IBM X-Force Report: menos registros comprometidos en 2017 y mayor número de ransomware y ataques destructivos

El error humano es responsable de dos tercios de registros comprometidos, incluyendo el salto histórico del 424% del número de filtraciones debidas a mala configuración de infraestructura cloud

Cambridge (MA) - 12 abr 2018: IBM Security (NYSE: IBM) ha dado a conocer los resultados de su informe IBM X-Force Threat Intelligence Index 2018, que revela que el número de informes comprometidos se redujo en un 25 por ciento en 2017. Esto se debe a que los cibercriminales están centrándose más en lanzar ransomware y ataques que bloquean o destruyen datos salvo si la víctima paga un rescate.

El pasado año, se comprometieron más de 2.900 millones de registros de datos, una cifra inferior a los 4.000 millones de 2016. Si bien el número de registros afectados sigue siendo significativo, el *ransomware reinó* en 2017 con ataques como WannaCry, NotPetya y Bad Rabbit, que causaron grandes problemas en todas las industrias.

Otras conclusiones relevantes del informe son:

- Un salto histórico del 424% en el número de brechas de seguridad relacionadas con infraestructuras cloud mal configuradas, debido en gran parte a errores humanos.
- Por segundo año consecutivo, la industria financiera sufrió la porción mayor de los ciberataques representando el 27% del total de los ataques sobre todas las industrias.

El informe IBM X-Force Threat Intelligence Index recoge información y observaciones de datos analizados en cientos de miles de puestos y servidores de más de 100 países. IBM X-Force supervisa decenas de millones de ataques de *spam* y *phishing* diariamente mientras analiza miles de millones de páginas web e imágenes para detectar actividades fraudulentas y de abuso de marca.

Los ataques de *ransomware* ejercen presión sobre la respuesta a incidentes

El *ransomware* y los ataques destructivos, como WannaCry, NotPetya y Bad Rabbit, no solo acapararon los titulares en 2017, sino que también frenaron la actividad de grandes compañías dado que los cibercriminales tomaron el control y bloquearon la infraestructura crítica en distintos sectores. En general, los incidentes de *ransomware* le han costado a las organizaciones más de 8.000 mil millones de dólares en 2017. Esta situación ha incrementado la presión en las organizaciones para disponer de estrategias de respuesta apropiadas con el fin de limitar el impacto de un ataque.

El error humano sigue siendo el eslabón débil

En 2017 los ciberdelincuentes continuaron aprovechándose de los errores humanos en la configuración de infraestructuras para lanzar sus ataques -este tipo de amenaza creció un 424%-. De hecho, el informe muestra que los errores involuntarios como, por ejemplo, la mala configuración de la infraestructura cloud, fueron responsables de la vulnerabilidad de casi el 70% de los registros comprometidos rastreados por IBM X-Force en 2017.

Más allá de los errores de configuración, los usuarios que sufrieron ataques de phishing representaron un tercio de la actividad involuntaria que provocó incidentes de seguridad en 2017.

Éxito en los ciberataques a clientes del sector financiero

En los años anteriores, la industria de servicios financieros ha sido la más atacada por cibercriminales. Aunque en 2017 fue el tercer sector más atacado (17%), detrás de tecnologías de la información y comunicaciones (33%) y fabricación (18%), el sector financiero fue el que registró la mayoría de los incidentes de seguridad (27% sobre el total de todas las industrias). Aunque las empresas de servicios financieros han invertido mucho en tecnologías de seguridad para protegerse, los ciberdelincuentes han puesto foco en ataques de *malware* dirigidos a consumidores y usuarios finales del sector. El informe revela que Gozi, el troyano financiero más activo y sus variantes, fueron los más utilizados contra la industria de servicios financieros.

El informe completo IBM X-Force Threat Index 2018 puede descargarse aquí:

Más información en www.ibm.com/security, IBMSecurity en Twitter o visita el IBM Security Intelligence blog.