Inversión cobra importancia ante el incremento de ciberataques y robo de información

Fecha de creación: 12-10-2021
Medio: NotiPress
Autor: Ali Figueroa

Robo de información y credenciales se mantienen como los incidentes más comunes

Especialistas en ciberseguridad realizaron estudios sobre la importancia de incrementar la inversión ante el crecimiento de los ciberataques en la pandemia

De acuerdo con la compañía y consultora de Tecnologías de la Información (IT) Purple Security (PurpleSec), los ciberataques aumentaron 600% con la pandemia por Covid-19. Asimismo, un reporte de la firma Security Intelligence indicó, para las empresas el costo promedio por ciberataques con robo de información es de 4.24 millones de dólares (md). Ante este hecho, especialistas en ciberseguridad indicaron que es indispensable la inversión medidas de protección, enfocadas principalmente en bases de datos e información personal de los empleados.

Las vulnerabilidades de ciberseguridad que afectan al mundo como consecuencia de mayor uso de herramientas digitales e Internet han provocado un aumento de ciberataques entre todos los niveles y sectores. El Reporte Global de Riesgos 2021 realizado por el Foro Económico Mundial (WEF, por sus siglas en inglés) indicó, los ciberataques significativos, con repercusiones multimillonarias, aumentaron 156 en Estados Unidos, seguido por 47 en Reino Unido y 23 en India. El WEF advirtió, el seguimiento y medición de ataques en países con industrias menos desarrolladas se mantiene problemático, y requiere atención por parte de los participantes económicos y gubernamentales, sobre todo en materia de inversión.

Por esta parte, en entrevista con NotiPress, Jesús Navarro, director general de Data Warden, explicó el impacto de la pandemia en los negocios: "la mayoría de las empresas le dio prioridad a mantener la operación [del negocio]". Esto condujo a algunas compañías a dejar abierta una brecha de seguridad para concentrarse en el negocio, pero también aceleró la transformación digital. Estas condiciones

derivadas de la abrupta adopción del trabajo remoto modificaron los riesgos informáticos de las organizaciones y pusieron en jaque a los profesionales.

El 4 de octubre la red social Facebook sufrió una interrupción de servicios que generó dificultades en su infraestructura y red. Este hecho generó una pérdida aproximada de 66 md en publicidad para la gigante tecnológica según informó la plataforma de fact checking Snopes. Si bien el reporte oficial de Facebook indicó, durante la interrupción de la red no hubo vulnerabilidades que comprometieran información confidencial o credenciales, el incidente incrementó las preocupaciones en materia de ciberseguridad.

Por su parte el estudio de riesgos de la red Leoxology indicó, en la Unión Europea (UE) hay una iniciativa general para proteger las redes de información y datos personales. Entre las recomendaciones destacadas por su análisis se encuentran: desarrollar soberanía y resiliencia informática, implementar capacidad operativa para responder a los ataques más comunes, y cooperación de los sectores involucrados con visibilidad e inversión.

Con respecto al uso de la tecnología como entretenimiento, la industria de los videojuegos ha sido objeto de ciberataques junto con el resto de los sectores. La compañía Akamai informó para NotiPress, estos incidentes aumentaron 340% tan solo en el primer año de la crisis sanitaria. De los 240 millones de ciberataques registrados en el sector, solo 6 millones 300 fueron rastreados, lo que representa el 4%. Las vulnerabilidades habituales emplean robo de información y credenciales de los usuarios, motivo por el cual el ataque repercute tanto en el ecosistema de juegos como en el sistema financiero.

Security Intelligence agregó, en medio de este incremento de los ciberataques, la concientización sobre los riesgos debe estar enfocada en primer lugar al robo de identidad. Según su investigación, los piratas informáticos emplean cuentas falsas para tener acceso a la validación de credenciales por parte de los empleados. Las

consecuencias de dichos ataques son variadas, y pueden abarcar desde información de acceso a las empresas, hasta robo de tarjetas de débito y crédito de las víctimas.