EDSI Trend

TREND MICRO

Cambiando la marea

Predicciones de ciberseguridad para el 2021

EDSI Trend

https://www.edsitrend.com/

INTRODUCCIÓN

La pandemia del Coronavirus cambió la forma de operar de muchísimas organizaciones, convirtiéndose el teletrabajo en un nuevo estándar. Sin embargo, esta transición del trabajo día a día desde la oficina hacia el hogar (en muchos casos, definiéndose como algo a largo plazo) representa nuevos riesgos para las organizaciones debido al foco que han puesto los cibercriminales tanto sobre esta nueva forma de trabajar como sobre la relevancia del Covid-19.

En las predicciones de seguridad para el año 2020, Trend Micro afirmaba que la estructura tradicional de una red completamente aislada detrás de un firewall corporativo sería cosa del pasado. Debido principalmente al hecho de que protecciones y despliegues tradicionales ya no serían tan adecuados para el ecosistema actual donde se requieren de tantos servicios y plataformas tan diversos.

El duro golpe de la pandemia del Covid-19 hizo a muchas organizaciones enfrentarse a esta realidad. Obligándoles a replantearse qué tan preparados se encuentran para escenarios como puede ser un ciberataque, una crisis global y otros riesgos que siempre han estado. Pero nunca en un primer plano como el que se ha vivido este año.

En el 2021, las organizaciones tendrán que recorrer un duro camino para lidiar con las consecuencias a largo plazo mientras hacen un esfuerzo por mantenerse seguros en un mundo donde la necesidad de estar operativos online es cada día mayor. En las predicciones de Trend Micro, se discuten no sólo posibles desarrollos, sino también algunos a los que deberíamos anticiparnos todos. Analizando cómo las organizaciones deberán adaptarse al futuro cercano en que las amenazas y tecnologías tendrán un papel aún más protagónico.

LOS ESCENARIOS DE TRABAJO DESDE CASA SE CONVERTIRAN EN UN ATRACTIVO PUNTO DE ENTRADA PARA UN ATACANTE

El teletrabajo plantea diversos riesgos para una organización que hasta el momento eran inexistentes, ya que un atacante puede acceder a una red hogareña con mucha mayor facilidad que a una red corporativa, por motivos obvios de que la seguridad a nivel perimetral es mucho más deficiente. Existiendo en muchos casos la presencia de routers u otros dispositivos con vulnerabilidades que puedan ser explotadas.

La facilidad de un atacante para acceder a una red hogareña claramente representa un gran riesgo ya que una vez dentro de cualquier equipo en esta red, podría desplazarse al equipo de uso corporativo, y a partir de este, si llegase a darse el escenario de que por ejemplo una conexión VPN no sea del todo segura, podría moverse hacia la red corporativa y una vez dentro llevar a cabo cualquier tarea que desee: desde espionaje o robo de información hasta distribución de malware o causar una denegación de servicio.

Los routers siempre han sido un objetivo bastante fácil de explotar, y hay todo un negocio por detrás en que cibercriminales ofrecen routers hackeados, con lo cual un atacante puede fácilmente adquirir el acceso a una red hogareña. Teniendo en cuenta el entorno actual de teletrabajo, en que pueden existir incluso varias personas en una misma red hogareña trabajando (y con conexión VPN) para diferentes organizaciones, la venta de estos accesos se convertirá en un modelo de negocios bastante lucrativo para los cibercriminales.

LA PANDEMIA DEL COVID-19 SEGUIRA TENIENDO PAPEL DE PROTAGONISTA EN DIVERSAS CAMPAÑAS MALICIOSAS

Todo evento relevante es una oportunidad para los atacantes, que tomarán ventaja de ello para, mediante manipulación o sabotaje, aumentar la probabilidad de éxito de sus ciberataques. Y la pandemia del Covid-19 no fue para nada diferente, pudiéndose notar a mediados de este año un aumento enorme en la cantidad de correos fraudulentos, malspam, e incluso phishing donde se hacía mención del Coronavirus, el cual resultó ser un cebo más que efectivo.

El sector de salud, por su parte, será uno de los más afectados. El hecho de que muchos profesionales de la salud se encuentren trabajando de forma remota y también que la situación actual haya ameritado que la infraestructura de servicios médicos se haya vuelto más crítica que de costumbre, plantea un escenario donde los responsables de seguridad de estos sistemas estarán en constante desafío. No sólo en lo que respecta a los riesgos de siempre relacionados con la información sensible de pacientes y las infecciones de malware, sino a la posibilidad de ataques orientados al espionaje médico.

Un objetivo más que claro de los atacantes también serán laboratorios que se encuentren trabajando en vacunas para el coronavirus, principalmente aquellos que han hablado abiertamente sobre sus trabajos de investigación y desarrollo en relación con el Covid-19. Los atacantes podrían dirigir sus esfuerzos hacia estas organizaciones con el fin de robar información relacionada con las investigaciones en curso, lo que podría resultar en que se generen demoras en los desarrollos de los laboratorios e incluso generar problemas con relación a la distribución de posibles tratamientos.

Todas aquellas organizaciones y personas ajenas al sector de la salud seguirán estando en riesgo, de igual manera, ya que como mencionábamos anteriormente los atacantes continuarán aprovechando toda noticia en relación con el Covid-19 para lanzar campañas de desinformación y usar el interés público generado por la situación que ha generado el Coronavirus para atraer a los usuarios a que caigan en sus adjuntos y enlaces maliciosos. Aunque este uso del Covid-19 como cebo no se limita a correos electrónicos, sino al desarrollo de aplicaciones o sitios web maliciosos que sean hechos públicos bajo el pretexto de informar a la población sobre cualquier novedad. Lo mismo sucederá con las vacunas, que pasarán a ser también usadas como cebo en posteriores campañas.

EL TELETRABAJO OBLIGARA A LAS ORGANIZACIONES A ENFRENTARSE A ENTORNOS HIBRIDOS Y ARQUITECTURAS DE SEGURIDAD DIFICILES DE MANTENER

A medida que continúa el teletrabajo, los entornos híbridos (donde tanto información del trabajo como personal conviven en un mismo ordenador) seguirán siendo un desafío para las organizaciones, donde el uso que el empleado brinde al equipo informático no puede ser tan controlado como solía serlo. Los posibles casos de uso mixto de un ordenador desdibujan la línea acerca de dónde se almacena la información y dónde es procesada, aumentando aún más las dificultades de visibilidad que sufren las organizaciones en estos entornos, permitiendo que surjan también interrogantes como pueden ser:

¿Qué hacemos si se infecta un equipo?
¿Qué hacer con la información personal en caso de tener que hacer un formateo?
¿Podemos tener conocimiento de la información transferida o impresa?

A partir de los casos de tecnologías usadas en teletrabajo que han mostrado tener fallos de seguridad, los modelos de Zero Trust van a ganar un impulso importante en 2021, convirtiéndose en una aproximación efectiva para apoyar a las fuerzas de trabajo distribuidas. Al eliminar cualquier tipo de confianza implícita en todo lo que esté dentro o fuera de la red, todo será verificado. A través de la microsegmentación, una arquitectura de Zero Trust permite brindar a los usuarios acceso únicamente a los recursos específicos que requiera, dentro de determinados parámetros. Esto permite mantener una postura de seguridad robusta, dificultando a cualquier atacante el ingreso a su red. Mejor aún, resulta fácil integrar una estrategia Zero Trust con algún SASE (Secure Access Service Edge) en nube, brindando a los equipos de seguridad informática una visibilidad crítica sobre todo tráfico entrante y saliente.

Otra transición que muchas organizaciones habrán llevado a cabo a raíz de la pandemia sería la del viaje a la nube. Infraestructuras que normalmente hubieran tenido dificultades o requerido de un largo periodo para migrar sus tecnologías, están ahora bajo un proceso de transformación acelerado, debido a la dificultad que representa cumplir con las demandas actuales para una solución on-premises, las cuales pueden ser fácilmente satisfechas por una solución basada en nube. Es un hecho que toda organización, independientemente de su sector o industria, se esforzará para mantenerse versátil y ágil para superar los desafíos que aguardan.

En lo que respecta a la reevaluación de estrategia de seguridad y subsecuente necesidad de proteger a los trabajadores de forma remota para garantizar la continuidad de negocio, los equipos de IT deberán prepararse para mantener una estrategia de seguridad robusta y a largo plazo. Resultando en muchos casos una medida efectiva la implementación de políticas que definan cómo se debe trabajar de forma remota, manipular correctamente la información, y garantizar que la línea entre el uso personal y corporativo de dispositivos se mantenga fija.

LAS NUEVAS NECESIDADES DE SEGUIMIENTO DIRIGIRAN LA ATENCION DE LOS CRIMINALES HACIA LA INFORMACION RECOLECTADA POR PARTE DE LOS USUARIOS

Una necesidad sin precedentes de recolectar información y llevar un seguimiento del estado de salud de los individuos, atraerá tanto a cibercriminales como grupos de activistas políticos a obtener toda esa información. Jugando también en contra se encuentra a la velocidad con la que estas medidas de seguimiento han debido de ser implementadas, debido a que pueden haber sido desarrolladas de forma veloz y por ello podrían estar en riesgo de filtrar accidentalmente información o tener vulnerabilidades que puedan exponer la misma.

El facilitar el acceso a la información, debido al rápido acceso que debe hacerse a la misma, lleva a una variedad de problemas que exponen a diversos riesgos de seguridad. Una mezcla de bases de datos con muchísima información y una implementación apresurada resulta en un objetivo rico e interesante para cibercriminales. Dirigiendo sus esfuerzos a obtener la misma para, por ejemplo, venderla posteriormente al mejor postor.

Sumado a los puntos anteriores, se encuentra en muchos casos la previa ausencia de protocolos y una protección estricta para servidores o base de datos en diversos entornos que no han tenido un foco en la seguridad y tendrán que afrontar el desafío de tomar medidas para mantener la información lo más segura posible.

Asimismo, también resulta un desafío en sí mismo las dificultades económicas que puede haber generado la pandemia de Covid-19, debido a que como consecuencias de estas muchas organizaciones podrían tener que mantener su postura de seguridad a partir de un presupuesto para seguridad que se haya visto recortado.

AUMENTARA EL USO DE VULNERABILIDADES QUE SEAN RECIENTES, APROVECHANDO LA DIFICULTAD DE REALIZAR TAREAS DE PARCHEADO

En el 2021, los atacantes tenderán a explotar vulnerabilidades que hayan sido recientemente hechas públicas, sumado al uso de vulnerabilidades de día cero que se ha visto en este año. Este incremento será principalmente a raíz de la facilidad que plantea el uso de vulnerabilidades y exploits que son conocidos y pasan a ser documentados, en contraste con el tiempo y trabajo que conlleva encontrar y explotar una vulnerabilidad de día cero.

Esto claramente aumentará el riesgo para las organizaciones en lo que respecta a la gestión de vulnerabilidades sobre los ordenadores de trabajo que se encuentren en un entorno hogareño, principalmente debido a la dificultad que representa gestionar las tareas de parcheado para los equipos fuera de la red corporativa.

Posiblemente se vea también un incremento en el uso de herramientas legítimas de penetration testing, como sucedió recientemente con Cobalt Strike que fue utilizada para movimiento lateral en ataques de distribución del ransomware Ryuk.

LAS APIs SE CONVERTIRAN EN UN VECTOR FAVORITO PARA LAS FUGAS DE INFORMACIÓN

Muchas organizaciones dependen de APIs actuando como intermediarios para el acceso a sus sistemas internos y la interacción con los usuarios finales mediante aplicaciones, y es por esto por lo que los atacantes buscarán utilizarles como punto de entrada hacia las redes corporativas, ya que a medida que estas se vuelven más y más prominentes, aumenta con su uso la potencial superficie de ataque. Principalmente por su uso también como conductos para integraciones con terceros.

El principal problema que plantean las APIs, es que su desarrollo en lo que respecta a seguridad está aún dando sus primeros pasos, y pueden presentar diversas vulnerabilidades que podrían convertirse en un vector para fugas de información en aplicaciones corporativas, por ejemplo. Habiéndose visto ya casos donde se podía obtener fácilmente acceso a la información personal de los usuarios e incluso a código fuente expuesto y servicios de backend.

La superficie de ataque de las APIs aparece principalmente por lo relativamente fácil que resulta descubrirles, así como el uso que hacen de múltiples parámetros que podrían ser comprometidos. Los métodos tradicionales de defensa para las mismas (Como pueden ser Captchas o JavaScript), podrían no resultar efectivos para prevenir un ataque automatizado, lo que significa que de momento su protección es apenas parcial. Una recomendación importante sería la configuración de mecanismos de control de acceso y autenticación en profundidad, así como la revisión frecuente de logs de acceso.

SE DESCUBRIRAN MUCHAS VULNERABILIDADES CRITICAS EN APLICACIONES EN NUBE Y SOFTWARE NECESARIOS PARA EL TELETRABAJO

Debido al aumento en su uso (y, por consiguiente, investigación) es más que seguro que sean descubiertas múltiples vulnerabilidades en los software y servicios más utilizados en el teletrabajo. Gran parte de los esfuerzos y atención de investigadores y cibercriminales por igual serán seguramente destinados hacia software popular como pueden ser Microsoft Teams, SharePoint u Office 365.

Ahora más que nunca, la seguridad en nube pasará a ser uno de los principales temas de conversación, principalmente impulsada por la veloz transición hacia la misma que han experimentado muchas organizaciones, así como la necesidad del uso de herramientas de colaboración.

Los atacantes, por su parte, se enfocarán en vulnerar la nube para buscar obtener información valiosa y sensible que pueda permitirles encontrar algún punto de entrada a una red corporativa. Sin embargo, también harán su esfuerzo para tomar control de servidores en nube y desplegar imágenes de contenedores maliciosos, así como también a recorrer la nube en busca de información expuesta accidentalmente por organizaciones.

RECOMENDACIONES DE SEGURIDAD

Impulsar la educación y entrenamiento a usuarios

Los atacantes seguirán intentando aprovechar el miedo alrededor de la situación del Covid-19, por lo que se debe mantener informados a los usuarios acerca de las tácticas utilizadas y posibles vectores de ataque. Las organizaciones por su parte deberán reforzar el conocimiento acerca de amenazas e intentar extender las mejores prácticas hacia el hogar de sus empleados. Indicando de forma clara qué se debería y no debería hacer, además de recomendar que se evite el uso de dispositivos personales.

Mantener un control de acceso estricto a la red corporativa y la oficina en el hogar

Las organizaciones deberían enfocarse en crear políticas enfocadas en seguridad, así como tener un plan para respuesta a incidentes que cubra todo el perímetro de sus operaciones. Esto logrará endurecer la seguridad en servicios, workstations y la información corporativa mientras robustece su metodología de teletrabajo. Debe intentarse evitar la implementación de confianza implícita en recursos o cuentas de usuario, independientemente de su ubicación.

Reiterar las medidas de seguridad básicas y programas de gestión de parches

Los puntos débiles seguirán en aumento en los próximos meses de teletrabajo. Será imperativo implementar un sistema de actualización e implementación de parches sobre aplicaciones y sistemas operativos, debido a que estarán en una posición vulnerable ahora más que nunca.

Aumentar la detección de amenazas con especialización en seguridad

Garantizar de la mano de especialistas de seguridad, una respuesta a incidentes y detección de amenazas continua y avanzada tanto en la nube como el correo, endpoints, la red y servidores. Asimismo, se debe buscar tener la mejor comprensión de ataques y en base a ello priorizar las aletas de seguridad, a partir de inteligencia ante amenazas y soluciones líderes en la industria de la seguridad.

REFERENCIAS E INFORMACION ADICIONAL

Este documento fue elaborado a partir de ***Turning the Tide: Trend Micro Security Predictions for 2021***, a modo no sólo de traducción al español de este sino también como resumen de sus contenidos más relevantes.

Invitamos a todos aquellos interesados en profundizar los detalles mencionados en este documento, a visitar a través del siguiente enlace la página de Trend Micro y leer su informe completo en inglés con las predicciones de seguridad para el año 2021.

Turning the Tide: Trend Micro Security Predictions for 2021