Microsoft

Crear una empresa resiliente y de confianza

El trabajo híbrido llegó para quedarse. Si bien se presentan nuevos retos, también nuevas posibilidades de reinventar la forma en que personas la seguridad. A continuación, conoce algunos consejos e información que te darán, como líder en la seguridad de tu empresa, más argumentos para tomar mejores decisiones y fortalecer en los clientes el establecimiento de una relación de confianza.

Tendencias y riesgos en seguridad cibernética

Todo lo que debes tener en cuenta a la hora de tomar una decisión sobre la arquitectura de seguridad en tu empresa según las encuestas 2021 Gartner CIO Survey y 2020 Gartner CISO Effectiveness Survey.

1 Malla de ciberseguridad

Un enfoque moderno de arquitectura que permite implementar y distribuir la seguridad donde más se necesite.

2 Tableros cibernéticos inteligentes

Las juntas están formando comités dedicados que se enfocan en discutir asuntos de seguridad cibernética, aumentando el poder de escrutinio y ayudando a los CISO a mejorar su comunicación y toma de decisiones.

3 Consolidación de proveedores

Los grandes proveedores de seguridad están respondiendo con productos mejor integrados.

4 Identidades seguras

La "seguridad de la identidad ante todo" representa ahora la forma en que funcionarán todos los trabajadores de la información - independientemente de si se encuentran en lugares remotos o en la oficina.

5 Gestionar las identidades de las máquinas como una capacidad de seguridad crítica

A medida que aumenta la cantidad de dispositivos, los certificados de las máquinas permitirán asegurar mejor la transformación digital.

6 El trabajo remoto ahora es solo trabajo

El 64% de los empleados ahora pueden trabajar desde casa, y 2/5 partes están trabajando desde casa.

7 Simulación de infracciones y ataques

La simulación de violaciones y ataques (BAS) ofrece pruebas y validaciones continuas de los controles de seguridad y, a través de una variedad de técnicas de ataque, permite mejores evaluaciones de seguridad casi en tiempo real.

8 Técnicas de computación que mejoran la privacidad

Están surgiendo técnicas de computación para mejorar la privacidad (PEC) que protegen los datos mientras se utilizan, en lugar de cuando están en reposo o en movimiento, para permitir el procesamiento, intercambio, transferencias transfronterizas y análisis de datos seguros - incluso en entornos que no son de confianza.

Simplificar la seguridad

Calificación

Muchas empresas tienen arquitecturas de seguridad complicadas con una pila de soluciones de endpoint. Podemos ayudarte a fortalecer tu seguridad al:

- Eliminar silos difíciles de supervisar
- Automatizar procesos manuales intensivos
- Simplificar la gestión con soluciones integradas

El 82% de las organizaciones que consolidan su portfolio de seguridad informan un menor riesgo de violación.

Consolidación para alcanzar la efectividad de costos

El 81% de los profesionales de seguridad informan sentirse presionados para reducir costos. Al consolidar tus soluciones de seguridad, podrás:

- Reducir costos de licencia al reemplazar hasta 40 productos diferentes
- Reducir los costos de las operaciones de seguridad
- Reducir los costos de implementación al aumentar la eficiencia de la integración y obtener un acceso de valor más rápido

Caso de éxito

Caribbean Development Bank mejora la seguridad y permite el trabajo remoto gracias a soluciones de Microsoft.

El banco consolidó su transformación digital al descontinuar varias soluciones de terceros y centralizar la gestión de dispositivos en una plataforma única y fácil de usar. Esto les asegura el acceso a apps de productividad con capacidades avanzadas de analítica, así como capacidades de cumplimiento normativo que otorgan una estricta protección de la identidad y los datos.

Sus administradores ahora pueden agregar y asignar rápidamente apps móviles a grupos de usuarios, configurar apps para que se ejecuten con configuraciones específicas habilitadas, además de actualizar sistemas y apps - todo con seguridad avanzada y automatizada.

> *Una vez que empezamos a aprovechar las soluciones en la nube, nuestro equipo de TI tuvo tiempo para interactuar de manera más proactiva con los usuarios empresariales, permitiéndoles enfocarse en soluciones automatizadas y en la creación de aplicaciones rápidas y fáciles de usar.*
>
> Julio Lima, CIO, Caribbean Development Bank.

> *Al implementar las soluciones de seguridad de Microsoft y trasladar nuestras operaciones a la nube, hemos logrado un desempeño que, de otra manera, solo hubiera sido posible si la gran mayoría de nuestro personal estuviera totalmente dedicado al reconocimiento y prevención de amenazas.*
>
> Angus Aird, jefe de prestación de servicios, Caribbean Development Bank.

Beneficios:

- Mayor visibilidad y control sobre los datos
- Mejora en la analítica para identificar y combatir las ciberamenazas en todos los servicios de nube
- Reducción del footprint de su app en más del 30%
- Migración del 90% de las antiguas apps del banco hacia máquinas virtuales en Azure

Una mirada más amplia

Si no logras mirar tu empresa en su totalidad, se abren las brechas para las vulnerabilidades. Busca soluciones que:

- Te brinden la máxima visibilidad de todo tu patrimonio digital
- Utilicen inteligencia artificial incorporada para hacer que la detección de amenazas sea más inteligente y rápida
- Reúnan datos de todas las fuentes

Desarrollar fundamentos bajo el concepto de ciberhigiene

- Estar al día con la claridad de los datos
- Actualizar los parches
- Utilizar la autenticación multifactorial (MFA) y el inicio de sesión único
- Implementar un enfoque Zero Trust
- Realizar una evaluación Zero Trust para analizar tu panorama de identidad de usuario existente y aprender a implementar una estrategia Zero Trust eficiente.

Aprovechar la inteligencia

Brinda a los equipos de seguridad mejores herramientas y capacitación para detectar amenazas y reducir el riesgo interno.

- Capacitar al equipo ayuda a las personas a concentrarse en los incidentes de seguridad clave
- Reducir el "estrés por alerta" y liberar tiempo para enfocar en lo que realmente importa
- Obtener una solución completa para la detección de alertas y la respuesta a amenazas

Hacer de las personas el centro de la estrategia cibernética

Ofrece una experiencia unificada para el usuario final

Dado que el trabajo remoto juega un rol clave en las estrategias de trabajo flexible, brinda a los empleados:

- Herramientas familiares y seguras
- Acceso a apps y datos desde sus propios dispositivos
- Seguridad fácil de usar con inicio de sesión único y MFA

Conexión constante

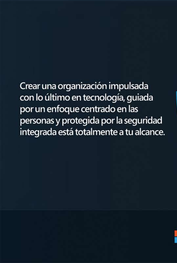
Mantente en contacto con socios y clientes, sin comprometer la seguridad. Aplica las funciones de seguridad que utilizas dentro de tu empresa, como MFA, a todas las identidades externas.

> *El tema de la ciberseguridad debe estar cada vez más presente en las agendas de los altos ejecutivos y consejos de administración, después de todo con el mundo virtual y real cada vez más conectado, es esencial tomar medidas para aumentar la resiliencia operativa frente a los ciberataques. No se trata de si tu empresa será atacada o no, sino cuando. Sólo hay dos tipos de empresas, las que han sido atacadas y conocen y las que no saben.*
>
> Marcelo Zillo, Chief Security Advisor, Microsoft Latin America

Invertir en la creación de equipos diversos

Cultivar un equipo cibernético diverso puede impulsar la innovación. Las empresas con visión de futuro buscarán:

- Emplear a más mujeres y personas pertenecientes a minorías étnicas
- Crear equipos con un rango de edad y una distribución geográfica más amplios
- Cerrar la brecha de habilidades digitales con una mejor capacitación y una cultura de seguridad cuidadosamente desarrollada



Crear una organización impulsada con lo último en tecnología, guiada por un enfoque centrado en las personas y protegida por la seguridad integrada está totalmente a tu alcance.