Lucas Paus: “Manejar efectivo, sobre todo en tiempos de pandemia, implica muchos riesgos, no solo en temas de salud sino en seguridad física, incluyendo la acumulación de efectivo en un comercio. Es necesario que el negocio no te vea como un stopper sino como un driver, recordando que la seguridad es calidad, un diferencial.”

Mara Misto Macías: “‘Transferencias 3.0’ es el nombre marquetinero; en realidad es implementar pagos con transferencias, y el primer producto que se propone es pago con QR. Y que ese QR sea interoperable.”
Lorenzo Aracena: “El CISO necesita entender el negocio que debe proteger. Si una empresa sufrió un ataque, su relación con el CISO será diferente de aquella que no lo ha sufrido.”
Karen Collante: “es buena la corriente de DevSecOps , donde nuestras opiniones se meten dentro de ese ciclo de vida, y además el CISO debe aprender a hablar no solo en términos de seguridad sino en términos de producto”
Marcelo Dalceggio: “Se requiere de colaboradores que sepan codear, y que no tengamos que llevar de la mano, que les guste aprender y sean capaces de agregar valor, y ofrecer un ambiente donde puedan aportar ideas y que esas ideas sean escuchadas.”

Otro de los muy interesantes paneles de la jornada fue “CISOS Iberoamérica - Cómo mejorar la estrategia en ciberseguridad, ¿Qué tan seguros y expuestos estamos?” en el cual obró como moderador el CISO de Banco Patagonia, Claudio Colace.

“‘Transferencias 3.0’ es el nombre marquetinero; en realidad es implementar pagos con transferencias, y el primer producto que se propone es pago con QR. Y que ese QR sea interoperable.” - Misto Macías

Sus integrantes fueron André Pires Ferreira Magalhaes, CISO, Gerencia Corporativa de Seguridad de la Información, Falabella; Sergi Carmona, CISO, AGBAR Iberoamérica y Felipe Ernesto Roel Montellanos, Gerente de Tecnologías de Información, Banco Central de Reserva del Perú.

Entre otros temas, se habló de cuál es el impacto de una situación como la que se está viviendo; la postura de seguridad adoptada en la organización o en la región; si se agregan nuevos escenarios de ciberataques o ciberresiliencia en la organización o en los ejercicios.

Ferreira Magalhaes desde un video: “las medidas son reforzar el monitoreo, tolerancia cero en los procesos de gestión de vulnerabilidades, comprobar la capacidad de respuesta a incidencias, reforzar el plan y el proceso de gestión de crisis; es lo mínimo esperado de nosotros, básico en una empresa de gran porte.” “debe verificarse cuan fácil seria mover toda una nube a otra.”

Durante la presentación dialogaron sobre las amenazas informáticas que afloran, sobre todo en tiempo de pandemia. Dispositivos IoT, cámaras de seguridad, relojes digitales. Sugirieron que la automatización tiene que ser adaptativa, para ejecutar acciones de mitigación o ejecutar reglas. Carmona: “Las estrategias de seguridad son algo vivo, el profesional debe adaptarse a las estrategias cambiantes de acuerdo a la situación”. “El empleado que no recibe ningún tipo de capacitación es un riesgo para la empresa, dado que en algún momento producirá un clic letal, o se hará pasar por un ejecutivo para que se realice un pago.” “Es necesario un tipo de macro CERT, un grupo global donde se pueda tomar la información, con un moderador.”

Roel Montellanos: contó una experiencia en la que un proveedor de servicios fue afectado por ransomware, relacionado con el conflicto bélico actual, y estuvo fuera de servicio más de 10 días. Una situación de ese tipo produciría la necesidad de tener planificaciones adecuadas, completadas con anticipación, armando un esquema

Otro panel, esta vez por video, fue “Ciberseguridad en la Región, la visión de referentes gubernamentales.”

Entrega de la plaqueta de reconocimiento a Patricia Prandini

El moderador fue David Moreno, Oficial del programa de Ciberseguridad en OEA y los participantes, Juan Miguel Correa Diez, Jefe del departamento de Operaciones del Comando Conjunto Cibernético (CCOCI), Ministerio de Defensa de Colombia; Gabriela Ratti, Directora General Ciberseguridad y Protección de la Información, Ministerio de Tecnologías de la Información y las Comunicaciones, Paraguay; Marushka Chocobar Reyes, Secretaría del Gobierno Digital de la PCM, Perú; Juan Ramón Anria, Director Nacional de Ciberseguridad de la Autoridad Nacional para la Innovación Gubernamental (AIG), Panamá; José Callero, Director del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) en AGESIC, Uruguay; Abel Decaroli, Director de Prevención en Seguridad de Sistemas y Redes Informáticas en Secretaría de Innovación Pública, Presidencia de la Nación Argentina; Jorge Mora Flores, Director de Gobernanza Digital-Ministerio de Ciencia, Tecnología y Telecomunicaciones, Costa Rica.

Entre otros temas, se conversó acerca de los mecanismos más efectivos que están usando los países para fortalecer la ciberseguridad, y las lecciones aprendidas; hicieron especial hincapié en la capacitación, tanto de los empleados públicos como de la población en general, “que la ciberseguridad debe ser una tarea compartida entre autoridades de defensa, de educación y del alto mando político”; cómo tuvieron que adecuar medidas a la aparición de la pandemia, durante la cual “se observaron brechas de seguridad no consideradas”; finalmente, que se debe trabajar en planes de contingencia, para prever otros acontecimientos similares.

La siguiente actividad fue el panel “Ciberseguridad Nacional, Provincial y Municipal”. Contó con Nicolás Smirnoff, CEO de Prensario Internacional, como moderador y los integrantes del panel fueron Oscar Niss, Subsecretario de Ciberdefensa de la Nación, Ministerio de Defensa; Olga Cavalli, Subsecretaria de Tecnologías de la Información, Jefatura de Gabinete de Ministros, Presidencia de la Nación, y Gustavo Sain, Director Nacional de Ciberseguridad en la Jefatura de Gabinete de Ministros, Presidencia de la Nación.

Algunas opiniones destacadas:
Olga Cavalli: sus principales desafíos son: concientizar a nivel estatal, de empresas privadas y usuarios finales, incluyendo una buena política de claves, y para las empresas chicas y medianas, que tienen presencia en Internet, incluir en su cadena de valor la tecnología virtual y protecciones adecuadas. “El ataque va a ser permanente, la creatividad y la sofisticación de los ataques cada vez es mayor, eso no va a cambiar. La clave es la concientización y ser resiliente, estar preparado para volver a funcionar lo más rápido posible.”

Oscar Niss: indica que la ciberdefensa tiene que ver con la protección del ciberespacio con interés militar. Sus bienes a proteger incluyen las redes del sistema de defensa nacional, más la defensa de los sistemas de armas, de los cuales muchos están informatizados. Dado que la ciberdefensa es una capacidad nueva dentro de las fuerzas armadas, “en nuestro país este área necesita de la definición normativa de la política.” “Se debe ir hacia una reconfiguración de Internet, a mejorar protocolos, La red mundial de hoy no sirve para las exigencias de las tecnologías disruptivas que siguen apareciendo constantemente.”

Santiago Ramos, Sales Specialist, Network & Security LATAM, VMWare, presentó "Simplificando la Complejidad de la Seguridad". Introdujo el concepto de seguridad intrínseca, proveyendo seguridad directamente en la infraestructura (usuarios, endpoints, workloads y redes), y trató de demostrar cómo modernizar el SOC.

A continuación, Pablo Garay, Jefe de servicios de consultoría de seguridad en Telecom Cybersecurity Solutions, expuso sobre "La evolución del CISO: actualidad y futuros desafíos". Presentó el concepto de BISO, donde la B es por el vínculo con el negocio, y el Virtual CISO. Luego se preguntó en qué invierte el tiempo laboral un CISO, entre su equipo y el directorio, cuáles son sus futuros desafíos, y formalizó propuestas para el futuro.

La siguiente presentación, "60 segundos en Internet, conoce los riesgos a los cuales está expuesta tu organización" estuvo a cargo de Miguel Caruso, Manager Research and Development, Telecom Cybersecurity Solutions, quien comenzó por comentar que un solo minuto puede ser insignificante, pero en un gráfico demostró la cantidad de instancias, transacciones de dinero, fotografías compartidas, tweets, búsquedas, mensajes, conexiones de equipos de trabajo, visualización de videos, y otra miríada de cosas que suceden en un minuto del día en internet.

A continuación la empresa Netskope presentó "La evolución de la seguridad con SSE - Security Service Edge", a cargo de Roberto Araneda, Solutions Engineer.

Analizó la situación de los usuarios, trabajando desde cualquier lugar, y con cualquier equipo (BYOD o corporativo) sobre aplicaciones externas (de Web o SAAS), o internas, en el datacenter, y tanto en casa central como en una sucursal.

La empresa Thales, representada por Patricio Jaca, Cybersecurity Manager, presentó

> "La ingeniería social aumentó un 500% desde 2018, y el 98% de los ataques se inicia con una instancia de ingeniería social."- Viviana Basso

"Como proteger el dato del Ransomware". Mostró el aumento del flujo de datos en un día a nivel usuarios de Internet o corporaciones, que no todos están cifrados, y cómo se protegen en un modelo Zero Trust.
Viviana Basso, Manager de PwC Argentina, presentó "Ciberseguridad - X Fit training Mindset". La disertación tomó como tema la ingeniería social, y los riesgos que ella impone a las empresas. Este tipo de ataques aumentó un 500% desde 2018, y el 98% de los ataques se inicia con una instancia de ingeniería social.

Siguió "Fortaleciendo los accesos privilegiados: una tarea más simple", presentado por Andrés Mendoza, Regional Technical Manager de ManageEngine. Inició comentando diferentes temas relacionados con la ciberseguridad, incluyendo desde los ataques convencionales hasta los malos hábitos de uso, y se detuvo en la gestión de usuarios de los cuatro tipos de cuentas privilegiadas, o con permisos elevados: administrativas locales, administrativas de dominio, de servicio o de aplicación, y sus características de respaldo, acceso y control

Panel "Ciberseguridad Nacional, Provincial y Municipal". Izq. a der.: Nicolás Smirnoff, Prensario Internacional - Oscar Niss, Ministerio de Defensa - Olga Cavalli, Jefatura de Gabinete de Ministros y Gustavo Sain, Jefatura de Gabinete de Ministros

"Reduciendo el riesgo de Amenazas Internas con Zero Trust", estuvo a cargo de Gastón Rodríguez, Cyber Security Architect, IBM Argentina, Uruguay & Paraguay. Caracterizó al enfoque de Zero Trust de su empresa, una solución integrada que aplica políticas de protección, detecta anomalías, responde automáticamente y mejora las políticas de protección, en tres etapas crecientes de madurez.

Gastón Gualdoni, Regional Sales Manager, SOLA, de Crowdstrike presentó "Ataques sin Malware, Importancia de la velocidad en la protección". Señaló el aumento en la sofisticación de las amenazas, y que los ataques pueden ser con o sin malware. Mostró la categorización de los atacantes según su motivación, y cómo se observa que muchas de las detecciones de actividad maliciosa realizadas por su equipo Overwatch no estaban basadas en malware.

También en video

Al cierre de la actividad del día se emitieron los videos de las Presentaciones de Trabajos. La autora del primero fue la Dra. Johanna Caterina Faliero con "Ciberinteligencia vs. Ciberseguridad: Contrastes y aristas legales estratégicas en el ciclo de inteligencia y el cumplimiento normativo"

En su trabajo, la Dra. Faliero define ciberinteligencia como un concepto de carácter híbrido, que fusiona la seguridad a la ciberseguridad y la inteligencia, en un contexto actual de amenazas novedosas, avanzadas y persistentes de acción creciente.

El siguiente trabajo fue de Daniel Zacarias Hernández quien, desde México, presentó "Bloqueando al enemigo, cerrando las puertas". En él menciona la gran cantidad de ciberataques exitosos y un gran enemigo: la inexistencia de una cultura de ciberseguridad

El tercer y último trabajo pertenece a Luis Antonio Zafra Labrador, y se titula "Los retos del SOC, como evitar los sesgos y daltonismos en nuestro SOC"

Además de mentar tríada operacional —personas con habilidades y conocimientos en el tema, con continua capacitación; procesos homologados y documentados, y tecnología adecuada para cubrir las necesidades de operación de la empresa— señaló diferentes fuentes de metodología y marcos de referencia como la guía de seguridad sobre gestión de incidentes de NIST, la herramienta SOC-CMM para medición de madurez de capacidades, MITRE ATT&CK, ISO 27001 e ITIL V4, entre otras.

En el Ciclo de Emprendedores, se presentó Next Generation Cybersecurity por el Founder & CEO de la empresa Strike, Santiago Rosenblatt. Su compañía se basa en un concepto que llama Continuous Pentesting, y que está llevando hacia Continuous Security.

> "Las personas: sistemas con cientos de vulnerabilidades conocidas desde el principio de los tiempos, la gran mayoría de las cuales siguen sin corregirse."

Finalmente se otorgó una Plaqueta de Reconocimiento a la trayectoria a la Magister en Seguridad Patricia Prandini.

Principales riesgos de seguridad de IAM (Segunda parte)

Mucho antes de que COVID-19 tomara al mundo por sorpresa, las empresas comprendieron las ventajas y las infinitas posibilidades de transferir datos y servicios a la nube. A medida que los empleados comenzaron a trabajar de forma remota, las demandas sin precedentes de la pandemia obligaron a las organizaciones a migrar sus datos a la nube, incluso más rápido de lo esperado.

Esta transición entre los tres modelos principales de implementación en la nube (SaaS, IaaS y PaaS) no sólo mejoró la flexibilidad y la eficiencia dentro de las organizaciones, sino que también presentó nuevos riesgos. A medida que las brechas de seguridad se vuelven una realidad aún mayor, es crucial que los protectores de la nube consideren la importancia de salvaguardar su información y fortalecer su Gestión de Identidad y Acceso (IAM por sus siglas en inglés), al tiempo que reconocen los principales riesgos de seguridad que han surgido a la superficie. Acá, la segunda parte de los riesgos de seguridad de la Gestión de Identidad y Acceso.

El acceso privilegiado

Así como existen cuentas privilegiadas en entornos locales, la nube también tiene su propia forma de otorgar acceso privilegiado según el proveedor de la nube. Estas cuentas se pueden asociar con cuentas humanas y no humanas y varían entre todos los modelos de implementación en la nube (IaaS, SaaS, PaaS, Data, etc.). Las superficies de ataque relacionadas con los privilegios en los entornos empresariales modernos son cada vez más frecuentes a medida que los sistemas, las aplicaciones y las identidades continúan creciendo.

El ataque SolarWinds en 2020 mostró un ejemplo clave de acceso privilegiado como objetivo. Cuando se trataba de acceso privilegiado, las soluciones tradicionales que no "revertían la provisión" del acceso efectivo real a los permisos privilegiados (de ninguna manera) y los validaban en función de los registros del sistema registrados, no brindaban la cobertura necesaria para proteger el estado de la nube. El acceso privilegiado no es sólo una concesión directa de un rol o permiso, también es cualquier control sobre los grupos o atributos que pueden otorgar el rol, así como cualquier rol que contenga tales privilegios, sea o no oficialmente un rol de "administrador".

Ejemplos de permisos excesivos:

- Los permisos de exhibición de documentos electrónicos en Microsoft 365 (Office 365) pueden proporcionar acceso a cualquier buzón de correo o archivo, que por lo tanto debe ser monitoreado para otorgar antigüedad y eliminación.

- Los roles que parecen menos críticos, como el rol de "editor" en Google Cloud Platform, en realidad consisten en múltiples roles que se consideran "administrativos". Incluso si se otorgan a nivel organizacional o incluso delicado de proyecto / carpeta, los riesgos aún podrían ser profundos.

- Control sobre un grupo específico que otorga acceso a otros administradores de dominio.

- El control (por ejemplo, HRBP) sobre los atributos del usuario, como el rango, el gerente o un rol organizacional, puede otorgar acceso privilegiado relevante en la mayoría de las implementaciones de tipo Cómo mitigar este riesgo: Al final del día, "no puedes proteger lo que no puedes ver". La implementación de una solución eficiente que ofrece una visibilidad profunda de los puntos de acceso de riesgo, cómo el superadministrador y otras cuentas con privilegios, puede aplicar barreras en torno al uso, la actividad y el comportamiento de las cuentas. Es crucial encontrar una solución que permita una visibilidad de 360 °

sobrecómo se otorgan los permisos, aplicando medidas de seguridad en el acceso y la actividad sospechosa, asegurándose de que las cuentas privilegiadas no se utilicen con un propósito diario y de que se puedan ver los datos históricos anormales. para mitigar este riesgo.

Empleados de baja

Uno de los principales desafíos para los gerentes de TI es manejar la deslocalización. A medida que los empleados abandonan las organizaciones, es cada vez más difícil garantizar la eliminación total de todos los permisos y accesos. Algunos de estos riesgos se pueden remediar mediante el uso de soluciones SSO estrictas como fuente de la verdad; sin embargo, es probable que sigan existiendo brechas por múltiples razones. Revocar el acceso de SSO o de cualquier otro proveedor de identidad puede evadir sistemas fuera de su cobertura, lo que deja abundantes cuentas que representan inmensas amenazas de seguridad y cumplimiento para las organizaciones.

(Crédito: Anne Nygård - Unsplash)

El empleado fue excluido de los sistemas de recursos humanos, **Ejemplos de empleados que dejan de trabajar:**

- El empleado fue excluido de los sistemas de recursos humanos, pero tenía una cuenta válida en sistemas no conectados a recursos humanos.
- La propiedad de la cuenta no se transfirió del empleado fallecido

(Crédito: Folco Masi - Unsplash)

Cómo mitigar este riesgo:

Las organizaciones deben monitorear continuamente la eliminación parcial en todas las aplicaciones críticas. Esta monitorización depende de la integración en el IDP, fuente de verdad y / o aplicaciones. Es importante monitorear la rotación de claves, la propiedad de las cuentas de servicio, así como la información que pueda haber sido compartida externamente, antes de la salida.

La seguridad en la nube es un viaje continuo

Las infinitas oportunidades de transferir datos y servicios a la nube nunca han sido más claras. Dado que las organizaciones se ven obligadas a migrar a la nube más rápido de lo que se considera, el fortalecimiento de la gestión de identidades y accesos no es una tarea para “mañana”.

Las posibles brechas de seguridad de un IAM inseguro podrían resultar en daños permanentes irreparables. Es en esta realidad y en esta tasa de migración que los protectores de la nube deben familiarizarse con los probables riesgos y hackeos. Las empresas deben centrarse en estrategias para aprovechar de forma segura su información a fin de aprovechar al máximo los beneficios de la nube. Esto no solo hará que las empresas sean más seguras, sino que también les dará a las organizaciones una ventaja mucho más allá del COVID-19.

> “Es crucial encontrar una solución que permita una visibilidad de 360 ° sobre cómo se otorgan los permisos”

Los aportes de Blockchain a Cloud Computing

El beneficio fundamental de integrar Blockchain en la tecnología de computación en nube es aumentar la seguridad de los datos. Combinar la tecnología Blockchain y la computación en la nube es como disfrutar de lo mejor de ambos mundos en una sola unidad. La integración de Blockchain con la computación en la nube nos lleva a la próxima era de seguridad de datos y disponibilidad de servicios.

> “Incluso con medidas de protección implementadas, eventualmente un ataque de ransomware aún puede tener éxito.”

Para ayudar a las organizaciones a protegerse contra los ataques de ransomware y recuperarse de ellos si ocurren, el Instituto Nacional de Estándares y Tecnología (NIST) ha publicado una infografía que ofrece una serie de consejos y tácticas simples.

Blockchain es la tecnología que permite a todos los miembros mantener un ledger que contiene todos los datos de las transacciones y se actualiza para mantener la integridad cuando hay una nueva transacción. Desde que el avance de Internet y la tecnología de encriptación han hecho posible que todos los miembros verifiquen la fiabilidad de una transacción, se ha resuelto el único punto de fallo derivado de la confiabilidad en un tercero autorizado.

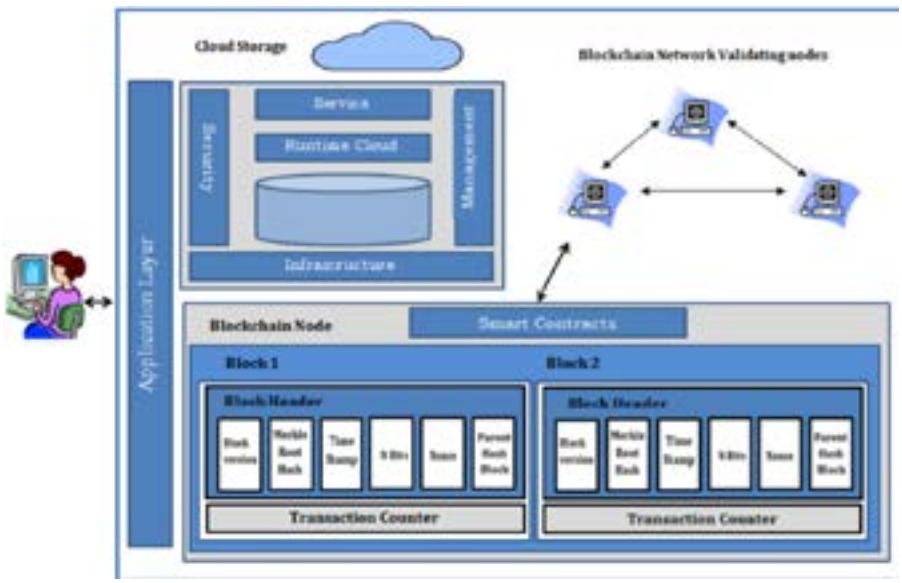
La tecnología Blockchain es el futuro de las industrias que se esfuerzan por mejorar la seguridad y la privacidad. Se trata de un libro de contabilidad distribuido que registra los datos de la cadena sin ninguna autoridad central. Los participantes o los dispositivos de la tecnología blockchain se denominan nodos. Blockchain proporciona una red descentralizada en la que todos los nodos de la red tienen una participación activa para validar y verificar los datos.

Interoperabilidad

En las nubes públicas, la comunicación interna no está permitida, y hace que muchas industrias se echen atrás en el uso de la nube. Cuando la nube se integra con Blockchain, se considera a las diferentes nubes como nodos. La comunicación entre nodos es posible en la cadena de bloques. Todos los nodos presentes en la misma red comparten los datos entre ellos, de modo que cada nodo contiene una copia de las transacciones. Esto aporta transparencia a la red. Actualizan cada transacción en el ledger, que se publica a todos los demás nodos. De este modo, las empresas pueden añadir cualquier número de redes y preservar la accesibilidad de los datos, lo que aportará autenticidad a la red.

Cifrado de datos

Como todos sabemos, los datos se descifran antes de almacenarlos en la nube, lo que cuestiona la integridad de los datos. En la red Blockchain, todos los datos de los bloques se convierten en un código hash utilizando algoritmos criptográficos, y se genera una clave hash para cada bloque. Para garantizar la oportunidad y la integridad permanente de los datos, el sistema de control que recoge los datos de la programación de tareas produce el código hash y lo registra en la red de cadena de bloques de forma inmediata.
Debido a que la Blockchain tiene la facilidad de los mecanismos de consenso de descubrimiento de bloques, la integridad de los datos de los bloques se mantiene. Cada nodo de la red contiene una copia de cada transacción que nos proporciona la disponibilidad y la persistencia que ayuda a la red a soportar posibles puntos de fallo y ataques. Mientras que los datos recogidos en la nube son fiables, los nodos de la cadena de bloques maximizan la disponibilidad de los datos y la validez de estos, proyectándolos como



(Crédito: medium.com)

un servicio bajo demanda sin tiempo de inactividad. En la figura se muestra la arquitectura de la integración de la computación en la nube con la tecnología Blockchain. El usuario interactúa con el servidor con la ayuda de la capa de aplicación. Supongamos que cuando un usuario solicita una transacción a través de esta capa, los detalles de las transacciones se almacenan creando un bloque para cada transacción. Para añadir el bloque a la red Blockchain, los datos serán verificados por los nodos de validación de la red. La validación se hará en base al consenso. Una vez que el bloque se considera legítimo, todos los demás nodos de la red se conectarían a la misma y se enviarían los datos.

Todos los datos de la cadena de bloques se almacenan en la nube de protección de la cadena de bloques. La incorporación de Blockchain en

> “Combinar la tecnología Blockchain y la computación en la nube es como disfrutar de lo mejor de ambos mundos en una sola unidad.”

la nube proporciona protección de datos y también proporciona transparencia.

Gestión de datos en la nube

Los datos se almacenan en la nube de forma bastante desestructurada, mientras que en la cadena de bloques están muy estructurados. Los datos pueden rastrearse utilizando la clave hash generada para cada bloque. Cada bloque contiene la clave hash del bloque anterior, y es clave para seguir el rastro de la red.

Los datos del bloque se validan y los nodos presentes en la red pueden acceder a ellos. La nube soporta la elasticidad y puede manejar las fluctuaciones en las cargas computacionales como y cuando sea necesario. Utilizando un ledger distribuido, esto puede ser fácilmente manejado por la gestión de un gran número de eventos que causan una variedad de contratos inteligentes, asegurando la calidad del servicio.

Blockchain también garantiza el anonimato del usuario, y su registro puede ser eliminado de forma segura del sistema para evitar el acceso de terceros a la información del usuario. La integración de la nube con Blockchain también garantizará que muchas empresas tengan confianza en su arquitectura de seguridad, y se convertiría en un servicio bajo demanda.

Muchas aplicaciones de Blockchain-Cloud pueden emplearse en nuestras actividades diarias, haciendo que nuestros datos estén más seguros y protegidos. Varias industrias pueden utilizar los servicios de Blockchain-Cloud. Esta integración puede proporcionarnos más flexibilidad de almacenamiento, y al mismo tiempo, mantiene los datos validados. La autorización a la red será monitoreada, y también aumenta su resiliencia.

La computación en nube es una tecnología muy conocida, ya que existe desde hace muchos años. Pero la gente sigue luchando por superar algunos retos como la seguridad de los datos, la gestión de los mismos, la interoperabilidad, etc.

Blockchain es una tecnología emergente muy conocida por su seguridad y autenticidad, que son las principales características que están haciendo que el mundo se ponga de su lado. Al integrar Blockchain con la computación en nube, habrá muchas ventajas en cuanto a usabilidad, confianza, seguridad, escalabilidad, gestión de datos, y muchas más ventajas.

(Crédito: rawpixel.com - www.freepik.com)

Qué es SSDLC

El ciclo de vida de desarrollo de software seguro (SSDLC) generalmente se refiere a un proceso sistemático de varios pasos que agiliza el desarrollo de software desde el inicio hasta el lanzamiento.

Es un modelo de procedimiento paso a paso fácil de seguir que permite a las organizaciones:

- Desarrollar software en tiempo y forma
- Reforzar la línea de tiempo del producto de la planificación inicial
- Diseño y eventual despliegue.

Establecido a fines de la década de 1960, el ciclo de vida de desarrollo de software seguro (SSDLC) se ha arraigado en casi todas las empresas de software modernas. Es un procedimiento paso a paso para desarrollar software con varios objetivos, que incluyen:
Debido a la estructura regulatoria

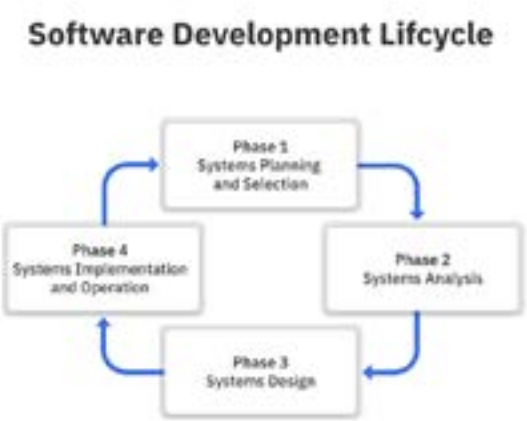
- Racionalización escalable de la canalización de productos/ software y
- Optimizar el diseño, despliegue y mantenimiento de dicho software.

Con el crecimiento multifacético de las demandas modernas de desarrollo, es crucial contar con una metodología de desarrollo todo en uno que agilice y estructure las fases del proyecto. Imagínese un gerente de proyecto que se acerque sin pensar a un equipo de desarrollo de software con una visión vaga de los entregables y el proyecto final. Suena aterrador, ¿verdad?

Independientemente de las capacidades técnicas y los talentos del equipo, SSDLC es esencial para regular cada fase del ciclo de desarrollo. Tal vez la ventaja más pragmática del SSDLC es que permite controlar el proceso de desarrollo sin dejar de garantizar que el sistema de software cumple con todos los requisitos estimados en todas y cada una de las fases.

Aunque el SSDLC puede parecer una receta mágica para el cronograma de gestión de proyectos de una organización, no funciona bien cuando hay incertidumbre sobre las expectativas y la visión del proyecto de software. Más importante aún, SSDLC no permite que los miembros del equipo agreguen aportes creativos, ya que todo el ciclo de vida se basa en la fase de planificación.

y bastante rígida del SSDLC, muchas empresas optan por un enfoque de desarrollo de software ágil con cumplimientos incrementales y fases hacia la implementación del producto final. Sin embargo, el enfoque SSDLC es quizás una de las metodologías más seguras, ya que garantiza que cada requisito del proyecto se cumpla de manera estricta sin problemas ni inconsistencias durante cada paso, desde la planificación hasta la implementación del producto.



Los 6 pasos de un ciclo de vida de desarrollo de software seguro
Al asegurarse de que su organización cumpla con el ciclo de vida de desarrollo de software seguro, establecerá un modelo sostenible para la planificación/inicio y lanzamiento final del producto.

El ciclo de vida del desarrollo de software seguro es progresivo y está estructurado sistemáticamente, con las siguientes etapas:

1. Planificación y Análisis de Requerimientos

La planificación preliminar y el análisis de requisitos es la etapa más fundamental en un ciclo de vida de desarrollo de software seguro.
Generalmente lo realizan miembros senior del equipo junto con los comentarios de los clientes correspondientes y la cooperación con el departamento de ventas, las encuestas de marketing y los expertos en la industria.
Una vez que se ha agregado esta información, se utiliza para planificar un enfoque de proyecto básico y realizar un estudio de viabilidad preliminar.
Un estudio de factibilidad estima la viabilidad a corto y largo plazo del proyecto desde una perspectiva económica, operativa y técnica.
Además, los gerentes de proyecto pueden estimar, planificar y crear requisitos de control de calidad durante esta fase.
Con el resultado del estudio de viabilidad, se pueden definir una variedad de enfoques técnicos para implementar el proyecto sin problemas, con riesgos mínimos y optimizados.
Una vez que los miembros senior han cumplido con un requisito de referencia y un análisis de factibilidad, deben definir y documentar claramente los requisitos específicos del producto y abordarlos con analistas de clientes/mercado.
Este proceso de aprobación se puede ejecutar, en última instancia, a través de un documento de especificación de requisitos de software (SRS), una descripción completa de los requisitos del producto que se diseñará y desarrollará a lo largo del ciclo de vida del proyecto.

2. Arquitectura y diseño de productos

Mediante el uso de un SRS como plantilla base para la arquitectura del producto, los arquitectos pueden entregar de manera eficaz un diseño de producto de backend de acuerdo con la viabilidad y los requisitos preliminares. Normalmente se propone y documenta más de un enfoque de diseño en la especificación del documento de diseño (DDS).
Eventualmente, el DDS es revisado por todas las principales partes interesadas del proyecto y, en función de parámetros críticos como la evaluación de riesgos, la solidez del producto, las limitaciones de presupuesto y tiempo, y la modularidad del diseño, se selecciona el enfoque arquitectónico más viable.
El enfoque de diseño en un ciclo de vida de desarrollo de software seguro es integral. Define claramente todos los módulos arquitectónicos del producto junto con su comunicación con módulos externos y de terceros fuera de la arquitectura interna a través de ilustraciones de flujo de datos.

“La planificación preliminar y el análisis de requisitos es la etapa más fundamental en un ciclo de vida de desarrollo de software seguro”

3. Planificación de pruebas

En un ciclo de vida de desarrollo de software seguro, un plan de prueba describe:
La estrategia utilizada para probar una aplicación.
Recursos que se utilizarán
Entorno de prueba
Las posibles limitaciones de las pruebas, y
El cronograma proyectado de las actividades de prueba.
El líder del equipo de control de calidad normalmente llevará a cabo la planificación de pruebas y la asignación/garantía de recursos durante esta etapa.
Un plan de prueba generalmente incluye lo siguiente:
Una introducción o breve resumen del documento del plan de prueba
Expectativas sobre las limitaciones comerciales y técnicas al probar el software
Lista completa de casos de prueba que se incluirán en la prueba de la aplicación
Características probadas
Enfoque que se utilizará durante las pruebas de software
Entregables a cumplir y probar
Recursos asignados para pruebas de aplicaciones

Posibles riesgos generales involucrados durante el proceso de prueba
Cronograma de tareas e hitos que deben lograrse dentro del marco de tiempo de prueba

4. Codificación

Ahora es el momento de construir y desarrollar el producto. En esta etapa del ciclo de vida de desarrollo de software seguro, el desarrollo de código se ejecuta de conformidad con el DDS.
Siempre que el diseño/arquitectura se haya realizado de manera detallada y organizada, la generación de código se puede lograr sin muchos obstáculos logísticos.
Es imperativo que los desarrolladores sigan las pautas de codificación definidas por su organización y las herramientas específicas del programa, incluidos los compiladores, intérpretes y depuradores que se utilizan para optimizar el proceso de generación de código.
Varios lenguajes de programación de alto nivel como C, C++, Pascal, PHP y Java se implementan normalmente para el desarrollo de aplicaciones.
En cualquier caso, el lenguaje de programación elegido depende totalmente del tipo de software, sus casos de uso en la industria y las especificaciones técnicas del proyecto.

5. Pruebas y resultados del producto

Después de varias rondas de revisión de código y control de calidad, las pruebas de productos se pueden implementar en el ciclo de vida de desarrollo de software seguro.
Es importante tener en cuenta que esta etapa suele ser un subconjunto de todas las etapas de los modelos SSDLC modernizados. En otras palabras, las pruebas deben optimizarse activamente en tiempo real a través de cada paso del SSDLC para garantizar un proceso de desarrollo sostenible.
Sin embargo, esta quinta etapa es solo una etapa de prueba del producto en la que los defectos críticos se informan, rastrean/localizan, reparan y vuelven a probar de manera efectiva para la implementación final y la reimplementación.
Este proceso de aclarado y repetición se repite hasta que se cumplan las normas de calidad definidas en el SRS.
casos de uso en la industria y las especificaciones técnicas del proyecto.

6. Liberación en el Mercado y Mantenimiento

Una vez que el producto de su organización se ha sometido a pruebas y control de calidad, el producto está listo para ser lanzado formalmente al mercado apropiado.
Dependiendo de la estrategia de su organización a nivel de mercado, el producto puede ser lanzado primero en un segmento/sector limitado del mercado primario antes de ser probado en un entorno empresarial real.
Por el contrario, muchas empresas y startups lanzan su producto en agua fría y revisan los comentarios de los clientes para optimizar continuamente las características del producto y la usabilidad del software.

“Siempre que el diseño/ arquitectura se haya realizado de manera detallada y organizada, la generación de código se puede lograr sin muchos obstáculos logísticos.”

¿Cómo se hace seguro un SSDLC?
Puede hacer que un SSDLC sea más seguro agregando medidas de seguridad adicionales a la base existente de su proceso de desarrollo de SSDLC.
Por ejemplo, un líder tecnológico podría escribir, redactar y hacer cumplir los requisitos de seguridad junto con la recopilación de requisitos funcionales en el SSDLC.
Y durante la fase de arquitectura y diseño, puede realizar un análisis de riesgos para detectar vulnerabilidades específicas.
Se han propuesto una variedad de modelos de ciclo de vida de desarrollo de software seguro y se han aplicado de manera efectiva en frameworks modernos.

Éstos son algunos de ellos:
NIST 800-64: Desarrolladas por los Institutos Nacionales de Estándares y Tecnología, las pautas brindan consideraciones y parámetros de seguridad dentro del SSDLC que deben observar las agencias federales de EE. UU.
Ciclo de vida de desarrollo de seguridad de MS (MS SDL): propuesto por Microsoft en asociación con las fases de un SSDLC clásico, MS SDL es uno de los primeros de su tipo y proporciona consideraciones de seguridad confiables que funcionan para la mayoría de las canales de desarrollo modernas.
OWASP CLASP (proceso de seguridad de aplicaciones ligero y completo): basado en MS SDL, OWASP es muy fácil de integrar en su plan de arquitectura de software existente. Asigna actividades de seguridad a roles en una organización.

Con las crecientes demandas para crear modelos de desarrollo más optimizados y sostenibles con arquitecturas seguras, es fundamental comprender los seis pasos del SSDLC y sus factores de seguridad.
Un SSDLC es metodológico, lo que garantiza que usted, su organización y las partes interesadas involucradas planifiquen, creen e implementen un producto final de manera oportuna y programáticamente eficiente.
Sin embargo, crear el SSDLC correcto requiere los mejores desarrolladores que pueda tener en sus manos.
Por eso, necesitas contratar desarrolladores calificados y confiables que garanticen la calidad e integridad de tus proyectos.

(Crédito: Dreamstime.com)

Implementar la ISO 27701

La norma ISO 27701 se creó como una extensión del Estándar de gestión de seguridad de la información (ISO 27001) y analiza específicamente la protección de la privacidad y cómo las empresas administran la información personal.

Con una aplicación más amplia en comparación con otros estándares, como BS 10012, ayuda a las empresas a cumplir con múltiples regulaciones de privacidad, como el RGPD (Reglamento general de protección de la información) de la UE.

Representa una mejora de ISO 27001, lo que permite a las empresas implementar un sistema que les ayudará a evaluar, reaccionar y reducir los riesgos relacionados con la recopilación, gestión y procesamiento de información personal. Cuando se combinan de esta manera, los dos Estándares crean un Sistema de Gestión de Información de Privacidad (PIMS).

Estos son los principales beneficios de usar el marco ISO 27701:

- Consiente el cumplimiento de una variedad de regulaciones de privacidad, como el RGPD de la UE y la DPA (Ley de protección de datos) del Reino Unido de 2018
  Define roles y responsabilidades clave entre quienes crean, recopilan y procesan información personal (controladores de datos y procesadores de datos)
- Facilita la transferencia segura de información y PII entre diferentes organizaciones y países
- Genera confianza entre clientes, proveedores y stakeholders para acuerdos comerciales más cercanos y efectivos
- Testifica que el contexto del procesamiento de PII se comprenda y se tenga en cuenta para ayudar a las organizaciones a responder a las diferencias jurisdiccionales relevantes.
- Gracias a su marco común, se puede integrar fácilmente con otros sistemas populares, como el Estándar de Continuidad de Negocios (ISO 22301)

Reduce la probabilidad de costosas multas por incumplimiento de las leyes de privacidad
Mejora la reputación global de una empresa
¿Cuánto cuesta la ISO 27701?
El costo de ISO 27701 depende de varios factores. Estos incluyen el sector, la facturación anual y la cantidad de oficinas y empleados que se tiene.

El precio también dependerá de si ya se ha implementado y se ha obtenido la certificación ISO 27001. Esto se debe a que ISO 27701 es una extensión de esta norma y los requisitos para ISO 27701 abarcan ocho cláusulas diferentes y seis anexos.

Si aún no se tiene un sistema de gestión de seguridad de la información ISO 27001, esto no implica que no pueda obtener la certificación. Simplemente se necesita implementarlo al mismo tiempo que ISO 27701, formando un sistema de gestión combinado ISO 27001/ISO 27701.

Suplantación de identidad en redes sociales y aplicaciones móviles: una amenaza en crecimiento

Por Daniel Rojas, Marketing Director LATAM de BlueVoyant

Daniel Rojas
Marketing Director LATAM de BlueVoyant

Al momento de generar una estrategia de protección y mitigación en contra de riesgos cibernéticos es importante lograr una visión en tiempo real de las amenazas digitales. Es mediante la supervisión continua de los dominios y sitios web; las redes sociales; las aplicaciones en las tiendas oficiales y no oficiales; la deep y dark web; la mensajería instantánea y el código abierto, que es posible mitigar las vulnerabilidades de forma rápida y eficaz.

Tal como lo distingue su nombre, el 'brand protection' es el proceso de auxilio y protección a la propiedad intelectual (PI) de las empresas y sus marcas asociadas contra todo tipo de ciberdelincuentes, como hackers o estafadores. La cuestión más importante es la necesidad de detectar y eliminar de forma proactiva los sitios de phishing y los dominios de suplantación de identidad que a menudo tienen como objetivo los servicios financieros, el comercio electrónico, el transporte y otros sectores empresariales.

Esta es quizás una de las herramientas más significativas. Sin embargo, se ignora por completo la actividad que implica la protección continua contra ataques dirigidos a la marca y a sus ejecutivos, directivos, colaboradores y demás usuarios. Partiendo de esta premisa, surgen esfuerzos para fortalecer las acciones que constituyen la protección de la marca, posicionándola como una de las actividades que, a pesar de tener poco reconocimiento, es fundamental para mitigar las amenazas de suplantación y falsificación.

El informe Cost of a Data Breach 2021 de IBM descubrió que las organizaciones afectadas por las vulneraciones de datos sufrieron una media de 4,24 millones de dólares en daños por cada filtración, frente a los 3,86 millones de dólares de sólo un año antes. Las violaciones derivadas de estafas de phishing costaron 4,65 millones de dólares de media, lo que subraya la gravedad potencial de los ataques de phishing que aprovechan los activos de las marcas corporativas.

Según la investigación de BlueVoyant sobre las amenazas potenciales, uno de cada tres consumidores responsabilizaría a la organización perjudicada cerrando su cuenta en línea después de una brecha o poniendo fin a su relación con la empresa por completo.

La idea es tener presente esta información para implementar las mejores prácticas y establecer una columna vertebral de desarrollo de software que conducirá a mejores resultados de productos.

A diario, los atacantes emplean diversos métodos para robar información personal y corporativa, ya sea creando sitios web falsos o difundiendo acciones maliciosas a gran escala a través del correo electrónico.

A medida que varias empresas amplían su presencia digital, los delincuentes intensifican el uso de aplicaciones y redes sociales como vectores de ataque, aprovechando las limitaciones de visibilidad de los activos móviles y las redes sociales de las organizaciones para atacarlas a ellas y a sus clientes.

Las redes sociales y el auge de los influencers digitales constituyen el escenario perfecto para el desarrollo de acciones de fraude coordinadas y agresivas por parte de los ciberdelincuentes. Estas acciones se dirigen tanto a los seguidores de estos famosos como a los mismos influencers digitales con cuentas de valor en plataformas como Instagram o YouTube. Las cifras no mienten y casi el 40% de los influencers en redes sociales tienen seguidores inflados, según el Invesp.

Las actividades en redes sociales, asociadas a los seguidores y a los influencers suponen una relación de desconocimiento o de conocimiento a medias donde grandes cuentas con seguidores inflados pueden ser objeto de afectaciones y amenazas en términos de suplantación, engaño y falsificación. Una media del 55,39% de los influencers realizan actividades fraudulentas, según datos compartidos por el Departamento de Investigación de Statista. El crecimiento de las reclamaciones de recuperación de campañas de phishing exitosas está impactando negativamente en la confianza de los clientes y en la reputación de su marca, desviando los ingresos de su negocio.
Desafortunadamente, las defensas de ciberseguridad a menudo se centran en eventos dentro del perímetro, o son de naturaleza pasiva, lo que puede significar que las amenazas emergentes, como las campañas de malware a gran escala y los ataques dirigidos a una organización específica, sus líderes y empleados, o su ecosistema de proveedores pueden pasar desapercibidos.

La solución propuesta combina el aprendizaje automático con la experiencia en ciberseguridad para descubrir sitios web, cuentas de redes sociales y aplicaciones que suplantan la identidad de una marca, un conglomerado o una organización, al tiempo que ajusta continuamente los parámetros de detección a medida que evoluciona el panorama de las amenazas. Es imperativo destacar que la suplantación de identidad en la web, las redes sociales, así como en las aplicaciones móviles, son los medios utilizados para lograr un grado de éxito en el daño a la marca, debilitando así cualquier esfuerzo previo para proteger o blindar la marca.

Las empresas afectadas se enfrentan a daños en su reputación, costes de litigio, cumplimiento de la normativa, reestructuración de la seguridad, pérdida de producción y productividad. A medida que el panorama de las amenazas se amplía, también lo hacen las consecuencias de unas prácticas de ciberseguridad poco rigurosas.

emBlue

Hacemos que la **omnicanalidad sea simple**

Marketing automation, email, sms, push notifications y más.

NOTICIAS DEL SECTOR IT EN LATINOAMÉRICA

ITWARE
LATAM.COM

- INFORMACION ACTUALIZADA PARA CIOs
- ENTREVISTAS EXCLUSIVAS.
- COBERTURA INTERNACIONAL DE EVENTOS

Manténgase informado suscribiendo a nuestros newsletter

@ITwareLatam @ITwareLatam ITware Latam

ITware Latam ITware Latam

10 AÑOS