Comunicados

Novedades no tan nuevas en ciberseguridad en Latinoamérica

La ciberseguridad es una competencia continua en la que los especialistas buscan constantemente formas nuevas y creativas de luchar contra estrategias cambiantes de ciberataques. En 2022, el desafío se volvió aun más intenso a medida que los ciberatacantes empleaban métodos tanto avanzados como antiguos, tomando a los expertos de seguridad por sorpresa y demostrando que las tácticas clásicas siguen siendo efectivas.

De hecho, según el IBM Security X-Force Threat Intelligence Index 2023, la reaparición de los *backdoors* o 'puertas traseras', donde los ciberatacantes obtienen acceso remoto a los sistemas, fue una ocurrencia común, pero con distintos resultados. El despliegue de *Backdoors* fue la segunda acción más realizada por los atacantes en Latinoamérica en 2022. Sin embargo, la mayoría fueron intentos de ransomware fallidos, pues los defensores interrumpieron antes de que se pudiera implementar el ransomware.

Otra tendencia antigua, los ataques por correo electrónico, han evolucionado y se han vuelto más difíciles de detectar debido a la adopción generalizada del trabajo remoto. En 2022, el phishing con archivos adjuntos o links maliciosos demostró ser uno de losmétodos preferidos de los ciberdelincuentes, causando el 10% de los ciberataques en la región. También estuvo a la alza el secuestro de hilos de conversación de e-mails, en los que los atacantes se hacen pasar por el participante original. Esta técnica es especialmente peligrosa porque se aprovecha de la confianza existente, haciendo que las víctimas sean más propensas a reaccionar rápidamente y hacer click en los enlaces maliciosos.

Para estar un paso adelante, mejorar la resiliencia y defenderse de las ciberamenazas, IBM recomienda:

- **Conocer la superficie de ataque**. Un tercio de los activos que pueden ser atacados en las redes de las organizaciones no esgestionado o es desconocido. Es necesario pensar como un atacante, descubrir las vulnerabilidades y formas en las que podrían entrar con un mínimo de detección.
- **Entrenar para una respuesta rápida.** Aceptar que las brechas de seguridad son inevitables y establecer métodos para una respuesta rápida es esencial, la velocidad es la clave para limitar el radio de alcance.
- **Hacer tests regularmente.** Formular un programa de pruebas ofensivas que incluyan la caza de amenazas, las pruebas de penetración y al 'red team' basado en objetivos es vital para descubrir debilidades en las defensas. Se recomienda realizarpruebas y cuestionar hipótesis con frecuencia.
- **Emplear tecnologías de endpoints o detección y respuesta ampliadas.** El aumento de los casos de *backdoors* señala

algunos éxitos en la detección. Estas tecnologías proporcionan los medios para identificar y mitigar amenazas antes de que los atacantes adopten medidas más peligrosas.

Si bien, la detección y respuesta a las ciberamenazas dio un paso adelante en 2022, la reaparición de métodos de ataque de la ‘viejaescuela’ evidencian la imposibilidad práctica de logar una cobertura completa contra los ciberdelincuentes, por eso, es tan crítico evaluar y estudiar sus acciones e implementar la tecnología correcta. Sólo aprendiendo del pasado, es posible que la historia no se repita.
