Ciberseguridad, un blindaje imprescindible

Pese a disponer de sistemas de protección robustos, cualquier mínima brecha de seguridad es suficiente para dejar expuesta a una gran corporación

Más allá de la mera tecnología, la ciberseguridad se ha convertido —y con razón— en una prioridad estratégica para las grandes empresas. La digitalización ha cambiado el modus operandi de muchos delincuentes, que desde hace tiempo centran sus esfuerzos en asediar a este tipo de compañías mediante ataques cibernéticos. Las amenazas se multiplican porque los métodos que utilizan los criminales son cada vez más sofisticados y dañinos, y las corporaciones son conscientes de los riesgos a los que se exponen.

En general, las organizaciones de mayor tamaño están mejor preparadas que las pymes. El problema es que también están más expuestas a los malhechores, lo que les obliga a invertir más recursos para detectar, bloquear y mitigar estas agresiones. “La proliferación de dispositivos IoT [internet de las cosas] que no se gestionan correctamente o la migración a entornos en la nube, unido a una deficiente gestión de vulnerabilidades y una pobre segmentación de redes, hace que los delincuentes tengan un amplio abanico de posibilidades a la hora de atacar a una empresa”, señala Josep Albors, responsable de Investigación y Concienciación de ESET España.

Datos preciosos

Hoy en día, la mayoría de ataques están relacionados con el robo de información, sobre todo credenciales como contraseñas y datos personales. Al acceder a este tipo de documentación, los piratas informáticos logran introducirse en entornos corporativos y, una vez dentro, pueden desarrollar las siguientes fases de su ofensiva, que puede desembocar, por ejemplo, en el robo y cifrado de información confidencial. Es entonces cuando chantajean a la empresa que han atacado con el pago de una cantidad elevada de dinero a cambio de no hacer públicos estos datos robados. En paralelo, prosigue Albors, los ciberdelincuentes “pueden haber cifrado varios sistemas de la organización”, lo que puede ocasionar que la compañía no pueda continuar con su actividad, con las consecuentes e importantes pérdidas económicas y reputacionales que eso supone.

Pese a que no todas las empresas están preparadas para afrontar una ciberagresión, es cierto que las de mayor volumen sí disponen de suficiente capacidad y medios para enfrentarse a una situación de peligro como la que supone una embestida de estas características. Al fin y al cabo, les va en ello la propia supervivencia del negocio. “El problema llega cuando se detectan afecciones masivas. Entonces la recuperación y la respuesta debe hacerse de forma coordinada, por lo que la colaboración público-privada es esencial”, apunta el responsable de Ciberseguridad de NTT DATA, Miguel Ángel Thomas. En estos casos, la evolución de los sistemas de defensa es esencial para mantener el nivel de resiliencia de estas corporaciones.

Directivos en la diana

No es casualidad que algunas de las áreas más atacadas sean las financieras y todas aquellas las relacionadas con la actividad del CEO, ámbitos donde se gestionan directamente las partidas económicas. Lo normal es que los agresores intenten engañar mediante ataques de phishing dirigidos a la alta dirección de la compañía o a personas de su confianza. “Otro de los departamentos más amenazados es el de innovación, donde se suele encontrar la propiedad intelectual de la empresa y sus secretos industriales”, recuerda Thomas.

Y como los ciberdelincuentes son conscientes de que cada vez es más complicado asaltar directamente a las grandes organizaciones, porque las medidas de seguridad que implementan son robustas, en muchas ocasiones pasar a colocar la diana sobre los colaboradores externos que participan en el desarrollo de su actividad a lo largo de toda la cadena digital.

El eslabón más débil

Aunque los ataques sean cada vez más sofisticados, en gran parte debido al uso de la inteligencia artificial (IA), el correo electrónico todavía se mantiene como la puerta de acceso preferida de los delincuentes. La poca preparación de los usuarios, sumado a la falta de herramientas de seguridad hace que la bandeja de entrada del e-mail sea un agujero por donde se cuelan gran parte de las amenazas. Los expertos coinciden en que las personas son a día de hoy el eslabón más débil de la cadena.

La solución pasa por la concienciación y la preparación. “Hay que formar a la plantilla en materia de seguridad, se deben refrescar esos cursos cada cierto tiempo y poner a prueba a la gente para ver si se han impregnado de esos conocimientos. Estos pasos evitan que haya muchísimos problemas en el futuro”, incide el cofundador y CEO de Barbara IoT, David Purón. Esta start-up especializada en el desarrollo de software industrial ha patentado un programa informático que ayuda a sus clientes a gestionar la seguridad de los dispositivos del internet de las cosas. “La cuestión no es si te van a hackear o no; es cuándo va a ocurrir, porque va a pasar seguro alguna vez en la vida, sobre todo en una empresa”, sostiene este ingeniero.

Después de los empleados, el segundo punto más vulnerable de las organizaciones tiene que ver con la desactualización de sus sistemas operativos. Para Purón es fundamental disponer de un plan de respuesta a incidentes, y activarlo cuando llegue el momento. El primer paso es contener el ataque. A continuación, debe comunicarse a todas las partes implicadas: trabajadores, autoridades, regulador, cuerpos de seguridad… Y por último, recuperar los sistemas y evaluar el impacto.

Fuente: https://elpais.com/

LINK DE LA NOTICIA