Predicciones
para este 2021
en Ciberseguridad

mexus®
Managed secure IT | no matter what

El 2020 puede haber terminado, pero las organizaciones seguirán sintiendo su impacto en 2021, cuando los planes y decisiones se verán profundamente influidos por desafiantes eventos del año pasado.

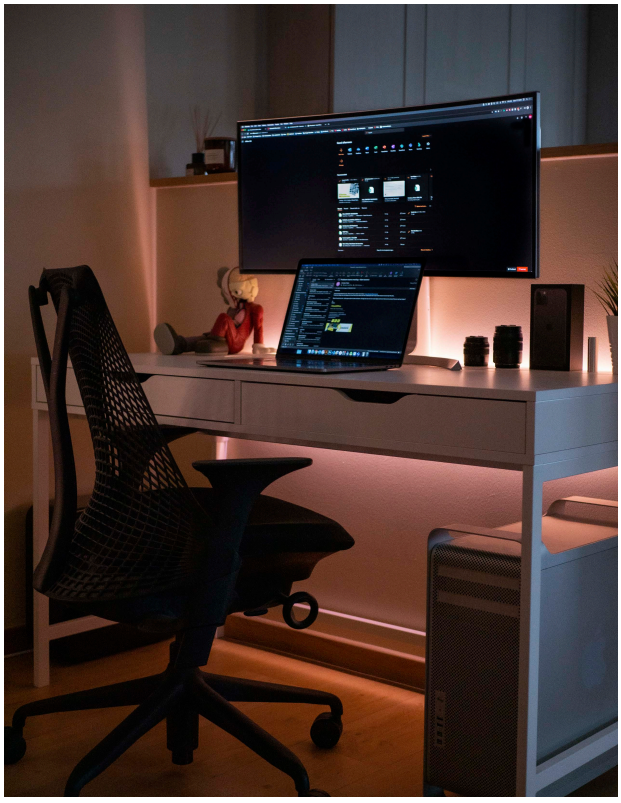
Los cambios sin precedentes en la forma en que trabajamos, y nos conectamos no desaparecerán pronto. Seguiremos trabajando desde casa, haremos más compras en línea. Estos cambios seguirán afectando la forma en que las organizaciones manejan gestión de identidad y acceso, detección y respuesta de amenazas, fraude prevención y gestión de riesgos en 2021 y más allá.

En el siguiente contenido compartimos una serie de predicciones para este 2021 en las que el 2020 cambió de forma acelerada la ciberseguridad.

1.Duplicar la transformación digital

Los eventos sin precedentes de 2020 no frenaron la transformación digital, lo aceleraron. Desde asegurar la fuerza de trabajo remota hasta ampliarciberseguridad a la nube, esta aceleración continuará.
Sobre los conocimientos y experiencias de 2020, las organizaciones adoptarán la transformación con una urgencia aún mayor para recuperar la ventaja competitiva.

Gestión de identidad y acceso.
Las organizaciones seguirán teniendo dificultades para garantizar que las personas sean quienes dicen ser cuando buscan acceso a aplicaciones y datos laborales, cuentas financieras personales y otros recursos en línea.



3. Los ciberdelincuentes se aprovechan de los cambios de acceso

Las organizaciones deben anticipar los intentos continuos de robar credenciales cuando muchos en la fuerza laboral continúan accediendo a recursos desde casa.
Es fundamental trabajar para limitar el impacto negativo abordando cuestiones como el uso de dispositivos no reforzados, acceso a aplicaciones en la nube fuera de la VPN y uso compartido de dispositivos de trabajo con miembros de la familia.

2. Un papel más crítico para el gobierno de la identidad

A medida que la fuerza laboral continúa evolucionando a la luz del regreso de algunas personas a la oficina y otros que continúan trabajando de forma remota, las organizaciones se beneficiarán de un enfoque y se asegurarán de que puedan gestionar fácilmente los cambios de derechos de usuario y privilegios de acceso.

4. El cambio a la confianza cero

La ciberseguridad pivotará para adoptar la confianza cero, a medida que los equipos de seguridad reconsideren sus posturas de defensa para adaptarse a una superficie de ataque en expansión y una dependencia creciente a terceros. Las posturas de defensa de confianza cero combinarán una gama de gobernabilidad procesos, métodos de autenticación multifactor y otras medidas para gestionar amenazas emergentes basadas en la identidad.

5.Ataques DDoS intensificados

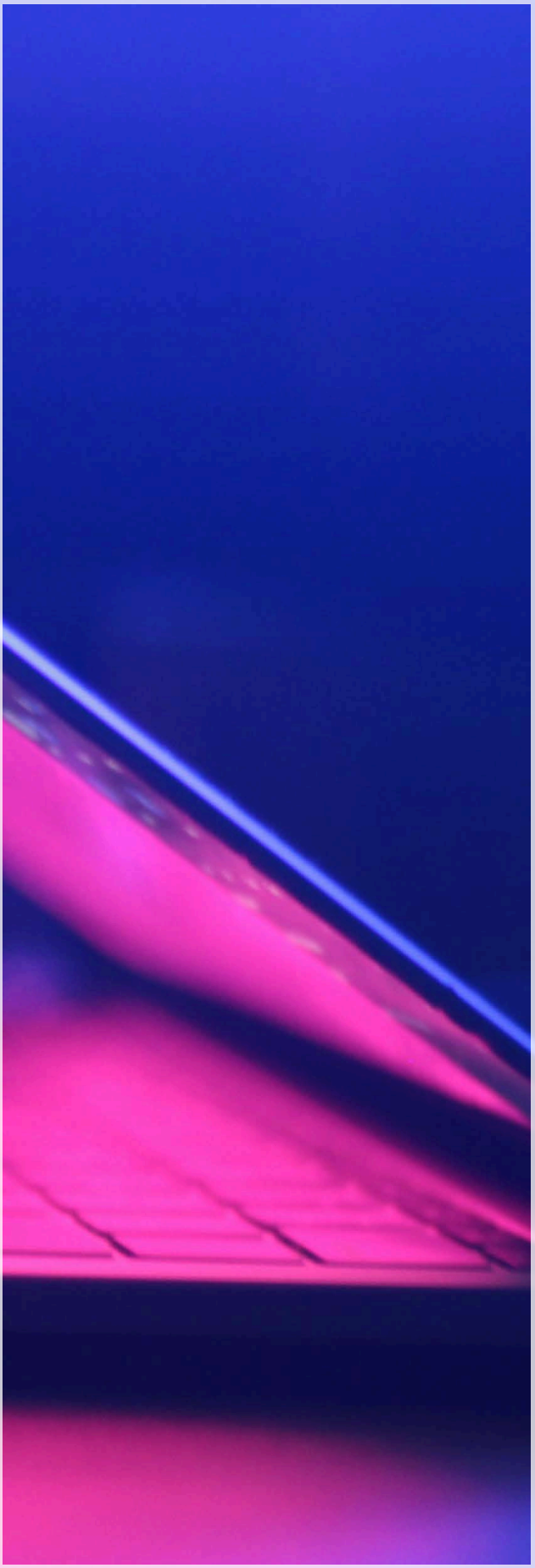
Los ataques distribuidos de denegación de servicio (DDoS) aumentarán a medida que el ataque la superficie se expande y la dependencia de Internet crece, construyendo en un aumento de tres veces en los ataques DDoS en 2020.

6.Vulnerabilidad juvenil e identidad sintética

Robo de identidad sintético, en el que se almacenan piezas de información legítima del usuario combinado con información ficticia para crear una identidad falsa, aumentará a medida que los estafadores se dirigen específicamente a los usuarios más jóvenes que pueden no controlar sus identidades cercanamente. En última instancia, esto conducirá a un aumento masivo del fraude de cuentas nuevas.

7. La fuerza de trabajo remota está aquí para quedarse, al igual que el riesgo que lo acompaña.

Si bien muchos trabajadores regresarán al lugar de trabajo, cierto grado de trabajo remoto siguen siendo una característica permanente de la jornada laboral de muchos empleados. La superficie de ataque expandida asociado con el trabajo remoto seguirá siendo motivo de preocupación a medida que la fuerza laboral continúe confiando en una combinación de redes personales, recursos de terceros y nuevos recursos.



8. Tiempos peligrosos para la salud.

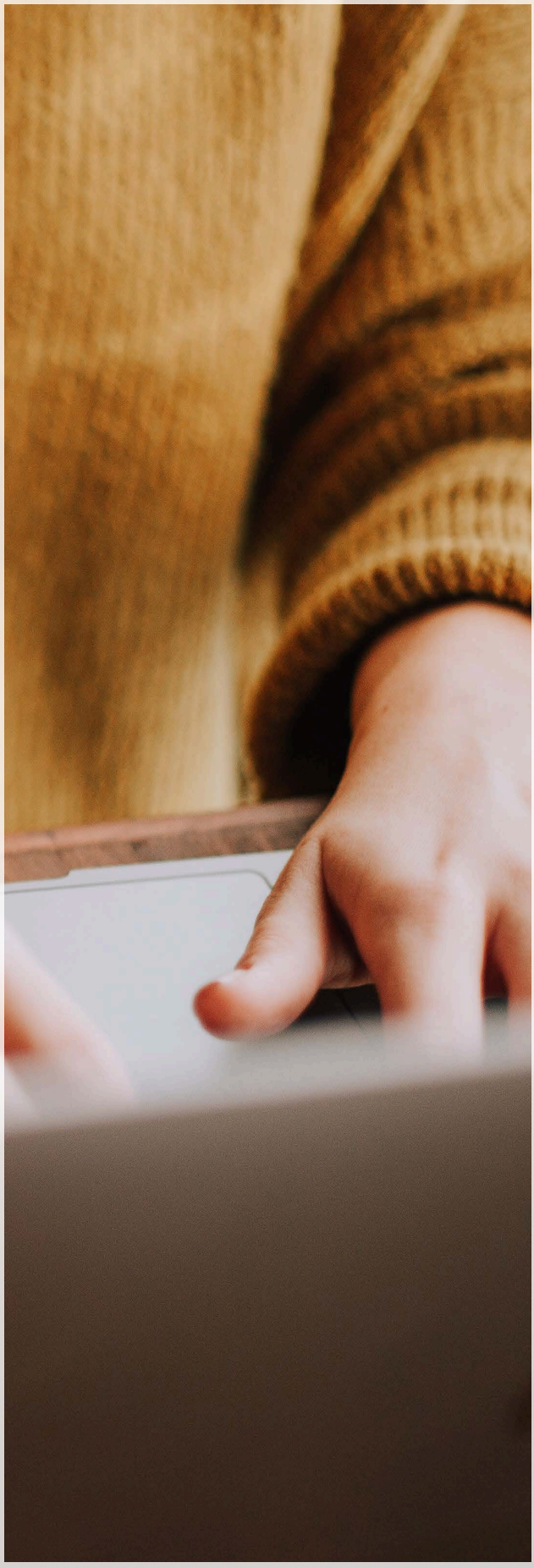
Organizaciones sanitarias, han sido objeto de ciberataques en toda
la pandemia, seguirán enfrentando amenazas de ransomware que advierten con exponer datos confidenciales, así como peligrosos ataques de spear-phishing dirigidos a robar propiedad intelectual.
Las empresas de vacunas, en particular, serán cada vez más el foco de ataques mientras corren para conseguir que las vacunas se distribuyan ampliamente.

9. Consolidación de la ciberseguridad

Obligado por la superficie de ataque expandida a repensar fundamentalmente la defensa, posturas y planes, las organizaciones continuarán avanzando hacia un estrategia de ciberseguridad basada en una única operación cohesiva. Esto contrasta con las soluciones de múltiples puntos en las que confiaban anteriormente para satisfacer necesidades específicas.

10.Victimizando a los vulnerables

Hasta que se produzca una sólida recuperación económica, los defraudadores seguirán encontrando formas de lucrar mediante la explotación de personas que se encuentran en una situación financiera desesperada. Usando phishing, aplicaciones móviles deshonestas y otros tipos de ataques de fraude para ofrecer dinero fácil, engañar a los destinatarios para que compartan números de cuentas bancarias u otra información confidencial.



Fuente de información:
www.rsa.com