La Covid-19 hace extremar las precacuciones

Segmentación, la nueva forma de abordar la seguridad TI

Data Center Market, en colaboración con Guardicore, ha organizado un desayuno virtual de trabajo con usuarios finales para analizar los nuevos retos de seguridad a los que se enfrentan empresas cada vez más provistas de ecosistemas de trabajo y operativos híbridos.

Cristina López Albarrán

Las organizaciones deben abordar la seguridad TI de manera diferente. Los tiempos han cambiado y las necesidades también. El tsunami de Covid-19 en su etapa inicial en nuestro país impuso el teletrabajo en la mayoría de las empresas. Era la manera de mantener en funcionamiento un negocio. Pero esta medida -que todo apunta a que perdurará en nuestro día a día-, implicó una adecuación de los sistemas y de las operativas con gran celeridad, así como grandes retos a la hora de proteger los recursos y activos de las compañías.

Y es que, sigamos o no con pandemia, los entornos son cada vez más enrevesados, con infraestructura de TI de mayor complejidad haciendo uso de múltiples nubes, contenedores, soluciones on premise… una amalgama híbrida que debe hacer frente a riesgos de diversa índole y que, si no saben protegerlos adecuadamente, pueden suponer un coste muy elevado para las empresas.

Para tratar estos asuntos, Data Center Market, en colaboración con Guardicore, ha organizado un desayuno virtual en el que han participado representantes de Asepeyo, Grupo Día, Haya Real Estate, Liberty Seguros, el Ministerio de Agricultura y Pesca, Alimentación y Medio Ambiente, Roche España y Wi-Zink Bank. Estas han sido las principales conclusiones del evento.

Cubrir el endpoint

El teletrabajo llegó, pero no estaba institucionalizado en muchas compañías. Bien es cierto que algunas tenían smartphones o portátiles preparados y planes en marcha 'work from home' con modalidades de acceso previstas de forma esporádica y pasiva, pero no para toda la plantilla y para que se funcionara a jornada completa y se conectase todo el mundo al mismo tiempo. Esto supuso para los responsables de seguridad informática duplicar los controles y las medidas, recurrir a conexiones VPN (a veces no habilitadas) y hacer ver a los empleados que teletrabajar es como trabajar en la oficina, pero en otro escenario diferente. Se tuvieron que desplegar muchos dispositivos en poco tiempo y activarse normas que costaron llevar a cabo, como el segundo factor de autenticación. Afrontar la disponibilidad de servicio fue un reto en toda regla que se resolvió adaptando la infraestructura para que absolutamente el cien por cien de los empleados pudieran operar en remoto de forma simultánea. Y esto incluyó a los contact center.

Lo primero fue proteger a los empleados, pero a algunas organizaciones se les sumó otro desafío: tener que colaborar con proveedores externos que no estaban preparados para esta modalidad y a los que había que facilitar su labor de manera segura. Para estas terceras partes relevantes se montaron escritorios virtuales (VDI) o se diseñó una solución acorde con los requisitos de protección de la empresa a la que han servido, manteniendo el aislamiento de la parte corporativa de las plataformas con las que funcionaban, de la parte personal que podría ser vía de entrada de malware.

"Protección a punto: parcheado, concienciación y segmentación"

Pese a que las organizaciones trataron de mitigar el impacto en aplicaciones críticas, las empresas siguen expuestas a todo tipo de ciberataques con el

Avishag Daniely, directora de Producto de Guardicore

Nos encontramos con entornos híbridos que combinan máquina física, on premise, contenedores, multicloud... diferentes ambientes que deben coordinarse e interconectarse. Esto supone un aumento de los riesgos a los que se enfrentan las organizaciones, pues necesitan controlar todos estos equipos y plataformas, así como sus comunicaciones, protegiendo los datos. Esto afecta a la posibilidad de sufrir un ataque exitoso y las brechas de seguridad tienen un precio muy alto. Según un estudio de IBM y Ponemon, el coste supera los 3,8 millones de dólares, es más alto que el del año pasado. Desde Guardicore ofrecemos una solución de segmentación que ayuda a asegurar todas las conexiones y a proteger este perímetro de acceso remoto. Como ejemplo podemos citar el de un banco del top 25 que recibió un mail en el que los ciberdelincuentes les decían que tenían acceso a su base de datos de Oracle. La entidad no entendía de dónde venía el ataque porque no disponía de visibilidad de ese acceso remoto al que habían recurrido para continuar con la labor de 3.000 agentes de su call center, un colectivo que antes de la pandemia trabajaba en el propio edificio. Gracias al despliegue de nuestra herramienta lograron detectar en apenas tres días de dónde provenía ese ataque.

"Es muy importante entender de dónde procede un ataque y poder tener la visibilidad suficiente, algo que se consigue con Guardicore"

phishing en primera línea. Cada vez son más elaborados y aunque se toman precauciones y se ponen trabas (tres capas de correo, refuerzo del sistema de alertas, etc), "saben dónde apuntar". Todos los sectores están en el punto de mira y el de salud, que parecía ajeno, también e, incluso, de forma abierta. La nueva realidad llevó a la determinación de que el perímetro que se tenía que cubrir era el endpoint y de que había que reducir la infraestructura para lograr un acceso seguro.

Asimismo, el terreno de exposición ahora es más amplio y conviene revisarlo. Los planes de contingencia que había en marcha se quedaron cortos, pues no se habían configurado para una situación tan prolongada en el tiempo. Esta situación ha impuesto el diseño de planes adicionales que contemplaran esta forma de trabajar mixta, híbrida, con nuevos escenarios de riesgo. Y completar estas estrategias con información externa de contexto sobre lo que ha ocurrido en otros países y corporaciones, recurriendo a sistemas de ciberinteligencia porque estamos en una situación de incertidumbre.

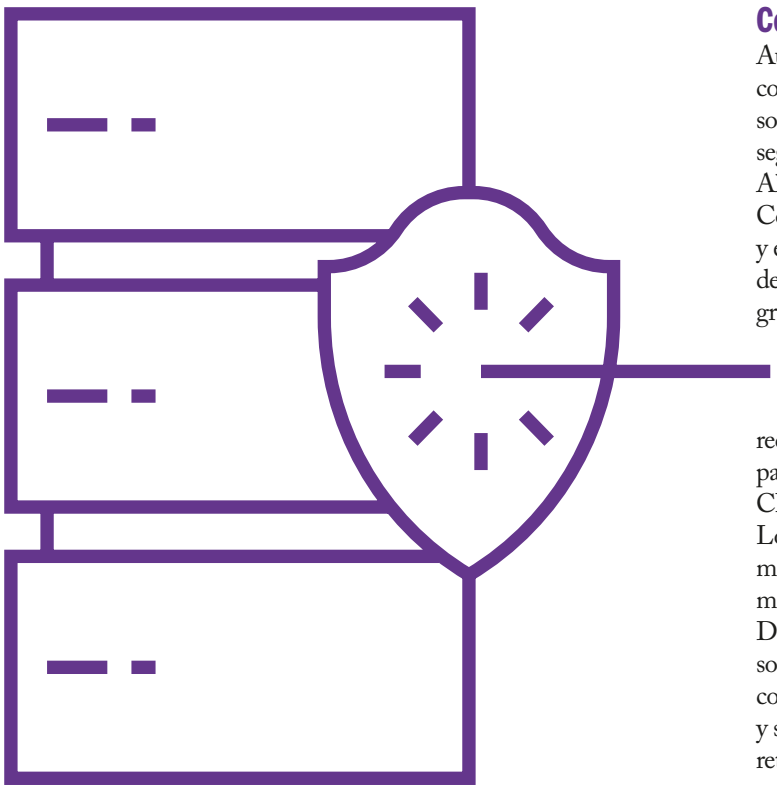
En definitiva, el perímetro está roto y las compañías han de ser más líquidas a escala organizativa, técnica y política. Se deben tener en cuenta otras variables a las que en algunos casos no se prestaba atención.

Julen Cordon, responsable de preventa para Iberia de Guardicore

Junto al parcheado, la concienciación es crítica para reducir el impacto de cualquier ataque de seguridad. Sin embargo, hay otra herramienta muy importante que es la segmentación. A día de hoy existe un desconocimiento en el mercado de lo que ofrece esta tecnología. Lo que se suele entender actualmente por este concepto es una segmentación de red, una técnica que antes resultaba insuficiente y que ahora, con la utilización de contenedores, con la nube... es aún menos. Por mucha doble autenticación y muchos sistemas que se empleen, cuando entra algo en ese endpoint, la segmentación que tenemos no es suficiente y el malware puede atacar a servidores críticos.

No somos conscientes de las posibilidades que nos dan las herramientas de segmentación vía software. No hace falta tener un WLAN con muchas conexiones o muchos accesos a servidores: esta propuesta mejora la postura de seguridad de una manera transversal, con una ratio de coste bajo y un beneficio significativo. Poniendo un símil en el panorama actual de pandemia, antes segmentábamos comunidades y ahora ponemos una "mascarilla" a los servidores y a todos los equipos de forma individual para que controlen lo que entra y sale de cada uno de ellos. Hablamos de segmentar a nivel de individuo y de equipo.

"Parcheado, concienciación y segmentación son tres patas fundamentales en seguridad "



Concienciación

Aunque siempre ha sido fundamental la labor de concienciación y evangelización de los empleados sobre las buenas prácticas a la hora de preservar la seguridad del negocio, con el decreto del Estado de Alarma y el confinamiento, esta tarea se volvió crítica. Como ya hemos dicho, el teletrabajo se popularizó y esto trajo consigo que se multiplicara la superficie de ataque, dibujando un perímetro más amplio, con gran cantidad de conexiones desde diferentes puntos y dispositivos. Hay empresas que controlaban los dispositivos que utilizaban los trabajadores para conectarse, pero hay otras donde cada trabajador recurría a sus propios móviles, equipos y redes escapando del control de los departamentos TI y de los CISO de su empresa.

Los ciberdelincuentes continúan atacando de la misma manera, focalizando sus esfuerzos en el eslabón más débil: el usuario no formado o no concienciado. De esto se han dado cuenta las empresas y cada vez son más habituales las campañas de sensibilización, con pruebas de hacking ético, ejercicios de formación y seminarios. Teniendo en cuenta que no se espera un retorno a corto plazo a las oficinas y que el teletrabajo

va a ser cada vez más normal, conviene recordar y hacer énfasis en que el empleado adopte el "ciberse-curity mode" en su domicilio o allí donde trabaje, es decir, que siga alerta y opere consciente de sus actos entendiendo las consecuencias de los mismos. "Las personas son el eslabón más débil de la cadena".

Herramientas de segmentación

Además de la utilización de parches para proteger los activos de una organización y de la tan necesaria

1 ASEPEYO. Edgard Ansola Munuera I **2** DIA GROUP. Rubén Fernández I **3** HAYA REAL ESTATE. Javier Sánchez I **4** LIBERTY SEGUROS. Alberto Bernáldez I **5** MINISTERIO DE AGRICULTURA Y PESCA, ALIMENTACIÓN Y MEDIO AMBIENTE. Miguel Ángel Martínez I **6** ROCHE - DIABETES CARE. Jairo Serrano I **7** WIZINK BANK. Luis Ballesteros

educación del empleado, existe en el mercado otra herramienta de gran ayuda para combatir un cibercrimen cada vez más persistente: la segmentación. Estos instrumentos proporcionan muchas posibilidades en materia de seguridad, ya que permiten acotar y controlar todo lo que entra y sale de cada

"Las personas no solo son la cadena más débil, sino que también constituyen la primera línea de defensa"

equipo. Es muy útil para poder atajar el problema de forma efectiva, y más en tiempos de Covid-19, porque pone las protecciones en cada endpoint de manera individual, y centraliza su gestión desde una misma consola. Sin embargo, no todas las compañías conocen estas soluciones y muy pocas tienen en mente emprender proyectos de este calado. Se trata de iniciativas que permiten acotar el alcance de lo que se quiere proteger, tomando un enfoque Zero Trust que, a pesar de la complejidad que pueda tener, se presenta como una alternativa eficaz para minimizar riesgos y ataques.

Asimismo, con ecosistemas híbridos y complejos, resulta vital la separación entre entornos para mantener a raya las vulnerabilidades.

Nueva normalidad

La pandemia ha cambiado la perspectiva de las empresas en materia de seguridad. Con la nueva normalidad, las organizaciones apuestan por soluciones más robustas, mayor concienciación del empleado,e instrumentos más sofisticados capaces de responder a entornos más complejos que mezclan lo virtual con lo físico, las nubes con las herramientas on premise. Se está reduciendo el número de centros de datos locales y se está apostando claramente por la nube.

Los responsables de seguridad de las empresas son conscientes de que la seguridad cien por cien no existe y de que hay que ir mejorando las capas, revisando los marcos de ciberseguridad, actualizándolos y fomentando un desarrollo seguro desde su estadio inicial, desde el mismo diseño (security by design).

También figura en su agenda el análisis de riegos con terceros, controlando las aplicaciones que vienen de fuera de la empresa; o la tecnología CASB (Cloud Access Security Manager) para responder a la gran demanda de aplicaciones en la nube. Y, por supuesto, tratan de que se vea la seguridad como una acción de valor porque las compañías tienen activos que proteger.