Publicado en Ciudad de México el 09/12/2022

# [Predicciones de ciberseguridad de Check Point Software para 2023: se esperan más ataques globales, regulación gubernamental y consolidación](http://www.notasdeprensa.es)

## El hacktivismo, los deepfakes, los ataques a las herramientas de colaboración empresarial, los nuevos mandatos normativos y la presión para reducir la complejidad serán las principales prioridades de las empresas en materia de seguridad durante el próximo año

 Check Point® Software Technologies Ltd. (NASDAQ: CHKP), un proveedor líder especializado en ciberseguridad a nivel mundial, ha publicado sus predicciones de ciberseguridad para 2023, detallando los principales retos de seguridad a los que se enfrentarán las organizaciones durante el próximo año. Los ciberataques en todos los sectores de la industria aumentaron un 28% en el tercer trimestre de 2022 en comparación con 2021, y Check Point Software predice que continuará un fuerte aumento en todo el mundo, impulsado por el aumento de los exploits de ransomware y del hacktivismo movilizado por el Estado debido a los conflictos internacionales.  Al mismo tiempo, los equipos de seguridad de las entidades se enfrentarán a una presión creciente a medida que la brecha de la ciberfuerza laboral mundial de 3.4 millones de empleados se amplíe aún más, y se espera que los gobiernos introduzcan nuevas ciber regulaciones para proteger a los ciudadanos contra las brechas de seguridad. En 2022, los ciberdelincuentes vinculados al Estado continuaron explotando las modalidades de trabajo híbridas de las empresas, y el incremento de estos ataques no muestra signos de desaceleración, ya que el conflicto entre Rusia y Ucrania sigue teniendo un profundo impacto a nivel mundial. Las compañías necesitan consolidar y automatizar su infraestructura de seguridad para poder supervisar y gestionar mejor sus superficies de ataque y prevenir todo tipo de amenazas con menos complejidad y menos demanda de recursos de personal. Las predicciones de ciberseguridad de Check Point Software para 2023 se dividen en cuatro categorías: malware y phishing; hacktivismo; regulaciones gubernamentales emergentes; y consolidación de la seguridad. Aumento del malware y de los exploits de hacking El ransomware no da tregua: fue la principal amenaza para las empresas en el primer semestre de 2022, y el ecosistema del ransomware seguirá evolucionando y creciendo con grupos criminales más pequeños y ágiles que se formarán para eludir la aplicación de la ley. Comprometer las herramientas de colaboración: si bien los intentos de phishing contra las cuentas de correo electrónico personales y de empresa son una amenaza cotidiana, en 2023 los ciberdelincuentes ampliarán su objetivo a las herramientas de colaboración como Slack, Teams, OneDrive y Google Drive con exploits de phishing.  Estas son una rica fuente de datos sensibles, ya que la mayoría de los empleados de las compañías siguen trabajando de forma remota. El hacktivismo y los deepfakes evolucionan Hacktivismo movilizado por el Estado: en el último año, el hacktivismo ha evolucionado desde grupos sociales con agendas fluidas (como Anonymous) hasta grupos respaldados por el Estado, más organizados, estructurados y sofisticados.  Estos colectivos han atacado objetivos en Estados Unidos, Alemania, Italia, Noruega, Finlandia, Polonia y Japón recientemente, y seguirán creciendo en 2023. Las armas de los deepfakes: en octubre de 2022, se difundió ampliamente un deepfake del presidente estadounidense Joe Biden cantando "Baby Shark" en lugar del himno nacional.  ¿Fue una broma o un intento de influir en las importantes elecciones intermedias de Estados Unidos?  Esta tecnología se utilizará cada vez más para dirigir y manipular opiniones, o para engañar a los empleados para que cedan sus credenciales de acceso. Los gobiernos intensifican las medidas para proteger a los ciudadanos Nuevas leyes en torno a las filtraciones y robos de datos: la fuga de datos de la empresa de telecomunicaciones australiana Optus ha llevado al Gobierno del país a introducir una nueva normativa sobre el tema que deberán seguir otras empresas de telecomunicaciones, para proteger a los clientes contra fraudes posteriores.  Veremos cómo otros gobiernos nacionales siguen este ejemplo en 2023, además de las medidas existentes, como el GDPR. Nuevos grupos nacionales de trabajo contra la ciberdelincuencia: más gobiernos seguirán el ejemplo de Singapur de crear equipos especiales interinstitucionales para luchar contra el ransomware y la ciberdelincuencia, reuniendo a empresas, departamentos estatales y fuerzas de seguridad para combatir la creciente amenaza para el comercio y los consumidores.  Estos esfuerzos son en parte el resultado de las preguntas sobre si se puede confiar en el sector de los ciberseguros como red de seguridad para los incidentes de ciberseguridad. Imponer la seguridad y la privacidad desde el diseño: la industria del automóvil ya ha tomado medidas para proteger los datos de los propietarios de vehículos.  Este ejemplo se seguirá en otros ámbitos de los bienes de consumo que almacenan y procesan datos, responsabilizando a los fabricantes de las vulnerabilidades de sus productos. La consolidación es importante Recortar la complejidad para reducir los riesgos: la brecha global de competencias en ciberseguridad creció más de un 25% en 2022. Y, sin embargo, las organizaciones tienen redes distribuidas y despliegues en la nube más complejos que nunca debido a la pandemia. Los equipos de seguridad necesitan consolidar sus infraestructuras de TI y seguridad para mejorar sus defensas y reducir su carga de trabajo, con el fin de ayudarles a adelantarse a las amenazas. Más de dos tercios de los CISO afirmaron que trabajar con menos soluciones de proveedores aumentaría la seguridad de su empresa. Predicciones de los ejecutivos de Check Point Software:  "Los deepfakes se generalizarán con los hacktivistas y los ciberdelincuentes que aprovechan los vídeos y los mensajes de voz para realizar con éxito ataques de phishing y ransomware", afirma Mark Ostrowski, oficina del CTO, Check Point Software. "Estamos entrando en una nueva era de hacktivismo, con crecientes ataques motivados por causas políticas y sociales. Los atancantes son cada vez más descarados y dirigirán su atención a las infraestructuras críticas", destaca Maya Horowitz, vicepresidenta de investigación de Check Point Software. "Veremos a una nación-estado liderar un ataque sostenido y prolongado contra la red eléctrica de los Estados Unidos, lo que provocará interrupciones en el suministro eléctrico que afectarán a las funciones críticas de las empresas y la sociedad", ha dicho Micki Boland, oficina del CTO, Check Point Software. "La transformación de la nube se ralentizará debido al coste y su complejidad, y muchas empresas se plantean volver a llevar los flujos de trabajo o a los centros de datos privados para reducir su superficie global de amenazas", detalla Deryck Mitchelson, CISO de EMEA, Check Point Software. "Veremos mucho más debate en torno a la regulación de la seguridad e impulso de la misma, ya que el enfoque actual no ha funcionado", recalca Deryck Mitchelson, CISO de EMEA, Check Point Software. "El sector de los ciberseguros está experimentando importantes cambios tectónicos. Lo más probable es que las empresas no puedan confiar en los seguros como red de seguridad para los incidentes de ciberseguridad. Al igual que hemos visto con la industria del automóvil, los responsables políticos actuarán para proteger a sus electores con una legislación que responsabilice a los fabricantes de los defectos de software que crean vulnerabilidades. A su vez, esto hará que los proveedores de software tengan que incorporar validaciones de seguridad", alerta Dan Wiley, jefe de Gestión de Amenazas, Check Point Software "Mientras que el correo electrónico y el phishing van de la mano y seguirán siendo peligrosos y proliferando, en 2023 los ciberdelincuentes también recurrirán al compromiso de la colaboración empresarial, con ataques de phishing utilizados para acceder a Slack, Teams, OneDrive, Google Drive, etc. Los empleados suelen ser poco rigurosos a la hora de compartir datos e información personal mientras utilizan estas apps, lo que las convierte en una lucrativa fuente de datos para los atacantes", Jeremy Fuchs, analista de investigación de Avanan, una empresa de Check Point Software. "En nuestro entorno multi-híbrido, muchos CISOs luchan por construir un programa de seguridad integral con múltiples proveedores. En 2023, disminuirán el número de soluciones de seguridad desplegadas en favor de una solución integral y única para la reducción de la complejidad", Jony Fischbein, CISO, Check Point Software. "Se ha producido un aumento drástico de las estafas digitales, debido a la desaceleración económica mundial y a la inflación. Los ciberdelincuentes recurrirán cada vez más a las campañas en las redes sociales a través de Telegram, WhatsApp y otras aplicaciones de mensajería populares. También habrá más ciberataques a las plataformas de blockchain Web3, principalmente para hacerse con las plataformas y los criptoactivos de sus usuarios", Oded Vanunu, jefe de investigación de vulnerabilidad de productos, Check Point Software. Acerca de Check Point Software Technologies Ltd.Check Point Software Technologies Ltd. es un proveedor líder de soluciones de ciberseguridad para empresas y gobiernos de todo el mundo.  La cartera de soluciones de Check Point Infinity protege a las empresas y organizaciones públicas de los ciberataques de 5ª generación con una tasa de captura líder en la industria de malware, ransomware y otras amenazas. Infinity se compone de cuatro pilares fundamentales que ofrecen una seguridad sin compromisos y una prevención de amenazas de quinta generación en todos los entornos empresariales: Check Point Harmony, para usuarios remotos; Check Point CloudGuard, para proteger automáticamente los entornos cloud; y Check Point Quantum, para proteger los perímetros de la red y los centros de datos, todo ello controlado por la gestión de seguridad unificada más completa e intuitiva de la industria; Check Point Horizon, una suite de operaciones de seguridad que da prioridad a la prevención. Check Point Software protege a más de 100.000 organizaciones de todos los tamaños. ©2022 Check Point Software Technologies Ltd. Todos los derechos reservados.

**Datos de contacto:**

Moises Hernandez

Market21 Mx

5544884729

Nota de prensa publicada en: [https://www.mexicopress.com.mx/predicciones-de-ciberseguridad-de-check-point](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Hardware Software Ciberseguridad Dispositivos móviles



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)