

# ¡Panorama de la Seguridad en TI!



ser title style

# Caso práctico (1/2)

## Cuentas confidenciales

- Administrador / usuario raíz (root) de los servidores, bases de datos, aplicaciones y dispositivos de red (“Recursos de TI”)
- Muy difundidas
- Acceso prácticamente ilimitado – las llaves del Reino
- Impersonales – no están vinculadas a ninguna persona
- Se utilizan en un entorno compartido

# Caso práctico (2/2)

## Cómo son administradas las contraseñas confidenciales – Prácticas comunes

- **Almacenamiento:** Archivos de texto, hojas de cálculo, notas adhesivas, impresas en papel y guardadas en bóvedas físicas
- **Accedidas por:** Administradores de TI y de redes, responsables de operaciones de TI, desarrolladores, DBAs
- **Compartidas libremente:** Generalmente a través del boca en boca, o emails

# Problemas

- No existe un control centralizado – contraseñas ampliamente conocidas
- Acceso ilimitado, descontrolado y sin ningún tipo de auditoría
- Falta de visibilidad
- Las acciones no se pueden rastrear y relacionar a individuos
- Falta de responsabilidad
- Falta de políticas – contraseñas simples, sin variaciones e iguales en todos los recursos
- Escenarios de bloqueo – cambios en las contraseñas no documentados

# Consecuencias

- Robos de identidad
- Incidentes de seguridad
- Sabotajes
- Colocación de bombas lógicas

# Amenazas internas – Creciendo a un ritmo alarmante

## HSBC de Suiza ..

- Toda la información de aproximadamente **24.000** cuentas bancarias fueron robadas y filtradas
- Los detalles se recolectaron durante un periodo de 3 años
- Esto condujo a la pérdida de reputación e ingresos

# Austin, TX ...

- **Cientos de autos comprados a un vendedor en particular, fueron inutilizados y su claxon comenzó a sonar sin parar!**
- **El sistema web de inmovilización de vehículos utilizado para llamar la atención de los consumidores morosos en sus pagos de préstamos para automóviles, fue empleado maliciosamente.**

# Más y más casos...

- Edward Snowden fuga de NSA – privilegio de analista de seguridad utilizado incorrectamente; contraseñas compartidas por medio del boca en boca
- Robo de \$45 millones en ATM



# INFILTRADOS!

- Los culpables fueron
  - Ex empleados que fueron desvinculados de la compañía / contratistas, etc...
  - ¡Esto puede pasarle a cualquier empresa!

# El cambio de enfoque

- Las organizaciones se enfocan en la seguridad perimetral (los malos están fuera de las instalaciones)
- Cambiando el enfoque hacia el interior
  - ¿Quién está en mi red?
  - ¿Quién tiene acceso a los recursos de TI?
  - ¿Qué es lo que pueden hacer con los recursos de TI?
  - ¿Qué es lo que hacen en realidad?

# Haciendo la seguridad de TI su prioridad

- Administración de eventos y de la seguridad de la información.
- Análisis de la actividad de logs de firewall & eventos.
- Administración de contraseñas privilegiadas.
- Administración de seguridad de redes.
- Administración y remediación de vulnerabilidades.
- Administración de Compliance IT empresarial.

# Productos ManageEngine

- Administración de Help Desk y Destop – ITSM
- Auditoría y administración de Active Directory
- Monitoreo y administración de performance de red
- Administración de performance de aplicaciones y servidores
- Análisis de logs, SIEM, seguridad y compliance TI
- Administración de dispositivos móviles
- Servicio de monitoreo de sitios y aplicaciones web

# Permanezca en contacto con ManageEngine

- Sitio web de ManageEngine - <http://www.manageengine.com/>
- Blogs de ManageEngine - <http://blogs.manageengine.com/>
- Facebook - <http://www.facebook.com/ManageEngine>
- Twitter - <http://www.twitter.com/ManageEngine>
- LinkedIn - [http://www.linkedin.com/company/manageengine-?trk=company\\_logo](http://www.linkedin.com/company/manageengine-?trk=company_logo)

¡Muchas gracias!