kaspersky PREPARADOS PARA EL FUTURO

Protección de un futuro posterior al COVID-19

Superación de los desafíos de ciberseguridad a los que se enfrentan las empresas en esta década de 2020

El teletrabajo ha tenido un éxito rotundo durante la pandemia, siendo los equipos de TI en gran medida los héroes anónimos tras este éxito. Las empresas que no dependen de interacciones presenciales han sobrevivido y prosperado durante los confinamientos y las restricciones, debido a que el personal ha podido seguir trabajando de forma eficaz y segura desde su casa, en sus equipos portátiles, PC y otros dispositivos corporativos o personales.

La adopción de prácticas de trabajo en casa ha demostrado una beneficios tales como un aumento de la productividad, reducidos niveles de absentismo, una mejora en la retención del personal y la reducción de los costes asociados con el espacio de trabajo. Así pues, aunque algunos empleados han perdido el entusiasmo inicial que les producía llevar a cabo su vida laboral completamente desde casa, es posible que en el futuro la norma sea un estilo de trabajo «mixto» que combine el trabajo en casa con el trabajo en la oficina.

Una investigación encargada por Kaspersky[1] ha descubierto lo siguiente:

- El 74 % de los empleados no quiere volver, al menos, a algunas de las dinámicas laborales del pasado.
- El 39 % de los empleados está dispuesto a escapar de la estructura de trabajo tradicional de 9 a 17:00.
- El 34 % no quiere volver a trabajar en una oficina fija.
- El 32 % quiere replantearse la semana laboral de cinco días.

«Los costes del delito cibernético pueden duplicarse debido a la pandemia del coronavirus».

Cybersecurity Ventures, julio de 2020

La historia de la ciberseguridad

¿Cómo ha afrontado el sector de la ciberseguridad este cambio tan drástico en las prácticas de trabajo? Si bien es cierto que el teletrabajo tiene muchos beneficios empresariales, también tiene sus aspectos negativos. Uno de ellos es el aumento de la vulnerabilidad frente a los ataques dirigidos a terminales ubicados y operados de forma remota. Y, a través de ellos, a toda la infraestructura de la empresa.

En resumen, los ciberdelincuentes han experimentado un período de bonanza.

- Antes de la pandemia, el Centro de Denuncias de Delitos en Internet del FBI recibía unas 1000 denuncias diarias por delitos cibernéticos. En la actualidad, recibe entre 3000 y 4000 al día[2].
- Un informe de la Interpol[3] publicado en agosto de 2020 reveló que hubo «un índice alarmante de ciberataques durante la pandemia de la COVID-19».
- Según la revista más importante del sector, Cybersecurity Ventures[4], las estafas de phishing y los ataques remotos a empleados se han disparado debido a que las personas que trabajan desde casa no toman las medidas adecuadas para proteger sus equipos.

[1] Securing the future of work, Kaspersky, 2020

[2] Combatting Cybercrime During COVID-19, Aspen Digital, 2020

[3] INTERPOL report shows alarming rate of cyberattacks during COVID-19, INTERPOL, August 2020

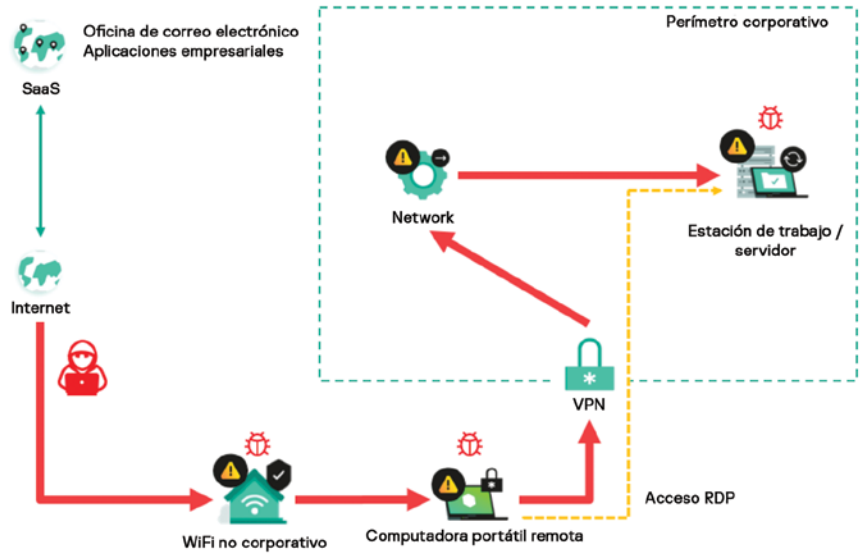
¿Cuáles son los problemas de seguridad?

- Los terminales remotos no se conectan a través de una LAN corporativa. Se conectan a Internet a través de enrutadores domésticos o mediante conexiones Wi-Fi no seguras en lugares públicos. Por este motivo, son más vulnerables frente los ataques de intermediarios (MITM, por sus siglas en inglés).
- En muchas ocasiones, los dispositivos corporativos en el hogar también suelen utilizarse como PC domésticos para consultar el correo electrónico personal, atender a intereses externos, etc. Además, al trabajar de forma individual en casa y no en una oficina con otras personas, los empleados suelen caer en la tentación de visitar sitios web sospechosos y potencialmente peligrosos utilizando su equipo portátil corporativo, lo que aumenta la exposición del dispositivo a las ciberamenazas.
- Estos riesgos s incrementan incluso más cuando las empresas adoptan políticas BYOD (traiga su propio dispositivo, por sus siglas en inglés). Ahora bien, el usuario es también administrador, por lo cual usted tiene poco o ningún control sobre la seguridad instalada en los dispositivos que interactúan con su infraestructura corporativa, ni sobre su configuración.

Si un terminal se encuentra en peligro, el usuario no puede trabajar, los datos valiosos almacenados en el dispositivo están en riesgo y pueden secuestrar la identidad de un usuario con el objetivo de atacar a sus clientes, por ejemplo, utilizando su cuenta de correo electrónico empresarial. Y lo que es más importante, incluso si los atacantes son capaces de vulnerar su perímetro desde un único terminal, esto les permitirá comenzar a moverse lateralmente por su red, para luego introducir y activar malware, y tomar el control de sus sistemas. Este es el modus operandi estándar incluso de los ataques corporativos más complejos, sofisticados y de gran alcance (y costosos): la incursión inicial desde un único dispositivo vulnerable.

Las VPN o RDP proporcionan comunicaciones seguras entre los diferentes terminales remotos y su red. No obstante, también pueden ser víctimas de ataques. Las credenciales robadas a los usuarios (obtenidas mediante ataques de fuerza bruta, phishing o ingeniería social) están en la web oscura a disposición de cualquier persona que cuente con algo de dinero y le interese atacar su empresa. Otro ejemplo son los RAT (troyano de acceso remoto, por sus siglas en inglés), que pueden instalarse en el terminal sin que usted o el usuario lo adviertan.

Cualquiera de estas entradas puede utilizarse para instalar ransomware, realizar operaciones financieras ilegales, robar datos o simplemente acceder a sus sistemas y vender ese acceso en línea al mejor postor.



También debe tener en cuenta que, cuando sus empleados llevan a la oficina dispositivos de uso remoto y los conectan directamente a la red, cualquier malware que pueda estar presente en esos dispositivos tendrá una ruta de acceso directo a sus sistemas.

La respuesta

Como suele suceder con la ciberseguridad, la respuesta se encuentra en un enfoque polivalente que utilice defensas multicapa, con particular énfasis en esos terminales remotos vulnerables.

Estas son algunas de las cosas que puede hacer:

A nivel de VPN/RDP

Desde principios de marzo, la cantidad de ataques de Bruteforce.Generic.RDP se ha disparado en casi todo el planeta[4]

- **Implemente MFA**, autenticación de varios factores (p. ej., contraseña + token de seguridad), para permitir el acceso de los terminales a la VPN.
- **Restrinja el acceso a RDP** exclusivamente a las direcciones IP procedentes de la VPN corporativa.
- Complique el acceso a los posibles atacantes **mediante la utilización de un número de puerto RDP no estándar** (diferente a 3389).
- Considere la posibilidad de **dirigir todo el tráfico web a través de su servidor proxy seguro**, siempre y cuando disponga de los recursos y la capacidad necesarios; algo que, por supuesto, no estará al alcance de todos.
- **Limite las funciones y aplicaciones a las que se puede acceder a** través de la VPN o RDP. El trabajo de configuración que esto requiere llevará tiempo, pero valdrá la pena si tiene la posibilidad de adoptar esta estrategia en su organización.
- **Considere la posibilidad de actualizar su protección perimetral**: las soluciones de seguridad del servidor de correo electrónico y de la puerta de enlace web, que bloquean la mayoría de las amenazas antes de que lleguen al nivel del terminal, suelen ser una buena inversión.

A nivel de estación de trabajo

Controlar el acceso a sitios web y aplicaciones que no son pertinentes para el trabajo tiene además el beneficio de reducir la utilización de las redes sociales, la navegación por Internet, las compras en línea y otras actividades que hacen perder el tiempo durante las horas de trabajo y, por lo tanto, aumentar la productividad, que suele ser una preocupación económica cuando se trabaja de forma remota.

Reduzca la superficie de ataque fortaleciendo sus sistemas. Restrinja o prohíba el acceso de las estaciones de trabajo a sitios web específicos o bloquee la ejecución de determinadas aplicaciones mediante las listas de sitios permitidos y prohibidos. También puede plantearse la posibilidad de aplicar una directiva de «denegación predeterminada», en la que solo se puedan ejecutar en el dispositivo determinadas aplicaciones específicas relacionadas con el trabajo y nativas del sistema. Este planteamiento no será bien recibido por los trabajadores remotos que también utilizan sus dispositivos corporativos como equipos personales, pero resulta ser un enfoque de seguridad de enorme efectividad.

Utilice cifrado para proteger los datos de la empresa. Los dispositivos móviles se pueden perder, y usted debe tener la seguridad de que los datos confidenciales que guardan sean inaccesibles y completamente inútiles para las personas ajenas a la empresa.

Esté al día con las revisiones. Puede parecer trivial, pero la aplicación de las revisiones a tiempo y por orden de prioridad es absolutamente fundamental. El aprovechamiento de las vulnerabilidades en las aplicaciones más habituales sigue siendo el punto de entrada ilícito utilizado con mayor frecuencia en los sistemas corporativos.

Utilice el control de anomalías para detectar cualquier actividad sospechosa en los terminales. ¿Hay algo que no encaja? ¿Ha detectado algún comportamiento extraño en alguna estación de trabajo remota? Su solución de seguridad debe ser capaz de detectar el problema automáticamente y solucionarlo con rapidez.

Utilice herramientas potentes de detección y corrección. Es bien sabido que disponer de una solución EDR (detección y respuesta en terminales, por sus siglas en inglés) eficaz, junto con una EPP (plataforma de protección de terminales, por sus siglas en inglés) sólida, es fundamental para una defensa eficaz de los terminales, sobre todo cuando hablamos de ciberataques evasivos. Esto no tiene por qué quitarle mucho tiempo: las detecciones automáticas pueden, en muchos casos, contrarrestarse con respuestas automáticas. Su personal solamente tendrá que intervenir cuando la solución detecte algún problema grave que justifique su atención.

[4] Primavera remota: el aumento de los ataques de fuerza bruta contra RDP, Kaspersky, 2020

El empleo en este sector debe crecer aproximadamente un 89 % en todo el mundo para poder satisfacer la demanda prevista.[5]

¿Y quién va a hacer todo esto?

Dar buenos consejos es más fácil que ponerlos en práctica. Esto es especialmente cierto cuando escasean los héroes anónimos de la pandemia, los profesionales de TI y, en concreto, los profesionales de seguridad de TI necesarios para llevar a cabo todo este trabajo. Muchas veces, los departamentos de TI disponen de menos personal del necesario, simplemente porque contratar (y retener) suficiente personal de seguridad de TI supone un gran desafío.

En un contexto en el que el teletrabajo o el trabajo mixto entre casa y oficina, con todos los demás aspectos informáticos que conlleva, puede ser el futuro, la industria del delito cibernético está obteniendo el máximo partido de las nuevas oportunidades que se generan. Por ello, es fundamental aprovechar por completo las horas disponibles del personal de seguridad de TI.

Automatización

Parte de la respuesta, se encuentra en la automatización. Muchas de las actividades enumeradas anteriormente (control de anomalías, aplicación de revisiones y otros elementos de detección y fortalecimiento del sistema) pueden automatizarse totalmente o en gran medida gracias a los actuales avances en el aprendizaje automático y la inteligencia artificial. Esto puede incluir incluso algunos de los procesos más avanzados, como los aspectos del análisis de la causa raíz y de la respuesta. Por tanto, su solución de seguridad debería hacer la mayor parte del trabajo, en lugar de usted y su personal.

Integración

Trabajar con un sistema de seguridad integrado es otra excelente forma de ahorrar tiempo. Implementar un único conjunto de directivas en todos los aspectos del sistema desde una única consola es más eficiente y reduce los riesgos, al dejar menos margen para errores administrativos. Así que piénselo dos veces antes de invertir en nuevos y llamativos productos específicos para una única función y con sus propias consolas, ya que pueden requerir mucho tiempo y consumir demasiados recursos para ofrecer muy pocos resultados.

Reducción de las alertas

Lo más probable es que su personal de seguridad también pierda mucho tiempo constatando alertas rutinarias, cuando podría estar centrándose en amenazas evasivas más peligrosas. La elección de su solución EPP base marcará la diferencia: aspectos fundamentales como el refuerzo de los sistemas, la aplicación eficiente de revisiones y la prevención automatizada de amenazas contribuyen a reducir drásticamente la cantidad de alertas que debe gestionar su atareado personal. Además, tiene derecho a exigir a su solución de seguridad una tasa casi nula de falsos positivos: su personal no debería perder el tiempo con ellos.

Una estrategia gestionada

Este también podría ser un buen momento para considerar una solución de seguridad gestionada. Las soluciones MDR (detección y respuesta gestionadas, por sus siglas en inglés) se están implementando de forma generalizada en los departamentos de TI que se encuentran en una situación difícil. La incorporación de una tercera parte especializada para gestionar los aspectos más exigentes de su seguridad y respaldar el trabajo de su

[5] (ISC)2 Cybersecurity workforce study, (ISC)2, 2020

personal de seguridad de TI conlleva grandes beneficios. Un proveedor externo debe tener el ancho de banda necesario para ofrecer una supervisión ininterrumpida de la seguridad, disponer de los conocimientos especializados necesarios para realizar tareas específicas tal como el análisis avanzado de las causas raíz, la búsqueda de amenazas e incluso los casos de respuesta guiada y remota. Además, debe contar con los recursos y los conocimientos técnicos adecuados para adaptarse a sus necesidades crecientes o fluctuantes. De una forma u otra, incorporar a una tercera parte de confianza que le respalde al asumir parte de la carga puede ser una buena inversión empresarial.

Una cultura de concienciación cibernética

«Si las personas que trabajan desde sus casas no se forman de inmediato, y si las empresas no proporcionan enseguida a sus empleados una formación de concienciación sobre la seguridad centrada en las amenazas que implica el teletrabajo, los costes de los delitos cibernéticos a nivel mundial podrían llegar a duplicarse a finales de este año».

Steve Morgan, fundador de Cybersecurity Ventures y redactor jefe de Cybercrime Magazine

Independientemente de dónde se encuentren, las cargas de trabajo del personal de TI disminuyen inevitablemente cuando se encuentran en una cultura corporativa en la que los usuarios son conscientes de las amenazas, cuentan con las habilidades prácticas necesarias para evitar poner en peligro la infraestructura por negligencia, o por simple desconocimiento, y llevan a cabo ciberprácticas adecuadas de forma instintiva. Es de vital importancia que exista una buena concienciación cibernética en todos los ámbitos, una cultura de comportamiento de ciberseguridad dentro de la empresa y disponer de conocimientos básicos de ciberseguridad para reducir la superficie de ataque y la cantidad de incidentes que resolver. Muchas veces, las empresas se esfuerzan por encontrar las herramientas y los métodos adecuados para formar con eficacia a sus empleados. Sin embargo, lograrlo desde cero es una tarea compleja que precisa mucho tiempo. Para lograr una cultura con conciencia de seguridad, hay que ofrecer una correcta formación en materia de ciberseguridad: una formación que incluya las últimas técnicas y tecnologías para la educación de adultos y, lo más importante, que ofrezca contenidos aplicables y actualizados.

Un departamento de TI contento y motivado

Como es lógico, los profesionales de la seguridad odian perder el tiempo en actividades rutinarias y aburridas y, por tanto, liberarles para que se ocupen de tareas más exigentes aumenta su nivel de satisfacción en el trabajo, lo que se traduce en mayores niveles de retención. Esto le permitirá invertir en el desarrollo de los conocimientos técnicos de su personal (ahora tienen la posibilidad de asistir a cursos de formación) y correrá menos riesgo de que otros se los lleven: una situación en la que todos salen ganando.

Cómo podemos ayudar

Los cambios impuestos en el entorno de la tecnología de la información (TI) han debilitado las medidas de ciberseguridad existentes, lo que ha convertido su rápida adaptación en todo un desafío. Al mismo tiempo, la ciberseguridad es clave para confiar en los nuevos casos de uso de los servicios digitales y, por tanto, tiene la oportunidad de facilitar la transformación.[6]

El enfoque que ahorra más tiempo y es más rentable, tanto si decide optar por una solución interna, como por una gestionada, o por ambas, será generalmente el de escoger un único proveedor, que pueda ofrecer una plataforma completa de EPP/EDR multicapa y más soluciones. Esto también implica buscar una solución que pueda escalar con su empresa a largo plazo, de modo que no tenga que gestionar productos comprados y complementarios con sus propias consolas y necesidades de formación en el futuro.

La solución Kaspersky Optimum Security está lista para ayudar a su creciente personal de seguridad de TI a afrontar y vencer los desafíos que plantean los entornos de trabajo combinados, con capacidades de protección de puntos finales escalables y fáciles de administrar.

[6] ENISA Threat landscape - The year in review, Agencia Europea de Seguridad en las Redes y de la Información (ENISA), 2020

Podemos ofrecerle una solución de seguridad multicapa para terminales sumamente automatizada, completamente escalable y basada en los fiables cimientos de una galardonada solución EPP, respaldada por una experiencia inigualable en MDR, en formación en habilidades y concienciación y, por supuesto, por nuestra inigualable asistencia especializada.

Para obtener más información sobre cómo puede ayudarle Kaspersky Optimum Security a proteger su empresa frente a las amenazas evasivas, visite http://go.kaspersky.com/optimum_ES.

Noticias sobre ciberamenazas: www.securelist.es
Noticias sobre seguridad de TI: business.kaspersky.es

www.kaspersky.es