Foto & vídeo
Carlos Entrena

Texto
R. Contreras

ES PRECISO LLEVAR LA CIBERSEGURIDAD A TODOS Y CADA UNO DE LOS USUARIOS

La estrategia de seguridad es la compañera del negocio

<< Son arduas las tareas del CISO para aleccionar a los empleados sobre cómo evitar el phishing y otros peligros externos con campañas de formación, así como para garantizar la seguridad de la información corporativa.

En su travesía por la geografía española para conocer de primera mano las inquietudes y quehacer diario de los responsables de seguridad de las organizaciones, Computing ha recalado en Bilbao, donde un nutrido grupo de directivos TIC compartieron sus puntos de vista sobre una materia tan compleja de manejar como es la ciberseguridad. Como patrones de barco contó con la colaboración de Bitdefender, HP, Pure Storage y Wise Security Global, proveedores que cubren diversas facetas del ecosistema de la seguridad tecnológica. Si antaño era el mar el escenario del pirateo y el asalto indiscriminado de barcos, ahora es en el ciberespacio donde se concentran los crecientes ataques, cada vez más sofisticados y nocivos para el bolsillo y prestigio de las empresas. La nueva normalidad laboral, donde se entrecruzan los puestos de trabajo entre oficinas y hogares, ha generado nuevos dolores de cabeza para el CISO, una figura cuya misión no ha sido nunca plácida, pero que en estos momentos asiste a una frenética situación de amenazas del exterior y controversias internas que le impiden trazar una estrategia clara y eficaz dentro las organizaciones.

Efectivamente, y así dejó constancia un interlocutor en la mesa, "el tipo de empresa es un factor determinante". No es lo mismo una compañía grande, tradicional y que tiene el lastre de los sistemas heredados que una joven firma que ha nacido al calor de las nuevas tecnologías, con un ADN digital y totalmente

SERGIO BRAVO, SALES MANAGER DE BITDEFENDER

"AYUDAMOS A NUESTROS CLIENTES A CONSEGUIR LA CIBERRESILIENCIA EN SEGURIDAD TI"

El modelo híbrido ha hecho que los perímetros a proteger se hayan distribuido. La superficie de ataque es mucho más amplia, lo cual supone mayores retos para los CISO. Esto hace necesario el uso de herramientas de seguridad avanzadas. Desde Bitdefender acompañamos y ayudamos a nuestros clientes a conseguir la ciberresiliencia, poder adaptarse y sobreponerse a esta problemática. Les ofrecemos una serie de tecnologías que van desde la protección tradicional del endpoint, pasando por soluciones de tecnología avanzada con machine learning e IA para poder detectar todo tipo de comportamientos anómalos, como es el caso de HyperDetect y otras herramientas antiransomware. También tenemos tecnologías EDR y XDR para la respuesta temprana ante cualquier comportamiento sospechoso y dar una visibilidad completa de lo que ocurre en la organización, e incluso ofrecemos nuestros servicios gestionados de MDR que aportan protección a compañías que no tienen departamento de seguridad TI y aquellas que quieren reforzarse en este ámbito.

MELCHOR SANZ, CTO DE HP

"EL ESLABÓN PRIMERO DE LA CADENA DE LA CIBERSEGURIDAD ES EL DISPOSITIVO"

Durante estos últimos meses, se está imponiendo una nueva forma de trabajar basada en un escenario híbrido. Cuando el dispositivo sale del perímetro, si está controlado, podemos establecer políticas de seguridad sobre el mismo. Desgraciadamente, esta situación ha favorecido que se accedan a las redes de información y sistemas informáticos de empresas con dispositivos a veces fuera de control; el típico portátil que andaba arrumbado por casa o el que te facilita algún familiar. Esto ha provocado que exista un buen número de parámetros de ataques posibles fuera de nuestro coto. De forma inesperada, estos sistemas acceden a la información corporativa y hay que securizarlos, pero no solo el acceso a la red corporativa, sino securizar cómo se utiliza el dispositivo. Hay que insistir que, dentro de los eslabones de la ciberseguridad, donde cada uno de los componentes es igual de importante, el eslabón primero es el dispositivo y si resulta ser el más débil, seguramente la cadena de seguridad se acabe rompiendo.

integrada con Internet. Así comentaba uno de los directivos asistentes su situación particular: "Las empresas como las nuestras somos más exigentes que las grandes organizaciones históricas (algunas entidades bancarias son auténticos dinosaurios), donde implantar medidas de seguridad resulta mucho más complejo". Este mismo portavoz destaca el "carácter talibán" de su filosofía de ciberseguridad, ya que llevan a cabo medidas más espartanas y radicales para extirpar cualquier posibilidad de ataque nocivo. Estos controles rígidos hacen que no les "preocupe en exceso el ransomware", es cuestión de cerrar los puertos clave y hacer que los switches de redes impidan movimientos laterales.

El tamaño de la organización también puede operar en contra. Una gran compañía tiene que actualizar parches de dos años en miles de puestos de trabajo, puede tardar mucho tiempo en regular la situación y cuando termina de actualizar todo tiene que volver manos a la obra pues ya hay nuevas vulnerabilidades que parchear. En este punto hubo algún desacuerdo, pues otro interviniente señaló que un aspecto crucial es "la mentalidad" y no necesariamente el volumen que tenga una firma: "Llevamos varios años hablando con negocio para que entiendan cómo de crítica resulta gestionar la seguridad de una compañía. Los altos directivos ya comprenden nuestro lenguaje y son los primeros que nos permiten activar medidas que en el pasado nos hubiera llevado siglos poner en marcha". Ha operado un cambio en la mentalidad de los ejecutivos que, obligados por

"¿En quién recae la responsabilidad en caso de una negligencia que permita la entrada de un ransomware u otro tipo de malware?"

JAVIER MARQUÉS, SYSTEM ENGINEER DE PURE STORAGE

"LA EMPRESA TIENE QUE SER CAPAZ DE RECUPERAR LA INFORMACIÓN MUY RÁPIDAMENTE"

Todas las organizaciones están preocupadas por los ciberataques de ransom- ware. Creo que no hay nadie que se libre de esta amenaza, en el sector público o en el sector privado. Por poner un símil, es como ir en moto e intentar coger la curva a mucha velocidad. La cuestión no es si te vas a caer, sino cuándo te vas a caer. En este mismo instante, es muy probable que alguien haya podido entrar en las instalaciones o en la infraestructura o en los servicios de una corporación y esté buscando la manera de cifrar su información y exigir por ella un rescate. Este proceso sucede durante 100 o 200 días, en los cuales el atacante va buscando todas las contraseñas con el objetivo de extraer su máximo beneficio. En caso de sufrir un ciberataque, la empresa tiene que ser capaz de recuperar su información muy rápidamente y saber que esa información es fiable. Desde Pure Storage ofrecemos las soluciones más sencillas y eficientes para conseguir ese reto y superar cualquier tipo de adversidad.

UNAI AZURMENDI, KEY ACCOUNT MANAGER DE WISE SECURITY GLOBAL

"WISE APUESTA POR LA IDENTIDAD SOBERANA DIGITAL DE LOS USUARIOS"

Las estrategias de gestión de identidad y accesos son clave para la protección de las empresas y de sus activos. Derivado de esta situación aparece la identidad digital, es decir, todos aquellos datos que se reflejan en Internet y que no tienen por qué ser solo datos personales: fotos, vídeos, redes sociales… La huella digital también es un aspecto relacionado. Las passwords siguen siendo necesarias aun siendo el verdadero talón de Aquiles de las organizaciones. Una mala higiene en el uso de contraseñas puede hacernos vulnerables al phishing, la ingeniería social y los ataques de fuerza bruta, por lo que se avanza hacia modelos passwordless. Desde Wise apostamos por la identidad digital soberana con tecnología blockchain. Permitimos que el usuario disponga de toda su soberanía para la gestión de los datos y decida quién, cómo y cuándo tienen acceso a los mismos. Con el asesoramiento de Gartner, estamos implantando Definitive ID que, a través de blockchain, dota de esa autonomía y garantía de privacidad a las personas.

"Las campañas de formación y concienciación son el pan de cada día"

el panorama actual, saben que tienen que actuar antes y con mayor agilidad. Los CISO son conscientes de que estamos en una carrera que "exige recursos y mayor velocidad, actualizar y volver a poner nuevas capas". La condición sine qua non es que las acciones vayan acompañadas por la Dirección, que es quien va a poder aprobar los presupuestos y habilitar los mecanismos para activar los proyectos, teniendo muy claro que difícilmente la ciberseguridad va a tener un retorno económico para la organización.

Gestionar la seguridad

Más que tecnológica, "la cuestión es organizativa", de nada sirve tener un sello de seguridad si no hay detrás una estrategia y una voluntad de gestión por parte del comité de dirección. "La certificación ISO no te garantiza nada, puede ser un postureo. ISO te habla de unas buenas prácticas, pero no de su aplicación". En este punto, alguien comenta lo complicado que resulta que el mercado te considere "una empresa segura, no hablamos de presentar un certificado sino de demostrarlo. Si monitorizas tu servicio a tus clientes y les avisas de cualquier problema que puedan tener demuestras que estás velando por su seguridad". Los presentes consideran que sería interesante convertir la ciberseguridad en un argumento de compra.

Responsabilidad del usuario

Un tema que acaparó parte del debate fue ¿en quién recae la responsabilidad en caso de una negligencia que permita la entrada de un

ASISTENTES

1 Luis Alberto Méndez, Ayuntamiento de Barakaldo | **2** Raúl Reliegos, Ayuntamiento de Barakaldo I **3** Juan Carlos Ávila, Consulmar Group | **4** Goizane Martínez, Consulmar Group | **5** César González, Estampaciones Mayo | **6** Jorge Arroniz, Eva Group | **7** Miguel Sanz, Focke Meler Gluing Solutions | **8** Miguel Ángel Pedrazo, Grupo Arteche | **9** Eneko Astorkiza, Grupo Retabet | **10** Alberto Rodríguez, Hospital San Juan de Dios | **11** Endika Eibar, Kaefer Servicios Industriales | **12** Andoni Valverde, Laboral Kutxa | **13** Antonio Eguizabal, Pernod Ricard

ransomware u otro tipo de malware? En este sentido, existe cierta 'inmunidad' para el usuario que comete el error, pues siempre se piden explicaciones a los responsables de infraestructuras y de TI. En algunas multinacionales, los empleados firman un compromiso de respetar las normas de ciberseguridad, cuya infracción puede conllevar consecuencias negativas para el trabajador. Pero son solo algunos casos. Alguno de los asistentes se mostró partidario de la mano dura para con los empleados negligentes.

De cualquier manera, el CISO tiene que bregar con la concienciación permanente, con el riesgo de terminar siendo tan pesado que los empleados hagan oídos sordos a su insistencia. Las campañas de formación y concienciación son el pan de cada día. Es preciso llevar la ciberseguridad a todos y cada uno de los usuarios, que entiendan que un ciberataque puede acabar con un negocio de un plumazo. Y, sin embargo, las personas siguen picando el anzuelo. Un tertuliano explica que en su empresa realizan campañas trampa para sus empleados y siguen haciendo clic donde no deben. De nuevo, se vuelve a señalar a la Dirección como la primera que debe atender los cursos y predicar con el ejemplo. "La estrategia de seguridad tiene que acompañar al negocio. Hay que simplificar las herramientas y buscar mensajes que calen en los empleados", pero también es responsabilidad del CISO minimizar las consecuencias, en cualquier caso, haciendo que el impacto sea el menor posible.

Una política más estricta

Como anécdota, una de las empresas asistentes ha establecido una política de seguridad tan estricta que no se permite el uso de pendrives a los empleados (el gerente ha llegado incluso a romper en pedazos algún dispositivo USB no autorizado). Pero aplicar estos criterios más exigentes a veces topan con un terreno baldío, "solo introducir un modelo de autenticación multifactor puede ser traumático para nuestros proveedores". Los departamentos de Seguridad TI tratan de aplicar innovaciones para extremar la seguridad, pero surgen inconvenientes que finalmente quedan sobrepasados por la terca realidad.

La externalización de la ciberseguridad es otro aspecto que quedó sobre la mesa como una medida recomendable, así como la necesidad de TI y Seguridad de trabajar en armonía. Y, sobre todo, es un imperativo que "las empresas recapaciten y se sienten a pensar". La sensación general es que ahora estamos más seguros, pues contamos con las armas defensivas mejores que nunca, pero a la vez estamos más expuestos, por la proliferación salvaje de los ciberataques. Es como ese juego del gato y el ratón que no termina nunca, y que es una amenaza permanente y contumaz para la reputación y viabilidad económica de las empresas. ■