10/08/2025

Verano: por qué hay que reforzar la ciberseguridad más si cabe

La clave está en adoptar una infraestructura de datos unificada, segura y sostenible, que permita integrar tecnologías avanzadas como la IA

Bajar la guardia no es lo más razonable en una época en la que los riesgos de ciberseguridad aumentan de manera notable; pues los ciberatacantes no descansan. Es más, están al tanto de lo que ocurre en esta época del año, de ahí que aprovechen la circunstancia para lanzar campañas más agresivas.

Verano. Tiempo de vacaciones, de merecido descanso tras un intenso año de actividad… Y también para ser objeto de un ciberataque. Si bien los ciberatacantes no tienen una época preferida, pues su actividad se extiende a lo largo de los 356 días, el verano tiene un color especial como la Sevilla de Los del Río. Bien sea por la guardia que se levanta más de la cuenta, porque el tiempo invita a relajarse o por lo que sea, distintos estudios reflejan que estamos en uno de los picos del año en lo que a la actividad delictiva se refiere en todos los ámbitos, y la ciberseguridad no podía ser menos.

CSO ha charlado con algunos de los grandes protagonistas del mercado a los que ha planteado una serie de cuestiones relacionadas con el asunto de este reportaje, y la conclusión es palmaria: el verano es un periodo que los ciberdelincuentes aprovechan para lanzar campañas más agresivas e indiscriminadas.

¿Por qué hay más ataques?

En primer lugar, el trabajo en remoto se intensifica en esta época. La playa, la montaña. Esa bicicleta que susurra con ojitos vueltos una vuelta matutina por la mañana o esa fina arena de playa que, ladina, incita a lo mismo. Demasiados atractivos como para no echarse en brazos del teletrabajo y que me encuentren si me pierdo.

“Muchas personas se conectan desde ubicaciones menos controladas, como segundas residencias, hoteles o aeropuertos, utilizando redes Wifi públicas o poco seguras, que son mucho más propensas a sufrir ataques como la suplantación de redes o la interceptación de datos”, explica Guillermo Fernández, ingeniero de Ventas para el Sur de Europa de WatchGuard Technologies, quien añade: “Además, quienes no están acostumbrados a trabajar en remoto de forma habitual pueden no estar concienciados ni contar con los conocimientos adecuados sobre buenas prácticas digitales. A eso se suma que, en muchos casos, para evitar llevarse el portátil corporativo, algunos empleados recurren a dispositivos personales que cuentan con menores medidas de seguridad (sistemas desactualizados, sin antivirus o sin cifrado, por ejemplo), lo que eleva aún más la exposición al riesgo”.

Otro punto importante es que, durante el verano, los atacantes saben que muchos equipos de TI y ciberseguridad están operando con recursos más limitados o con personal de vacaciones. “Esto lo aprovechan para lanzar campañas de phishing y otros ataques dirigidos, conscientes de que la atención y vigilancia suelen disminuir”, prosigue Fernández.

Por último, tampoco hay que olvidar el riesgo físico, pues la movilidad de los dispositivos también implica un aumento de las probabilidades de que se produzcan robos o pérdidas, con el consiguiente peligro de que información sensible caiga en manos equivocadas.

“En definitiva, el verano no es sólo un periodo de descanso, también es una época en la que las empresas deben extremar las precauciones y mantener sus políticas de ciberseguridad activas y adaptadas al contexto”, deja como consejo.

Aumento de los riesgos de ciberseguridad

Los riesgos de ciberseguridad suelen incrementarse de forma notable en verano, aunque parezca que debería ser al revés. De hecho, se calcula que sólo en los meses de verano de 2024 los ciberataques aumentaron de media un 30%, apunta Belén Ferreiro, gerente de cuentas de Ciberseguridad de Altia.

“Esto no es casualidad —explica por correo electrónico—: muchas empresas funcionan con menos personal, los equipos de TI y seguridad cuentan con menos recursos y se tiende a dejar para la vuelta tareas importantes como actualizaciones, revisión de accesos o copias de seguridad. Todo eso deja puertas abiertas que los atacantes saben aprovechar. A esto hay que añadir que mucha gente durante estos meses se conecta desde cualquier sitio: hoteles, aeropuertos, cafeterías… donde no siempre usamos medidas básicas de seguridad (VPN, doble factor de autenticación…)”.

Luego, hay que considerar toda la actividad propia del verano: es decir: reservas de todo tipo, compras online… “Los ciberdelincuentes lo saben y utilizan a su favor, lanzando campañas de phishing que imitan a la perfección correos de aerolíneas, apartamentos o plataformas de pago”, continua.

“Al final, el riesgo es doble: más intentos de ataque y menos ojos vigilando para detectarlos y reaccionar rápido. Si encima no hay un protocolo claro para saber quién actúa si pasa algo o no se han probado bien las copias de seguridad, un incidente puede convertirse en crítico sin que nadie lo detecte a tiempo”, argumenta Ferreiro.

Por eso no quiere que este mensaje caiga en saco roto: la ciberseguridad no se va de vacaciones. “Todo lo contrario, es justo el momento de repasar bien todo, reforzar controles y recordar a la plantilla que, aunque estemos desconectando, no podemos bajar la guardia”, añade.

Sí, pero…

No está de más recordar, como hace ahora Josep Albors, director de investigación y concienciación de ESET España, que todo depende del color con que se mire. O lo que es lo mismo: el sector al que nos refiramos. “Por ejemplo, si revisamos nuestros datos de telemetría, comprobaremos que en verano disminuyen las detecciones de ciberamenazas dirigidas al sector corporativo, algo normal debido a la menor actividad laboral durante este periodo. Por otro lado, en algunas amenazas dirigidas a usuario particulares, sí vemos repuntes durante el periodo estival, debido al mayor uso que damos a los dispositivos por motivos de ocio, lo que hace que no pocos usuarios se descuiden y sean un blanco atractivo para los ciberdelincuentes”, explica.

Amenazas más importantes

Aparte de las ensaladillas de más de un chiringuito y terraza o esa sangría que ha conocido épocas pretéritas merced a una buena conservación en el recipiente adecuado, Jaime Balañá, director técnico de NetApp para Latinoamérica, destaca una en especial cuyo poder devastador está a la altura de aquellas ensaladillas: el ransomware.

“El ransomware sigue siendo la principal amenaza, no únicamente por su capacidad destructiva; también por la velocidad con la que puede comprometer una infraestructura entera, ya que se ha vuelto más rápido, más dirigido y silencioso. A eso hay que sumar el auge del phishing personalizado, impulsado por herramientas de IA generativa que hacen muy difícil diferenciar una comunicación legítima de una maliciosa. También hay que considerar el riesgo interno, que crece cuando los equipos están sobrecargados o no tienen claros los protocolos de seguridad”, apunta al respecto.

Pero no son las únicas a las que los ciberdelincuentes recurre cual doctor Gang acariciando a su gato M.A.D —si ya peina canas, sabe de quiénes estamos hablando. Fijo—. Carlos Rubio, director de Soluciones de Arquitectura y Ciberseguridad de GFT, añade también el compromiso de credenciales, “ya que muchas veces se utilizan dispositivos personales o redes Wifi públicas sin medidas adecuadas, facilitando el robo de credenciales o la interceptación de comunicaciones; y el Shadow IT y uso de aplicaciones no

corporativas, pues con menos supervisión aumentan los comportamientos de riesgo, como trabajar desde apps no aprobadas o compartir documentos por medios inseguros".

Eso en cuanto a amenazas externas, pero es en esta época, como venimos viendo desde que comenzó este reportaje, cuando también nosotros ponemos nuestro granito de arena para ponérselo más fácil si cabe a los ciberdelincuente. Empezando por el uso de redes Wifi no seguras, especialmente en entornos públicos o residencias vacacionales, pues estas conexiones suelen carecer de cifrado adecuado, lo que las convierte en un objetivo fácil para los ciberdelincuentes.

Siguiendo por el uso de dispositivos personales para acceder a información corporativa. "Estos dispositivos suelen tener una menor protección frente a amenazas e incluso, en algunos casos, directamente carecen de soluciones de seguridad avanzada", asegura Guillermo Fernández.

Y acabando con la ingeniería social. "En verano, se incrementan los intentos de engaño porque los atacantes saben que las personas están más relajadas, desconectadas o incluso fuera de sus rutinas habituales, lo que facilita que caigan en correos fraudulentos, mensajes maliciosos o enlaces comprometidos", añade.

Nunca hay que bajar la guardia

"Existe una falsa sensación de pausa en verano, cuando en realidad los sistemas siguen funcionando, las amenazas continúan y los atacantes están activos. Muchas empresas bajan su nivel de vigilancia justo cuando deberían reforzarlo", sostiene Carlos Rubio.

En su opinión, el efecto confianza de dejar operaciones en piloto automático durante unas semanas genera una ventana de oportunidad que los atacantes conocen y explotan. "Hay que ser consciente de ello para mitigarlo", recuerda.

Cómo evitar los ataques

"La clave está en la anticipación y la preparación", dice Juan Francisco Cornago, director de Ciberseguridad en Babel, a través de correo electrónico. Tan fácil y difícil, apuntamos nosotros. Este especialista recomienda "revisar los planes de continuidad, reforzar la monitorización con herramientas automáticas, proteger los accesos remotos con autenticación robusta, forzar cambios de contraseñas, mantener operativos los equipos de respuesta y, sobre todo, alertar internamente de los riesgos propios del periodo estival".

Y es que, a su juicio —y esta conclusión es todo un eslogan—, "una campaña de concienciación bien diseñada antes de las vacaciones puede marcar una diferencia real".

Por eso, como interviene ahora Ángel Serrano, gerente de Consultoría de Soluciones en Palo Alto Networks, "en primer lugar, conviene revisar cómo, desde dónde y con qué protección se conectan los empleados durante el verano. Trabajar desde redes Wifi abiertas sin una VPN corporativa es un fallo grave, que no siempre se genera por desconocimiento, sino por comodidad. Asegurar el tráfico, verificar el dispositivo, aplicar autenticación multifactor y limitar los privilegios de acceso son medidas básicas, pero muchas veces no se aplican con el mismo rigor fuera de la oficina. Y es que, cuando el perímetro desaparece, el modelo Zero Trust se hace más importante que nunca".

"A eso hay que sumar la protección física de los dispositivos. Cifrado por defecto, gestión remota, bloqueo automático y políticas claras sobre el uso y almacenamiento de datos fuera de la oficina son medidas críticas", apostilla.

"Por último, es clave mantener a la plantilla activa en términos de concienciación. Simulacros de phishing, recordatorios operativos, píldoras formativas, todo ayuda. Y si los equipos de seguridad están bajo mínimos, la automatización basada en inteligencia artificial permite detectar anomalías de comportamiento y contener amenazas sin intervención humana inmediata", dice para concluir su explicación.

¡Más formación!

Juan Francisco Cornago considera que la formación en ciberseguridad sigue siendo uno de los puntos débiles más explotados por los atacantes. "La tecnología por sí sola no evita incidentes si el factor humano falla", destaca. "Por eso es tan importante

implantar una cultura de ciberseguridad transversal —añade—, donde todos los empleados —no sólo los técnicos— sepan cómo actuar, qué señales detectar y qué no deben hacer".

El director de Ciberseguridad en Babel considera que la formación no debe ser puntual, sino parte continua del ciclo de madurez de una organización, "pero todo esto ya lo sabemos y seguimos fallando". De ahí que "el problema no sea sólo el conocimiento, sino nuestra resiliencia cognitiva, y es precisamente allí donde las empresas deben dirigir sus esfuerzos. No sigamos cometiendo los mismos fallos una y otra vez", recomienda.

En conclusión, los riesgos de ciberseguridad se intensifican durante el verano. "La combinación de menor supervisión, teletrabajo desde ubicaciones poco seguras y la ausencia de personal clave crea un escenario propicio para que los atacantes operen con mayor eficacia", determina Cornago.

En su opinión, Phishing, accesos indebidos, suplantaciones o ataques a la cadena digital son sólo algunos de los riesgos que se incrementan cuando bajamos la guardia. "Paradójicamente, justo cuando más protegidos deberíamos estar, muchas organizaciones reducen sus capacidades de vigilancia y reacción", dice.

De ahí que recomiende anticipación y cultura y no depender exclusivamente de la tecnología. "Reforzar la monitorización, mantener turnos de guardia preparados y formar a los empleados en buenas prácticas digitales son medidas esenciales. La ciberseguridad no es estacional ni exclusiva del departamento técnico: es una responsabilidad compartida que debe mantenerse activa los 365 días del año por el 100% de la plantilla y su cadena de suministro", dice para concluir su participación en este reportaje.

Pues, como no hace mal en recordar Jaime Balañá, muchas brechas comienzan con un clic erróneo, una contraseña débil o un descuido aparentemente menor. "La formación no puede limitarse a una sesión anual ni quedarse en lo básico. Son necesarios programas continuos, adaptados a los distintos perfiles de la organización, que expliquen no sólo el qué hacer, sino también el por qué y el qué pasa si no lo hacemos bien".

De todas formas, como aporta en este punto del reportaje Carlos Rubio, todavía hay una gran oportunidad de mejora. Y eso pasa, en su opinión, evolucionar de las formaciones puntuales o genéricas a un enfoque más continuo, personalizado y vinculado a los riesgos reales de cada rol.

"El verano, por sus particularidades, es un momento ideal para reforzar este aprendizaje, ya que los cambios de rutina y la menor supervisión pueden poner a prueba los hábitos de seguridad adquiridos. Apostar por una formación práctica, contextualizada y periódica puede marcar la diferencia y fortalecer significativamente la cultura de ciberseguridad en la organización", argumenta para cerrar este reportaje.

Fuente: https://www.computerworld.es/

LINK DE LA NOTICIA