Empresas subestiman las amenazas internas de usuarios privilegiados

Forcepoint en asociación con el Ponemon Institute dieron a conocer los resultados del estudio La Inseguridad de los Usuarios Privilegiados, donde si bien las fugas de datos y los ataques se siguen multiplicando, el **58% de los directores de operaciones de TI y de seguridad** creen que las organizaciones le están dando a los individuos acceso innecesario más allá de sus funciones o responsabilidades, en tanto que **91% prevé que los riesgos de las amenazas internas seguirán en aumento** o permanecerán en los mismos niveles.

Más del 40% de los participantes de la encuesta coinciden en que los miembros internos de las compañías podrían utilizar técnicas de ingeniería social para obtener derechos de acceso como usuarios privilegiados no sorprende que la mayoría de ellos prevean que las amenazas internas sigan siendo un problema. En el estudio participaron más de 600 directores de operaciones comerciales y 142 directores de operaciones de TI federales y de seguridad.

Aproximadamente 70% de los grupos encuestados creen que es “muy probable” o “probable” que los usuarios privilegiados piensan que pueden tener acceso a toda la información. **Casi el 70% también cree que los usuarios privilegiados acceden a datos sensibles o confidenciales simplemente por curiosidad.** Al considerar estos grandes porcentajes, sólo 43% de las organizaciones comerciales y 51% de las organizaciones federales dijeron que tienen actualmente la capacidad de monitorear efectivamente las actividades de sus usuarios privilegiados. **La mayoría aseguró que sólo 10% o menos de su presupuesto se dedica a resolver este importante desafío.**

Aunque el presupuesto y el recurso humano son factores clave para enfrentar las amenazas internas, las deficiencias de la tecnología también juegan un papel relevante. La encuesta reveló que un número importante de los entrevistados utilizan las herramientas de seguridad cibernética para combatir las amenazas internas y no tecnologías más especializadas (por ejemplo, 48% de las organizaciones comerciales y 52% de las organizaciones federales utilizan un SIEM para determinar si una acción es una amenaza interna).

Como resultado, más del 60% indica que estas herramientas producen demasiados falsos positivos. En consecuencia la mayoría de las audiencias encuestadas **(63% de las organizaciones comerciales y 75% de las organizaciones federales) carecen de la información contextual necesaria para evitar que surjan amenazas internas.**