El foco puesto en la SEGURIDAD

BARCELONA

Texto
Laura del Río

Fotografía y vídeo
Jorge Pariente

RADIOGRAFÍA DE LA CIBERSEGURIDAD EN LA CIUDAD CONDAL

La compra de dominios con la palabra 'corona' se ha incrementado exponencialmente en los últimos días", prueba de que los ciberdelincuentes ya están preparando sus formas de ataque, -phising, ransomware…-, aprovechando la delicada situación a causa del Covid-19. Los ciberdelincuentes tienden múltiples y variadas trampas a sus potenciales víctimas sin darles nunca la oportunidad de bajar la guardia. "Pincha aquí para ver estos cinco importantes consejos para prevenir el coronavirus", es un ejemplo de engaño digital que pusieron sobre la mesa los expertos en ciberseguridad de distintas empresas públicas y privadas reunidos en Barcelona, la primera parada del Tour de Ciberseguridad 2020 organizado por Computing, con la colaboración de Epson, Samsung, V-Valley y Wise Security Global.

"Hace ya más de dos años que se aprobó la ley 15/2017, del 25 de julio, de la Agencia de Ciberseguridad de Catalunya pero, no ha sido hasta el 1 de enero de 2020 que la Generalitat ha puesto en marcha dicha Agencia", señalaron en el encuentro. Este organismo, que colabora estrechamente con el Centre de Telecomunicacions i Tecnologies de la Informació (CTTI) de la Generalitat, se encarga de desplegar la Estrategia de Ciberseguridad aprobada por el Gobierno catalán para el periodo de 2019-2022; que vela por la seguridad digital garantizando: el desarrollo de la cultura de

"CIO y CISO deben negociar y aunar esfuerzos, no establecer una lucha de influencias dentro de la compañía"

NÉSTOR GINER, MPS SPECIALIST DE EPSON

EL OBJETIVO SIGUEN SIENDO LOS DATOS AJENOS, CAMBIA LA FORMA DE ACCEDER A ELLOS

Lo que nos deparan los años venideros respecto a un mundo tan cambiante como el de la ciberseguridad es un misterio. La única certeza que tenemos es que el foco de los terroristas cibernéticos está puesto en los datos ajenos, y esto no tiene visos de cambiar. Lo que sin duda está cambiando es la forma en la que los ciberdelincuentes intentan acceder a estos datos. Los dispositivos de Epson son puntos de entrada y salida de información de la empresa, que deben contar con las barreras necesarias a los elementos poco fiables que puedan poner en riesgo los sistemas de la organización.

Trazar, controlar y dar los permisos adecuados, todo ello mediante: sistemas de autenticación dual, filtraje de rangos de IP, generación de documentos PDF cifrados y con contraseñas, o la destrucción adecuada de documentos; -cumpliendo a la vez con los requisitos de sostenibilidad y ahorro de agua-, son algunas de las funciones de la tecnología PaperLab o de P-7; que sitúan a Epson como un importante eslabón de la cadena de valor de las compañías.

JUAN PABLO GALLARDO, HEAD OF B2B LARGE ACCOUNTS DE SAMSUNG

LA INTELIGENCIA ARTIFICIAL CONTRIBUIRÁ A CREAR ATAQUES CADA VEZ MÁS COMPLEJOS

Ransomware, deepfake, ataques en la cloud… los patrones que vienen siguiendo los 'hackers malignos' en los últimos tiempos parece que van a acompañarnos, también, durante este año. No obstante, se irán haciendo cada vez más complejos y sutiles, gracias, en parte, a las nuevas tecnologías basadas en algoritmos de inteligencia artificial, -cuya mayor capacidad de cómputo multiplicará los efectos de los ataques-.

La expansión de la nube, el desarrollo progresivo del 5G y la consiguiente proliferación de las estrategias BYOD (bring your own device), -que impulsan la movilidad y el teletrabajo-, están engrosando la lista de objetivos de los ciberdelincuentes a diario. Para frenar los vectores de ataque que se están multiplicando exponencialmente, ya sea en pymes como en grandes empresas, Samsung proporciona herramientas, -tanto a nivel de hardware como de software-, para garantizar el desarrollo de la movilidad bajo los correctos estándares de seguridad a través de su plataforma Samsung Knox.

EDUARD ALEGRE, BUSINESS DEVELOPER DE V-VALLEY IT SECURITY

LOS USUARIOS Y SU IDENTIDAD DIGITAL PUEDEN SER LA PUERTA DE ENTRADA DEL ATACANTE

El inicio de 2020 ha confirmado la tendencia de 2019: avalancha de ciberataques cada vez más sofisticados y dirigidos, sobre todo, hacia aquellas áreas en las que las empresas aún no están invirtiendo lo suficiente en términos de securización como, por ejemplo: la nube pública, los dispositivos móviles y la gestión de la identidad digital de los usuarios.
Las compañías deben conocer cuál es la postura de seguridad de sus activos digitales, y ayudar a sus empleados a ser una pieza clave de la seguridad de la empresa y no ser, sin pretenderlo, la puerta de entrada del atacante. Por este motivo, Broadcom ha trabajado en desarrollar un completo portfolio de soluciones que incluyen la autenticación del usuario -para asegurarnos de que es quien dice ser- y del control de accesos a las aplicaciones, -y a qué nivel de profundidad, para que cada uno pueda acceder donde realmente necesita-, pasando por la gestión de las credenciales privilegiadas de los dispositivos críticos de la empresa. En definitiva, una gestión completa de la identidad del usuario.

JUANJO PÉREZ, COO DE WISE SECURITY GLOBAL

LA DIGITALIZACIÓN HA POTENCIADO EL NEGOCIO, PERO TAMBIÉN LOS RIESGOS

La transformación digital ha traído aparejadas nuevas herramientas que han aportado nuevas funcionalidades en el ámbito del negocio, pero también han incrementado los riesgos en cuanto a la ciberseguridad. Así las cosas, la seguridad y la protección de datos no es únicamente responsabilidad del CISO, sino que es cosa de todos.
Existen empresas con un alto nivel de madurez que buscan herramientas que les ayuden a realizar un buen gobierno de la ciberseguridad. Para lograrlo, Wise dispone de la solución Dryd Manager, que no solo gestiona la demanda a nivel de hacking de las compañías, sino que influye en las fases tempranas del ciclo de vida del desarrollo de aplicaciones, dotando de herramientas a los 'owners' para impedir que salgan al mercado soluciones con brechas de seguridad.
A las compañías con un menor nivel de madurez, la propuesta de Wise pasa por el CISO as a Service, que acompaña y guía a las empresas en el proceso de crear entornos seguros y confiables.

la ciberseguridad, -"dirigida, sobre todo, a la gente joven y a empresas"-; un servicio público de ciberseguridad, -"proyecto que aún está en sus fases más tempranas"-; una Administración cibersegura; y el fomento de la innovación, el talento y la actividad económica de la ciberseguridad, -"ya que se ha identificado un déficit de profesionales por el que cada vez cuesta más captar y retener el talento"-. Tener un programa de ciberseguridad definido para cada año en cada uno de los departamentos de la Administración "es fundamental".

Como "fundamental" es contar con un comité específico de ciberseguridad en las empresas, tanto privadas como públicas, en el que participe la dirección, así como las distintas áreas de la compañía, desde Negocio, hasta TI, pasando por Finanzas y Recursos Humanos. Para que las decisiones que se tomen en este foro tengan repercusión real en la compañía, es vital una correcta coordinación, "un director o directora de orquesta que lleve la batuta". CIO y CISO fueron los dos nombres que sonaron en la mesa para asumir este rol.

CIO y CISO, ¿enemigos o aliados?

Definir la posición en la empresa de cada uno no es tarea fácil. Hasta que muchas compañías no han empezado a considerar la ciberseguridad un mundo aparte de TI, las funciones de CIO y CISO han recaído sobre la misma persona. A medida que el mundo de la ciberseguridad ha ido alcanzando cotas de complejidad antes insospechadas, -ya no solo a nivel tecnológico, sino también organizati-

vo-, el surgimiento de nuevas figuras como la del Data Protection Officer (DPO) y la independencia del CISO se han hecho, por fin, efectivas en muchas compañías.

Ya sea al CIO, a la dirección o incluso al área jurídica de la empresa, -"a la que legislaciones como GDPR, el Esquema Nacional de Seguridad o la Agencia de Protección de Datos ha puesto en el centro del tablero del juego de la seguridad"-; la persona o equipo al que tiene que rendir cuentas el CISO "lo decide cada organización según sus necesidades". Lo importante es que, más allá de las jerarquías, CIO y CISO establezcan "una fluida relación de colaboración".

El 'choque' entre CIO y CISO se produce cuando el CISO depende del presupuesto de TI gestionado por el CIO. "A veces hay prioridades, como garantizar la continuidad del negocio, esencial para la supervivencia de la empresa". No obstante, "cuando el CISO pide presupuesto también lo hace para garantizar la seguridad del negocio, porque proteger el negocio significa garantizar su supervivencia". Los profesionales lo explicaban así: "A veces los de Negocio quieren sacar al mercado productos no aprobados por Seguridad y el CISO se encuentra en la encrucijada de apretar el botón rojo y frenar la producción o dejar que esta avance con vulnerabilidades y asumir las posibles consecuencias negativas". Por estas cuestiones, el papel de los CIO y CISO, muchas veces, no es fácil, y la unión de sus fuerzas se hace esencial para que sus decisiones adquieran peso en la organización. "Se trata de negociar y aunar esfuerzos, no de establecer una lucha de influencias", aclararon.

La responsabilidad del usuario

Es cierto que "un dispositivo no va a hacer nada que tú no le ordenes, -al menos de momento", rieron en el encuentro-; sin embargo, "no se puede dejar caer tanta presión sobre los hombros del usuario, la securización de la tecnología tiene que ser muy sólida". No obstante, la idea de que, aunque el dato no sea algo físico también se puede robar, debe penetrar en la mente y "formas de hacer" de los empleados mediante las campañas de concienciación y las actividades que mejor se adapten a su perfil. En este sentido, la filosofía 'Zero Trust' se está extendiendo en muchas compañías, "un modelo que se basa en estar alerta y no confiar al 100% ni en la tecnología ni en los procesos ni, por supuesto, en ninguna entidad, pertenezca o no a su red".

Tras la expansión de la nube y el 5G, la movilidad y el IoT "han hecho de las suyas" y han extendido "el perímetro de las interconexiones hasta cada uno de los individuos conectados", por lo que las intrusiones en las compañías se quedan como daños colaterales, "la verdadera intención de los ciberdelincuentes, más que llegar hasta los datos, es llegar a adentrarse en los sistemas de los clientes de las compañías a las que atacan". Por este motivo, ha ganado tanto peso la gestión de la identidad digital del usuario en los planes de seguridad. Y por esto mismo, existen empresas cuyo CISO lleva dos equipos distintos, por una parte, el de la seguridad corporativa, y por otra, el de la seguridad de los clientes. "Hasta existen aplicaciones que puntúan y clasifican a las empresas según su plan de resiliencia o capacidad de reacción a los ataques recibidos, los cuales son reportados a la app por las propias empresas".

A raíz de situaciones que pusieron a las compañías al límite, como las vividas en 2017 con el ransomware WannaCry o el malware Petya, se creó un 'awareness' en las organizaciones que les hizo "ponerse las pilas" respecto a la ciberseguridad. Las compañías tradicionales están añadiendo la seguridad capa por capa, mientras que las startups se construyen desde cero con los pilares de la ciberseguridad porque, hoy por hoy, cotizan más en Bolsa las empresas que cuentan con una estrategia de ciberseguridad definida, que las que no. "Cuanto más seguro eres, más vales". ■

ASISTENTES

1 José Vázquez, Barraquer | **2** Pere Solé, Cuatrecasas | **3** Sergio Juárez, Cuatrecasas | **4** Toni García, Damm | **5** Albert Haro, Centre de Seguretat de la Informació de Catalunya | **6** Gustavo Civantos, Itron | **7** Marc Planas, La Sirena | **8** Ramiro Cid, Linde Gas España | **9** Martín de Riquer, Médecins Sans Frontières | **10** Joan Centellas, Penguin Random House Grupo Editorial | **11** Óscar Sánchez, Puig | **12** Eduardo González, SABIS | **13** Víctor Huerta, Universitat Politècnica de Catalunya | **14** Susana Calvo, Volkswagen Group España Distribución | **15** María Viader, Volkswagen Group España Distribución | **16** Pablo Penalva, Werfen