PC COM Mayorista

censornet.

CIBERSEGURIDAD EN HOME OFFICE

Desafíos Críticos de Seguridad 2020

CIBERSEGURIDAD EN HOME OFFICE

Desafíos Críticos de Seguridad 2020

Estamos en un nuevo momento decisivo en la historia del trabajo y la tecnología. Desde que comenzo la cuarentena por el COVID-19, los profesionales de seguridad y TI de todo el mundo se han enfrentado a desafíos extraordinarios. Prácticamente de la noche a la mañana, casi todos los empleados se convirtieron en "trabajadores remotos", dejando a la mayoría de las organizaciones en una posición de mayor exposición en una escala creciente.

Ahora, con la incertidumbre que rodea al regreso de oficinas, y distanciamiento social, corresponde al equipo de seguridad de TI facilitar de forma segura el trabajo flexible y remoto para empoderar a las personas.

Solo el 34% de los profesionales de la seguridad se sintieron muy preparados para ayudar a los empleados que trabajan desde casa de forma segura.

Las organizaciones que alguna vez se ocuparon de un pequeño grupo de usuarios remotos o que viajaban, ahora están administrando fuerzas de trabajo completas que operan desde todos los lugares imaginables. Los equipos de liderazgo y seguridad ahora se enfrentan universalmente al mismo desafío:

> **¿Cómo podemos ayudar a nuestros empleados a trabajar de forma productiva, eficaz y segura desde cualquier lugar del mundo?**

Curiosamente, en el momento en que se anunció la cuarentena el 72% de los profesionales sintieron que la nube había mejorado la postura de seguridad de su organización, colocándolos en una posición sólida para hacer frente a las crecientes amenazas cibernéticas. Sin embargo, el cambio importante en el lugar de trabajo y el salto a la adopción de nuevas herramientas ha puesto de relieve los riesgos asociados con la nube y ha significado que muchos necesitaba reevaluar radicalmente su postura.

La investigación reciente ha revelado que, aunque muchas organizaciones se están beneficiando de la productividad al adoptar o aprovechar las aplicaciones en la nube para respaldar el trabajo remoto, también ha creado un panorama de amenazas complejo que debe abordarse con cierta urgencia.

Los hallazgos también muestran que, como era de esperar, los ciberdelincuentes están capitalizando esta exposición, lo que deja una necesidad clara e inmediata de que los profesionales de seguridad hagan balance, sean cautelosos y planteen las preguntas difíciles sobre la capacidad de su tecnología en el clima actual.

72%

de los profesionales consideró que la nube había mejorado la postura de seguridad de su organización.

Utilizando los conocimientos recopilados **de una encuesta a 300 profesionales de la seguridad cibernética y la orientación de los expertos** de la industria dentro del equipo de Censornet, este informe explora la realidad del papel de la seguridad durante una pandemia global.

Siga leyendo para ver cómo este cambio transformador ha creado brechas de seguridad tanto inmediatas como a largo plazo que deben abordarse, así como cómo sus pares están fortaleciendo su seguridad y superando desafíos comunes utilizando tácticas que puede implementar hoy.

Áreas clave:

SEGURIDAD CIBERNÉTICA EN 2020:
Un paisaje impredecible

SEGURIDAD CORREO ELECTRÓNICO:
Alinear la estrategia con el comportamiento del usuario

REALIDADES DE UNA CULTURA TRABAJADORA A DISTANCIA

TÁCTICAS PARA HOY

Con esta información, esperamos informarle y capacitarle, como profesionales de la seguridad, para adaptarse y prosperar en un momento en el que "los negocios como siempre" se están reinventando continuamente.

Sección 1

SEGURIDAD CIBERNÉTICA EN 2020

Un paisaje impredecible

59%

de las empresas esperan un incremento en el uso de la nube debido al COVID-19

Seguridad Cibernética en 2020

Desde que comenzó la pandemia, la cantidad de soluciones en la nube que se utilizan se ha disparado. Plataformas como Office 365 y G-Suite están ayudando a las organizaciones a migrar a la nube y alejarse de las redes locales tradicionales y, en algunos casos, de los planes de transformación digital de seguimiento rápido.

Si bien ofrecen claros beneficios de colaboración, los entornos híbridos y en la nube también pueden aportar su parte de riesgo y, aunque los méritos de la seguridad "superan los defectos", la escala en la que se utilizan (por los usuarios "menos familiarizados" con el trabajo móvil) deja a las organizaciones de forma alarmante vulnerable a la ingeniería social y sofisticados ataques de malware.

Un asombroso aumento del 50% en estos ataques ha enviado un mensaje claro de que las vulnerabilidades producidas por la pandemia no han escapado a la atención de los ciberdelincuentes. La nueva ola de usuarios remotos menos informados ha creado un aumento en los ataques de Business Email Compromise (BEC), Account Takeover (ATO), ataques phishing y whaling.

A medida que los ciberdelincuentes continúan modernizando y diversificando la tecnología y las tácticas utilizadas para atacar, los proveedores de nube pública, los profesionales de seguridad y los proveedores de seguridad deben actualizar su enfoque de defensa. Se deben superar las nuevas vulnerabilidades y debilidades en el entorno de trabajo pesado en la nube para crear confianza y potenciar las actividades de sus empleados.

Esto debería incluir una evaluación honesta y brutal de si su tecnología satisface las necesidades de sus usuarios en el clima actual.

En esta sección, analizaremos los principales desafíos y prioridades de seguridad que afectan a las organizaciones para resaltar áreas de su posición de seguridad actual que pueden necesitar refuerzo para hacer frente a estos cambios.

También se incluirán recomendaciones del equipo de expertos de Censornet combinadas con algunos estudios de casos de clientes anecdóticos para ilustrar lo que están logrando los profesionales con visión de futuro, que comparten desafíos similares.

58%

de los profesionales de la seguridad dijeron que su cambio a la nube hizo que la seguridad fuera más compleja

10%

cree que la seguridad en la nube ha empeorado

Principales desafíos y prioridades de seguridad

Es posible que el trabajo remoto no sea un problema "nuevo" a resolver, pero cuando de repente se vio motivado por la salud pública y las leyes gubernamentales, un gran número de personas que tienen una gran variación en la conciencia de seguridad se vieron envueltas en él, presentando un conjunto completamente nuevo de desafíos a resolver.

Muchos expertos también creen que este cambio cultural radical significa la desaparición de la oficina tradicional, que coloca el examen, la comprensión y el control de la "actividad del usuario" entre las principales prioridades de los profesionales de la seguridad.

> **"En este momento, se trata de cerrar las escotillas. Los profesionales de la seguridad cibernética y de TI han priorizado la función cuando se trata de la nube; ahora se trata de fortalecer la seguridad ".**
>
> **Charles Milton, VP de Estrategia Alianzas en Censornet**

Las 5 principales preocupaciones de seguridad en la nube en 2020:

1. PÉRDIDA DE DATOS
2. EL PROVEEDOR DE SERVICIOS EN LA NUBE ESTÁ COMPROMETIDO
3. ACCESO NO AUTORIZADO / ATO
4. FALTA DE TIEMPO
5. MALWARE

Las tres mayores preocupaciones entre los profesionales de la seguridad en términos de seguridad en la nube son la pérdida de datos (49%), que su proveedor de servicios en la nube esté comprometido (40%) o los ataques de adquisición de cuentas (37%).

Fortalecimiento del sistema y la seguridad para evitar la pérdida de datos

20%

de los profesionales dijo que la mala configuración de los servidores en la nube era un gran problema de seguridad para ellos

La pérdida de datos ha encabezado la lista de "sospechosos habituales" de las principales preocupaciones de seguridad durante algún tiempo, pero con el número de usuarios remotos que sigue aumentando, muchas organizaciones se han visto obligadas a movilizar a toda la fuerza laboral a la nube con relativamente pocos recursos o tiempo para centrarse en la seguridad.

Ahora el acceso remoto se considera la norma y, a medida que la regulación de los datos continúa endureciéndose, las organizaciones deben reconocer la necesidad de aplicar la seguridad de los datos en todos los dispositivos y todas las herramientas de comunicación, colaboración y almacenamiento.

Aunque se han tomado decisiones difíciles sobre qué nuevos sistemas, servicios y dispositivos implementar y qué protocolos de seguridad priorizar para permitir a los empleados, donde sea que estén trabajando, la revisión periódica de las políticas y la configuración para mantener a los equipos de seguridad al tanto de los desafíos de datos en el "nuevo núcleo de trabajo" centrado en la aplicación.

"Con el punto ciego que crean las aplicaciones móviles cifradas de extremo a extremo, la única opción puede ser usar soluciones MDM (o EMM) para obligar a los usuarios a regresar al navegador para restaurar la visibilidad y la administración".

Richard Walters,
CTO de Censornet

"Necesita herramientas para controlar las filtraciones de datos no deseadas. Utilice un CASB para bloquear las acciones del usuario que luego podrían causar una filtración de datos, como compartir datos organizacionales de manera externa ".

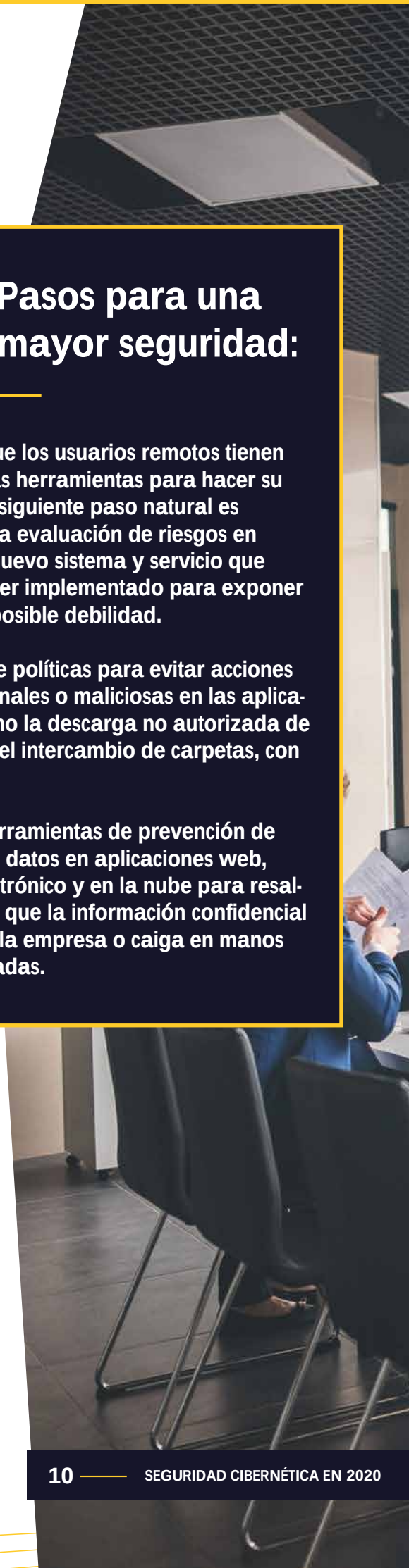
Ragnar Heil,
Gerente de cuentas de canal,
EMEA Central & Microsoft MVP

Pasos para una mayor seguridad:

Una vez que los usuarios remotos tienen acceso a las herramientas para hacer su trabajo, el siguiente paso natural es realizar una evaluación de riesgos en cualquier nuevo sistema y servicio que pueda haber implementado para exponer cualquier posible debilidad.

Implemente políticas para evitar acciones no intencionales o maliciosas en las aplicaciones, como la descarga no autorizada de archivos o el intercambio de carpetas, con un CASB.

Aplique herramientas de prevención de pérdida de datos en aplicaciones web, correo electrónico y en la nube para resaltar y evitar que la información confidencial abandone la empresa o caiga en manos no autorizadas.



Planificación para el peor de los casos

Durante el período de cuarentena inicial, el 40% de los profesionales identificaron el compromiso de su proveedor de servicios en la nube como una de sus principales preocupaciones.

El desafío principal que tendrán los CISOs y los equipos de seguridad cibernética en este momento será proteger sus instituciones y permitir que las operaciones continúen sin interrupciones, lo cual es comprensible dada la dependencia de muchos proveedores externos. De manera tranquilizadora, existe una probabilidad mucho menor de que plataformas como Microsoft Office y G-Suite se vean comprometidas en comparación con las infraestructuras locales tradicionales. Sin embargo, como hemos experimentado con COVID-19, no puede asumir nada.

De manera alarmante, el 25% de las organizaciones no cuenta actualmente con un plan de contingencia para el tiempo de inactividad en caso de que ocurriera lo peor.

Y dado que parece probable que el trabajo remoto juegue un papel más importante en "la nueva normalidad", es imperativo que los planes de recuperación ante desastres y continuidad empresarial se actualicen para reflejar los cambios en las prácticas laborales.

Esto no es solo para proteger a las organizaciones en caso de un apagón, sino también para prepararse para las posibilidades de ataques de denegación de servicio generalizados o la próxima inevitable violación de datos a gran escala.

Pasos para una mayor seguridad:

Ponga los pasos necesarios para reducir el impacto de interrupciones planificadas y no planificadas en los empleados y el personal de la mesa de ayuda manteniendo el componente más vital para proteger la productividad en funcionamiento: correo electrónico.

Proporcionar a los usuarios acceso de emergencia al correo electrónico, aislado de la infraestructura de Microsoft, puede ser un salvavidas vital. Las soluciones de "Bandeja de entrada de emergencia", a través de una interfaz de estilo de correo web, significan que los usuarios pueden leer y responder nuevos mensajes y revisar 30 días de correo enviado y recibido, incluso cuando Exchange Online está desconectado.

Para aquellos que tienen que cumplir con requisitos reglamentarios estrictos o que están sujetos a auditorías, Email Archiving proporciona acceso a prueba de manipulaciones a todo el correo electrónico histórico, con la capacidad de buscar mensajes rápidamente.

Protección de cuentas de usuario

El impacto potencial de un ataque de apropiación de cuenta es enorme, lo que lleva a campañas de suplantación de identidad sostenidas y variadas. La prisa por poner todo en la nube solo ha magnificado el problema, con grandes volúmenes de información crítica y procesos vitales ahora detrás de un simple nombre de usuario y contraseña. La superficie de ataque se ha fragmentado y se ha movido fuera del perímetro.

Pero con tantas rutas para recopilar datos de inicio de sesión y descifrar cuentas, se necesita más que una contraseña para mantener una cuenta segura. De hecho, los ataques BEC representaron el 50% de las pérdidas por delitos cibernéticos en 2019, y el ataque promedio costó $ 75,000*, por lo que merece nuestra atención.

Las cuentas de administrador y otras cuentas privilegiadas, el equipo financiero y las cuentas de ejecutivos son las más buscadas por los ciberdelincuentes, ya que brindan la mejor plataforma de lanzamiento para restablecer y otorgar acceso adicional a otras aplicaciones en la nube e iniciar ataques secundarios a proveedores, clientes o compañeros.

La idoneidad de las contraseñas por sí solas para proteger cuentas se ha cuestionado durante algún tiempo, pero el paso hacia los entornos en la nube está impulsando la autenticación contextual más avanzada al frente.

37%

de los profesionales citan el acceso no autorizado a la cuenta como una de sus principales preocupaciones, por lo que no es de extrañar que la autenticación sea una prioridad en la agenda

*Fuente Informe Interno sobre delitos del FBI 2019

“Utilice la autenticación multi-factor de forma predetermina-da. Esto es para minimizar el impacto de la captura de cre-denciales y eliminar la ad-quisición de cuentas. Asegúrese de que MFA esté configurado para usuarios administradores y luego para empleados en general, especialmente para usuarios móviles ".

Ian Moyse,
EMEA Director de Ventas,
Natterbox Ltd

Pasos para una mayor seguridad:

Eduque al personal sobre las mejores prácticas de contraseñas, es decir, no utilice la misma contraseña para varias cuentas, en particular cuentas corporati-vas y personales.

Utilice seguridad avanzada de correo electrónico, web y aplicaciones en la nube para bloquear los intentos de phishing que tienen como objetivo robar datos de inicio de sesión.

Aplique MFA contextual adaptable de manera coherente en todas las áreas del entorno para que no haya un eslabón débil en las defensas que permitiría a un pirata informático ingresar a su entorno.

Mantenerse un paso adelante del malware

1/3

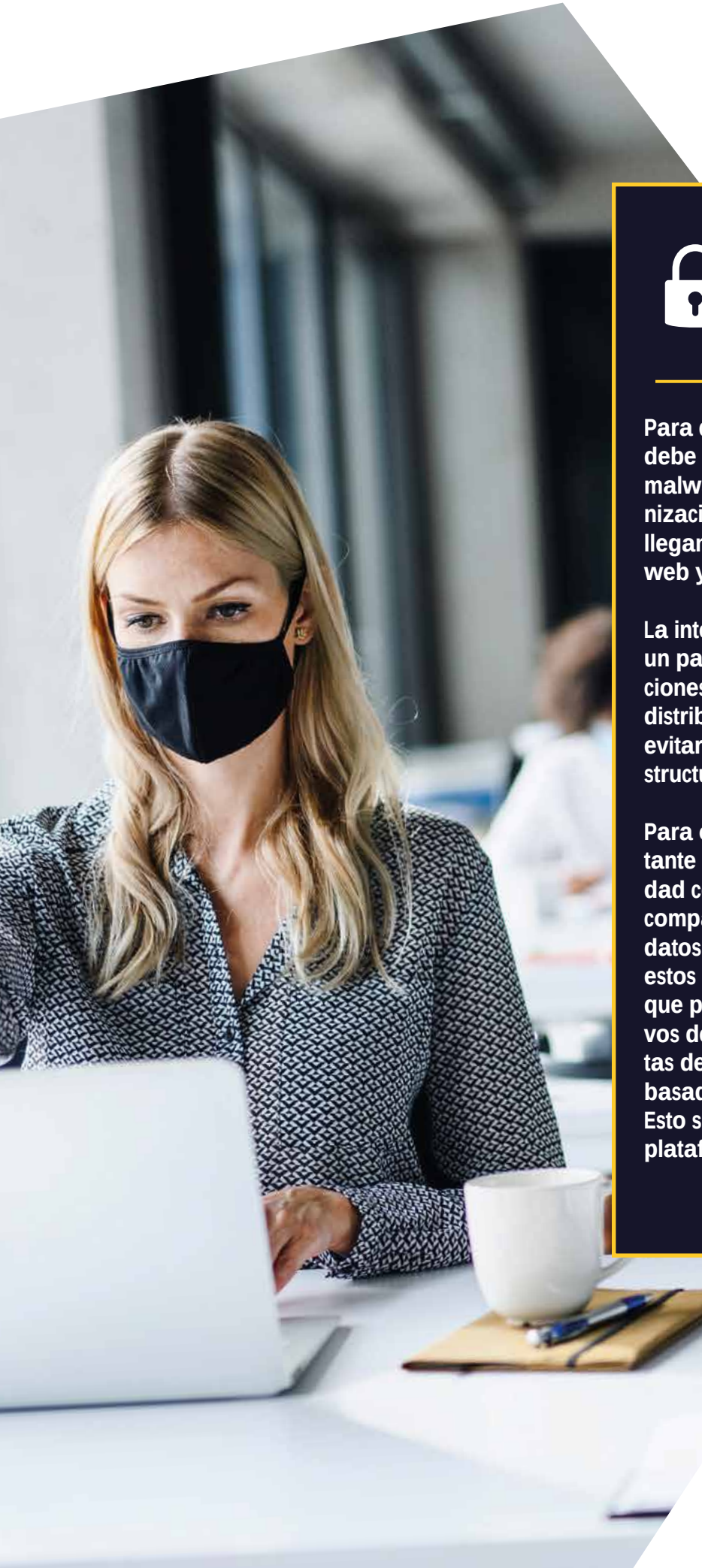
de los profesionales citan el malware como una de las principales preocupaciones

El malware es uno de los desafíos más duraderos en ciberseguridad. Viene en muchas formas y tamaños y de todos los canales; como tal, protegerse contra él es un pilar de cualquier postura de seguridad.

Grupos de ciberdelincuentes han estado explotando la pandemia, sorprendentemente incluso apuntando a las instalaciones de investigación de vacunas con malware.

El correo electrónico y la web son bien conocidos como los vectores de ataque más populares, pero debido a la rápida adopción de los servicios en la nube, el malware cada vez más solo en la nube escrito para propagarse entre los recursos compartidos en la nube es una amenaza. Si bien los usuarios generalmente están bien informados sobre los riesgos de abrir correos electrónicos no solicitados o desconocidos, o descargar materiales de sitios desconocidos, es menos probable que se pregunten si el contenido en una aplicación es "seguro" y / o "genuino".

Por lo tanto, es imperativo tener seguridad en varios canales para protegerse del malware.



Pasos para una mayor seguridad:

Para cada canal que esté utilizando, se debe implementar protección contra malware; eso significa proteger a su organización de las amenazas de malware que llegan por correo electrónico, desde sitios web y aplicaciones en la nube.

La inteligencia de amenazas también juega un papel importante para bloquear direcciones IP y dominios que son puntos de distribución de malware, así como para evitar que el malware llegue a la infraestructura de comando y control (2C).

Para obtener la mejor protección, es importante que todas las herramientas de seguridad centrales se comuniquen entre sí para compartir el contexto de seguridad, los datos de estado y los eventos. Al combinar estos datos con inteligencia de amenazas que proporciona información sobre archivos defectuosos conocidos, las herramientas de seguridad pueden tomar decisiones basadas en la información más reciente. Esto solo se puede implementar con un plataforma de seguridad.

LECCIONES DE SEGURIDAD DE LA GALERÍA NACIONAL DE RETRATOS

Cómo lograron la protección de espectro completo con seguridad consolidada

¿Quién?

Cómo lograron la protección de espectro completo con seguridad consolidada

¿Cuál fue el problema?

La galería necesitaba obtener la certificación Cyber Essentials para demostrar a los clientes y accionistas por igual que la galería cuenta con importantes medidas de seguridad cibernética.

¿Cómo lo arreglaron?

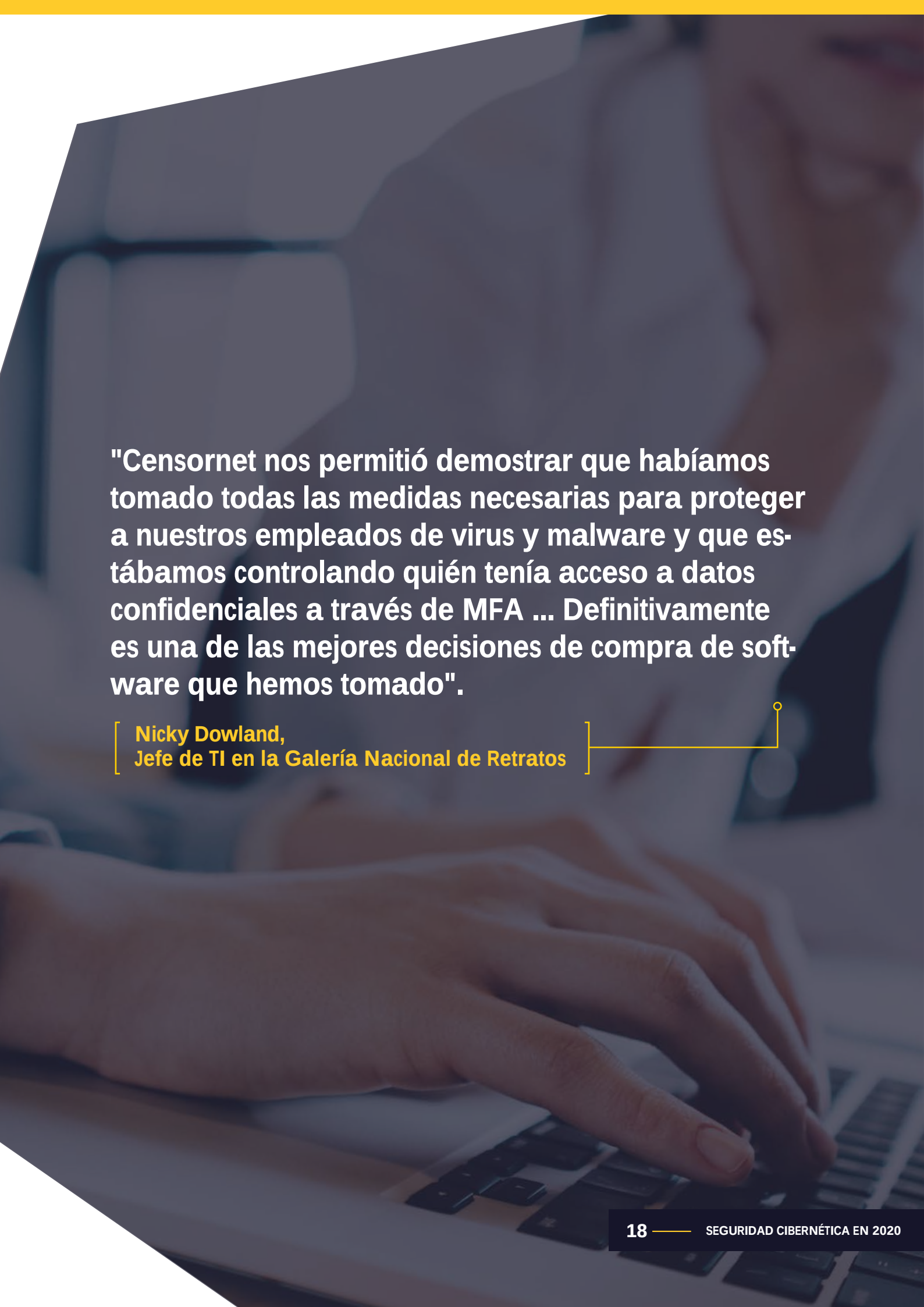
La galería Nacional de retratos eligió utilizar MFA, seguridad de correo electrónico, seguridad web y CASB integrados en una plataforma de seguridad en la nube para lograr la mejor cobertura y valor de seguridad, al tiempo que reduce la carga para el equipo de seguridad.

El impacto:

No solo las cuentas de usuario son seguras, sino que el equipo es capaz de identificar ataques y alertar al personal, bloquear la actividad riesgosa en la nube y en la web, y detener los ataques multicanal mediante la implementación de reglas para que las amenazas identificadas en diferentes canales puedan tener referencias cruzadas, bloqueado en la web, la nube y correo electrónico.

Lea la historia completa del cliente:

SABER MÁS



"Censornet nos permitió demostrar que habíamos tomado todas las medidas necesarias para proteger a nuestros empleados de virus y malware y que estábamos controlando quién tenía acceso a datos confidenciales a través de MFA ... Definitivamente es una de las mejores decisiones de compra de software que hemos tomado".

Nicky Dowland,
Jefe de TI en la Galería Nacional de Retratos

Sección 2

SEGURIDAD DE CORREO ELECTRÓNICO

Alinear la estrategia con el comportamiento del usuario

86% de los profesionales está de acuerdo en que las amenazas a la seguridad del correo electrónico se han vuelto más sofisticadas durante la última década.

"La defensa contra las amenazas de correo electrónico debe ser una combinación perfecta de personas, procesos y tecnología."

Richard Walters,
CTO de Censornet

El correo electrónico es el principal punto de partida para la mayoría de los ciberataques: eso no ha cambiado.

Cualquier oportunidad que tengan los ciberdelincuentes para crear nuevas campañas de ingeniería social, la aprovecharán, y esta pandemia ha abierto la puerta a un mundo aparentemente interminable de posibilidades ilegales.

Entre los más populares se encuentran los ataques de fraude de CEO y Business Email Compromise (BEC). Aunque este tipo de amenazas pueden ser bien conocidas, la sofisticación y personalización de los ataques en el clima actual significa que las estrategias de seguridad del correo electrónico también deben ser revisadas y sostenido para escrutinio. Esto incluye tener en cuenta el "comportamiento de los empleados", comprender dónde los empleados pueden necesitar más educación y qué tácticas se pueden implementar de inmediato para evitar que los ataques entren en la cadena de muerte de esta manera.

Para hacer esto de manera efectiva, necesitamos mirar a las personas, procesos y las tecnologías.

1. Personas

73%

de los profesionales dicen que confían en que los empleados seguirán las mejores prácticas, pero ...

87%

dijo que la mayoría de las amenazas se podrían prevenir si los empleados siguieran las mejores prácticas

Mitigar la amenaza del error humano natural durante el trabajo remoto es un desafío capaz de mantener despiertos a la mayoría de los profesionales de la seguridad durante la noche. Sin embargo, también debemos aceptar que muchos empleados han tenido que adaptarse a nuevos entornos en circunstancias bastante extraordinarias.

Incluso con capacitación previa y las mejores intenciones, quizás sea injusto colocar demasiada responsabilidad y expectativa en la comprensión "personal" de los ataques por correo electrónico o la seguridad. Por eso es vital revisar sus estrategias de formación de usuarios.

Pasos para una mayor seguridad:

Dado que muchos empleados se adaptan positivamente al trabajo remoto, es igualmente probable que sean más receptivos a la "educación de seguridad contextual" y a la formación de concienciación del usuario, que les ayudará a detectar estafas y nuevas técnicas innovadoras de phishing diseñadas para engañarlos.

Esto podría resultar particularmente útil y potencialmente evitar que los usuarios remotos sean víctimas de amenazas avanzadas como "fraude de facturas" ATO y estafas específicas de COVID-19.

"A menudo, etiquetar las líneas de asunto de los mensajes y los banners en la parte superior del cuerpo de los mensajes es suficiente para que el usuario se detenga y piense".

Richard Walters,
CTO de Censornet

2. Proceso

48% **de los profesionales está muy de acuerdo o algo de acuerdo en que su organización sería más segura si no usaran el correo electrónico.**

En nombre de la productividad, el uso de plataformas de comunicación en la nube como Slack, Microsoft Teams y Exchange Online está cambiando la forma en que funcionan muchas empresas. De hecho, el 56% de los profesionales ahora cree que las aplicaciones en la nube para la comunicación son más seguras que el correo electrónico.

Nuestra investigación ha demostrado que la "cultura remota" está claramente afectando y contribuyendo a la desaparición de la confianza en el correo electrónico. Tomemos como ejemplo al CEO o al fraude de facturas.

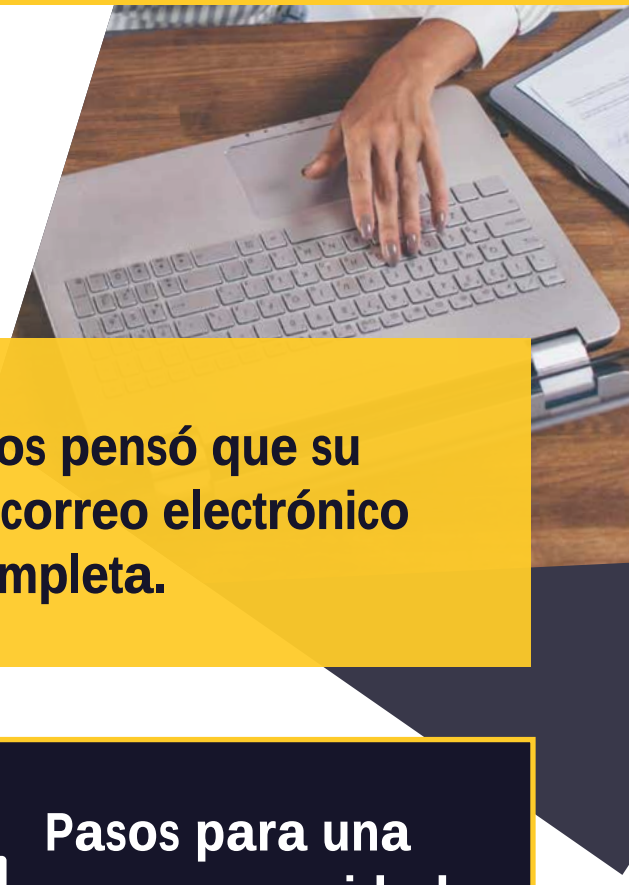
Los empleados habrían podido verificar previamente una solicitud de "transferencia bancaria urgente" con relativa facilidad caminando hacia el escritorio de una persona o preguntando un compañero miembro del equipo. Ahora confían en la autenticidad de las credenciales de correo electrónico que los estafadores pueden replicar fácilmente.

Pasos para una mayor seguridad:

Para ayudar a prevenir este tipo de ataques, es importante establecer o modificar los procesos de seguridad para que incluyan diferentes niveles de verificación para compensar las nuevas formas de trabajar.

Por ejemplo, los empleados deben marcar las solicitudes de pagos por encima de cierta cantidad utilizando un método que no sea el correo electrónico, ya sea con una llamada telefónica o una videoconferencia en línea.

3. Tecnología



85% de los encuestados pensó que su solución de seguridad de correo electrónico actual era adecuada o completa.

Aunque muchas organizaciones sienten que su solución de seguridad actual cubre las amenazas de correo electrónico, es vital evaluar su efectividad a través de un COVID-19 y una lente de trabajo remota. Después de todo, la tecnología implementada hoy debe ayudar a proteger contra el error humano y las vulnerabilidades que presenta una cultura remota.

Las soluciones de seguridad de correo electrónico heredadas no están diseñadas para abordar la complejidad de ataques dirigidos altamente sofisticados o manejar un flujo de correo complicado, y aunque algunos profesionales pueden sentir que la seguridad que ofrecen las empresas de tecnología que se especializan en otras áreas es adecuada, se recomienda la protección avanzada de correo electrónico por capas, analistas de la industria, expertos e incluso Microsoft.

"En las áreas de seguridad y cumplimiento, es probable que los proveedores de terceros más enfocados ofrezcan mejores capacidades que confiar únicamente en lo que Microsoft tiene para ofrecer". *

Pasos para una mayor seguridad:

Realice una evaluación honesta de su solución de seguridad de correo electrónico y evalúe si realmente cumple con el estándar de protección requerido.

Si su solución actual carece de las capas de análisis algorítmico, inteligencia de amenazas, monitoreo ejecutivo y escaneo de enlaces en tiempo real necesarios para defenderse de las amenazas de correo electrónico avanzadas, es posible que deba actualizar para mejorar su postura de seguridad.

Esta actualización también puede brindar funciones mejoradas de análisis de contenido de imágenes y prevención de pérdida de datos, y un mejor control sobre el flujo de correo, al tiempo que proporciona una forma eficaz de bloquear las amenazas avanzadas para que no entren en las bandejas de entrada dondequiera que se encuentre el usuario, incluso en plataformas como Microsoft 365 y Exchange Online.

*Osterman Research 2019 'Using third party solutions with Office 365'

LECCIONES DE SEGURIDAD DE ONECOM

Cómo bloquearon ataques sofisticados con seguridad de correo electrónico

¿Quién?

Onecom es líder en el Reino Unido en telecomunicaciones empresariales.

¿Cuál fue el problema?

Necesitaban una forma centralizada de proteger a su fuerza de trabajo remota de las amenazas cibernéticas en el correo electrónico, al tiempo que ahorraban tiempo y recursos.

¿Cómo lo arreglaron?

Para hacer esto, Onecom decidió invertir en una solución de correo electrónico en capas ultramoderna que se integra con inteligencia de amenazas para detectar sofisticados ataques de phishing. La protección de tiempo de clic contra enlaces maliciosos en correos electrónicos también se utilizó para brindar certeza de seguridad dondequiera que se encuentre el usuario y cuando acceda al correo electrónico.

El impacto:

El filtrado de correo electrónico en capas avanzado detecta los mensajes peligrosos antes de que lleguen a la bandeja de entrada. Al implementar la protección de "tiempo de clic" de los enlaces maliciosos en los correos electrónicos, los empleados ahora pueden trabajar de manera segura y confiable desde cualquier lugar del mundo.

"Los empleados tienen el mismo filtrado en su correo electrónico como cualquiera que hubiera estado usando una configuración estándar en la oficina, incluso si estuviera en casa ".

Alan Stanley,
Jefe de Operaciones Técnicas en Onecom

Vea la historia completa del cliente:

SABER MÁS

Sección 3

REALIDADES DE UNA CULTURA TRABAJADORA A DISTANCIA

REALIDADES DE UNA CULTURA TRABAJADORA A DISTANCIA

91% **de los profesionales confía en que sus soluciones de seguridad en la nube protegen eficazmente a las personas en el hogar.**

La nueva cultura en la que trabajamos es notablemente compleja: tiene muchas características técnicas, de comportamiento y culturales, diferentes en comparación con trabajar exclusivamente en una oficina.

Si bien es alentador ver a tantos profesionales seguros de que sus soluciones de seguridad en la nube están protegiendo a su fuerza laboral, la investigación de Censornet muestra una desconexión entre la percepción de cuán bien protegida está una organización cuando los empleados trabajan de forma remota y la verdad detrás de los riesgos que enfrentan.

En esta sección, exploramos las realidades y el comportamiento de los usuarios remotos cuando trabajan desde casa y las tácticas que puede implementar hoy para garantizar que sus estrategias de seguridad reflejen sus actividades.

Nuevos comportamientos de los empleados y TI en la sombra

Ya sea como resultado de un horario de trabajo más flexible, menos restricciones o políticas de acceso más relajadas en las computadoras portátiles del trabajo, los límites entre las actividades laborales y de la vida nunca han sido más difusos.

Desde que se anunció la cuarentena, el **67%** de los encuestados ha identificado que los empleados están comprometidos en actividades improductivas en la web, como el uso de servicios de transmisión en el trabajo como Netflix o Amazon Prime Video **(35%).**

Muchos de los profesionales de la seguridad encuestados también admitieron que tenían comportamientos que incluían:

22% UTILIZAN SERVICIOS DE STREAMING EN EL TRABAJO

22% USAN CREDENCIALES DE TRABAJO PARA CUENTAS PERSONALES

11% VISITAN SITIOS PARA ADULTOS EN EL TRABAJO

Si bien el impacto que este comportamiento tiene en la productividad del personal puede no ser responsabilidad directa de los profesionales de seguridad, las consecuencias naturales de Shadow IT, junto con los usuarios remotos `` menos informados'', han llevado a una falta de debida diligencia, lo que resulta en un aumento en credenciales robadas y ataques de adquisición de cuentas.

Las infracciones de cuentas, en particular las del personal de alto rango o los administradores con privilegios elevados, conllevan riesgos para los datos, la productividad y el acceso, con ataques sostenidos posibles cuando el intruso permanece por debajo del radar. A medida que los diversos lugares de trabajo se convierten en norma, y con tantas credenciales "en la naturaleza", las organizaciones van a necesitar más que contraseñas para proteger las cuentas y las bandejas de entrada.

34% ha encontrado empleados que utilizan credenciales laborales para cuentas personales como sitios de comercio electrónico, redes sociales, juegos, etc.

Pasos para una mayor seguridad:

Para proteger las cuentas de usuario de estas amenazas, muchas organizaciones están implementando la autenticación multifactor adaptativa o sensible al contexto siempre que sea posible.

Es importante interrogar el contexto del inicio de sesión para desafiar a los usuarios en función de un comportamiento inusual para reducir la fricción del usuario. Si se solicita el inicio de sesión desde una ubicación, hora, día o dispositivo extraño, la solución de autenticación debe recoger esto y garantizar una verificación adicional antes de permitir el acceso.

LECCIONES DE SEGURIDAD DE CAPSTICKS

Cómo aseguraron el trabajo remoto con MFA

¿Quién?

Capsticks es un bufete de abogados líder a nivel nacional, especializado en clientes de atención médica.

¿Cuál fue el problema?

El equipo de TI quería fortalecer su entorno de trabajo remoto con una protección de inicio de sesión más avanzada para proteger las cuentas de los usuarios y los datos confidenciales, sin crear fricciones entre los usuarios..

¿Cómo lo arreglaron?

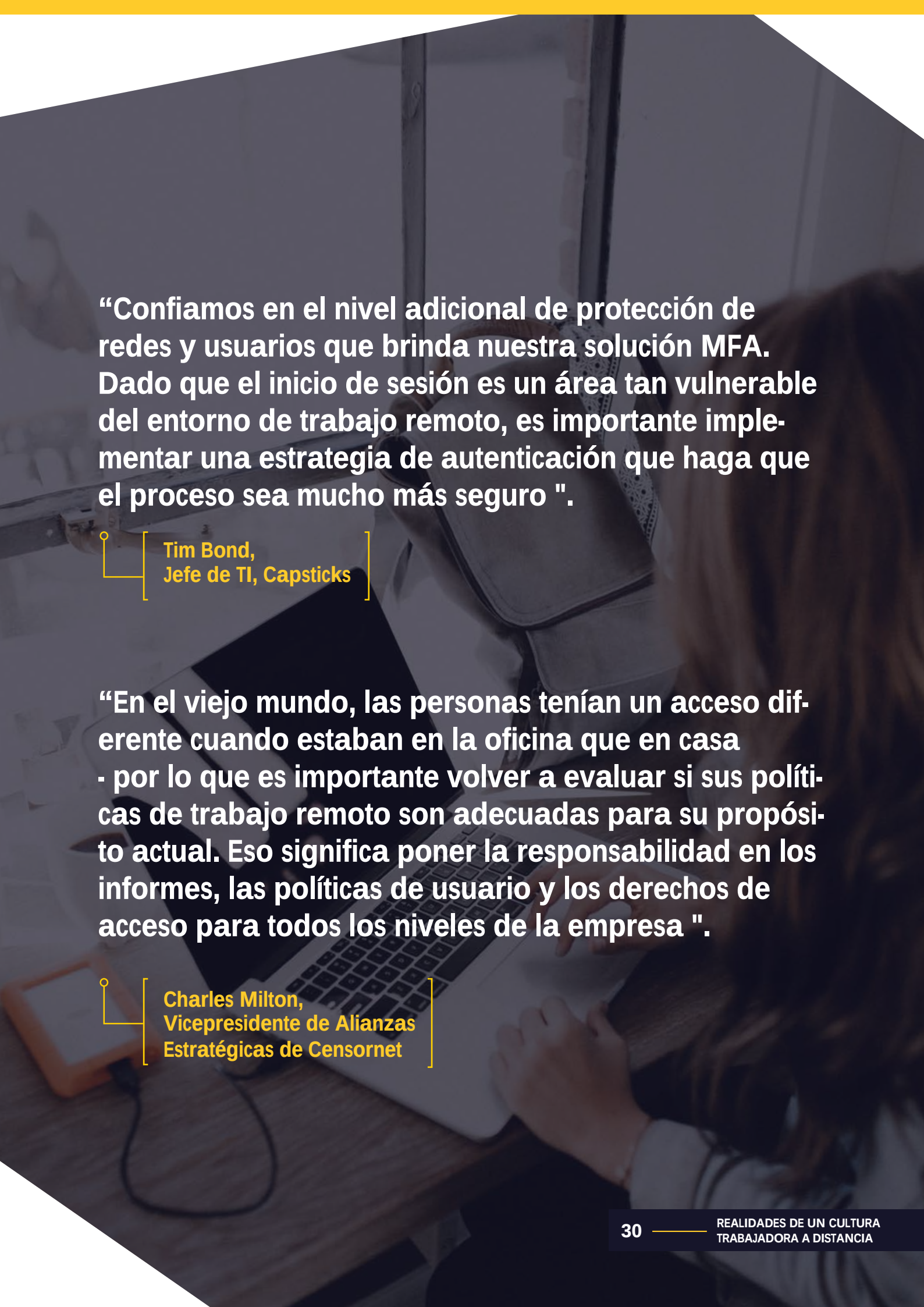
Para proteger los sistemas con algo más que una contraseña, Capsticks eligió una solución de autenticación multifactor adaptativa que utiliza códigos de acceso de un solo uso generados en tiempo real y conmutación por error automática a través de múltiples métodos de entrega para proporcionar autenticación segura para su solución de infraestructura de escritorio virtual y web. cliente de correo electrónico basado en.

El impacto:

MFA aseguró de manera efectiva la autenticación para Capsticks, brindando confianza en que las cuentas de usuario y el acceso a la red son seguros, sin interrumpir la vida laboral diaria de los empleados.
Esto no solo redujo las llamadas a la mesa de ayuda, sino que también ayudó para impulsar la productividad de la empresa.

Vea la historia completa del cliente:

SABER MÁS



“Confiamos en el nivel adicional de protección de redes y usuarios que brinda nuestra solución MFA. Dado que el inicio de sesión es un área tan vulnerable del entorno de trabajo remoto, es importante implementar una estrategia de autenticación que haga que el proceso sea mucho más seguro ".

Tim Bond,
Jefe de TI, Capsticks

“En el viejo mundo, las personas tenían un acceso diferente cuando estaban en la oficina que en casa - por lo que es importante volver a evaluar si sus políticas de trabajo remoto son adecuadas para su propósito actual. Eso significa poner la responsabilidad en los informes, las políticas de usuario y los derechos de acceso para todos los niveles de la empresa ".

Charles Milton,
Vicepresidente de Alianzas Estratégicas de Censornet

Pérdida involuntaria de datos y violaciones de seguridad

Aunque la confianza en los proveedores de seguridad en la nube está mejorando, el "comportamiento del usuario" sigue siendo una preocupación importante. El 76% de nuestros encuestados informó sobre el comportamiento de los empleados en la nube que podría poner en riesgo a su organización.

Los comportamientos de riesgo más comunes son:

41%

USANDO LA MISMA CONTRASEÑA

33%

ALMACENANDO DATOS SENSIBLES EN LA NUBE SIN LA PROTECCIÓN ADECUADA EN EL LUGAR

26%

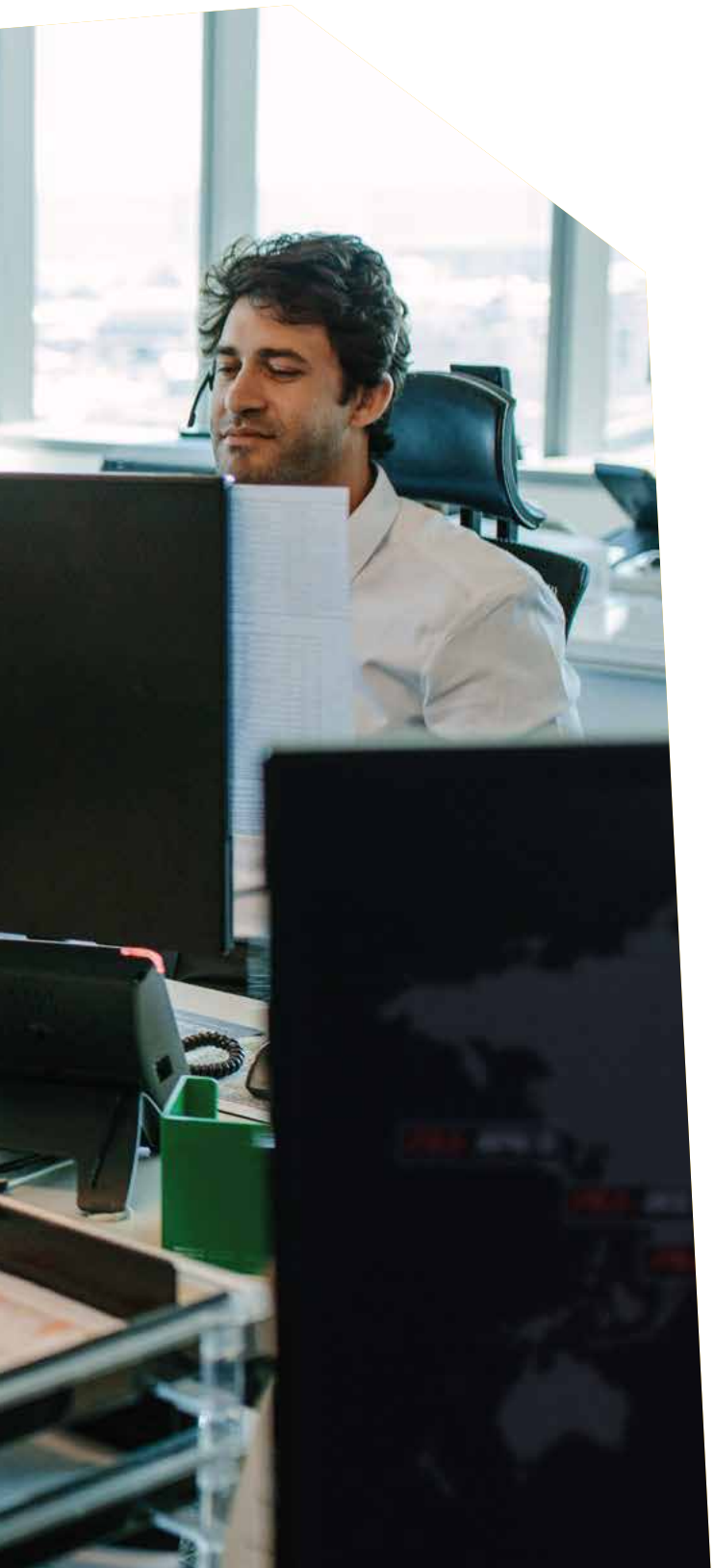
COMPARTEN ENLACES A DOCUMENTOS EN LA NUBE SIN AUTORIZACIÓN

Dado que el trabajo remoto se está volviendo más una necesidad que una opción para muchas organizaciones **(y con el 36% de las empresas que alojan su Active Directory en la nube)**, el riesgo de ATO, incumplimiento, intercambio de datos no autorizado o pérdida de datos no son solo preocupaciones importantes sino riesgos de considerable escala.

Las amenazas avanzadas como el malware transmitido por la web y las interacciones de usuario no administradas dentro de la nube también plantean grandes preocupaciones de seguridad para las organizaciones que se ocupan de TI autorizada y en la sombra, ya que muchos usuarios trabajan de manera intercambiable entre sitios web y aplicaciones sin darse cuenta de que lo están haciendo.

Se está revisando cómo y dónde se aplica la protección, ya que una combinación de VPN, túneles divididos y conexiones directas a Internet significa protección de punto final, en lugar de protección centralizada es requerido.

65% de los profesionales de la seguridad creen que la nube les brinda menos visibilidad y control de los datos confidenciales.



Pasos para una mayor seguridad:

Para recuperar el control de los datos almacenados en la nube, implemente una solución Cloud Access Security Broker (CASB) que funcione con una gran cantidad de aplicaciones comerciales como Office 365, Dropbox y Salesforce para que pueda proteger toda su infraestructura en la nube desde un solo lugar.

A partir de aquí, los equipos de seguridad obtienen una visión granular de la actividad del usuario para ver exactamente cuándo y dónde se manejan los datos de manera inapropiada y por quién. CASB proporciona la información necesaria para abordar el comportamiento a través de la educación, y las herramientas para implementar políticas para administrar acciones y accesos de usuarios privilegiados y estándar en todas las aplicaciones comerciales.

CASB vuelve a poner al equipo de seguridad a cargo y ayuda a satisfacer las necesidades del equipo de cumplimiento, reduciendo el riesgo de pérdida de datos y violaciones de seguridad de datos mientras mejora la protección con seguridad en la nube, prevención de pérdida de datos y funciones de análisis de contenido de imágenes.

LECCIONES DE SEGURIDAD DE ST ANNE'S

Cómo mejoraron la visibilidad y el control de los datos con CASB integrado y Web Security

¿Quién?

Desde atención domiciliaria y vida asistida, hasta apoyo con salud mental y abuso de sustancias, los servicios comunitarios de St Anne's brindan apoyo de todo tipo, en todo el norte de Inglaterra, a quienes más lo necesitan.

¿Cuál fue el problema?

Los cuidadores remotos experimentaron posiblemente el desafío más difícil de los últimos meses, en un momento en que dejar de trabajar simplemente no era una opción. St Anne's tomó la decisión de simplificar y fortalecer la seguridad de los datos en ocho ubicaciones, lo que permitió a sus cuidadores trabajar de forma segura, desde donde más se necesitaran.

¿Cómo lo arreglaron?

Para hacer esto, optaron por invertir en una solución integrada de **seguridad web y CASB** que les proporcionaría un nivel adicional de seguridad sobre sus productos Microsoft Azure y Office 365, además de proteger su fuerza de trabajo móvil con una configuración sin intervención. El filtrado de seguimiento del usuario de la solución ayudó a bloquear contenido peligroso y malware, detener los ataques multicanal y prevenir la actividad no autorizada en la aplicación.

El impacto:

Con seguridad en todas las aplicaciones web y en la nube que siempre está conectada, siempre disponible y siempre actualizada, el personal de St Anne puede enfocarse en lo que realmente importa, sabiendo que están a salvo de ataques cibernéticos multicanal, protegido de la realización de actividades no autorizadas en la aplicación y protegido de contenido dañino.

"Shadow IT es un desafío, pero con Web Security y CASB integrados podemos ver fácilmente el comportamiento del usuario y detener el uso inadecuado de las aplicaciones o la web".

Dave Johnson,
Gerente de TI en St Anne's

Obtenga más información sobre los productos censornet:

SEGURIDAD DE ACCESO A LA NUBE

SEGURIDAD WEB

Sección 4

TÁCTICAS PARA HOY

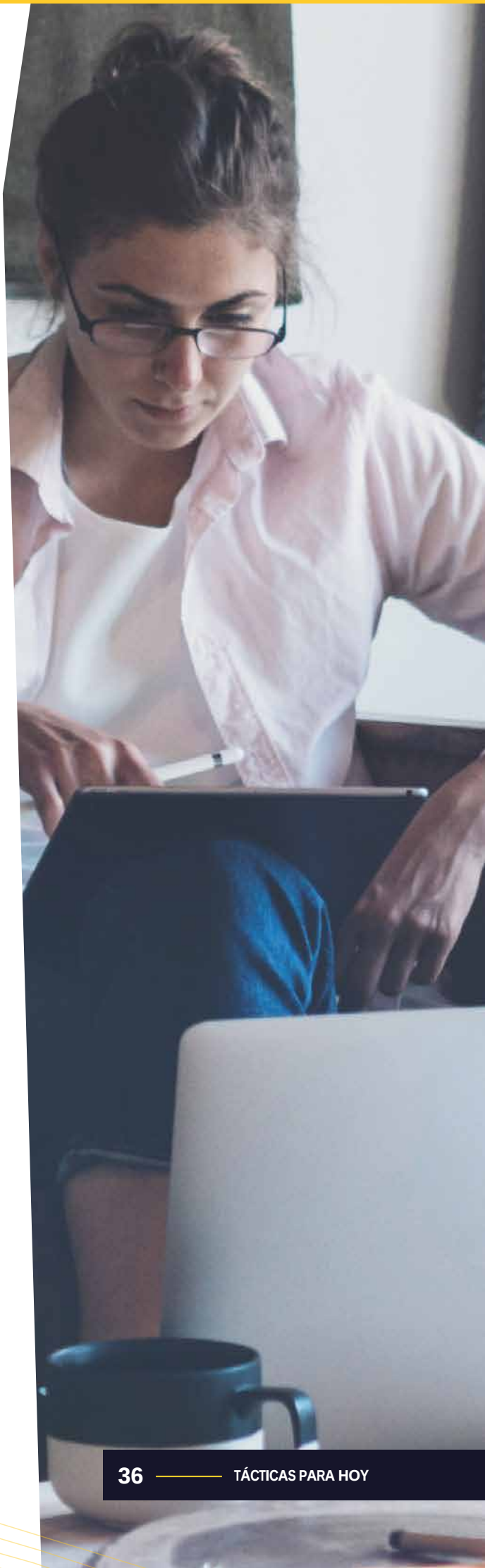
En 2020, los profesionales de la seguridad y las TI tienen lo que significa trabajar con resiliencia, adaptabilidad y fortaleza. Enfrentada con posiblemente el cambio más grande que probablemente veremos en nuestra vida, esta pandemia realmente ha marcado el final de los negocios como siempre como los conocemos.

Lo ame o lo deteste, el trabajo remoto está, en cualquier medida, aquí para quedarse, y dado que el ritmo del ciberdelito no muestra signos de desaceleración, la importancia de sacar tiempo para revisar la efectividad, el contexto y la relevancia de las soluciones de seguridad implementadas nunca ha sido mayor.

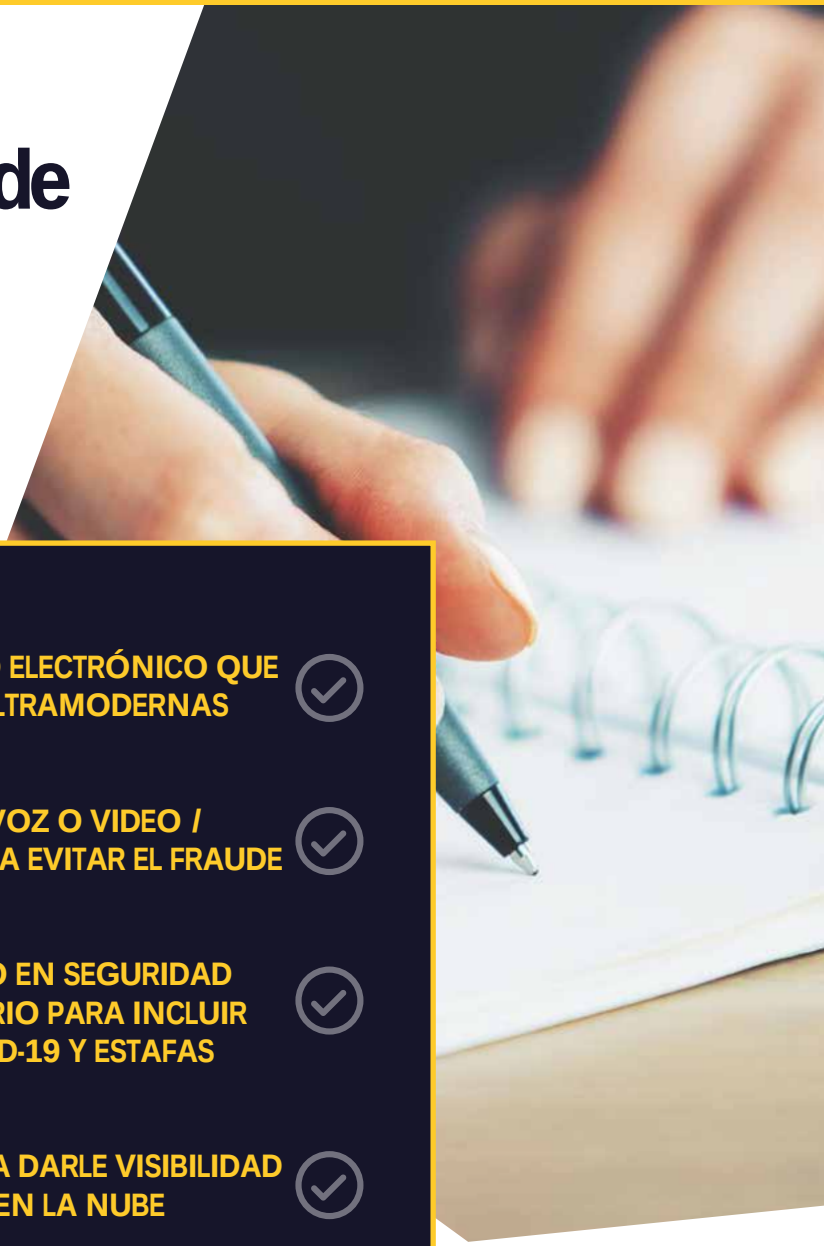
Se está volviendo de conocimiento común que los productos de seguridad tradicionales tendrán dificultades para brindar "protección contextual" a los usuarios remotos y con las ahora ubicuas "Plataformas de nube pública", firmemente en la mira del crimen cibernético, está en manos de proveedores de nube pública, profesionales de seguridad e industria de la seguridad en su conjunto para intensificar y actualizar su enfoque de la defensa.

La gran lección de 2020 es estar preparado para todo. Los conocimientos de este informe han destacado el desafiante papel que deben desempeñar los profesionales de la seguridad cibernética en un panorama dinámico donde las expectativas y los riesgos son altos; sin embargo, siguiendo los consejos de expertos y colegas sobre el fortalecimiento de su postura de seguridad, puede empoderar a las personas de su organización al facilitar de forma segura el trabajo colaborativo, flexible, dominante en la nube y remoto.

Para ayudar a iniciar su proceso de revisión, hemos compilado una lista de las principales tácticas que puede implementar de inmediato para garantizar que su postura de seguridad esté en la mejor forma posible.



Tu lista de verificación de seguridad para 2020



- UTILICE SEGURIDAD DE CORREO ELECTRÓNICO QUE INCLUYA CAPAS DE DEFENSA ULTRAMODERNAS
- IMPLEMENTAR CONTROLES DE VOZ O VIDEO / TRANSACCIONES EN LÍNEA PARA EVITAR EL FRAUDE
- ACTUALICE SU ENTRENAMIENTO EN SEGURIDAD Y CONCIENCIACIÓN DEL USUARIO PARA INCLUIR ATAQUES ESPECÍFICOS DE COVID-19 Y ESTAFAS DE PHISHING
- USE UNA SOLUCIÓN CASB PARA DARLE VISIBILIDAD Y CONTROL SOBRE LOS DATOS EN LA NUBE
- ASEGÚRESE DE QUE TODOS LOS USUARIOS TIENEN MFA CONSCIENTE DEL CONTEXTO
- REVISAR LAS POLÍTICAS DE USUARIO Y LOS DERECHOS DE ACCESO PARA ASEGURARSE DE QUE REFLEJEN LAS NECESIDADES ACTUALES
- USE SOLUCIONES MDM O EMM PARA APLICAR LAS POLÍTICAS EN DISPOSITIVOS MÓVILES
- UTILICE VPNS Y HABILITE AGENTES EN PUNTOS FINALES PARA ASEGURAR LAS REDES DOMÉSTICAS

censornet.

Seguridad en la nube transformada

W. WEB E. EMAIL C. CASB M. MFA ASE

Frente a una marea creciente de delitos cibernéticos, el aumento de las obligaciones de cumplimiento y los desafíos comerciales más amplios que afectan los recursos disponibles para la seguridad cibernética, ahora es el momento de adoptar soluciones conjuntas y deshacerse de las soluciones heredadas que no se ajustan al nuevo entorno de trabajo dominante en la nube.

¡Contáctenos para mayor información de cómo solucionar y/o frenar estas situaciones en su organización!

Censornet es la fuerza líder en seguridad en la nube innovadora y automatizada que ofrece soluciones sólidas y consolidadas para empresas y organizaciones de cualquier tamaño.

Su plataforma de seguridad en la nube integra seguridad web y de correo electrónico, agente de seguridad de acceso a la nube (CASB) y autenticación multifactor adaptativa (MFA), lo que permite que nuestro motor de seguridad autónomo (ASE) vaya más allá de la seguridad basada en alertas y se convierta en prevención de ataques automatizada en tiempo real, 24x7, 365 días al año.

Con más de 1.500 clientes y más de 750.000 usuarios de su plataforma en todo el mundo, Censornet es conocida por ayudar a sus clientes a hacer más con menos.

5599-0670 | https://pccommayorista.com | contacto@pccommayorista.com