Publicado en Latinoamérica el 23/08/2022

# [DigiCert y su visión acerca de la Ciberseguridad en la era del ransomware](http://www.notasdeprensa.es)

## Si bien las copias de seguridad meticulosas y regulares del sistema y de los datos son cruciales para la recuperación, el daño de un ataque de ransomware puede ir mucho más allá de una operación de restauración

 El Informe de amenazas cibernéticas de SonicWall 2022 muestra que en 2020, Brasil ocupó el noveno lugar en este ranking, con 3.800.000 ataques de ransomware. En 2021 subió a la cuarta posición, revelando el altísimo grado de vulnerabilidad del país ante este tipo de intentos de invasión. Por su parte, Check Point publicó nuevos datos sobre las tendencias de los ciberataques en los últimos meses. Así, este nuevo informe muestra que la media global semanal de organizaciones afectadas por ransomware alcanza ya 1 de cada 40, lo que supone un aumento del 59% interanual (1 de cada 64 empresas en el segundo trimestre de 2021). Para el caso de América Latina, la región experimentó el mayor aumento de ataques, con 1 de cada 23 organizaciones impactadas semanalmente, un aumento del 43% interanual, en comparación con 1 de cada 33 en el segundo trimestre de 2021, seguido por la región de Asia, que experimentó un aumento del 33% año contra año, alcanzando 1 de cada 17 empresas impactadas semanalmente. Una encuesta reciente de Kaspersky afirma que solo se puede culpar a ocho grupos de ransomware de los ataques a más de 500 empresas en todo el mundo. No solo eso, sino que los ataques siguieron un método idéntico, mostrando una "estandarización" del ransomware como servicio. Según Kaspersky, los ataques entre diferentes grupos se están volviendo similares debido al auge del concepto de ransomware como servicio (RaaS), en el que estos grupos no realizan sus ataques directamente, sino que ofrecen el software malicioso a un tercero. contratando sus servicios. Mirando este escenario, parece que apuntar a la infraestructura crítica señala una nueva normalidad. Con el nivel de contramedidas de riesgo y la capacitación de concientización requerida en las instituciones públicas y privadas, desde la junta directiva hasta los empleados, la perspectiva de controlar rápidamente la situación parece sombría por una variedad de razones. Se deben anticipar más ataques en los próximos meses y años, hay un elixir cibernético. En términos simples, el ransomware es un ataque bajo y lento que es un veneno de acción rápida una vez ejecutado. Los ciberdelincuentes han dominado las técnicas para diseñar malware avanzado, entregar la carga útil de "veneno" evadiendo el perímetro de la red y los métodos de detección y prevención de puntos finales. Los ciberdelincuentes saben explotar la psicología del usuario y la falta de controles de protección en tecnología de la información, Internet de las Cosas (IoT) y dispositivos IoT industriales. "Las amenazas internas (empleados maliciosos/descontentos) son reales sin controles de acceso basados en roles, separación dinámica de funciones y ceremonias de autorización de varias personas para la supervisión. Los desafíos para los operadores de redes y seguridad son empinados. La criptografía es el talón de Aquiles de la ciberseguridad, y los creadores de malware saben cómo convertir los métodos de cifrado en armas", afirmó Srinivas Kumar, vicepresidente de soluciones IOT en DigiCert Si bien las copias de seguridad meticulosas y regulares del sistema y de los datos son cruciales para la recuperación, el daño de un ataque de ransomware puede ir mucho más allá de una operación de restauración. La integridad de los dispositivos afectados requerirá un análisis forense extenso y costoso a escala en entornos de tecnología de operaciones. Si bien las ordenes ejecutivas y las pautas de las agencias gubernamentales son oportunas y bien intencionadas, la industria de la seguridad cibernética carece de la determinación para abordar la causa raíz de frente sin un retorno de la inversión justificado en términos monetarios. ¿Y la cadena de suministro?La detección, la prevención y el análisis forense es una industria multimillonaria en la actualidad, pero los fabricantes de dispositivos todavía perciben (erróneamente) el endurecimiento de los dispositivos y la protección de la cadena de suministro como un centro de costos, y no existe una regulación que motive la innovación. La protección cibernética debe comenzar en la fábrica y persistir en el campo durante todo el ciclo de vida operativo del dispositivo. Los ciberataques tienen como objetivo los datos, no los usuarios. El usuario es simplemente el carbono. Las infracciones ocurren porque los CISO (Chief Information Security Officer, por sus siglas en inglés) están dispuestos a correr riesgos con listas de verificación obsoletas y controles centrados en la entrada para la defensa de múltiples capas en los que los atacantes están bien versados. Los atacantes poseen la voluntad y los recursos para evadir la detección, persistir, propagarse lateralmente y tomar el control de los sistemas. "Si realmente está protegiendo sus dispositivos, ¿qué está tratando de detectar en su red? Si lleva un impermeable, ¿por qué necesita un paraguas? No puede solucionar un problema en el dispositivo con un parche en la red", añadió Srinivas Kumar. Es conveniente, pero la solución equivocada, que solo hace que la lata cibernética se desvanezca. DigiCert repasa algunos focos, los cuales los hackers siempre tienen en la mira: Contraseñas descifradas de un contratista o empleado crédulo Servidores oscuros e inseguros en la red con cuentas de servicio o de usuario de dominio desprotegidas. Acceso remoto a través de VPN a través de la red o el sistema de un proveedor de la cadena de suministro comprometido. Capacidades de firewall inadecuadas para bloquear comandos cifrados y balizas de control (mensajes de marcación inofensivos). Está muy claro que la inteligencia de amenazas de día cero es inadecuada y lograr el objetivo de una arquitectura de confianza cero, más allá de los eslóganes, requiere inversión y compromiso. Los fabricantes de dispositivos y su deber¿Qué significa esto para la industria de la ciberseguridad? La conexión de dispositivos desprotegidos agrava el problema. La industria casera del cibercrimen ha evolucionado a lo largo de los años hasta convertirse en una guerra cibernética estratégica por parte de actores del estado-nación y un sindicato del crimen cibernético que ha dominado el arte de capturar rehenes cibernéticos para obtener rescates y ganancias a gran escala. Los kits para desarrolladores de software y las mesas de ayuda en la web oscura están empoderando a los operativos en todo el mundo, sin seguimiento y localización o acciones punitivas como disuasión. Este es un llamado a la acción para que los fabricantes de dispositivos y los proveedores de servicios de seguridad administrados sean los primeros en responder y proteger el ciberespacio. Aunque la transformación digital ha sido una palabra de moda durante varios años, los CISO y los arquitectos de seguridad de productos han sido, lamentablemente, ineficaces a la hora de defender la causa de la transformación de dispositivos que iniciará el paso a la transformación digital. Si bien los proveedores de conjuntos de chips de silicio han intensificado las innovaciones de seguridad, la cadena de confianza no ha logrado expandir de manera efectiva la pila a la plataforma del dispositivo, las aplicaciones de línea de negocios y el ecosistema de la cadena de suministro de servicios cibervulnerables. "Proteger el tejido cibernético de las puertas de enlace de borde definidas por software y la pluralidad de dispositivos brownfield y greenfield conectados requerirá un esfuerzo colaborativo y entusiasta con asociaciones estratégicas entre innovadores y líderes de pensamiento en la industria de dispositivos", finaliza la vicepresidente de soluciones IOT en DigiCert.

**Datos de contacto:**

DigiCert PR Latam

3125893314

Nota de prensa publicada en: [https://www.mexicopress.com.mx/digicert-y-su-vision-acerca-de-la](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Internacional Software Ciberseguridad Dispositivos móviles



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