accenture

Emerger más fuertes con seguridad adaptable

Pasos para lograr un futuro más flexible y seguro

AHORA DESPUÉS

SUPERAR
LA INCERTIDUMBRE

A medida que los impactos sanitarios y humanitarios de la pandemia del COVID-19 evolucionan, también aumentan los desafíos económicos y de los negocios. Las organizaciones que buscan equilibrar sus necesidades inmediatas con oportunidades a más largo plazo percibirán las compensaciones a través de tres oleadas de impacto: el Ahora, el Después y la Nueva Normalidad.

El Ahora incluye un énfasis en respaldar a las personas, los clientes y los proveedores. El Después se caracterizará por reenfocar el negocio para resistir ante nuevas amenazas y aprovechar nuevas oportunidades. Y la Nueva Normalidad requerirá enfrentar cambios rápidos en las normas, los valores y los comportamientos.

Este es el momento para reinventar los modelos de negocios y reintegrar el valor proporcionado por las organizaciones en un nuevo contexto social. Ha llegado la hora de forjar una mentalidad audaz de transformación de los negocios, impulsada por nuevos enfoques de tecnología y liderazgo responsable.

Desafíos de seguridad

La resiliencia operativa se está convirtiendo rápidamente en una métrica clave de negocios para todas las industrias.[1] Los equipos de seguridad suelen responder ante las constantes amenazas y el cambio continuo. Cada día, defienden a sus organizaciones contra adversarios nuevos o ya existentes cuyos objetivos son robar, engañar o interrumpir las operaciones de negocios.

Todo ha cambiado. Para los directivos de las organizaciones, las conversaciones diarias sobre las operaciones y los beneficios ahora incluyen la supervivencia del negocio, la seguridad y la resiliencia . Más aún, el trabajo remoto desde los hogares ha abierto nuevos vectores de ataque y desafíos para la fuerza laboral, incluyendo las amenazas internas.

Los líderes de seguridad están bien posicionados para realizar los cambios prácticos que mantengan a sus organizaciones seguras y protegidas y ayuden a las personas a adaptarse a nuevas formas de trabajo que mejoren la seguridad a largo plazo. Sin embargo, deben adaptarse de dos maneras. En primer lugar, deben trasladar el actual foco en el riesgo y la resiliencia de los negocios a las discusiones más amplias de planificación ejecutiva. En segundo lugar, deben adoptar medidas para construir un nuevo negocio más resiliente desde cero.

Los líderes de seguridad están en una posición privilegiada para actuar como personas claves e influyentes.

Desafío 1

Las organizaciones se replantean su cultura, sus prácticas colaborativas y la tecnología necesaria para viabilizar ambientes de trabajo distribuidos a escala. Si bien algunos cambios son a corto plazo, deben prepararse para superar la incertidumbre del futuro.

Desafío 2

Los atacantes maliciosos se aprovechan que las organizaciones reconfiguran sus cadenas de abastecimiento vulnerables, ofrecen más experiencias digitales y satisfacen las crecientes demandas de una fuerza laboral remota.

Desafío 3

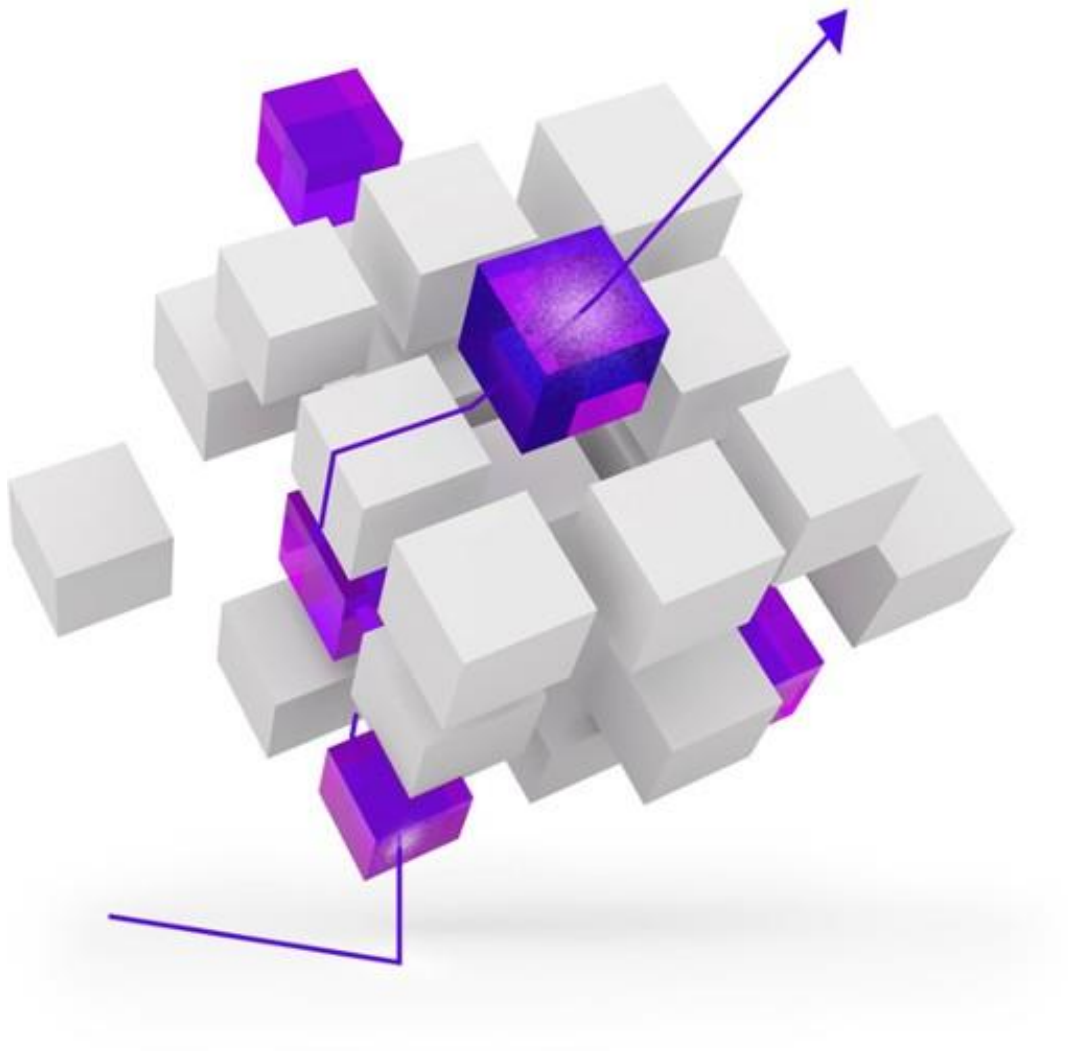
Los líderes de seguridad deben adaptarse para proveer servicios a nuevas prioridades de negocios, mejorando la manera de detectar, defenderse y recuperarse de las amenazas, frente a demandas sin precedentes.

¿Dónde estamos ahora?

Los ciber atacantes se aprovechan de la susceptibilidad de los nuevos trabajadores remotos, ofreciendo señuelos y trampas que imitan fuentes creíbles.

Los Centros de Operaciones de Seguridad deben aprovechar la inteligencia de las amenazas tácticas, operativas y estratégicas para identificar las tendencias y tecnologías que amenazan la continuidad del negocio.

En estos tiempos difíciles, los líderes de seguridad tienen la oportunidad de replantear su estrategia y las tecnologías desde cero.



Entender los riesgos

Cinco preguntas fundamentales pueden determinar cómo proteger mejor el ambiente de trabajo.

¿Quién es una amenaza potencial?

Los ciberatacantes que han intentando violar la seguridad antes seguramente lo intentarán de nuevo. Cabe recordar que constantemente surgen nuevas amenazas, por ejemplo, mientras las naciones tratan de aprovechar los nuevos entornos de trabajo remoto[2].

¿Cuáles son los vectores lógicos de las amenazas?

Consideremos los miles de nombres de dominio relacionados con el coronavirus que surgieron desde enero de 2020, creando nuevas oportunidades de violar las defensas de ciberseguridad[3].

¿Cuál es el impacto de la desinformación?

A medida que las personas buscan información, los atacantes intentan aprovecharse de la confusión e incertidumbre para penetrar las cíber defensas.

Comunicar primero puede ayudar a que la desinformación pierda su poder.

¿Dónde están tus vulnerabilidades?

Preguntar qué acciones concretas puede adoptar la empresa para mejorar la ciberseguridad en el contexto actual. Reconocer los presupuestos que pueden verse afectados casi inmediatamente y planificar en consecuencia.

¿Cómo se puede construir un negocio más resiliente?

Considerar a futuro las vulnerabilidades adicionales de seguridad y el soporte cultural necesario para el trabajo remoto, la importancia de la identidad y autenticación digital, y los datos, las herramientas y técnicas necesarias para mitigar los nuevos desafíos para monitorear a toda la organización.

Actuar ahora

A medida que las organizaciones estabilizan sus operaciones actuales, los líderes de seguridad pueden establecer los controles adecuados para crear un ambiente de trabajo seguro y protegido para su organización. A continuación presentamos cuatro elementos de seguridad adaptable* que se pueden aplicar ahora:

01

Mentalidad segura

Priorizar el factor humano

Los líderes de seguridad continúan desempeñando un rol en el mantenimiento de la salud y el bienestar de la fuerza laboral, que es esencial para la continuidad operativa de la organización y ayuda a mitigar los riesgos para la comunidad en general.

02

Acceso seguro a la red

Proteger la infraestructura de la empresa

Los líderes de seguridad pueden informar a los empleados sobre las vulnerabilidades conocidas y asegurarse de que sus equipos sean diligentes en lo que respecta a pruebas e inteligencia.

03

Ambientes de trabajo seguros

Ser brillante en lo básico

Dado que los empleados trabajan ahora de manera remota, los líderes de seguridad deben cambiar el enfoque de seguridad de la información de una infraestructura empresarial a un entorno virtual y en la nube.

04

Colaboración segura

Proporcionar las herramientas y los equipos para enfrentar los riesgos

Los líderes de seguridad están bien posicionados para evaluar y promover soluciones que permitan a los equipos distribuidos conectarse y colaborar en forma segura, protegida y eficiente, ayudando a sus organizaciones a crear mejores experiencias para los empleados, y mejorando, al mismo tiempo, su productividad.

*Ver página 10 del Apéndice para más información sobre estos cuatro elementos

Actuar después

Las decisiones sobre cómo las organizaciones funcionan a corto plazo tienen un efecto en cadena sobre cómo funcionarán en el futuro. A medida que se revisen o eliminen las restricciones relacionadas con el COVID-19 para la actividad social y empresarial, las organizaciones deben pensar de manera más amplia cuál será su enfoque de seguridad.

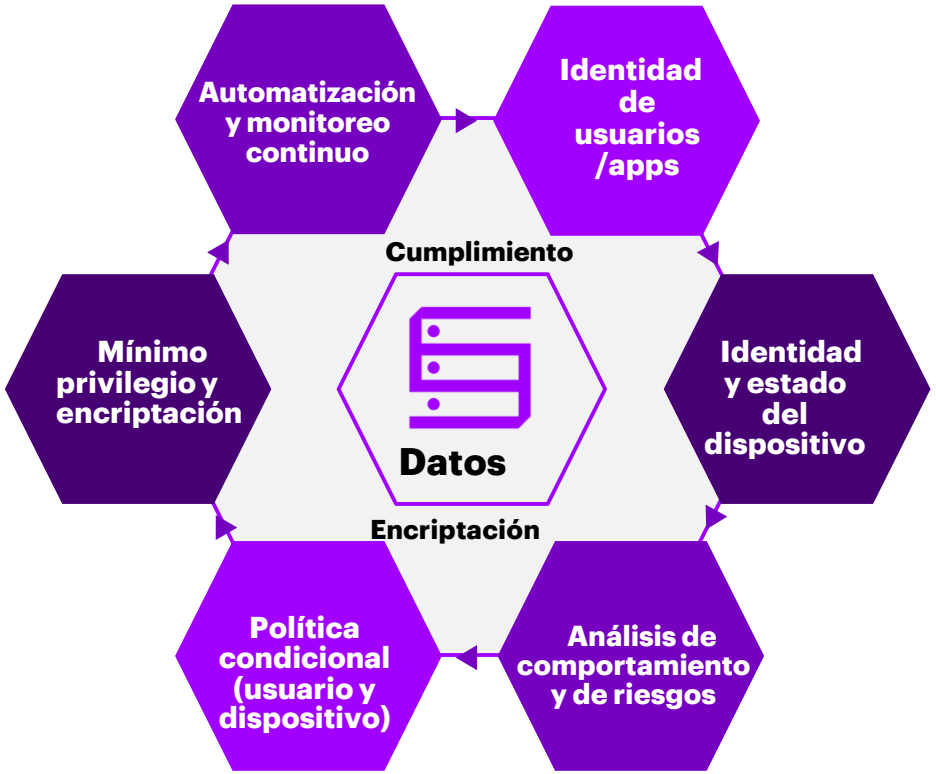
La seguridad adaptable permite que las organizaciones proporcionen una experiencia segura y protegida para continuar las operaciones. Los líderes de seguridad pueden reinventar los accesos usando soluciones basadas en cloud para satisfacer la mayor demanda de acceso remoto rápido, seguro y protegido a los datos y aplicaciones de la empresa.

El uso de un marco de confianza cero para para la autenticación ayuda a proteger el acceso remoto mediante la autenticación multi-factor, autenticación adaptable, prevención de fraude, prueba de identidad, análisis de comportamiento y biometría, y telemetría de dispositivos.

Los empleados empoderados pueden colabora mejor y proteger los datos de la compañía , pero se debe equilibrar la confianza con vigilancia. Los profesionales de seguridad pueden ayudar, proporcionando simulaciones para realizar una prueba de estrés de los procesos existentes, usando al mismo tiempo pruebas de penetración y *red teams* para identificar las brechas o áreas de mejora.

La implementación rápida de un marco de confianza cero con tecnología incorporada puede facilitar el acceso remoto seguro, sin tener que basarse en las soluciones tradicionales de red privada virtual (VPN).

SEGURIDAD ADAPTABLE —UN MODELO DE CONFIANZA CERO



Emerger más fuertes

AHORA DESPUÉS

Las prácticas de seguridad que sirven tanto para las necesidades actuales como para las futuras, requieren que los líderes de seguridad y sus organizaciones:

01 PIENSEN "EN CUALQUIER MOMENTO , EN CUALQUIER LUGAR"

Asegurar a todos los usuarios, dispositivos y tráfico de red de manera uniforme con el mismo grado de efectividad, independientemente de dónde se encuentren. Recordar que el acceso seguro a la red y las aplicaciones son tan rápidos con seguridad como sin ella, o incluso más rápidos.

02 SEAN TRANSPARENTES

Dar acceso a los usuarios a lo que necesitan y cuándo lo necesitan. Hacer que estos cambios sean transparentes para ellos, sin crearles "obstáculos" para que hagan su trabajo de manera efectiva.

03 INSPIREN CALMA Y CONFIANZA

Los líderes de seguridad pueden ser los catalizadores del cambio, usando la empatía y compasión para proporcionar una respuesta más ágil. El uso de seguridad adaptable crea confianza; por ejemplo, las organizaciones pueden usar cloud o expandir el acceso a usuarios más remotos.

04 SIMPLIFIQUEN, CUANDO SEA POSIBLE

Considerar los servicios gestionados y automatizar cuando tenga sentido. Por ejemplo, la respuesta ante eventos de seguridad, la implementación de herramientas y la gestión de reglas pueden beneficiarse a partir de una intervención humana limitada.

05 CONSTRUYAN PARA LOGRAR RESILIENCIA

A medida que las organizaciones buscan salir fortalecidas, los planes de continuidad del negocio y gestión de crisis deben ser adecuados para este propósito. Interactuar con los líderes del negocio para planificar, prepararse y practicar para lograr una mayor resiliencia en ciberseguridad, respaldada por los recursos y las inversiones adecuadas.

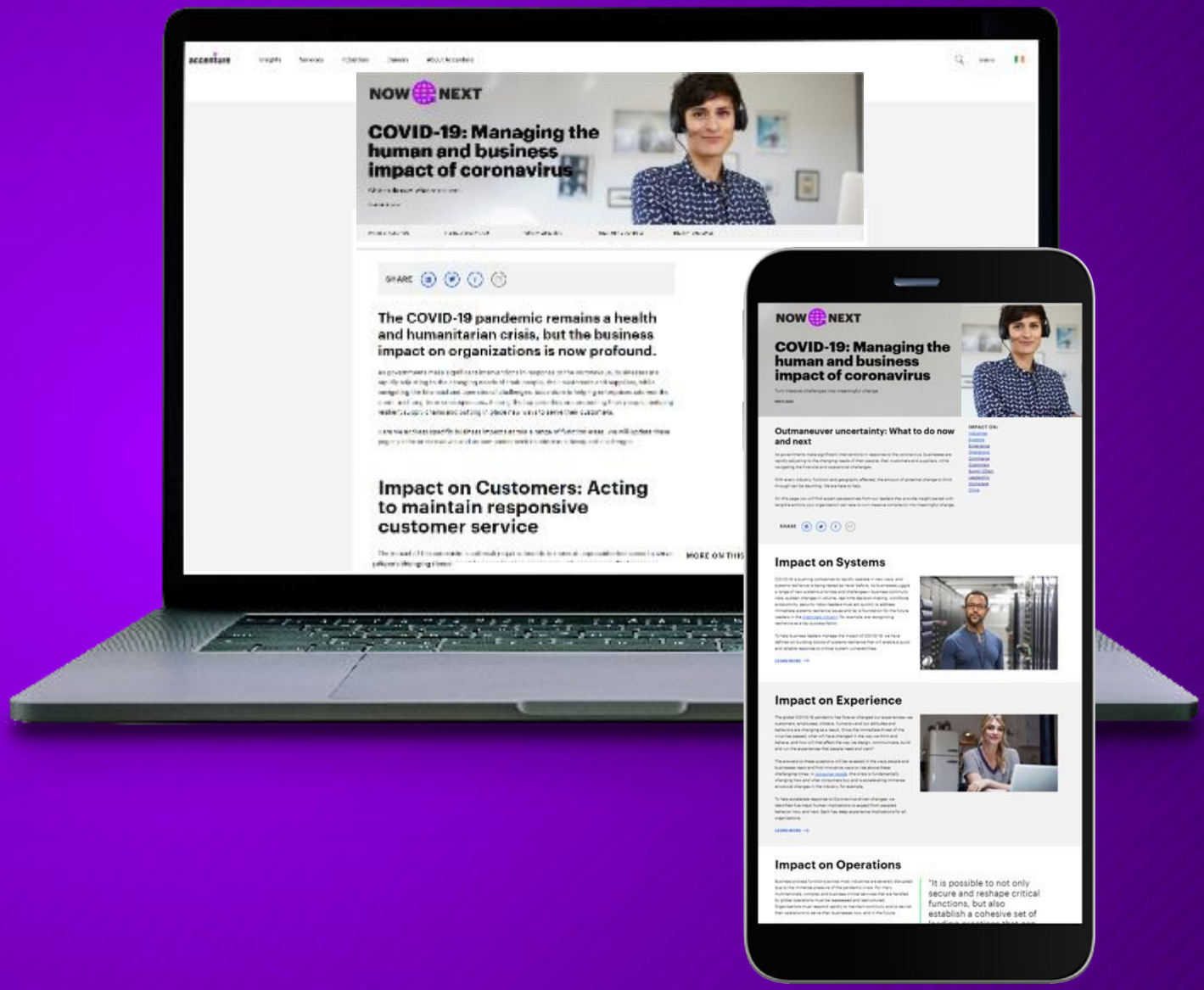
Accenture cree que una estrategia de gestión de crisis multidimensional, con varios flujos y equipos de trabajo que colaboren estrechamente a diario, es la respuesta a la resiliencia de la seguridad y puede ayudar a proteger a las personas.

Para ayudar a nuestros clientes a enfrentar el impacto del COVID-19 en los seres humanos y los negocios, hemos creado un sitio que contiene nuestras más recientes opiniones y tendencias sobre una amplia variedad de temas relacionados.

Cada tema destaca acciones específicas que podrían adoptarse ahora y qué debemos considerar después, a medida que las industrias avanzan hacia la nueva normalidad.

Actualizamos el sitio constantemente con temas que abarcan desde los aspectos esenciales de liderazgo hasta la productividad para tus equipos de empleados y de servicio al cliente, y la construcción de una cadena de abastecimiento resiliente. Visitalo periódicamente para ver los nuevos contenidos y perspectivas.

VISITÁ NUESTRO SITIO AQUÍ



Apéndice

Una lista de acciones para ayudar a reaccionar y estabilizarse ahora

A medida que las organizaciones estabilizan sus operaciones actuales, los líderes de seguridad pueden implementar los controles adecuados para crear un ambiente de trabajo seguro para su organización. A continuación presentamos cuatro elementos de seguridad adaptable que se pueden aplicar ahora:

1. MENTALIDAD SEGURA

Priorizar el factor humano

Los líderes de seguridad continúan desempeñando un rol en el mantenimiento de la salud y el bienestar de la fuerza laboral, que es esencial para la continuidad operativa de la organización y ayuda a mitigar los riesgos para la comunidad en general. Estos líderes deben:

- Ser pragmáticos y colaboradores para dar un mejor soporte a la fuerza de trabajo remota. Capacitar rápidamente a los usuarios sobre los riesgos potenciales del trabajo remoto, incluyendo el *phishing* o el uso de aplicaciones de Software-as-a-Service (SaaS) de colaboración no autorizadas.
- Inculcar un espíritu de trabajo entre los empleados donde la seguridad siempre esté primero, manteniéndolos informados sobre los procedimientos de protección de la información de la compañía, incluyendo a aquellos relacionados con encriptación de discos rígidos y archivos almacenados y en tránsito. Es posible que se necesite cierto compromiso, como por ejemplo que los empleados utilicen dispositivos personales en ciertas circunstancias o como medida provisoria. Asegurarse que las computadoras y los dispositivos incluyan las versiones más recientes del sistema y las aplicaciones.
- Considerar el lado humano de mantener la continuidad de las operaciones. Las personas están lidiando con miedos y dificultades personales que deben manejarse con sensibilidad y apoyo. Por ejemplo, el cierre de las escuelas puede tener un impacto significativo en la capacidad de los empleados para ser productivos. Además, trabajar con otros líderes de negocios para reconocer a los empleados, cuando corresponda, con el objetivo de mejorar el bienestar y el compromiso entre los equipos, tanto a nivel local como global, lo que contribuye a mantener la continuidad del negocio.[4]
- Ser empáticos y estar disponibles para sus equipos. Utilizar tecnología de transmisión de video aprobadas por la empresa para discutir la situación y las acciones que su organización está tomando para proteger a su gente y permitirles trabajar con mínima interrupción.[5]

Apéndice

2. ACCESO SEGURO A LA RED

Proteger la infraestructura de la empresa

Los líderes de seguridad pueden informar a los empleados sobre las vulnerabilidades conocidas y asegurarse de que sus equipos sean diligentes en lo que respecta a pruebas e inteligencia.. Estos líderes deben:
:

- Realizar pureas de penetración para evaluar las capacidades existentes de acceso remoro seguro, inclusive las limitaciones relacionadas con el ancho de banda y los usuarios, y complementar las soluciones existentes con conectividad segura basada en cloud que pueda ser implementada en cuestión de días.
- Aprovechar la inteligencia de las amenazas para identificar Tácticas, Técnicas y Procedimientos (TTPs) y métodos de ataque comunes que apuntan a los empleados que trabajan en forma remota y acceden a las redes de la empresa. Capacitar a la fuerza laboral para identificar estas señales de alerta temprana.
- Reconocer que el trabajo remoto depende de *routers* domésticos de WiFi y de conexiones a través de VPN con la infraestructura de la empresa, que podrían generar configuraciones erróneas con riesgo de pérdida y hurto de información confidencial de la compañía. Capacitar a los empleados sobre las mejores prácticas de las redes domésticas de la siguiente manera:
    - Planificando medidas de emergencia para trabajar y realizar comunicaciones telefónicas y fuera de la red, ya que muchos proveedores de VPN pueden experimentar problemas con la gran afluencia de usuarios que se conectan a la red.
    - Recordándoles a los empleados que cambien la contraseña de administrador que viene por defecto en sus *routers* para que sea sólida y única, habiliten WPA2 o WPA3 para encriptar la actividad *online* y creen una sólida contraseña para el uso de la red. También deberían deshabilitar la búsqueda de otras redes y las carpetas compartidas al conectarse a una nueva red.
- Investigar las soluciones VPN u otras soluciones de gestión de activos que posibiliten el inventario y la aplicación de parches en sistemas distribuidos y endpoint.

Apéndice

3. AMBIENTES DE TRABAJO SEGUROS

Ser brillante en lo básico

Dado que los empleados trabajan ahora de manera remota, los líderes de seguridad deben cambiar el enfoque de seguridad de la información de una infraestructura empresarial a un entorno virtual y en la nube. Los líderes de seguridad deben:

:

1. **Asegurar los escritorios virtuales**

- Invertir e implementar herramientas de respuesta y detección de endpoints (EDR). Incorporar analytics y automatización para reducir la cantidad de intervención humana requerida y proteger mejor múltiples dispositivos en ubicaciones menos seguras. Introducir directivas claras (definición de acceso, *provisioning/deprovisioning*, controles de segregación de tareas y recertificación) para reducir la superficie de ataque y limitar la oportunidad de errores y atacantes maliciosos.
- Incorporar soluciones de escritorios virtuales seguros, como por ejemplo Citrix, para evitar exposición a internet pública a raíz del uso en dispositivos no gestionados sin autenticación de dos factores ni imágenes de escritorio seguras.

3.2 Dispositivos personales gestionados seguros

- Saber que las nuevas soluciones del tipo “traiga su propio dispositivo” (BYOD) pueden crear riesgos de seguridad. La actual infraestructura de actualización / aplicación de parches puede asumir que los dispositivos están dentro de las instalaciones o son gestionados.
- Usar inteligencia ante amenazas para identificar si se han recolectado credenciales o si los atacantes están vendiendo el acceso en la Deep Web y Darknet.

3.3 Acceso seguro, basado en políticas

- Implementar gestión de acceso privilegiado para el acceso de alto impacto (mayor seguridad, como por ejemplo rotación de contraseñas, grabación de sesiones y analytics relacionado con el acceso privilegiado) para reducir el riesgo de escalamiento de privilegios por parte de un atacante que ingresa a través de su ruta de acceso remota. Incorporar accesos basados en políticas que creen accesos a “todo o nada” para las aplicaciones de SaaS que requieren dispositivos totalmente gestionados sin riesgo. Implementar gestión avanzada de accesos (autenticación basada en riesgos y autenticación multi-factor) para reducir el compromiso de riesgo con el acceso proporcionado.

Apéndice

4. COLABORACIÓN SEGURA

Proporcionar las herramientas y los equipos para enfrentar los riesgos

Los líderes de seguridad están bien posicionados para evaluar y promover soluciones que permitan a los equipos distribuidos conectarse y colaborar en forma segura, protegida y eficiente, ayudando a sus organizaciones a crear mejores experiencias para los empleados, y mejorando, al mismo tiempo, su productividad. Estos lideres deben:

:

- Adoptar y medir la colaboración con la implementación y el uso de herramientas de colaboración a gran escala, y mediante la provisión de lineamientos específicos y prescriptivos sobre la seguridad en el trabajo remoto. Establecer lineamientos claros sobre cómo compartir información de manera segura, en base a la clasificación de los datos, la audiencia y el tipo de contenido.
- Aprovechar al máximo las prácticas líderes, aceptando que no todo el trabajo puede realzarse de manera remota. En función de esto, ajustar las expectativas tanto dentro de los equipos de la organización y a lo largo del ecosistema de *stakeholders*.
- Ser flexibles e innovadores con las últimas tecnologías. Comunicar claramente qué software y herramientas oficialmente aprobados pueden ser usados para el trabajo remoto, incluso el que permite compartir archivos, realizar videoconferencias, colaboración virtual tipo *whiteboard* y chats.
- Anticipar el aumento en el volumen y la carga proveniente del uso de herramientas de colaboración, a raíz de una mayor cantidad de empleados que trabajan de manera remota, mejorando al mismo tiempo la usabilidad y productividad. Fomentar la realización de sesiones virtuales a gran escala usando plataformas de transmisión interactivas y conferencias web para respaldar el cambio de talleres y conferencias presenciales a virtuales.

Contactos

Kelly Bissell
Senior Managing Director
Global Lead
Accenture Security
kelly.bissell
@accenture.com

Ryan LaSalle
Managing Director
North America Lead
Accenture Security
ryan.m.lasalle
@accenture.com

Paolo Dal Cin
Managing Director
Europe Lead
Accenture Security
paolo.dal.cin
@accenture.com

Andrew McLauchlan
Managing Director
Growth Markets Lead
Accenture Security
andrew.mclauchlan
@accenture.com

David Fitch
Managing Director
Accenture Security
david.fitch
@accenture.com

Wayne Mattadeen
Managing Director
Accenture Security
wayne.o.mattadeen
@accenture.com

Referencias

1. Productivity in Uncertain Times through the Elastic Digital Workplace, Accenture, marzo 2020. https://www.accenture.com/us-en/about/company/coronavirus-solution-elastic-digital-workplace

2. Communication is the answer to cyberthreats in a crisis, Accenture, abril 2020. https://www.accenture.com/us-en/blogs/cyber-defense/communication-is-the-answer-to-cyberthreats-in-a-crisis

3. Ibid.

4. Continuity in Crisis: How to run effective business operations during the COVID-19 pandemic, Accenture, abril 2020. https://www.accenture.com/us-en/insights/operations/coronavirus-effective-business-operations

5. Productivity in uncertain times through the elastic digital workplace, Accenture, marzo 2020. https://www.accenture.com/us-en/about/company/coronavirus-solution-elastic-digital-workplace

Acerca de Accenture

Accenture es una compañía global líder en servicios profesionales que provee una amplia gama de servicios y soluciones en estrategia, consultoría, desarrollos digitales, tecnología y operaciones. Combinando su experiencia inigualable y sus habilidades especializadas en más de 40 industrias y en todas las funciones de negocios —respaldadas por la red de Delivery Centers más importante del mundo— Accenture trabaja en la intersección del negocio y la tecnología para ayudar a sus clientes a mejorar su desempeño y crear un valor sostenible para todos los involucrados. Con 509.000 empleados que prestan servicios a clientes en más de 120 países, Accenture impulsa la innovación para mejorar la manera en que el mundo trabaja y vive.

Visitanos en **www.accenture.com**

Acerca de AccentureSecurity

Accenture Security es proveedor líder de servicios integrales de ciberseguridad, que incluyen ciberdefensa avanzada, soluciones de ciberseguridad aplicada y operaciones de seguridad gestionada. Aportamos innovación en materia de seguridad, sumada a la escala global y a una capacidad de provisión de soluciones a nivel mundial a través de nuestra red de Advanced Technology e Intelligent Operations centers. Con el respaldo de nuestro equipo de profesionales idóneos, ayudamos a los clientes a innovar de manera segura, desarrollar cíber resiliencia y crecer con confianza. Seguí a @AccentureSecure en Twitter o visitanos en www.accenture.com/security.