Tendencias en ciberseguridad en la Argentina: cuáles serán los ataques más comunes en el futuro

06/08/2021

Según un reciente estudio, **las empresas argentinas están tomando más medidas y mejoran sus capacidades en materia de ciberseguridad,** luego del aumento de ataques cibernéticos durante la pandemia. Así lo indica el informe de amenazas 2021 ***Cyber Threatscape Report*** de Accenture que además señala cuáles serán las **tendencias de ataques** más frecuentes en el país durante los próximos meses.

El estudio señala que **el 43% de los ejecutivos de compañías en la Argentina ya ha escalado sus capacidades en materia de ciberseguridad (con infraestructura, sistemas y capacitación).** Mientras tanto, el 45% dice que lo hará durante este año.

Incidentes como por ejemplo el ataque a la plataforma **SolarWinds** junto con el aumento de delitos informáticos como el **ransomware** (**malware que solicita "rescate"** de información a través de pagos con criptomonedas), ilustran el creciente impacto de la actividad de las ciberamenazas en todas las industrias.

El estudio identifica tendencias de ciberseguridad que marcarán a las empresas los próximos meses. Entre ellas, el denominador común es el **aumento de ataques a nivel mundial,** producto de la pandemia.

Ransomware: nuevos métodos

Una captura de pantalla del mensaje que se veía en las computadoras afectadas por el ransomware WannaCry (AP)

Está creciendo la extorsión por fuga de datos y los ciberdelincuentes han encontrado nuevos métodos para presionar a las víctimas. Así, **ahora tienen su foco en personas que están trabajando desde sus hogares**, apuntando a **nuevas industrias**, con tácticas de mayor presión para aumentar las consecuencias de la infección y desplegando cargas útiles más rápidas para que los métodos de detección sean más lentos.

Los casos de los primeros meses de 2021 tuvieron como objetivo infraestructuras críticas. En mayo de este año, un ataque de ransomware a la compañía de oleoductos **Colonial Pipeline** la obligó a cerrar su sistema, y paralizó la distribución en gran parte del sureste de Estados Unidos. De esta forma, quienes están detrás del ransomware interrumpen la producción en **organizaciones que no pueden permitirse un tiempo de inactividad y se sienten presionados para pagar los rescates**.

Ahora, en una nueva modalidad bautizada como **"cuádruple extorsión", los grupos no sólo encriptan archivos y amenazan con filtrar datos, sino que también amenazan con ataques de denegación de servicio distribuidos (DDoS**) o contactan a clientes o socios comerciales de las víctimas y los presionan para que paguen los rescates.

El aumento de ataques de Cobalt Strike

Los ciberatacantes siempre buscan formas económicas de evadir la detección y complicar la atribución de los ataques. Una de estas formas es integrar herramientas comerciales y de código abierto comerciales en su arsenal.

Desde diciembre de 2020, ha aumentado notablemente el número des ciberatacantes que adoptan versiones piratas de pruebas de penetración comercial del software malicioso **Cobalt Strike**. Entre 2019 y 2020, este tipo de ataques tuvo un crecimiento de más de un 160%.

Se trata de un software pirata que ha permitido campañas de gran impacto, incluyendo las recientemente descubiertas

en **SolarWinds**, así como los ataques de ransomware ***"name-and-shame"***. **Su crecimiento continuará durante este año.**

El commodity malware

También denominado ***"crimeware* de gran volumen"** (un tipo de software diseñado para la ejecución de delitos financieros en línea), presenta un desafío único y universal debido a su alta disponibilidad y escala. Es un peligro en el **endpoint** (es decir una URL que responde a una petición), que permite intrusiones en la red víctima.

Para enfrentar esta amenaza, las empresas deben **parchear** los sistemas de punto final, identificar potenciales vectores de infección, actualizar el software antivirus, mantener copias de seguridad y utilizar listas blancas de aplicaciones. Y además, es fundamental realizar programas regulares de concientización sobre el **phishing (suplantación de identidad)** para todo el personal, entre otras recomendaciones.

La Dark Web

Dark web

Los ciberatacantes se reúnen en los foros de la **Dark Web** para compartir e intercambiar herramientas y datos de las víctimas. Están aumentando sus tácticas de presión, aprendiendo a traspasar la seguridad, al mismo tiempo que encuentran **nuevas formas de monetizar los registros de malware**.

Desde principios de 2021, ha habido un notable aumento de ciberatacantes que venden registros de malware en la Dark Web. Federico Tandeter, Director Ejecutivo de Ciberseguridad para Accenture Hispanoamérica, señala: "Para enfrentar esta situación, las empresas deben realizar un seguimiento, buscar el alerta temprana de posibles accesos no autorizados a través de la supervisión responsable de la Dark Web, ya sea directamente o a través de un proveedor de inteligencia de amenazas".

Finaliza: “Se debe aumentar el intercambio de inteligencia de análisis de respuesta a incidentes. Compartir información para identificar potenciales amenazas, planificar y ejecutar la defensa de la red y las operaciones. Las organizaciones deben también preparar un **plan de continuidad de las operaciones**”.

Fuente: Infobae