GRUPO SMARTEKH S.A DE C.V.

CYBERSEC TRENDS 2023

SIETE TENDENCIAS CLAVE PARA CUBRIR TUS NECESIDADES TÉCNICAS Y DE NEGOCIO

Grupo Smartekh

CONTENIDO

¿QUÉ ESPERAR DEL 2023 Y CÓMO ÉVITAR DISMINUIR RIESGOS? 01
#CYBERSECTRENDS23

TOMA EN CUENTA EL IMPACTO DE LOS ATAQUES DE RANSOMWARE 02
#RANSOMWARE

CONSIDERA LA IMPLEMENTACIÓN DE LAS MEJORES PRACTICAS DE CIBERSEGURIDAD 03
#IAM

AUMENTARÁ LA IMPORTANCIA DE LA ARQUITECTURA ZERO-TRUST 04
#ZEROTRUST

PRIORIZAR LA CIBERSEGURIDAD EN NUEVOS AMBIENTES 05
#SEGURIDADENNUBE

INCORPORAR PRÁCTICAS DE CIBERSEGURIDAD 06
#DEVOPS&AUTOMATIZACIÓN

LA ADOPCIÓN DE IA CRECERÁ EN POPULARIDAD PARA LAS HERRAMIENTAS DE SEGURIDAD 07
#IA

RECONSTRUCCIÓN DE UN CICLO DE ATAQUE EN ENDPOINTS CON UNA PLATAFORMA UNIFICADA 08
#EDR,MDR,XDR

CONCLUSIONES 09
#RECOMENDACIONES

REFERENCIAS 10
#AUTORES

¿QUÉ ESPERAR DEL 2023?

01

A medida que las empresas desarrollan su estrategia para el crecimiento y evolución, los ciberdelincuentes planean nuevas formas de involucrarse con tu equipo, tu información, tus procesos y tu nivel de resiliencia.

NUEVAS FORMAS DE PRIORIZAR

Parece ser que muchas de las industrias después de la pandemia comenzaron a adoptar nuevas tecnologías, identificar la importancia de la ciberseguridad y priorizar la transformación digital en pro de la eficiencia de procesos, aumento de competitividad y resolución de escasez de recursos.

La evolución de las industrias trae consigo muchos beneficios y al mismo tiempo nuevos retos, por lo que es muy importante tomar en cuenta las tendencias tecnológicas para enfrentar de la mejor forma las amenazas, las estrategias, las tácticas tan modernizadas y sofisticadas que los ciberatacantes están por emplear.

Hoy además de contar con tecnología compatible con nuestra infraestructura, debemos aliarnos con especialistas y expertos que nos ayudan a identificar, reaccionar y responder más rápido y mejor. Con la nueva forma en la que los negocios están ejecutando su operación, no solo debemos planificar para proteger nuestros activos más críticos si no para tomar acción en caso de que estos se vean comprometidos y por supuesto asegurar a nuestro equipo de trabajo.

CADA INCIDENTE DE VULNERACIÓN DE DATOS COSTARÁ MÁS DE 5 MILLONES DE DÓLARES EN 2023
-ACRONIS

PARA FINES DE 2023, HABRÁ TRES VECES MÁS DISPOSITIVOS IOT QUE HUMANOS. LA INTERACCCIÓN ENTRE LOS DOS SERÁ CADA 18"
-GARTNER

LA BRECHA DE HABILIDADES EN CIBERSEGURIDAD ACTUAL SE ESTIMA EN 3,4 MILLONES
-(ISC)2

¡HABLEMOS DE CIBERSEGURIDAD!

Opinión

Estamos ante una nueva era de ciberataques, en donde ya no basta con asumir que seremos vulnerados, sino que debemos tener un plan de acción y respuesta ágil que disminuya el impacto al negocio.

@NATMEJIA

Hoy no solo se trata de la estrategia del CIO o el área de TI, debemos contemplar todas las áreas de la organización para contar con una defensa integral.

@RMEJIA

www.smartekh.com

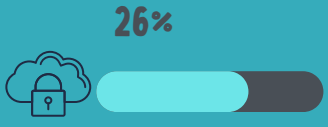
#CyberSecTrends23

¿QUÉ OBJETIVOS DE CIBERSEGURIDAD SE VISUALIZAN EN MÉXICO?

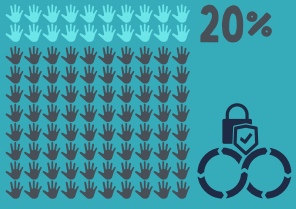
FORTALECER LA CULTURA DE CONCIENTIZACIÓN

CISO AS A SERVICE

Preguntamos a 100 profesionales, entre los que destacan líderes de Seguridad, Responsables de Nube y de Transformación Digital de más de 70 empresas en México. **#CyberSecTrends23**

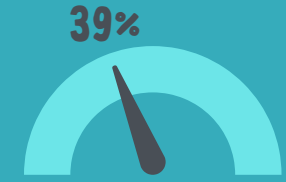


DESPLIEGUE SEGURO DE LA NUBE

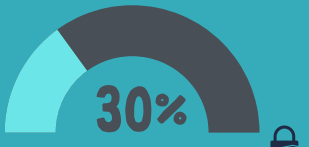


IMPLEMENTACIÓN DE DEVSECOPS

CUMPLIMIENTO DE ESTÁNDARES DE SEGURIDAD



IMPLEMENTACIÓN O CONTRATACIÓN DE SOC



PLAN DE RESPUESTA A INCIDENTES Y RESILIENCIA

¡HABLEMOS DE CIBERSEGURIDAD!

Opinión

Los objetivos de muchas de las organizaciones este 2023 se crearon conforme al crecimiento del negocio, la mejora continua y el aseguramiento de los activos más importantes, entre otros. Los datos presentados en este ebook son estadísticos y fueron obtenidos del registro para el webinar #CyberSecTrends23 realizado el 12 de Enero del 2023 por Grupo Smartekh.

@NATMEJIA

02

TOMA EN CUENTA EL IMPACTO DE LOS ATAQUES DE RANSOMWARE

Existen dos tipos de personas en el mundo: las que ya fueron ciber atacadas y las que serán atacadas en el futuro. Y es que, de acuerdo con los especialistas en ciberseguridad, nadie se salva; personas, empresas y gobiernos son vulnerables a sufrir ciberataques este 2023.

#RANSOMWARE

RANSOMWARE 4.0 AUTOMATIZACIÓN

#RANSOMWARE

Los ciber atacantes también lo automatizaron todo. En este momento, la mayoría del ransomware obtiene acceso inicial, luego se instala como una puerta trasera, y notifica a los servidores de comando y control (C&C) de la pandilla, para que la pandilla de ransomware o sus afiliados puedan conocer a la nueva víctima comprometida.

Tienen todo fríamente calculado, el programa malicioso inicial puede recopilar algunas contraseñas y detalles clave del entorno, descargar e instalar otro malware, en lo que esperan los pasos a seguir o más instrucciones.

Por lo general, se encargan de entrar y usar programas legítimos existentes y scripts personalizados para investigar el entorno y entonces deciden que estrategia pondrán en marcha. Después, comienzan su jugada con nuevas acciones, ya sea la exfiltración de datos o el inicio de las rutinas de cifrado. Esto es lo que hacen actualmente, la mayoría de las veces todo esto es operado y dirigido por humanos después del acceso inicial y la propagación. Sin embargo, utilizar humanos para la investigación, la instalación y la exfiltración requiere mucho tiempo invertido, por ello implementaron la automatización.

Si bien el ransomware es omnipresente y potencialmente devastador, es un modelo para monetizar el acceso a una organización.
El bloqueo del robo de credenciales, phishing, la explotación de vulnerabilidades y botnets ayuda a bloquear las rutas comunes que este malware utiliza para invadir tu red.

RANSOMWARE CON UNA NUEVA VISIÓN: NUBE

13%

AUMENTO EN LAS INFRACCIONES DE RANSOMWARE, MÁS QUE EN LOS ÚLTIMOS 5 AÑOS COMBINADOS.

-VERIZON

70%

EL APOGEO DEL RANSOMWARE CONTINÚA Y ESTÁ PRESENTE EN GRAN PARTE LAS INFRACCIONES DE MALWARE DEL 2022.

-VERIZON

3.6M USD

HUBO UN PROMEDIO DE 270 CIBERATAQUES POR ORGANIZACIÓN EN 2022, Y CADA CIBERATAQUE EXITOSO LE COSTÓ A LA EMPRESA 3,6 MILLONES DE DÓLARES.

-WORLD ECONOMIC FORUM

¡HABLEMOS DE CIBERSEGURIDAD!

Opinión

Un ataque de ransomware abarca los dos primeros de la tríada de la CIA (el 38 % de estos ciberataques tienen algún compromiso de confidencialidad) y por lo tanto la disponibilidad.

@NATMEJIA

Los expertos en seguridad coinciden en que la mejor manera de protegerte frente al ransomware es evitar la infección. Por lo que desarrollar un gran programa de seguridad informática, con protección en tiempo real y puntos clave de concientización es primordial.

@LCRUZ

IMPLEMENTAR UNA ESTRATEGIA DE DEFENSA Y CONCIENTIZACIÓN PARA DISMINUIR EL RIESGO

#RANSOMWARE

Además de mantener un adecuado nivel en la postura de seguridad y desarrollar un plan de concientización sobre la ciberseguridad, hay diez pasos a seguir que ayudarán a disminuir el riesgo y minimizar el impacto de un ataque de ransomware.

Manténte informado del panorama de amenazas en evolución.

Siempre asegúrate de que puedes detectar las amenazas más recientes e implementar las medidas de seguridad nuevas para proteger a tu organización.

Analiza el impacto comercial de la pérdida de datos críticos.

Con ello podrás comprender lo que realmente se encuentra en riesgo, así como las posibles consecuencias ascendentes y descendentes, así podrás priorizar los esfuerzos.

Evalúa la preparación interna y externa.

No olvides incluir terceros, socios o elementos de la cadena de suministro pues son elementos que podrían presentar riesgos, con esta información podrás desarrollar una hoja de ruta integral para la mitigación.

Revisa y pon a prueba tu plan de respuesta a incidentes.

Incluye ejercicios simulados y pon a prueba a los equipos Red, Blue y Purple para solucionar los problemas y reforzar su capacidad de recuperación.

Implementa una estrategia Zero Trust.

Con ello podrás eliminar esa confianza implícita, asegúrate de validar continuamente cada etapa de cada interacción digital para dificultar el trabajo de los atacantes.

Identifica todos tus activos expuestos.

Todo lo que está en la Internet de forma pública, para que puedas tomar medidas y reducir la superficie de ataque.

Prevén las amenazas conocidas y desconocidas.

Al identificar y bloquear continuamente las vulnerabilidades, el malware y el tráfico de comando y control para quitarles cualquier ventaja a los atacantes

Automatiza siempre que sea posible.

Con la ayuda de herramientas como SOAR que admitan la corrección automatizada de eventos para acelerar la capacidad de responder y recuperarte de incidentes.

Asegura las cargas de trabajo en Nube.

Implementa las mejores prácticas y medidas de seguridad a lo largo del ciclo de vida del desarrollo.

Reduce el tiempo de respuesta.

Convierte a los expertos de respuesta a incidentes en una parte de tu equipo, así podrán crear un presupuesto predecible y tomar medidas mucho más rápidas para minimizar el impacto de un ataque.

¡HABLEMOS DE CIBERSEGURIDAD!

Opinión

Una de las mejores formas de defensa contra ransomware es implementar Zero Trust en la organización y si además, se puede adoptar una plataforma de ciberseguridad unificada esto ayudará a obtener visibilidad de un ataque en toda la red.

@NATMEJIA

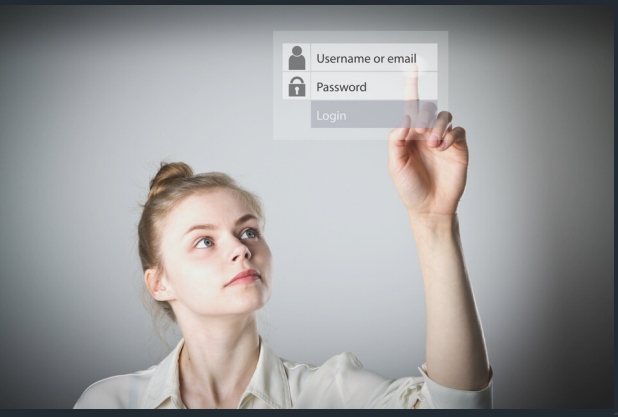
Teniendo en cuenta que, el ransomware es un modelo de monetización del acceso a una organización comprometida. Los operadores de ransomware no tienen que buscar datos específicos como tarjetas de crédito o información bancaria, basta con interrumpir las funciones críticas de las organizaciones cifrando sus datos.

@LCRUZ

CONSIDERA LA IMPLEMENTACIÓN DE LAS MEJORES PRÁCTICAS DE CIBERSEGURIDAD

Las empresas basan su negocio en la confianza digital, la cual está habilitada por IAM, la seguridad y la identidad son hoy más que nunca, una base esencial del ecosistema comercial de una organización.
Es fundamental que los líderes de gestión de riesgos y seguridad diseñen una infraestructura de IAM más flexible y que los equipos de IAM se asocien con otras funciones para cumplir con los requisitos organizacionales cambiantes

#IAM



El uso de credenciales y los permisos que se otorgan son muy importantes dentro de una organización. ¿Te imaginas qué pasaría si no existiera este control? La información, recursos internos o servicios brindados a clientes suelen ser sensibles o de uso restringido o confidencial por ello es muy importante definir un control de acceso con autenticación para poder visualizar, editar o tener control de esta información. Algunas aplicaciones utilizan los controles de acceso de forma automatizada.

#EXPOSICIÓNDEDATOS

AUTENTICACIÓN AUTOMATIZADA

Cada vez son más las empresas que emplean la automatización para la eficiencia de los procesos.

Un escenario de esto, es la obtención del estado de cuenta bancario de forma digital. ¿Qué pasa del lado del usuario? Para lograr visualizar su estado de cuenta, el usuario debe autenticarse a los sistemas del banco mediante credenciales que solo él conoce, una vez autenticado, solicita su estado de cuenta y ¡listo!.

¿Qué pasa del lado del sistema? El sistema principal se autentica a un sistema de almacenamiento (el cual contiene los estados de cuenta) usando credenciales internas que podrían contener indicadores del usuario para identificar quien es el solicitante, así como el permiso del sistema para acceder a la información solicitada, con esto, se valida la información y se brinda el acceso al usuario para visualizar su estado de cuenta.

En ambientes de nube el uso de credenciales y los permisos que se le otorgan al sistema o al administrador de nube se vuelve más crucial, ya que no solo autentican los recursos si no también la infraestructura.

El impacto de no contar con una buena gestión de credenciales puede ser devastador, ya que el atacante podría obtener no solo información privada del usuario, sino también del sistema bancario, lo cual pone en riesgo que se exponga la información del banco y los clientes de manera pública. En nube esto puede ir más allá, pues si un administrador de nube cuenta con permisos excesivos el atacante podría adueñarse de la infraestructura sin que la organización lo note.

¡HABLEMOS DE CIBERSEGURIDAD!

Opinión

De acuerdo con Gartner IAM es una tarea crucial para cualquier empresa. Las empresas que desarrollan capacidades maduras de IAM pueden reducir costos de administración de identidad y lo mejor, pueden ser más ágiles para respaldar nuevas iniciativas comerciales.

@NATMEJIA

Debemos tener presente que si no implementamos las políticas adecuadas de administración de identidad y acceso (IAM), contar con una estrategia de seguridad integral nunca será posible.

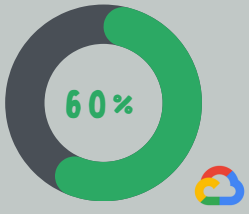
@CSUAREZ

SEGURIDAD EN IAM

los entornos en la nube son más susceptibles a los ataques que en 2020.

Los investigadores de la Unidad 42 de Palo Alto Networks pudieron descubrir y aprovechar las configuraciones incorrectas de IAM para obtener acceso de administrador a todo el entorno de nube de Amazon Web Services (AWS) de un cliente, **una posible violación de datos multimillonaria en el mundo real**. Estos ejemplos resaltan el nivel de gravedad que implica la falta de seguridad de IAM para una organización.

Entre enero y junio de 2021, los investigadores de la Unidad 42 descubrieron que **los entornos en la nube son más susceptibles a los ataques que en octubre de 2020.** En particular, los investigadores realizaron descubrimientos adicionales, que incluyen:

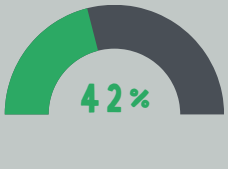


LA CANTIDAD DE ORGANIZACIONES QUE CONFIGURARON EL ALMACENAMIENTO DE GOOGLE CLOUD PARA HACERLOS ACCESIBLE PARA TODOS LOS USUARIOS AUMENTÓ EN UN SESENTA POR CIENTO.

LO QUE PONE LOS DATOS EN MAYOR RIESGO DE SER ROBADOS O EXFILTRADOS.

LA CANTIDAD DE ORGANIZACIONES QUE UTILIZAN AWS AUMENTÓ EN UN VEINTIDOS POR CIENTO.

DONDE LAS CLAVES DE ACCESO NO SE ROTAN DURANTE MÁS DE 90 DÍAS, AUMENTANDO EL RIESGO DE ROBO DE ACCESOS.



LA CANTIDAD DE ORGANIZACIONES QUE NO HABILITARON LA CONFIGURACIÓN DE MFA PARA LAS CUENTAS ROOT EN AWS AUMENTÓ EN UN CUARENTA Y DOS POR CIENTO.

LO QUE ABRE UN GAP DE SEGURIDAD Y ELEVA EL NIVEL DE RIESGO DE ROBO DE CREDENCIALES.

#IAM

IAM ES SOLO UN ASPECTO, AUNQUE CRUCIAL, DE LA SEGURIDAD EN LA NUBE. LAS EMPRESAS DEBEN CONSIDERAR A IAM COMO PARTE DE SU POSTURA DE SEGURIDAD GENERAL

La mejor forma de identificar si tienes que implementar IAM en tu organización ya mismo, es tomarte unos minutos para considerar los siguientes indicadores de un sistema de identidad vulnerable.

- ¿Confías en los sistemas tradicionales basados en contraseñas?
- ¿Confías en el cifrado es suficiente para asegurar tus datos confidenciales?
- ¿Conoces el impacto que podrían tener las credenciales si éstas llegan a ser comprometidas?
- ¿No empleas el inicio de sesión de MFA?
- ¿Utilizas software no integrado, sin soporte o desactualizado?

Si respondiste **¡SI!** a cualquiera de estas preguntas, entonces necesitas fortalecer tu estrategia de IAM para hacer frente a las realidades de 2023.

¡HABLEMOS DE CIBERSEGURIDAD!

Opinión

Los líderes y profesionales de TI se encuentran bajo una gran presión regulatoria y organizacional para proteger el acceso a los recursos. Hoy debemos aprovechar IAM para automatizar estas tareas y contar con el control de acceso granular y la auditoría de los activos en las instalaciones y en la nube.

@KGUARDADO

La innovación alrededor de IAM crece y crece, cada vez son más las empresas que están implementando estas tecnologías obteniendo beneficios inmediatos. Existen diversas soluciones diseñadas para reducir el riesgo al mantener la información de identificación personal con el propietario, no distribuida a través de bases de datos vulnerables a violaciones y robos.

@CSUAREZ

TIPS DE SEGURIDAD PARA IAM

Los proveedores de la nube brindan una excelente línea de base para implementar un enfoque de permisos con privilegios mínimos. A medida que la adopción de la nube aumenta en tu organización, los desafíos se harán evidentes. Se pueden tener en cuenta los siguientes puntos como punto de partida.

CINCO PUNTOS CLAVE A CONSIDERAR:

UNIT 42 BY PALO ALTO NETWORKS

1. **No utilizar cuentas root.** Crea siempre usuarios de IAM individuales con los permisos correspondientes y no proporciones las credenciales root a nadie.
2. **Adoptar un modelo de roles por grupo:** Asigna políticas a grupos de usuarios en función de las cosas específicas que esos usuarios deben hacer. No "acumules" roles de IAM asignando roles a usuarios individuales y luego agregándolos a grupos. Esto hará que resulte más difícil comprender los permisos de forma efectiva.
3. **Otorgar privilegios mínimos:** Solo otorga la cantidad mínima de permisos necesarios para un trabajo. Esto asegurará que, si un usuario o recurso se ve comprometido, el radio de explosión se reduce a una o pocas cosas que se le permitió hacer a esa entidad. Esta es una tarea continua. Como la aplicación esta cambiando debes asegurarte de que los permisos se adapten en consecuencia.
4. **Aprovechar las herramientas del proveedor de la Nube.** Administrar muchos perfiles de permisos a escala es un desafío. Aprovecha las plataformas que ya utilizas para generar conjuntos de permisos con privilegios mínimos y analiza los servicios existentes. Recuerda que la recomendación del proveedor de la nube es revisar siempre manualmente los perfiles generados antes de realizar su implementación.
5. **No utilizar roles o políticas por default.** Los roles y políticas definidos por los proveedores de nube tienen permisos excesivos, los cuales llegan a ser innecesarios para los usuarios y aplicaciones, el usarlos llevaría a un mayor rango de explotación en caso de robo de credenciales. Siempre será más seguro crear los roles y políticas con los permisos mínimos.

#IAM

¡HABLEMOS DE CIBERSEGURIDAD!

Opinión

Grupo Smartekh cuenta con personal especializado y certificado en seguridad de Nube, un hecho de esto son los conocimientos y certificaciones adquiridas por nuestro equipo como son AWS, Azure, CCSK y SANS Institute. Lo cual nos permite brindar servicios especializados comenzado con un Assessment de Nube, que permite conocer si su ambiente sigue las mejores prácticas de seguridad, o qué es lo que falta para cumplir una regulación. El servicio administrado de nube también puede ayudar, ya que se cubriría la necesidad de contratación de personal especializado y brindaría personas con los conocimientos necesarios para mantener la nube segura.

@CSUAREZ

#ZEROTRUST

AUMENTARÁ LA IMPORTANCIA DE LA ARQUITECTURA ZERO-TRUST

Antes del 2020, nadie podría haber previsto una pandemia global que enviaría a los trabajadores a casa y que dejaría a las empresas luchando por comprar dispositivos e implementar soluciones de trabajo remoto. ¿Y quién esperaba el tipo de desafíos brutales en la cadena de suministro que vimos obstaculizando los despliegues tecnológicos y aumentando los costos?

UNA ARQUITECTURA SEGURA CON CONFIANZA CERO

Aun así, mirando hacia atrás, las organizaciones que estaban mejor preparadas para lo inesperado eran aquellas que ya habían estado adoptando tecnologías emergentes que hicieron que sus entornos fueran más ágiles, seguros y fáciles de usar.

ZERO TRUST EL CAMINO A SEGUIR

Del mismo modo, es probable que en 2023 las organizaciones aumenten sus inversiones en áreas clave que los líderes empresariales y de TI con visión de futuro ya han comenzado a implementar como la adopción de nube para promover la agilidad, la disponibilidad y el rendimiento, las medidas de seguridad como el modelo "Zero Trust" ayudan a proteger los entornos de TI en un mundo donde los perímetros físicos han desaparecido.

Las predicciones actuales están reforzando algunas de las principales tendencias del año pasado.

Zero Trust está cobrando impulso en cada empresa, ya que los CISO enfrentan muchos desafíos como la protección de identidades, la gestión de configuraciones de nube cada vez más complejas y una base de endpoints que son remotos.

La transformación digital sin duda es algo que seguirá siendo tendencia en los próximos años debido a la gran cantidad de demanda de fuerza de trabajo remota para las organizaciones y debemos estar preparados para los retos de seguridad que esto demanda, sin duda, ZeroTrust es el camino para seguir.

¡HABLEMOS DE CIBERSEGURIDAD!

ZTNA

ZERO TRUST NETWORK ACCESS (ZTNA) SERÁ EL SEGMENTO DE MERCADO DE SEGURIDAD DE RED MÁS RÁPIDO EN CRECIMIENTO EN TODO EL MUNDO.
-GARTNER

ZERO TRUST

SE PREVÉ QUE ALCANCE UNA TASA DE CRECIMIENTO ANUAL DEL 27.5 % ENTRE 2021 Y 2026.
-GARTNER

ZERO TRUST

EL 90% DE LAS EMPRESAS QUE ESTÁN MIGRANDO A NUBE OPTAN POR UNA ARQUITECTURA DE ZERO TRUST.
-GARTNER

Opinión

De acuerdo con el informe violación de datos de 2022 de Verizon, el 80 % de los ataques a aplicaciones web básicas se pueden atribuir a credenciales robadas. Estos nuevos riesgos señalan la necesidad de un nuevo cambio de paradigma en la seguridad de la red: la respuesta implementar Zero Trust.

@LCRUZ

Si estás pensando en pasar a un modelo de seguridad de Zero Trust, en Grupo Smartekh contamos con equipo certificado y especializado para ayudarte en esta transición de una forma que tal vez no habías pensado. Centrarse en los diferentes componentes que conforman una arquitectura de confianza cero y aprovechar tus herramientas tecnológicas para aplicar esos componentes no tiene por qué ser un dolor de cabeza.

@OFUENTES

Durante años, a los líderes empresariales y de TI se les prometieron herramientas de análisis predictivo en donde se utilizan datos históricos, modelos estadísticos y aprendizaje automático para ir más allá del análisis de las condiciones actuales y pronosticar ágilmente los resultados comerciales. Esas herramientas finalmente están madurando hasta el punto en que las empresas las están implementando en serio.

Pero ¿de qué nos sirve adoptar un modelo de aprendizaje automático basado en estadísticas? Bueno, aprender del pasado, analizar el presente y prepararnos para lo que venga, es el camino que la humanidad sigue para fortalecer las técnicas, tácticas o protocolos a seguir ante el cambio inminente al futuro.

La evolución de “ZeroTrust” con el pasar de los años va añadiendo enfoque en puntos clave como son : gestión de identidades, fuerza de trabajo remoto, accesos a servicios SaaS, adopción de trabajo en nube, accesos seguros, identificación de usuarios, analítica de conexiones entre muchas otras con las que **"nunca debemos confiar, siempre debemos verificar".**

El aumento en el costo de la seguridad empresarial año con año debido a que las filtraciones de seguridad se volvieron cada vez mayores, impulsa a las organizaciones a adoptar una arquitectura de ZeroTrust de manera explícita.

LA ADOPCIÓN DE ZEROTRUST ES UN "MUST"

En un mundo donde las filtraciones de seguridad aumentan año tras año.

El modelo de ZeroTrust argumenta que en ninguna circunstancia se debe confiar en las conexiones de red, ya sea dentro o fuera del entorno de la organización, lo que la adopción de nuevas tecnologías, asignación de privilegios y acceso a recursos debe ser auditado y controlado por las organizaciones.

Adicional, la gestión de accesos debe estar claramente auditada, así mismo asignar el mínimo privilegio acorde al rol del usuario, el acceso debe delimitarse a ciertos retos dependiendo su origen, por ejemplo: estaciones de trabajo, geolocalización, tipo de conexión, entre otros factores.

¡HABLEMOS DE CIBERSEGURIDAD!

Opinión

Implementar este modelo de seguridad ayuda a mitigar el nivel de riesgo. Al verificar quién está accediendo (usuario), a qué recursos (redes, aplicaciones, datos) y desde que dispositivo (equipo de cómputo, dispositivo móvil, IoT y desde que lugar; se puede restringir y tener el control de lo que pasa.

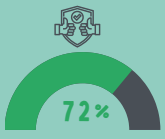
@NMEJIA

Cuando hablamos de seguridad de TI, lo mejor es asumir siempre lo peor. Es por eso que tenemos que pensar en la protección para todas las redes, datos y aplicaciones, implementando las medidas de seguridad de Zero Trust con un enfoque de "privilegio mínimo" en todos los aspectos de la estrategia de ciberseguridad de una empresa.

@OFUENTES

Imaginemos un escenario a inicios de pandemia en 2020; la premura de migrar servicios a nube y facilitar accesos remotos, en varias organizaciones crearon un hueco gigante de seguridad; pero ¿por qué paso esto?. Al crear accesos sin gestionar los privilegios se crearon redes de acceso “seguro” por VPN a recursos internos, pero sin poner foco en las estaciones de trabajo, algunas de ellas de uso personal donde claramente no hay un control de seguridad establecido. La incertidumbre de saber si la persona que está accediendo al recurso realmente es quien dice ser creció y de pronto la seguridad establecida por años dejo de existir en cuestión de semanas. Para finalizar con este trágico escenario, sumemos que los ciber delincuentes obviamente aprovecharon esta situación, comenzaron con el principal vector de ataque: el Phishing. Al caer en la trampa con un phishing destinado a robo de credenciales, imagínate la cantidad de información que estuvo en riesgo...

LA CANTIDAD DE ORGANIZACIONES QUE ESTÁN EN PROCESO DE ADOPTAR ZERO TRUST O YA LO HAN ADOPTADO SON EL SETENTA Y DOS POR CIENTO.



LA CANTIDAD DE ORGANIZACIONES QUE AFIRMAN QUE PROMOVER ZERO TRUST REPRESENTA UNA DE SUS TRES PRINCIPALES PRIORIDADDES DE TI Y SEGURIDAD.

ZERO TRUST PUEDE REDUCIR EL COSTO DE UNA VIOLACIÓN DE DATOS EN APROXIMADAMENTE $ 1.76 MILLONES.

LAS EFICIENCIAS DE SEGMENTACIÓN DE ZERO TRUST SE TRADUCEN EN LA LIBERACIÓN DE CASI 40 HORAS-PERSONA POR SEMANA..

LAS ORGANIZACIONES QUE APROVECHAN ZERO TRUST TIENEN 2 VECES MÁS PROBABILIDADES DE EVITAR INTERRUPCIONES CRÍTICAS DE ATAQUES EN LOS 24 MESES PASADOS.

PARA 2026, SE PROYECTA QUE EL MERCADO ZERO TRUST ALCANCE LOS $ 52 MIL MILLONES.

EXISTEN TRES PUNTOS CLAVE

para disminuir el nivel de riesgo siguiendo el modelo de Zero Trust.

Descubrir e identificar dispositivos.

Necesitas saber quién y qué está en la red en todo momento. Por lo tanto, el primer paso es usar el control de acceso a la red (NAC) para descubrir e identificar cada dispositivo que esté conectado o que busque acceso a la red y asegurarte de que aún no se haya visto comprometido. Los dispositivos que acceden a las redes incluyen dispositivos móviles y de escritorio del usuario final: equipos de oficina en red, sistemas de punto de venta minorista, tecnologías operativas, numerosos sensores distribuidos y dispositivos IoT.

Segmentar la red

Con la microsegmentación de red, cada dispositivo se asigna a una zona de red adecuada en función de una serie de factores, incluidos el tipo de dispositivo, la función y el propósito dentro de la red.

Y la segmentación basada en la intención puede segmentar dispositivos de manera inteligente en función de objetivos comerciales específicos, como requisitos de cumplimiento como las leyes de privacidad GDPR o la protección de transacciones PCI-DSS. La microsegmentación fortalece la red de dos maneras. En primer lugar, rompe la ruta lateral (este-oeste) a través de la red, lo que dificulta que los piratas informáticos y los gusanos accedan a los dispositivos. En segundo lugar, reduce el riesgo de que un hacker utilice un dispositivo infectado como vector para atacar el resto de la red.

Identificar usuarios y roles

La identidad del usuario es otra piedra angular. Al igual que los dispositivos, cada usuario debe identificarse junto con el rol que desempeña dentro de una organización. El modelo de Zero Trust se centra en una "política de acceso mínimo" que solo otorga a un usuario acceso a los recursos que son necesarios para su función o trabajo. Y el acceso a recursos adicionales solo se brinda caso por caso.

#ZEROTRUST

¡HABLEMOS DE CIBERSEGURIDAD!

Opinión

Grupo Smartekh cuenta con servicios especializados y consultoría experta enfocados en el framework de Zero Trust en los que se identifican las herramientas y estrategias que se pueden implementar como la administración de privilegios, la implementación del doble factor de autenticación, el uso de bóvedas de contraseña, el uso y gestión de VPN para conexiones remotas seguras, inspección de integridad del host y campañas de concientización para los usuarios.

@OFUENTES

05

PRIORIZAR LA CIBERSEGURIDAD EN NUEVOS AMBIENTES

Las tecnologías cloud serán uno de los modelos empresariales que más cobrarán sentido en este 2023, gracias a su escalabilidad, almacenamiento, distribución de las cargas de trabajo y seguridad de la información, así como los datos que alojan.

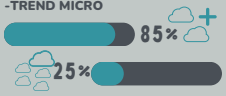
#SEGURIDADENNUBE

RIESGOS DE NUBE QUE COBRAN RELEVANCIA EN 2023

#SEGURIDADENNUBE

LA CONFIGURACIÓN INCORRECTA HA SIDO EL RIESGO DE NUBE MÁS IMPORTANTE Y REPRESENTA HASTA EL SETENTA POR CIENTO DE LOS DESAFÍOS DE SEGURIDAD EN NUBE

-TREND MICRO



HASTA EL OCHENTA Y CINCO POR CIENTO DE LAS EMPRESAS UTILIZAN DOS O MÁS PLATAFORMAS EN LA NUBE, Y EL VEINTICINCO POR CIENTO UTILIZA AL MENOS CINCO

-DELOITTE

LOS RESPONSABLES DE LA TOMA DE DECISIONES DE INFRAESTRUCTURA EN EMPRESAS ESTADOUNIDENSES YA TIENEN EL CUARENTA Y CINCO POR CIENTO DE SU CARTERA TOTAL DE APLICACIONES MIGRADO A A UNA NUBE PÚBLICA.

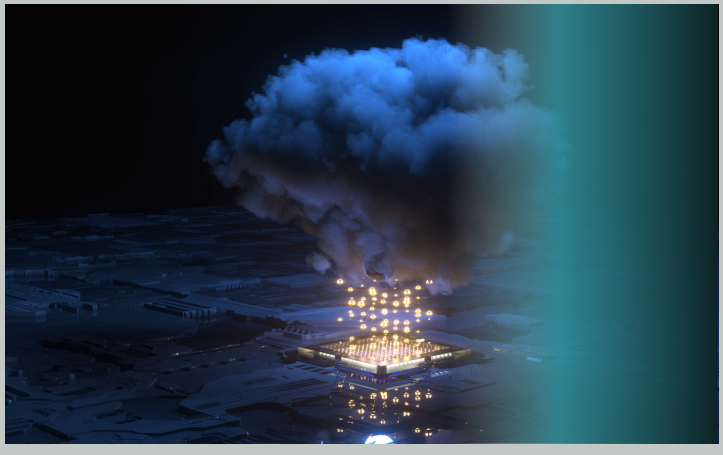
-FORRESTER

Las tendencias dictan que las organizaciones todavía necesitan una postura madura en cuanto a la seguridad de la Nube , independientemente del modelo adoptado. Hay varios retos importantes que los líderes de seguridad, nube y transformación están dejando pasar como el Shadow IT, la gestión de la configuración y cumplimiento de las mejores prácticas de seguridad.

Con la llegada de la Nube y despliegue de nuevos servicios, aplicativos y modelos de negocio, algunos de los equipos se vuelven deshonestos y aceleran los recursos de la nube porque el área de TI es demasiado lenta o mejor dicho, es más sencillo eludir a la administración de TI.

Con ello, el nivel de riesgo aumenta y deja expuestos activos críticos sin que nadie se de cuenta. Sumado a esto, muchas de las organizaciones implementan protecciones dispares en su entorno de nube, sin tomar en cuenta que los controles de cada proveedor suelen ser diferentes; por ejemplo, los controles implementados en Azure son totalmente distintos a los de AWS, tal vez cumplan la misma misión pero su configuración y gestión suele variar.

Para muchos equipos de TI que adoptaron la nube de manera abrupta, implementar conjuntos de reglas y políticas de cumplimiento similares en múltiples nubes se vuelve complejo y lento.



Con la evolución de la Nube, los proveedores agregaron muchas más capacidades con funciones avanzadas como el aprendizaje automático, así la nube se convirtió en una gran opción para cubrir todas las necesidades, en todas partes. Así que a medida que crecía el entusiasmo de los desarrolladores por los últimos servicios y herramientas en la nube, también crecía la cantidad de plataformas que las empresas admitían. Con esto, hoy se ha creado una red enredada de herramientas en la nube que a veces están interconectadas pero con la misma frecuencia son redundantes.

¡HABLEMOS DE CIBERSEGURIDAD!

Opinión

De acuerdo con Deloitte los proveedores de software y nube ahora ofrecen soluciones verticales específicas que modernizan los procesos heredados e impulsan la innovación. Implementarlos es un proceso de ensamblaje, esto libera a los líderes para centrarse en la diferenciación competitiva.

@KGUARDADO

Para simplificar la gestión de múltiples nubes, las empresas están comenzando a recurrir a una capa de abstracción y automatización que ofrece un único panel de control.

@NMEJIA

LOS PASOS A SEGUIR AL ESTAR ENCIMA DE LAS NUBES

Ahora la tendencia nos dicta que los entornos de red se están volviendo cada vez más distribuidos y la fuerza laboral híbrida o remota al cien por ciento crece, por ello es necesario crear una estrategia de defensa para disminuir el riesgo que estas acciones traen consigo pues, abren la puerta a los ataques y al uso indebido de los recursos de la nube. **En este 2023 tenemos que tener muy presente:**

- Como cliente de nube necesitas comprender con precisión el estado de nube completo, tanto interna como externamente.
- Como cliente de nube no se puede gestionar lo desconocido, la visibilidad es clave por lo que es esencial realizar un inventario preciso de los activos en la nube.
- Como cliente de nube debes implementar el cumplimiento y las mejores prácticas de manera integral en todo el estado de la nube, incluidos los entornos de múltiples nubes.
- Como cliente de nube debes hacer cumplir las mejores prácticas y remediar las configuraciones incorrectas antes de un incidente, estas acciones son clave en un programa de seguridad efectivo.

Debido a la complejidad de la nube, la automatización es crucial para fortalecer la postura de ciberseguridad. No es práctico para los equipos verificar de la forma tradicional (manualmente) todo el entorno para obtener las configuraciones correctas. El software nativo de la nube basado en plataforma que puede escanear y verificar la configuración sin intervención humana tiene el doble beneficio de aliviar la carga y detectar errores en tiempo real para reaccionar a tiempo.

EXISTEN CINCO PUNTOS BÁSICOS

para disminuir el nivel de riesgo siguiendo estas buenas prácticas de seguridad.

1. **Monitoreo activo**
   Tener un monitoreo constante y predictivo con alertas instantáneas de amenazas y protocolos de reacción ante incidentes o eventos de seguridad.

2. **Cultura DevSecOps**
   Habilitar y profundizar en una cultura de seguridad y devops.

3. **Herramientas automatizadas**
   Contar con herramientas que permitan tener una automatización para simplificar procesos como la gestión de parches, actualizaciones y monitorización, al mismo tiempo que se gana rapidez y se estandarizan los procesos.

4. **Eficiencia en cargas de trabajo**
   Hacer eficientes las cargas de trabajo con la cantidad justa de información.

5. **Gestión de roles**
   Realizar un barrido de los permisos administrados en operaciones con los que cuentan los usuarios y mantener esto en radar de revisión por lo menos cada mes.

#SEGURIDADENNUBE

¡HABLEMOS DE CIBERSEGURIDAD!

Opinión

Trabajar de la mano con especialistas de ciberseguridad en ambientes multinube, cloud native e híbridos es vital para aprovechar los beneficios, hacer eficiente el proceso de adopción y desarrollar una estrategia de seguridad que minimice la nueva ola de amenazas. En Grupo Smartekh contamos con un equipo especializado en estos ambientes para ayudarte.

@KGUARDADO

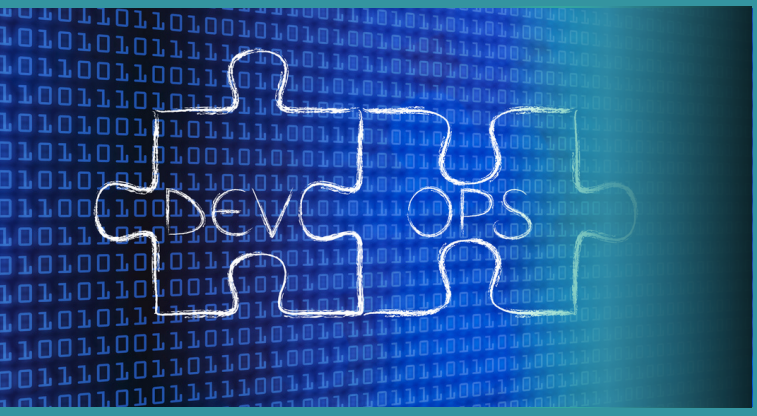
INCORPORAR PRÁCTICAS DE CIBERSEGURIDAD

El panorama económico obligara a las empresas a hacer más con menos, incluidos los departamentos de tecnologías y justamente la cultura DevOps tiene como propósito unificar las áreas de desarrollo y operaciones en un flujo de trabajo continuo para reducir el tiempo y hacer más eficiente la entrega de proyectos.

06

#DEVOPS&AUTOMATIZACIÓN

UNA INTEGRACIÓN Y ADAPTACIÓN CON GRANDES BENEFICIOS



El modelo de DevOps ha tenido una gran adopción en las organizaciones, gracias a que este cambio en la cultura trae muchos beneficios; sin embargo, esta adopción presenta un reto importante para los equipos de seguridad, pues deben integrarse a este cambio de cultura organizacional, adaptando sus procesos y herramientas a este modelo con entregas mucho más agiles.

PARA EL 47% DE LOS PROFESIONALES DEVOPS & DEVSECOPS ES LA METODOLOGÍA DE ELECCIÓN.

-GITLAB

EL 57% DE MIEMBROS DE SEGURIDAD YA CAMBIARON A LA IZQUIERDA O PLANEAN HACERLO ESTE AÑO

-GITLAB

GRAN MEJORA EN AUTOMATIZACIÓN DE PRUEBAS. 47% DE LOS EQUIPOS YA ESTÁN TOTALMENTE AUTOMATIZADOS, UN AUMENTO DEL 25% TRAS EL AÑO ANTERIOR

-GITLAB

EL RETO: SEGURIDAD DESDE EL DISEÑO

La adopción del modelo de DevOps le permitirá a las organizaciones automatizar cada vez más procesos y gracias a esta automatización los profesionales de cada área se centraran cada vez más en decisiones estratégicas y les permitirá hacer más con menos recursos.

Las organizaciones tienen que empezar a adoptar un modelo de seguridad desde el diseño, e integrar capa de seguridad automatizadas en el ciclo de desarrollo de software.
Implementar los controles de seguridad en un modelo DevOps es una tarea complicada pero no imposible.

La complejidad surge debido a que normalmente los equipos de desarrollo son más agiles en sus entregas que el resto de los equipos de TI, por lo que el equipo de seguridad es visto como un "stopper" debido a sus controles y procesos. Todo esto puede generar fricción en el proceso al intentar pasar de un DevOps a DevSecOps. Es por esto que, como responsables y líderes de seguridad tenemos que alinear los procesos y políticas de seguridad con los procesos de DevOps desde el inicio, haciendo que los controles y reglas de seguridad funcionen de forma automatizada.

¡HABLEMOS DE CIBERSEGURIDAD!

Opinión

Algunos controles de seguridad que debemos tener en cuenta para implementar en un entorno de DevOps son: Arquitectura segura y modelado de amenazas en el diseño de la aplicación, Análisis de código estático, Monitoreo continuo de la infraestructura en nube, Seguridad para contenedores, Gestión de llaves y secretos. Si estás pensando en pasar a un modelo DevSecOps, en Grupo Smartekh contamos con equipo certificado y especializado para ayudarte.

@ASANCHEZ

07

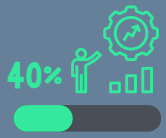
LA ADOPCIÓN DE IA CRECERÁ EN POPULARIDAD PARA LAS HERRAMIENTAS DE SEGURIDAD

Cada vez son más las empresas que adoptan sistemas de inteligencia artificial para optimizar el servicio al cliente, diseñar soluciones inteligentes y autosuficientes; y mejorar su posición competitiva en el mercado.

LA IA YA ES PARTE DE NUESTRO DÍA

El impacto de la inteligencia artificial (IA, o AI por sus siglas en inglés) en las vidas humanas y la economía ha sido enorme. La inteligencia artificial puede agregar alrededor de $15,7 billones de dólares a la economía mundial para 2030. Con varias empresas prediciendo que el uso de IA puede aumentar la productividad empresarial hasta en un 40%, el dramático aumento en el número de nuevas empresas de IA se ha magnificado 14 veces desde 2000. En este panorama se evidencian grandes beneficios de esta tecnología para todas las industrias, pero a ello vienen ligados algunos retos y desafíos.

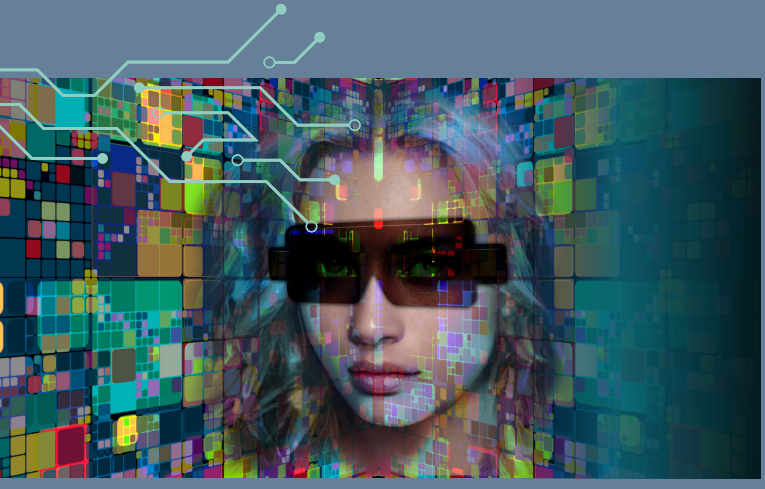
especialmente para las empresas que no están preparadas para competir en un mercado colmado de **automatización robótica de procesos**. El 2022 nos ha dejado grandes avances en IA; si bien su valor es indudable, la pregunta que surge ahora es ¿Cómo usarla mejor?. Y eso, a menudo, se reduce a cuánto confían los profesionales y los usuarios en esta tecnología. Estamos al borde de un cambio, muy grande en 2023.



EL USO DE IA PUEDE AUMENTAR LA PRODUCTIVIDAD EMPRESARIAL HASTA EN UN CUARENTA POR CIENTO.

LA PANDEMIA OBLIGÓ A QUE LOS AVANCES TECNOLÓGICOS DE LOS PRÓXIMOS 7 AÑOS, SE INTRODUJERA DENTRO DE LA REALIDAD SOCIAL EN UN AÑO, ENTRE ELLOS LA IA Y VR.

LAS EMPRESAS ESTÁN INVIRTIENDO EL CINCO POR CIENTO EN NUEVAS TECNOLOGÍAS Y SE PREDICE QUE ESTA INVERSIÓN PUEDE LLEGAR AL VEINTE POR CIENTO EN ESTE AÑO.



De acuerdo con los expertos este año se potenciarán los avances en IA, cada vez más adaptada a los cambios del mundo real, así como las posibilidades del metaverso y las super aplicaciones que reúnen gran cantidad de servicios. Además de innovaciones en tecnologías médicas y el internet de las cosas.

LA IA GENERATIVA DEMUESTRA SU CAPACIDAD EN HABILIDADES HUMANAS QUE HASTA HACE POCO SE CREÍAN A PRUEBA DE LA AUTOMATIZACIÓN: LITERATURA, PINTURA, MÚSICA, ARGUMENTACIÓN JURÍDICA, ETC.

¡HABLEMOS DE CIBERSEGURIDAD!

Opinión

¡Súbete al tren de la IA o quédate atrás! De acuerdo con Forrester el 73% de los responsables de la toma de decisiones en materia de datos y análisis están construyendo tecnologías de IA y el 74% ven un impacto positivo en sus organizaciones por su uso.

@NMEJIA

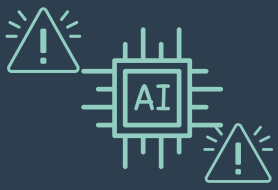
La IA está avanzando muy rápido tanto que, sustituirá muchos empleos, y nos ayudará hacer más rápido y eficientes muchas tareas.

@RRODRIGUEZ

En el caso de la IA adaptativa, la tendencia dicta que surgirán grandes innovaciones para superar los modelos tradicionales de aprendizaje automático que se venían aplicando con el fin de lograr una mejor y más rápida adaptación a las circunstancias del mundo real. Una de las características clave de la IA adaptativa es que permite cambiar el comportamiento del modelo una vez implementado, mediante el uso de feedback en tiempo real. Así el sistema puede monitorear y aprender de los cambios que se producen para reentrenar continuamente los modelos a partir de los nuevos datos y los objetivos ajustados.

LOS RIESGOS Y RETOS DETRÁS DE IA

no solo tecnológicos, también sociales y políticos.



#IA

De acuerdo con un informe de ***The Economist Intelligence Unit (EIU)*** una firma de consultoría trata de responder a las preguntas más frecuentes que seguro surgirán con el desarrollo o implementación de la inteligencia artificial en cuatro sectores principales: la industria, la sanidad, la energía y el transporte.[*1]

El informe se enfoca en las actividades que van a cambiar debido a la IA y los retos que conllevan.

Por ejemplo, la destrucción de empleo en la industria, las dudas sobre la seguridad de los datos privados de los enfermos, la ciberseguridad de las redes eléctricas inteligentes y/o predictivas, y las normas sobre accidentes de tráfico con vehículos autónomos.

Estas son las cinco más importantes:

1. Reconocer los riesgos sociales que implica la Inteligencia Artificial.

El primer paso para solucionar un problema es reconocer que existe, y de acuerdo con los datos del informe es innegable que la IA supone **"un riesgo" para el futuro del empleo**.

2. Regular y mejorar el tratamiento de los datos con la Inteligencia Artificial.

"El uso y abuso de los datos va a ser una de las cuestiones definitorias del siglo XXI", dice el informe, pidiendo la creación de regulaciones específicas que permitan el uso correcto de conjuntos de datos anónimos, respondiendo a las dudas actuales sobre ciberseguridad y privacidad. Pero muy importante: esas regulaciones no deben impedir la circulación de los datos más allá de las fronteras estatales.

3. Explicar, educar y fomentar la transparencia con el uso de la Inteligencia Artificial.

Pedir confianza ciega en los algoritmos es el mejor camino para la desinformación y las distorsiones sobre la IA. **"El mayor reto que afronta la IA es la posible falta de confianza en la tecnología por la ausencia de transparencia sobre cómo toman sus decisiones las máquinas"**, dice Manuela Veloso, jefa del departamento de Machine Learning de la Universidad Carnegie Mellon y uno de los catorce expertos mundiales entrevistados para el informe. Es necesario que los que protagonizan la revolución de la IA expliquen su trabajo y sus intenciones a la sociedad de la forma más sencilla posible.
Tienen un gran poder, y eso conlleva una gran responsabilidad, dice EIU.

4. Adaptar la formación y la educación a la nueva sociedad de la Inteligencia Artificial.

Se trata de trabajar en tres herramientas: La primera: la formación profesional, "que hoy en día está de capa caída en muchos países y deberá cobrar más importancia". La segunda: mantener el foco en las materias de Ciencia, Tecnología, Ingeniería y Matemáticas y no olvidar la importancia de las humanidades, cuya importancia crecerá "por el esperado aumento de la demanda de 'soft skills' como la construcción de equipos, la cooperación y el pensamiento crítico". La tercera: crear una estrecha colaboración entre docentes, empresa y legisladores, ahora más que nunca se necesita esta integración ante la continua evolución de las necesidades formativas.

5. Tender puentes y aumentar la comunicación

De acuerdo a los resultados hay muchas "brechas de entendimiento" respecto al desarrollo de la inteligencia artificial, pero probablemente la más importante sea la que separa a los expertos técnicos de las empresas y los dirigentes políticos. Para maximizar los potenciales beneficios del impacto económico y social de la inteligencia artificial, son necesarias políticas públicas que puedan mitigar sus efectos negativos, por ejemplo en el mercado laboral, sin limitar los positivos.

Opinión

Uno de los retos más relevantes de la llegada de IA es la privacidad y seguridad de los datos. Lo cierto es que el factor principal en el que se basan todos los modelos de aprendizaje automático es la disponibilidad de datos y recursos para entrenarlos. Pero, debido a que estos datos se generan a partir de millones de usuarios a nivel mundial, hay un alto porcentaje de que que existan vulnerabilidades y se utilicen con malos propósitos. La recomendación aquí empezar a crear estrategias de defensa y protección para evitar el compromiso de los datos.

@RRODRIGUEZ

¡HABLEMOS DE CIBERSEGURIDAD!

*1 https://www.eiu.com/n/

#EDR,XDR,MDR

08 RECONSTRUCCIÓN DE UN CICLO DE ATAQUE EN ENDPOINTS CON UNA PLATAFORMA UNIFICADA

EDR, MDR y XDR son soluciones de detección y respuesta vitales para reconstrucción de los endpoints. Estas soluciones monitorean TI todo el tiempo (las 24 horas del día, los 7 días de la semana, los 365 días del año) y nos alertan sobre cualquier amenaza potencial.

DETECCIÓN Y RESPUESTA

gestionadas proporcionan una ventaja importante sobre los atacantes.

Seguro recuerdas el clásico episodio de “I Love Lucy” y su aventura en la fábrica de chocolates. Están trabajando en la línea de producción de una fábrica de chocolate y les indican que serán despedidos si les pasa algún chocolate sin envolver. Todo comienza de maravilla, pero de repente la línea se acelera y comienzan a recibir más y más chocolates, intentan de todo hasta que no pueden seguir el ritmo; así que deciden envolver solo unos cuantos chocolates al azar. ¿Qué tiene que ver esto con las tendencias de seguridad? Aquí vamos, imagínate que los chocolates son alertas de seguridad; "chocolates" que tu equipo recibe de distintas tecnologías. ¿A cuál deberían darle prioridad?, ¿Qué maniobras deberían realizar para poder revisar todas las alertas? ó al menos las marcadas como urgentes o críticas.

Día a día los equipos de seguridad se enfrentan a muchas más herramientas que informan miles de alertas a uno, dos o tres profesionales; si algunos carecen de las habilidades para contextualizar o analizar la información y filtrar las vulnerabilidades críticas del ruido, imagínate lo que sucede. Hay muchas vulnerabilidades críticas que pasan desapercibidas y que pueden provocar grandes daños a la organización.

Las predicciones dictan que el aumento en ataques de ransomware, filtraciones de datos y explotación de vulnerabilidades continuará y se sofisticará para 2023. De tal forma que se estarán enviando más "chocolates" a los equipos de seguridad de la cantidad máxima que pueden manejar. Por ello, además de la implementación de las mejores prácticas de seguridad, los líderes deben desarrollar una estrategia que les permita monitorear activamente las amenazas al mismo tiempo que buscan nuevas y se preparan para responder en cualquier momento. La implementación de sistemas EDR (Endpoint Detection and Response) de la mano de una estrategia de formación o concientización a los usuarios son primordiales para disminuir el riesgo.

#EDR,XDR,MDR

¿POR QUÉ ES IMPORTANTE?

CUANDO NUESTRO EQUIPO DE SERVICIOS Y THREAT HUNTING REALIZA LA INTEGRACIÓN CON PLATAFORMAS EDR, XDR, MDR OBTIENE INFORMACIÓN DE FORMA INMEDIATA, LA ANALIZA Y CONTEXTUALIZA PARA IDENTIFICAR LA ACTIVIDAD DE LOS CIBERATACANTES Y TOMAR ACCIONES A TIEMPO.
EN MUCHOS CASOS, EL BLOQUEO EN ALGUNA DE LAS FASES DE LA CADENA DE ATAQUE YA SUCEDIÓ GRACIAS A LA AUTOMATIZACIÓN, BASTA CON VERIFICAR Y VALIDAR ESTAS ACCIONES. CON ESTO, SE HAN DETENIDO A TIEMPO CIENTOS DE ATAQUES "INVISIBLES" PARA MUCHOS.

La visibilidad, protección y mitigación que otorgan las soluciones de detección y respuesta para endpoint (EDR) son esenciales para el análisis, la protección y la remediación en tiempo real, sin importar desde dónde se trabaje, cómo se trabaje y cuándo se trabaje.

¡HABLEMOS DE CIBERSEGURIDAD!

Opinión

No solo debemos pensar en que nuestro equipo cuente con herramientas que les ayuden abordar la llegada de más y más chocolates para responder con éxito, sino que debemos desarrollar una estrategia en donde además de aprovechar la tecnología, se considere la integración de las herramientas y el expertise para contextualizar los datos recibidos, profundizar en el análisis y tomar acciones de recuperarse que impacten mínimamente a la organización.

@NATMEJIA

#VISIBILIDAD

¿POR QUÉ LA ADOPCIÓN DE PLATAFORMAS EDR, XDR, MDR?

Las organizaciones que buscan activamente más visibilidad en su "superficie de ataque" como las, nubes, redes, activos, cuentas y sistemas optarán por un enfoque de plataforma propio o administrado.

En promedio las organizaciones cuentan con 46 herramientas de monitoreo de seguridad individuales, esto se vuelve un verdadero reto para los equipos de seguridad, al recibir alertas diarias que no están correlacionadas y muchos falsos positivos, lo que aumenta el riesgo de que un verdadero ataque pase desapercibido. Ante la nueva ola de amenazas y estrategias que se avecinan en 2023 los líderes deben priorizar la implementación de una plataforma de ciberseguridad unificada que brinde visibilidad y permita automatizar para disminuir el riesgo.

Lo que debemos tener muy presente es que para ser realmente eficaz, una plataforma deberá combinar la información de seguridad y la gestión de eventos (SIEM) con detección y respuesta ampliadas (XDR) , inteligencia artificial y análisis, para proporcionar una vista integrada de todo el entorno de TI/nube y correlaciones a profundidad y de una adecuada contextualización de alertas para disminuir los falsos positivos y priorizar la atención, Es aquí donde cobra sentido un EDR sofisticado, ya que con toda esta integración también se puede incluir la detección de endpoints, el monitoreo de la defensa de la red, así como la defensa contra las vulnerabilidades de día cero

Para los equipos de TI abordar cada tipo de vulnerabilidad por separado requeriría docenas o más de soluciones dedicadas.

Debido a que cada solución se enfoca en su propio nicho, no existe una correlación de datos de todo el entorno o si existe es muy limitada para identificar, analizar y priorizar las amenazas. Por ello, la adopción de plataformas es necesaria.

Forrester ve un valor creciente y prometedor en la Detección y respuesta extendida (XDR) y detección y respuesta gestionada (MDR) de la mano de especialistas y a través de servicios de seguridad administrados. Pues consideran que las soluciones XDR proporcionan detecciones de comportamiento en todas las herramientas de seguridad para brindar alertas de alta eficacia, contexto adicional dentro de las alertas y la capacidad de detectar, investigar y responder desde una única plataforma.

¡HABLEMOS DE CIBERSEGURIDAD!

Opinión

Hay cuatro objetivos clave de las estrategias de los ciberatacantes: Credenciales, Phishing, Explotación de vulnerabilidades y Botnets. Los cuatro son omnipresentes en todas las áreas según el DBIR 2022, y ninguna organización está segura sin un plan para manejar cada uno de ellos. Por esto, implementar una estrategia con plataformas EDR, XDR y MDR es una de las mejores opciones para los líderes.

@NATMEJIA

Con una plataforma de ciberseguridad unificada, las organizaciones pueden proteger los datos y los recursos en entornos públicos, privados, híbridos y de múltiples nubes con visibilidad de extremo a extremo.

@KGUARDADO

Si bien, muchas organizaciones ya cuentan con equipos de SOC, la mayoría de las ocasiones terminan persiguiendo una infinidad de alertas día tras día; en donde los falsos positivos generan mucho ruido y solo algunos llegan a indicar el mismo problema raíz al tener una visión diferente desde diversas aristas. Por ejemplo, una de las herramientas puede indicar una amenaza de correo electrónico, al mismo tiempo que otra genera una alarma sobre las credenciales mal utilizadas, cuando en realidad estas alertas separadas son parte del mismo ataque, y esto se descubre hasta que el atacante ya logro su cometido.

43% DE LOS GERENTES DE SOC INFORMAN HABER DESACTIVADO LAS ALERTAS

DE LOS GERENTES DE SOC INFORMAN QUE LAS HAN IGNORADO POR COMPLETO **40%**

-Estudio Global de Trend Micro

Adoptar este tipo de plataformas brinda enormes beneficios empezando porque puedan identificar amenazas de alta prioridad y calcular su puntaje de riesgo por sí solas, y además; ofrecer acciones recomendadas de mitigación. Por ejemplo, hablando de un escenario híbrido, el uso de estas plataformas no solo puede notificar sobre una configuración incorrecta de la nube, sino que además puede sugerir la solución, y con esto se disminuye la carga operativa para el equipo de seguridad. Así mismo, las plataformas más avanzadas también ayudan a acelerar la capacidad de respuesta del SOC al llevar a cabo esquemas de remediación automática e incluso funciones de cumplimiento para contar con reportes para las auditorías.

Apostar por estas plataformas también permite a los líderes, lograr más con menos, ya que muchas de las organizaciones cuentan con equipos pequeños o escasez de talento. Así, en lugar de realizar grandes inversiones para el aprendizaje o expertise de diversas herramientas y marcos de seguridad, las organizaciones pueden utilizar tecnología automatizada, inteligente e integrada para cubrir toda la superficie de ataque, evaluar y priorizar el riesgo, integrarse con proveedores líderes en la nube y cubrir las amenazas que afectan los endpoints, el correo electrónico y la red. , entornos IoT y más.

O bien, pueden optar por contratar estos servicios con terceros que cuentan con un alto nivel de expertise, profundo conocimiento en tecnologías y análisis de amenazas centrados en detectar y detener amenazas más rápido, al mismo tiempo que se mejora la madurez de la ciberseguridad y ciberdefensa de la organización.

"No quiere un enfoque dividido y no quiere concentrarse en cada punto individual. Podría capacitar a expertos en la materia si tiene suficiente gente y tiempo, pero la mayoría de las organizaciones no lo hacen" .

MIKE MILNER, VICEPRESIDENTE DE TECNOLOGÍA EN LA NUBE, TREND MICRO

#EDR,XDR,MDR

¡HABLEMOS DE CIBERSEGURIDAD!

Opinión

En Grupo Smartekh creemos que la gestión del riesgo cibernético de la superficie de ataque exige un ciclo continuo y repetitivo de descubrimiento, evaluación y mitigación. Por ello, ayudamos a nuestros clientes con servicios administrados de la mano de plataformas de seguridad unificadas con funcionalidades automatizadas para sostener este ciclo y personal experto en el análisis y contextualización de la información.

@NATMEJIA

ENTONCES PARA 2023,

Los líderes de Ciberseguridad, Nube y Transformación Digital deberán desarrollar sus estrategias apegándose a los frameworks de seguridad y cumplimiento para disminuir la superficie de ataque, aumentar su competitividad y fortalecer su postura de seguridad.

Para hacer frente a amenazas cada vez más sofisticadas, a las estrategias de ransomware en expansión y ciberatacantes que también aprovechan la automatización, Nube, DevOps, IA, IoT para lograr su cometido. Aquí compartimos acciones clave para tomar el desarrollo de una estrategia de ciberseguridad integral.

- Implementar Zero Trust y ZTNA aprovechando los marcos existentes.
- Desarrollar Secure Culture Management ó un plan de concientización a usuarios.
- Desarrollar un plan para adoptar "Shift Left" a fin de detectar los errores en el diseño que pueden aprovecharse en una estrategia de ataque.
- Crear un Plan de Respuesta a Incidentes que permita a la organización recuperarse lo más pronto posible y con el mínimo impacto.
- Priorizar políticas para gestionar las identidades y detener gran parte de los ataques modernos.
- Crear un plan con seguridad para Nube desde su adopción, haciendo frente a los retos y riesgos en crecimiento y sofisticación.
- Implementar controles de seguridad desde el diseño de arquitecturas DevOps acorde con los requisitos de la industria.
- Trabajar de la mano de especialistas y expertos, pues la brecha de habilidades es un reto importante y la curva de aprendizaje suele ser lenta..

#CONCLUSIONES

Las organizaciones que buscan más visibilidad en la "superficie de ataque" que incluye las nubes, redes, activos, cuentas y sistemas optarán por un enfoque de plataforma propio o administrado.

-Trend Micro

REFERENCIAS

RANSOMWARE
https://blog.knowbe4.com/ransomware-3.0-it-is-about-to-get-much-worse
https://blog.knowbe4.com/these-grim-figures-show-that-the-ransomware-problem-isnt-going-away
https://blog.knowbe4.com/ransomware-and-fraudulent-funds-transfer-are-the-two-main-drivers-of-cyber-loss
https://www.zdnet.com/article/these-grim-figures-show-that-the-ransomware-problem-isnt-going-away/
https://www.weforum.org/agenda/2022/04/cybersecurity-ransomware-radio-davos/
https://www.ibm.com/es-es/topics/ransomware
https://www.infobae.com/america/tecno/2022/12/12/brasil-mexico-y-peru-son-los-paises-latinos-con-mas-ciberataques-en-2022/
https://www.verizon.com/business/resources/reports/dbir/2022/results-and-analysis-intro-to-patterns/
https://www.ibm.com/downloads/cas/EV6NAQR4
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2022-unit42-ransomware-threat-report-final.pdf
https://unit42.paloaltonetworks.com/2022-ransomware-threat-report-highlights/
https://www.trendmicro.com/fr_fr/ciso/22/l/cyber-security-posture-2023-predictions.html
IAM
https://www.gartner.com/en/articles/iam-leaders-plan-to-adopt-these-6-identity-and-access-management-trends
https://valasys.com/importance-of-cloud-iam/
https://www.techtarget.com/whatis/8-Reasons-Identity-and-Access-Management-Is-Important
https://www.paloaltonetworks.com/blog/2020/02/cloud-iam-security/
https://unit42.paloaltonetworks.com/highlight-cloud-threat-report-iam/
https://unit42.paloaltonetworks.com/iam-misconfigurations/
https://simeio.com/blogs/identity-security-lessons-from-2022-and-trends-in-2023/

Zero Trust
https://venturebeat.com/security/2023-cybersecurity-forecasts-zero-trust-cloud-security-will-top-spending/
https://biztechmagazine.com/article/2022/12/tech-trends-2023-predictive-analytics-edge-computing-and-zero-trust-will-be-hot?utm_source=Social+Media&utm_medium=Twitter&utm_campaign=Edge+Computing+News&utm_term=
https://www.cybertalk.org/2022/08/05/12-zero-trust-statistics-and-trends-in-2022/#:~:text=Zero%20Trust%20Statistics%202022,three%20IT%20and%20security%20priorities.
https://www.sctelecom.com.mx/post/tres-consejos-para-mejorar-la-seguridad-con-zero-trust

IA
https://softimiza.co/blog/retos-y-desafios-de-la-implementacion-de-inteligencia-artificial
https://blogs.elconfidencial.com/tecnologia/tribuna/2022-12-29/tendencias-tecnologicas-telefonica-tech-jose-cerdan-2023-inteligencia-artificial_3549010/
https://www.iproup.com/innovacion/36899-tendencias-que-se-viene-en-tecnologia-en-el-2023
https://www.merca20.com/predicciones-de-la-inteligencia-artificial-para-el-2023/
https://www.bbva.com/es/cinco-recomendaciones-revolucion-inteligencia-artificial/

DEVOPS & AUTOMATIZACIÓN
https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-integrating-and-automating-security-into-a-devsecops-model.pdf
https://about.gitlab.com/developer-survey/
https://www.paloaltonetworks.com/cyberpedia/what-is-devsecops

EDR, XDR, MDR
https://www.siriuscom.com/2021/10/how-managed-detection-and-response-expands-team-resources/
https://www.forrester.com/bold/planning-guide-2023-technology-executives/
https://www.optiv.com/insights/source-zero
https://www.issa.org/cybersecurity-skills-crisis-continues-for-fifth-year-perpetuated-by-lack-of-business-investment/
https://revistabyte.es/tendencias-tic/xdr-estrategias-de-seguridad/
https://www.ibm.com/downloads/cas/3VANOMEA
https://cambiodigital-ol.com/2022/11/5-formas-en-que-forrester-predice-que-la-ia-sera-indispensable-en-2023/
https://www.issa.org/cybersecurity-professionals-push-their-organizations-toward-vendor-consolidation-and-product-integration%ef%bf%bc/
https://www.tec-innova.mx/predicciones-de-amenazas-para-2023/
https://www.spiceworks.com/it-security/cyber-risk-management/interviews/top-cybersecurity-trends-2023/
https://www.rapid7.com/blog/post/2022/09/21/prioritizing-xdr-in-2023-stronger-detection-and-response-with-less-complexity/
https://www.ibm.com/blogs/ibm-anz/this-type-of-data-breach-will-cost-you-more-time-and-money/
https://www.trendmicro.com/fr_fr/ciso/22/l/cyber-security-posture-2023-predictions.html
https://www.trendmicro.com/fr_fr/ciso/22/k/unified-security-platform.html

SEGURIDAD EN NUBE
https://www.forrester.com/bold/planning-guide-2023-security-risk/
https://www.paloaltonetworks.com/blog/prisma-cloud/secure-cloud-express-2-0/
https://www.trendmicro.com/es_mx/business/products/hybrid-cloud/cloud-one-workload-security.html
https://www2.deloitte.com/mx/es/pages/technology/articles/tech-trends-2022.html

#CYBERSEC TRENDS23

Este ebook fue desarrollado por el equipo de Grupo Smarekh para brindarte información de valor que ayude a tu organización y a todo tu equipo para tomar decisiones estratégicas y minimizar la superficie de ataque.

Ayudo a las organizaciones a desarrollar e impulsar estrategias de ciberseguridad, adecuándose a las necesidades del negocio para lograr una transformación digital segura y exitosa.
@OFUENTES

Ayudo a las organizaciones a impulsar el negocio con la tecnología de manera segura, creando sinergia entre gente, herramientas y procesos.
@LCRUZ

Desarrollo estrategias de ciberseguridad para impulsar el poder de la tecnología y hacer más competitivo al negocio, minimizando la superficie de ataque en ambientes de Nube y DevOps.
@RRODRIGUEZ

Diseño estrategias de seguridad para Nube alineados a los marcos de seguridad y cumplimiento que se adecuen al modelo de negocio, disminuyendo el nivel de riesgo.
@CSUAREZ

Ayudo a empresas a desarrollar una estrategia de ciberseguridad ad hoc con los retos y necesidades del negocio.
@NMEJIA

Creo estrategias de ciberseguridad para asegurar los activos en infraestructura de Nube y DevOps, impulsando los beneficios y minimizando la superficie de ataque.
@ASANCHEZ

Ayudo a potenciar a las empresas a través de canales digitales, mediante estrategias de contenido, posicionamiento de marca, fidelización y generación de clientes potenciales.
@KGUARDADO

Ayudo a las empresas a proteger sus activos críticos y planificando la conciencia de seguridad del usuario final. Te ayudaré a hacer de la tecnología de seguridad una parte fundamental en las decisiones empresariales.
@RMEJIA

Si estás pensando en implementar algunas de las acciones clave o quieres profundizar en recomendaciones puntuales para tu negocio en Grupo Smartekh contamos con equipo certificado y especializado para ayudarte en esta transición de una forma que tal vez no habías pensado.

Agenda aquí una charla con uno de nuestros Consultores Expertos.

Grupo Smartekh

CYBERSEC TRENDS 2023

Grupo Smartekh

www.smartekh.com