Texto
Laura del Río

Fotografía y vídeo
Carlos Entrena

A PESAR DE LOS CIBERATAQUES, EL NEGOCIO SIEMPRE NECESITA "MÁS MADERA"

Salvaguardar el negocio

BILBAO

La ciberseguridad ha cambiado completamente de aspecto y de escenario en los últimos años. Atrás quedaron los virus que infectaban nuestros PC para dar paso a un perímetro mucho mayor que extiende el recorrido de los ciberataques hasta cualquier dispositivo móvil que acompañe al individuo, donde y cuando sea. Endpoints y puntos de acceso del usuario digital se han convertido en las dianas de los ciberdelincuentes para acceder a las redes ajenas y campar a sus anchas. En este laberinto plagado de ratoneras dirigidas a empresas y usuarios, combaten cada día los expertos TI que acudieron al encuentro celebrado en Bilbao del Tour de Ciberseguridad 2020 organizado por Computing.

Las organizaciones son víctimas de todo tipo de ataques, pero para las pequeñas compañías, hasta el ataque más sencillo puede tener grandes consecuencias. "Nosotros somos una pyme", contó Oscar López, responsable de Sistemas de Viconsa. "Cuando se marchó el informático de mi empresa, tuve que 'lidiar yo con el toro' de la ciberseguridad, y me las veía y me las deseaba para que las medidas de seguridad no lastraran la continuidad del negocio". Óscar López confesó que el responsable de seguridad debe conocer "ciertos atajos o puertas traseras para sacar adelante un proyecto" y "acudir a ellos si es estrictamente necesario". No obstante, "el responsable de ciberseguridad es, prácticamente, el único de toda la compañía que debe conocerlos porque, si cada uno tirara por su propio camino cuando quisiera, se generaría un caos".

En busca de la seguridad rentable

Analizar los propios riesgos de la compañía, realizando una auditoría en caso de que fuera necesario, es muy importante para hacer una correcta inversión en seguridad. Porque "aunque los tamaños y los presupuestos de las diferentes empresas sean distintos, todas deben ser igual de seguras", puntualizó Wenceslao Basterra, Business Development Director de Wise Security Global. No hace tanto tiempo que la dirección se implica en trazar un plan estratégico de seguridad sincronizado al que se le asigna un presupuesto. Y eso, en el mejor

WENCESLAO BASTERRA, BUSINESS DEVELOPMENT DIRECTOR DE WISE SECURITY GLOBAL

"EL CIBERCRIMEN APUESTA POR EL RANSOMWARE Y LA SUPLANTACIÓN DE IDENTIDADES"

Las ciberamenazas se están automatizando y profesionalizando a pasos agigantados. En este sentido, la inteligencia artificial va a jugar un papel importante tanto para optimizar las herramientas de ataque como las de protección. En 2020, la extorsión va a seguir siendo la protagonista del cibercrimen, materializándose en el ransomware, el malware en smartphones y el phishing, que no se limitará al canal del correo electrónico. La apertura del perímetro de las interconexiones deja las redes más expuestas que nunca, y las operaciones entre compañías o con la Administración Pública, o las transacciones con los bancos, nos convierten en presa fácil para los cibercriminales. Por no hablar de la suplantación de identidades, -o 'CEO fraud'-, debido al uso ilegítimo de los patrones biométricos de un tercero comprometidos inocentemente en procesos de registro por huella.

Este escenario tan heterogéneo precisa de soluciones a la altura derivadas de la innovación como son: el cibernotario MEE y los sistemas blockchain, que Wise pone a disposición de las empresas para blindar sus infraestructuras empresariales.

MARIO MADRID, BUSINESS DEVELOPER V-VALLEY IT SECURITY

"LOS DIFERENTES MODELOS DE ACCESO CONVIERTEN AL USUARIO EN FOCO DE ATAQUES"

Este tiempo convulso que nos ha tocado vivir, nos ha llevado a cambiar el paradigma de la seguridad digital, forzándonos irremediablemente a establecer nuevas formas de trabajo. Obligados en el aislamiento, el acceso remoto ha constituido la esencia de la productividad y, por ello, el perímetro anteriormente estanco ha tornado a modelos de acceso allá donde estemos. Plataformas multicloud donde asegurar la conectividad y una correcta gestión de accesos son piezas, ya no claves, sino fundamentales para el nuevo mundo que se avecina. Esto conlleva a que el usuario, en su necesitada accesibilidad, pasa a ser foco de ataques e intentos de suplantación. Desde V-Valley, apostamos por la tecnología de Broadcom, ya que nos proporciona soluciones automatizadas de autenticación y gestión de identidades y accesos privilegiados. Gestionar los privilegios y permisos a las aplicaciones de la compañía, así como poder alertar, reparar, rastrear y registrar las actividades de los usuarios, serán herramientas prioritarias en la seguridad de cualquier empresa.

de los casos. Aún existen entidades, grandes y pequeñas, en el que el equipo de TI son 'chicos y chicas para todo', que cumplen funciones de informática, negocio, ciberseguridad... "y sin un presupuesto asegurado; tienen que ir pidiendo recursos según van surgiendo las necesidades, tanto económicas como de talento, que también escasea", lamentaron en el encuentro.

Implicar a toda la organización en preservar la seguridad y que los empleados la tengan muy presente en su día a día, pero sabiendo actuar de forma independiente, "no pidiendo permiso a TI cada vez que tienen que hacer un clic", fue la reclamación de los expertos, para lo que admitieron que "aún hace falta mucha concienciación". Los usuarios quieren estar seguros, pero sin que eso les suponga ninguna interrupción en su rutina. "En el momento en el que los trabajadores se encuentran ciertas páginas capadas, tienen que renovar la contraseña periódicamente, conectarse a través de un cliente VPN a la red para ver solo las cosas que le competen o hacer una doble identificación -todas ellas medidas básicas de seguridad-, a muchos se les tuerce el gesto", admitieron. "Pero los de seguridad estamos para ser unos pelmas", bromeó Roberto Cejudo, del departamento de Sistemas de Viconsa.

Si bien todos expusieron las dificultades a la hora de afrontar la ciberseguridad en los entornos TI y de negocio, Jorge Arroniz, director IT de Eva Group, habló de un ámbito cada vez más vulnerable y no siempre puesto

ASISTENTES

1 Jorge Arroniz, EVA Group | **2** Antonio Vasco, Grupo Acha | **3** Miguel Sanz, Sunsundegui | **4** Óscar López, Viconsa | **5** Roberto Cejudo, Viconsa

"Muchas empresas no tienen un presupuesto para ciberseguridad asignado, y tienen que ir pidiendo recursos según van surgiendo las necesidades"

en primera línea, el ámbito industrial. El auge del Internet de las Cosas, la sensorización y la robotización han convertido a las fábricas en entornos inteligentes que llevan la fabricación un paso más allá. Hablamos de la Industria 4.0. No obstante, securizar un escenario tan complejo ha llegado a ser todo un desafío, en el que conviven máquinas de varias generaciones, -"algunas de ellas cuyos fabricantes ya ni existen, pero que siguen funcionando a pleno rendimiento"-, que no son tan fáciles de actualizar por infraestructuras con la seguridad desde el diseño para contener los ataques, -"en su mayoría encriptados"-, de la mejor manera posible. En este sentido, Arroniz habla de la monitorización de la red para detectar incidencias y patrones anómalos como principal medida de ciberseguridad en la que se está embarcando Eva Group.

Por su parte, en Grupo Acha han renovado sus servidores obsoletos creando un cluster de servidores más actualizado y acorde con los sistemas de contingencia que les "obligan a tener según los pliegos de la Diputación de Bizkaia", contó Antonio Vasco, responsable IT de la compañía. Una empresa de ciberseguridad subcontratada por Grupo Acha se encarga de hacer un backup de los datos almacenados en estos servidores en otra sede y en la nube híbrida, así como sendas copias virtuales de dos CPD realizadas cada hora. "De este modo, si hay alguna caída solo se pierde el trabajo llevado a cabo en la última hora".

Que el ritmo no pare

Garantizar la continuidad del negocio es la obsesión de todas las empresas. En Sunsundegui, compañía dedicada al carrozado de vehículos de gran tonelaje, están reelaborando su Plan de Contingencia y actualizando los procesos críticos de continuidad de servicio. "En nuestra organización no hay un área específica de ciberseguridad, sino que TI se encarga de gestionarlo", explicó Miguel Sanz, IT Manager de la empresa vasca. Actualmente están "en pleno proceso de selección de un proveedor con el que podamos delegar parcialmente la gestión de la seguridad". Aunque la fabricación de Sunsundegui es 100% artesanal, están evolucionando hacia un concepto ("más ligado a las smart cities") basado en un análisis en la cloud de los datos que se generan en los autobuses, a los que colocan el chasis y la carrocería, con el objetivo de mejorar el servicio ofrecido a los viajeros. "Podemos controlar desde el mantenimiento del bus, hasta la eficiencia y calidad de la conducción, pasando por medir la huella de carbono que deja, y todo ello conectado con Google", contó Miguel Sanz.

Un partner pequeño, "a ser posible local", fue el consejo que le dieron algunos de los presentes argumentando "que un integrador más pequeño, aunque a priori parezca que tiene menor capacidad, se puede implicar más en tu proyecto". Wenceslao Basterra propuso la solución del 'CISO as a Service', un servicio de Wise "que acompaña y guía a las empresas en el proceso de crear entornos seguros y confiables". Y justo la existencia de empresas que "gestionen la seguridad como un servicio 24/7" es lo que confesaron echar de menos muchos de los expertos. Además de que aporten herramientas abiertas, que se puedan integrar con otras soluciones, "algo vital en un ecosistema tan heterogéneo como en el que vivimos".

Un buen experto en ciberseguridad debe contar con que va a ser atacado, y lo que marca la diferencia es la capacidad de recuperación tras ese ataque, la manera de defenderte. "Igual que hay compañías que se quedan esperando a apagar los fuegos, otras asumen un papel más activo". Innovar en seguridad, -"como las entidades que ya están haciendo sus pinitos en blockchain, solo por probar"-, es lo único que nos va a permitir protegernos y no defendernos solo con palos cuando nuestros atacantes vienen con bazucas. El cibercrimen nunca duerme. ■