IDG
RESEARCH SERVICES

EXECUTIVE BRIEFING

ZERO TRUST: ENFOQUE DE SEGURIDAD PARA EMPLEADOS Y COLABORADORES EN REMOTO

El pasado 21 de enero de 2021, IDG Research reunió en una mesa de debate a grandes empresas multinacionales junto con el proveedor tecnológico Okta, para analizar los retos de seguridad que conlleva el trabajo en remoto.

El punto de partida de cada organización ha sido distinto, en función de las iniciativas de digitalización que ya estaban en marcha y del grado en el que se encontraba habilitado el trabajo en remoto. No obstante, todos han tenido que absorber una disrupción.

Este documento recoge las principales conclusiones extraídas por los analistas de IDG Research.

INTRODUCCIÓN

El trabajo en remoto se ha adoptado con urgencia para garantizar la continuidad de la actividad. Sin embargo, las arquitecturas de empresa no estaban diseñadas para esta forma de operar ni contaban con un gobierno orientado a esta realidad.

En realidad, la puesta en marcha del trabajo remoto a escala ha precedido a su planificación y normativa. Esta secuencia está lejos de ser la ideal, pero ha sido forzada por las circunstancias.

En consecuencia, se ha producido un desfase: ha aumentado la heterogeneidad de equipos, usos y accesos, pero se necesita una postura de seguridad homogénea en la organización.

En este resumen ejecutivo se describen los efectos del trabajo remoto en las organizaciones, cómo impacta en la seguridad y qué acciones están tomando tanto en el presente como mirando a futuro.

EFECTOS DEL TRABAJO REMOTO

La adopción repentina y a escala del trabajo remoto ha causado tres efectos principales que se describen a continuación:

1. Los usuarios externos han abierto nuevas vulnerabilidades. Las empresas cuentan con un conjunto de colaboradores externos y proveedores que han cambiado su forma de conectarse a la organización. Esto ha ocurrido de forma súbita, creando un escenario que no estaba contemplado a esta escala. Como consecuencia, han surgido los siguientes retos:

a. Vulnerabilidades desde la cadena de valor. Esta se ha convertido en uno de los vectores de ataque preferidos por los ciberdelincuentes.

i. Riesgos en cadena*. El eslabón más débil se convierte en un punto de entrada a toda la cadena, lo que maximiza el impacto de un ataque. Muchas empresas tienen una dependencia de sus proveedores críticos, por lo que tienen que asumir riesgos de terceros, dado que su poder de influencia sobre las políticas de seguridad de estos es limitado.*

ii. Disparidad de políticas de seguridad. *Cada uno de los actores en la cadena tiene una postura diferente de seguridad y apenas existen protocolos compartidos o transparencia ante un evento adverso. Esto hace difícil una respuesta orquestada y la asignación de responsabilidades.*

b. Visibilidad y control sobre usuarios externos. Las empresas se han visto empujadas a asumir el modelo de organización en red, con recursos internos y externos conectados. Esto conlleva varias implicacio nes:

i. Cambian los patrones de acceso y tráfico. *Los colaboradores que trabajaban desde dentro de la organización han pasado a hacerlo desde fuera. Esto hace que se reduzca la visibilidad sobre su actividad.*

ii. Menor control sobre los dispositivos. *En el caso de colaboradores que pasan a acceder desde dispositivos personales, la capacidad de supervisión es limitada.*

2. Las tecnologías del puesto se hacen heterogéneas y difíciles de gestionar. La proliferación del trabajo remoto ha multiplicado los dispositivos y conectividad a los que accede el empleado, y muchos de ellos están fuera del control y plataformado de la empresa. Además, esta variabilidad se extiende a otros aspectos como los horarios de trabajo y las ubicaciones, saliendo del marco habitual.

Todo ello incrementa la complejidad en su gestión y se manifiesta en los siguientes aspectos:

a. Uso personal de dispositivos corporativos. Cuando el empleado utiliza su equipo corporativo en el domicilio puede acceder a todo tipo de correos y contenidos, y hacerlo en horarios fuera de oficina.

b. Uso corporativo de dispositivos personales (BYOD). Muchas empresas se han visto forzadas a aceptar el uso de dispositivos domésticos (no plataformados) y sobre los que el departamento de seguridad posee un menor control.

c. Conectividad heterogénea. Las empresas utilizaban diferentes mecanismos de conectividad para diferentes grupos de usuarios que eran minoritarios. Ahora ha entrado el uso de las redes domésticas para el grueso de los empleados. Además, para no tener que redirigir todo el tráfico a la red corporativa, se ha potenciado la conexión directa a soluciones en cloud.

3. Las necesidades del empleado varían según el perfil. El trabajo en remoto no impacta a todos los empleados por igual, dado que el nivel de tecnificación de cada puesto es distinto. Por ello, un enfoque único de equipamiento y conectividad no resuelve la disparidad de necesidades del usuario en función de su perfil. Esto se manifiesta en dos aspectos:

a. Uso intensivo de datos. Algunos departamentos realizan un uso más intensivo de datos, lo que en remoto significa mayores requerimientos de conectividad.

b. Acceso a aplicaciones críticas. Algunos empleados acceden en remoto a aplicaciones críticas, lo que eleva el riesgo y las necesidades de protección.

IMPLICACIONES PARA EL ÁREA DE SEGURIDAD

Los aspectos descritos anteriormente, como la heterogeneidad en el puesto y las vulnerabilidades vinculadas a proveedores y usuarios externos, se traducen en un conjunto de retos para el área de seguridad:

1. Las plataformas para dar acceso remoto pasan a ser críticas, al tener que operar a escala. Esto hace que un incidente afecte a la continuidad de negocio y no solo a un grupo de empleados.

2. Emergen nuevos eventos. Las conexiones externas se han multiplicado, lo que ha generado nuevos patrones de tráfico. Esto hace que aparezcan eventos más allá de las casuísticas habituales, así como un mayor número de incidentes (muchos de ellos falsos positivos).

3. Los entornos se gestionan de forma fragmentada. Se están utilizando herramientas específicas para cada entorno sin que exista una visión integrada. Por ejemplo, se necesitan varias consolas, lo que hace más compleja la gestión.

4. Dinámica de cambios bruscos. Los cambios abruptos generan ventanas de riesgo, dado que la seguridad entra como una medida a posteriori. Un ejemplo son los despliegues súbitos y masivos de puesto en remoto, donde se ha primado la continuidad de la actividad.

5. Riesgo y regulación vinculados a datos sensibles. El acceso fuera del contexto habitual a datos sensibles, así como la regulación en sectores críticos, condicionan las opciones de trabajo en remoto.

6. Transparencia insuficiente. La compartición de información es limitada, no solo internamente, sino también con proveedores y otros agentes. Esto dificulta la detección, así como la respuesta.

ACCIONES PREVISTAS POR LOS RESPONSABLES DE SEGURIDAD

Los responsables de seguridad están trabajando en proteger un puesto que abarque las nuevas casuísticas. Para ello, están perfilando a los usuarios, reajustando sus políticas y avanzando en estrategias de Zero Trust.

1. Revisar los Perfiles de usuarios. Los aspectos prioritarios son:

a. Inventariar los nuevos modos de acceso y usos para agruparlos en perfiles. No se trata de reubicar los perfiles existentes, sino de crear nuevos que reflejen la nueva forma de trabajar. Muchas empresas están incluyendo criterios adicionales para definirlos; por ejemplo, su contexto de trabajo doméstico.

b. Definir un nuevo entorno de trabajo para los nuevos perfiles, de forma que se ajuste la provisión tecnológica y su protección a cada uno de ellos.

2. Adaptar los estándares, normativa interna y controles a la nueva realidad. Los elementos más destacados son:

a. Estandarizar y racionalizar la conectividad; es decir, simplificar los distintos mecanismos hacia un estándar común en la organización.

b. Reajustar la normativa interna. Redefinir los requisitos tecnológicos para el trabajo remoto en función de los diferentes perfiles (ej. ancho de banda).

c. Adaptar políticas en función del uso; es decir, flexibilizar algunos controles, dado que el régimen de uso es distinto en función de los equipos. Por ejemplo, los equipos que no se conectan en meses requieren un cambio de políticas.

3. Acelerar la estrategia Zero Trust. Esta se apoya en los siguientes aspectos:

a. Asumir que el equipo está comprometido a la hora de definir políticas de seguridad.

b. Segmentar la red para evitar los movimientos laterales, particularmente en el caso de colaboradores externos.

c. Contextualizar la seguridad integrando datos de diferentes fuentes. Se trata de que la seguridad acompañe al usuario independientemente de su ubicación y acceso.

4. Concienciar al usuario. Este aspecto es esencial para la efectividad de las medidas anteriores.

a. Cultura de empresa: los empleados se han encontrado con una realidad radicalmente distinta y las empresas están ayudándoles a adaptarse, de modo que su experiencia sea lo más satisfactoria posible.

b. Concienciación y formación: la psicología de los empleados cambia cuando trabajan en remoto, y son más proclives a los ataques de ingeniería social. Se están realizando acciones dirigidas a concienciarles sobre estos riesgos.

MIRANDO A FUTURO

Los participantes en el debate mostraron un consenso sobre su actitud hacia el futuro: la situación no puede tratarse como un elemento transitorio, sino que apunta a un nuevo modelo de gestión. La forma de trabajar no va a revertirse a la situación anterior, sino que va a confluir hacia un híbrido entre trabajo presencial y remoto. A continuación, se describen los aspectos más destacados:

1. Las empresas ven una evolución de sus arquitecturas que se adapte a la nueva realidad del trabajo (ej. SASE).

2. El futuro pasa por un mayor uso de cloud, lo que implica revisar el gobierno, la visibilidad y un mayor foco en los accesos e identidades.

3. Los entornos legacy marcarán el ritmo de la transformación de la arquitectura, así como el de la migración a cloud. Las principales razones son:

a. Muchas cargas críticas se encuentran todavía en el legacy

b. Hay aplicaciones y componentes que no funcionan adecuadamente en los dispositivos domésticos

c. Existe un condicionante económico, principalmente la amortización de la inversión realizada

4. Las organizaciones van a revisar su postura y prácticas de seguridad al completo, en particular los casos de multinacionales, lo que permitirá incorporar el aprendizaje de cada uno de sus países o regiones.

Zero trust: enfoque de seguridad para empleados y colaboradores en remoto

Alberto Belle
Fernando Maldonado
@FmaldonadoF

Analistas principales de
IDG Research
@IDGResearch_ES

RESEARCH SERVICES
Calle Velázquez, 105 - 5ª planta
28006 Madrid
Teléfono +3491 349 6600
research@idg.es