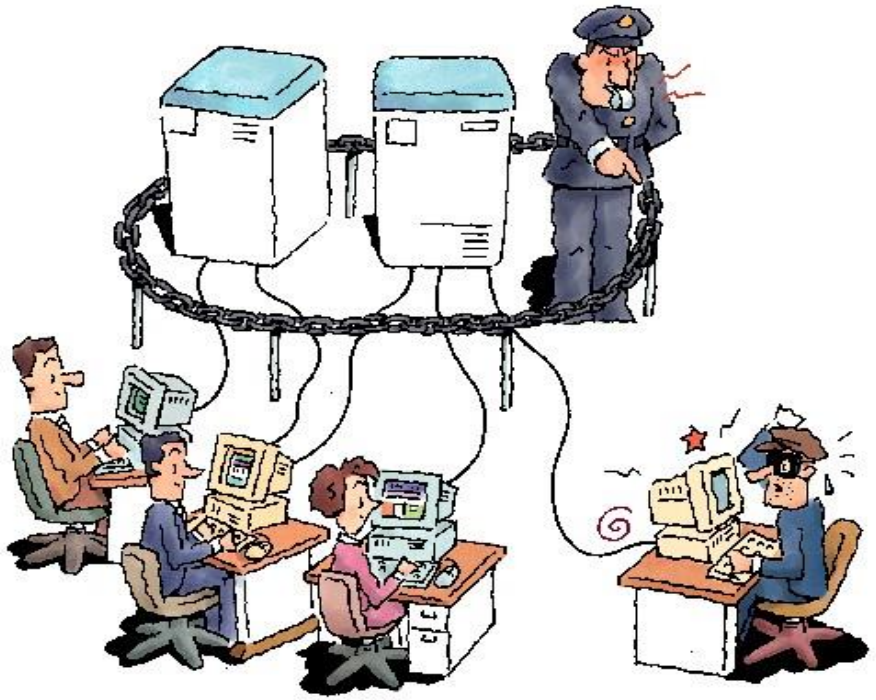
Seguridad en Base de Datos Corporativas



Ing. Armando Caballero Alvarado
acaballeroa@upao.edu.pe

Agenda

- ✓ Introducción
- ✓ Conceptos clave
- ✓ Amenazas a la Base de Datos
- ✓ Resumen

Introducción

- **Reporte Verizon 2012**

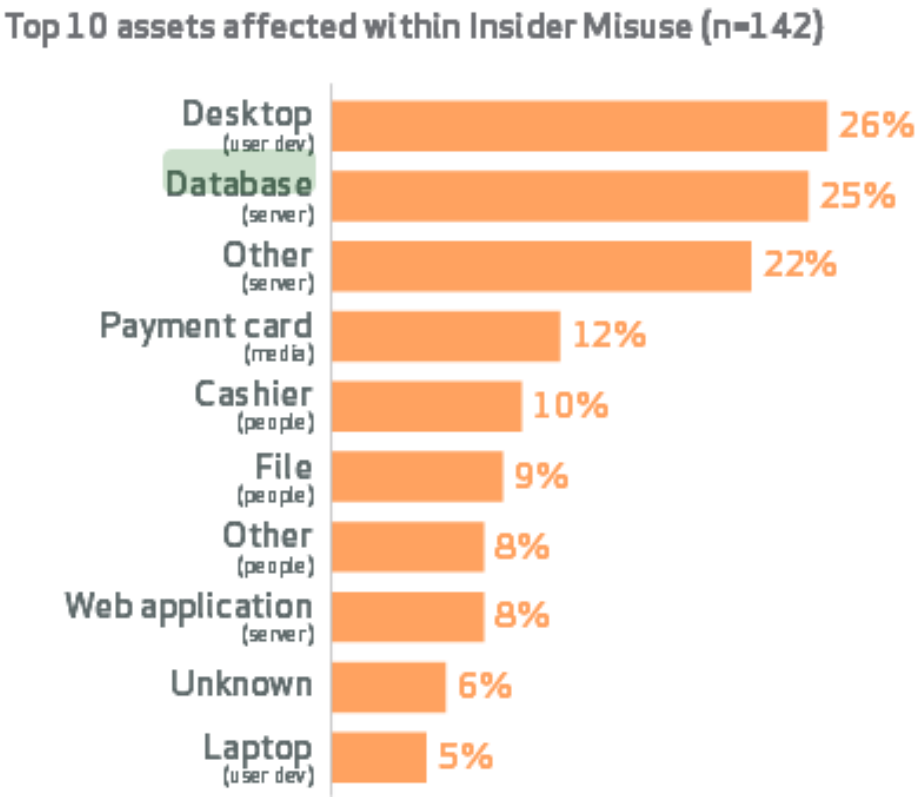
Table 10. Compromised assets by percent of breaches and percent of records*

Type	Category	All Orgs		Larger Orgs	
POS server (store controller)	Servers	50%	1%	2%	<1%
POS terminal	User devices	35%	<1%	2%	<1%
Desktop/Workstation	User devices	18%	34%	12%	36%
Automated Teller Machine (ATM)	User devices	8%	<1%	13%	<1%
Web/application server	Servers	6%	80%	33%	82%
Database server	Servers	6%	96%	33%	98%
Regular employee/end-user	People	3%	1%	5%	<1%
Mail server	Servers	3%	2%	10%	2%
Payment card (credit, debit, etc.)	Offline data	3%	<1%	0%	<1%
Cashier/Teller/Waiter	People	2%	<1%	2%	<1%
Pay at the Pump terminal	User devices	2%	<1%	0%	<1%
File server	Servers	1%	<1%	5%	<1%
Laptop/Netbook	User devices	1%	<1%	5%	<1%
Remote Access server	Servers	1%	<1%	7%	<1%
Call Center Staff	People	1%	<1%	7%	<1%

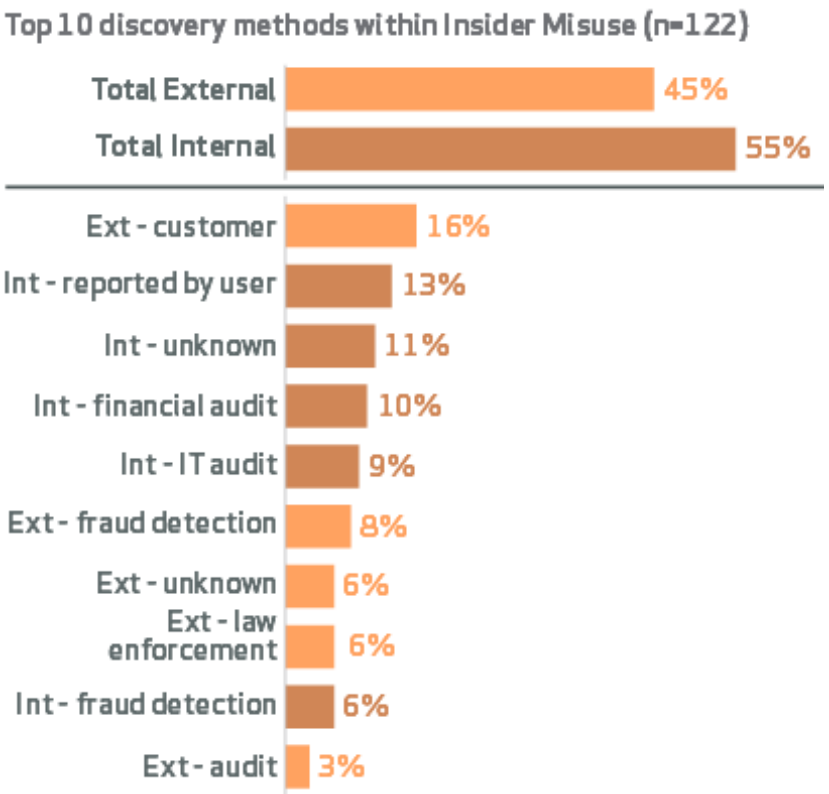
A nivel empresarial un ataque de base de datos significa mas pérdida por los datos perdidos.

Introducción (Cont.)

- **Reporte de Verizon 2014**



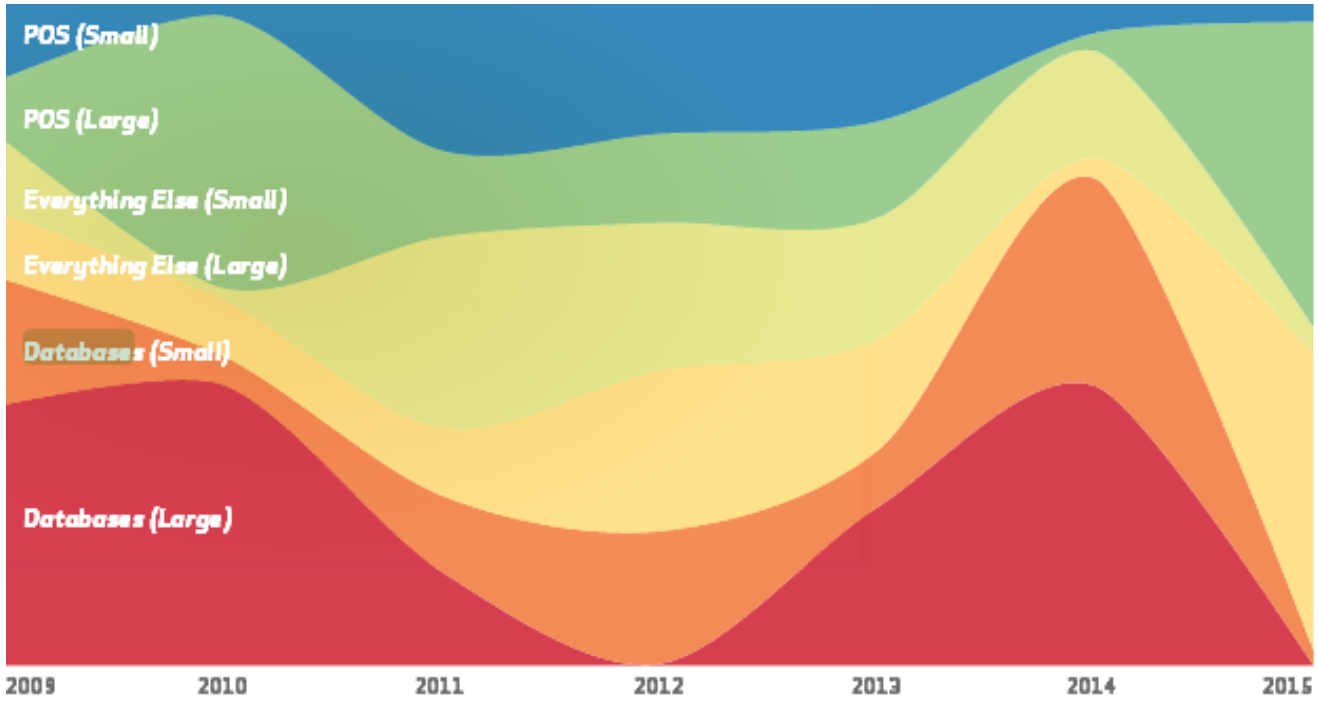
Activos afectados por abuso de privilegios



Descubrimiento información por abuso de privilegios

Introducción (Cont.)

- **Reporte de Verizon 2015**



40 Yep, we did. That's how we roll. But, we're *really* fun at parties. Honest.

Figure 30.

Compromised payment card records from assets by organizational size (small is less than 1,000 employees) over time

Sistemas mas afectados por ataques

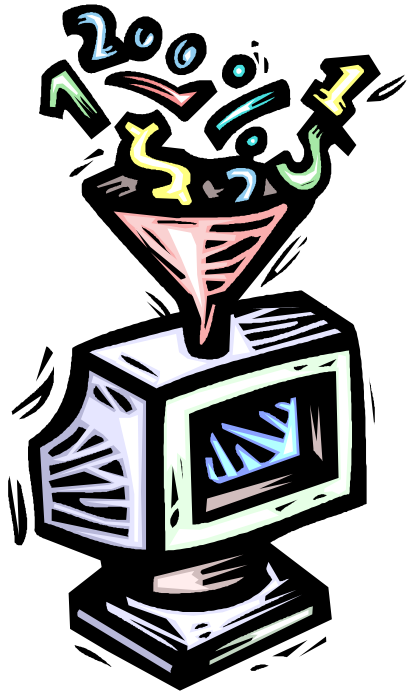
Introducción (Cont.)

¿Están los datos seguros en una Base de Datos?

- La seguridad en el mundo es una de las tareas mas importantes y desafiantes que se enfrenta hoy en día.
- Existen Base de Datos complejas y no cuentan con profesionales conscientes de la seguridad, riesgos y problemas de seguridad referidos a diferentes base de datos.
- Proteger los datos confidencial/sensible en el repositorio de la base de datos implica varios niveles: DBA, administrador del sistema, oficial de seguridad, desarrollador y empleado, la seguridad puede ser violada en cualquiera de estas capas.

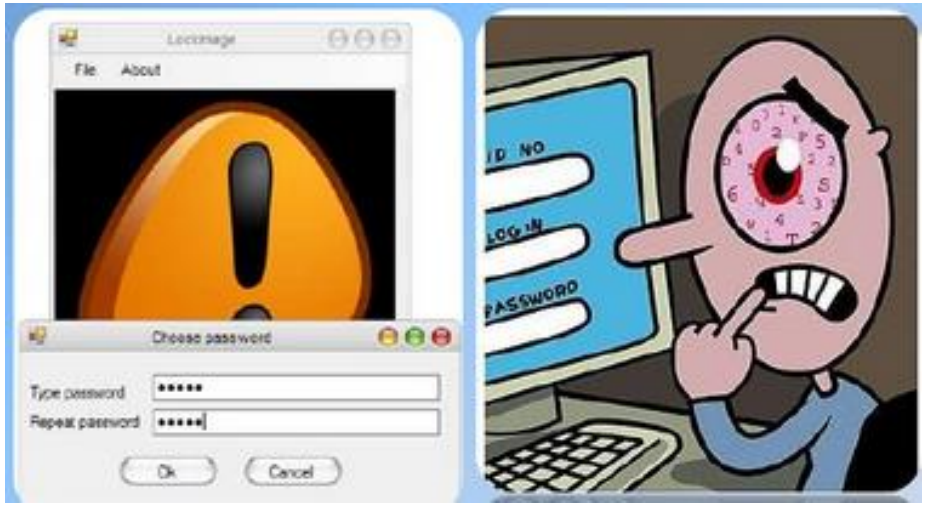
Conceptos clave

- **Seguridad de Base de Datos:** protección de los intentos maliciosos por robar (ver) o modificar los datos.



Conceptos clave (Cont.)

- **Identificación, Autenticación y Autorización**
  - **Identificación:** medio por el cual un usuario se identifica a través de un sistema o software especializado. Incluye username, DNI, huella digital, etc.
  - **Autenticación**: ¿Quién es usted? !Demuéstralo! Verifica la identidad
  - **Autorización:** Que le está permitido hacer después de haberse autenticado.



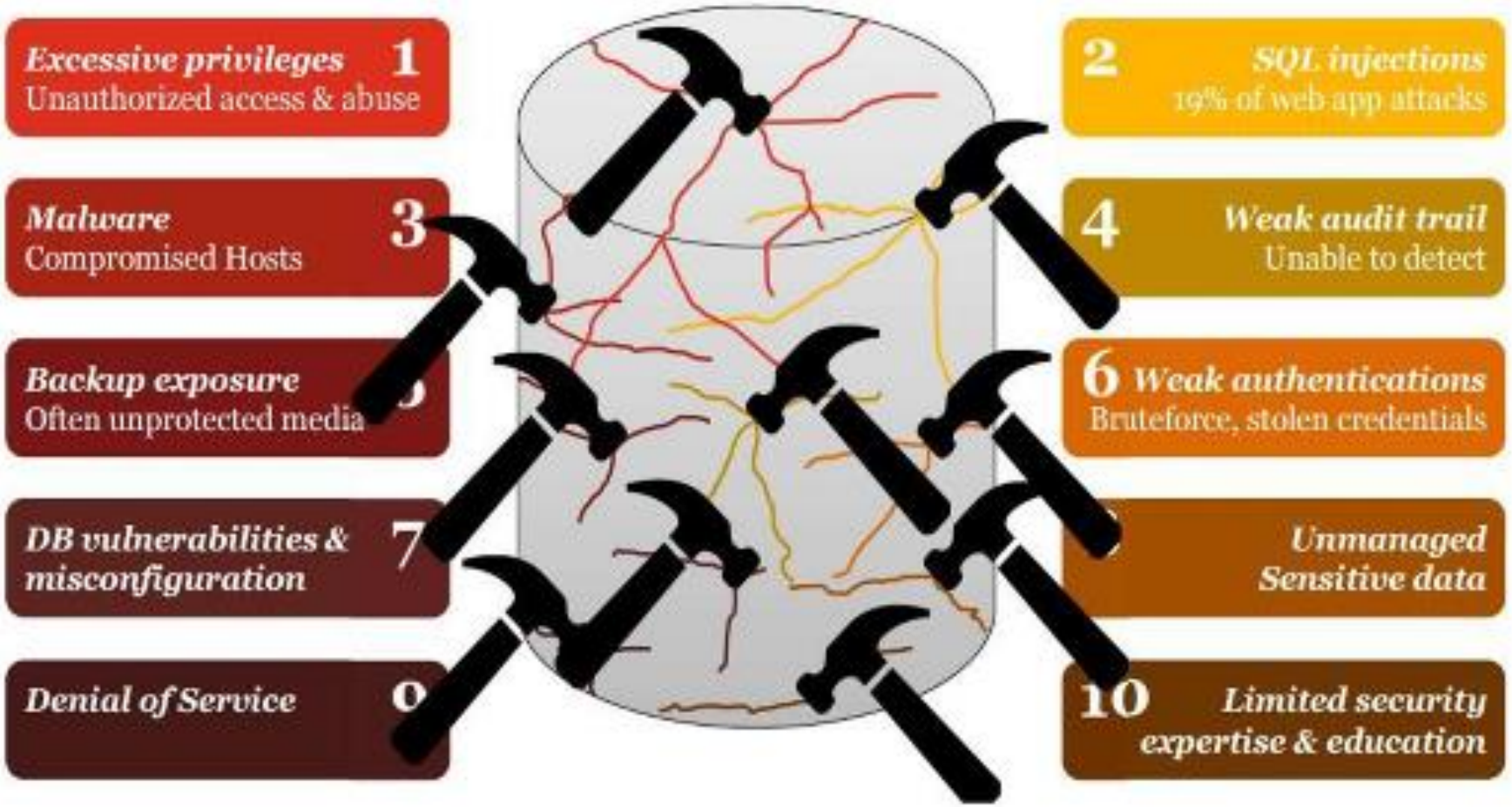
Conceptos clave (Cont.)

- **Amenaza**
  - Posible peligro del sistema. Puede ser un cracker, virus, gusanos, etc. Representan los posibles atacantes o factores que aprovechan las debilidades del sistema.
- **Vulnerabilidad**
  - Punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Representa las debilidades o aspectos falibles o atacables en un sistema informático.
- **Contramedida**
  - Técnicas de protección del sistema contra las amenazas.

Conceptos clave (Cont.)

- **Robo de identidad**
  - El robo de identidad es un delito serio. Tiene lugar cuando alguien se hace pasar por usted, y utiliza información personal de índole financiero para solicitar préstamos, tarjetas de crédito, o tramitar distintos servicios. El ladrón se aprovecha de sus sólidos registros crediticios, y deja un registro negativo a su nombre.
  - *¿Cómo obtienen sus datos?*
    - Robar información que se llega a su buzón de correo electrónico
    - Observar las transacciones que realiza en cajeros/computadoras para averiguar su PIN (numero de identificación personal). Phishing y Pharming.
    - Revisar la basura en busca de información confidencial (trashing).
    - Robar registros o información, soborno a trabajadores que tienen acceso a registros.

Amenazas a la Base de Datos



Fuente: International Journal of Information Sciences and Techniques (IJIST) Vol.6, No.1/2, March 2016

Amenazas a la Base de Datos

- Privilegios excesivo
- SQL injections
- Malware
- Pistas de auditoria débil
- Exposición de respaldos
- Autenticación débil
- Mala configuración y vulnerabilidad de la base de datos
- Datos sensibles no administrados
- Denegación de servicios
- Educación y experiencia limitada en seguridad

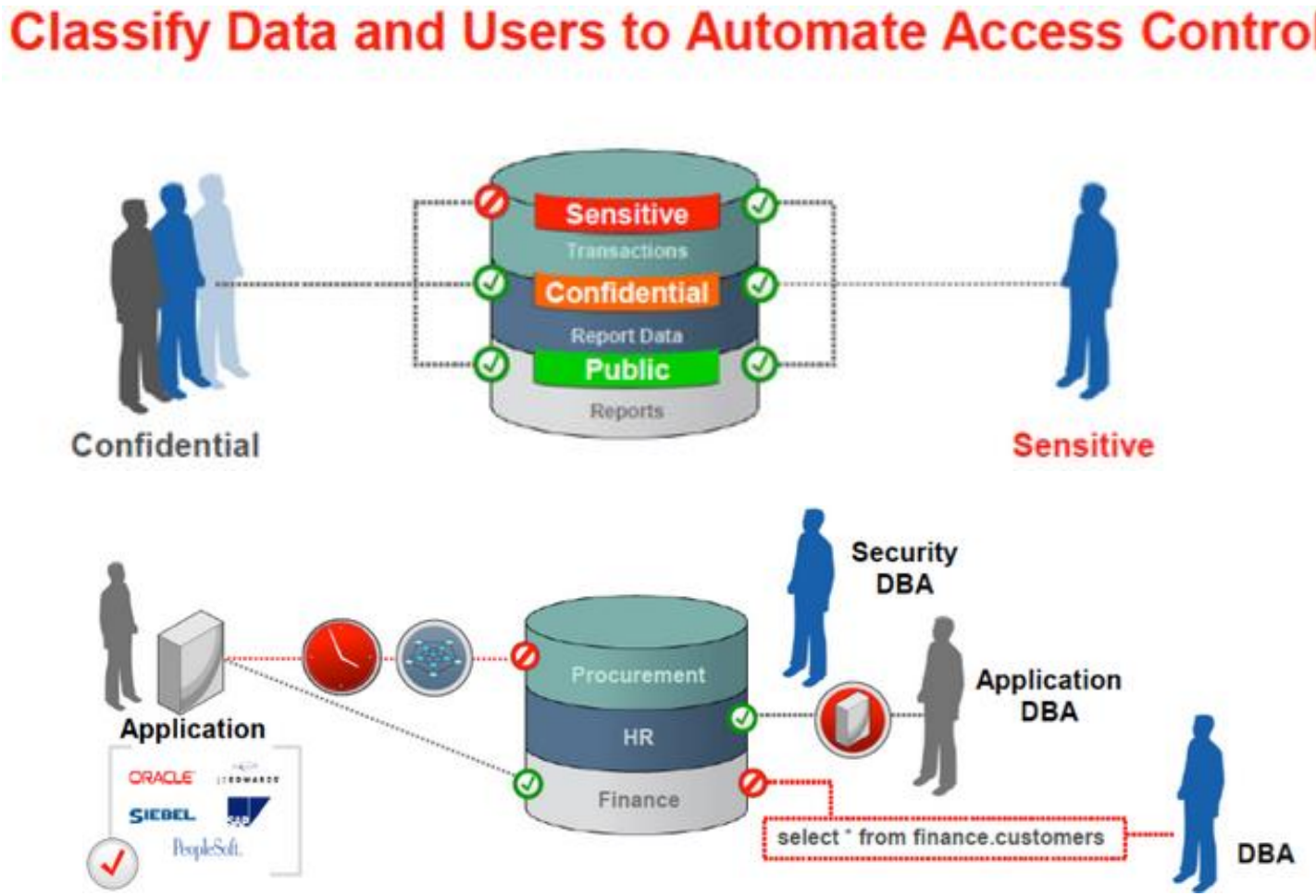
1. Privilegios Excesivo

- Abuso de privilegios para propósitos no autorizados
- Este abuso se presenta de diferentes maneras:
  - **Abuso excesivo de privilegios** (se otorga demasiado)
  - **Abuso de privilegios legítimos** (cuenta con autorización)
  - **Abuso de privilegios no utilizados** (no son necesarios otorgar)
- Es la mas peligrosa, los usuarios autorizados hacen mal uso de los datos
- El **80% de los ataques** a los datos corporativos son ejecutados por empleados o ex empleados.

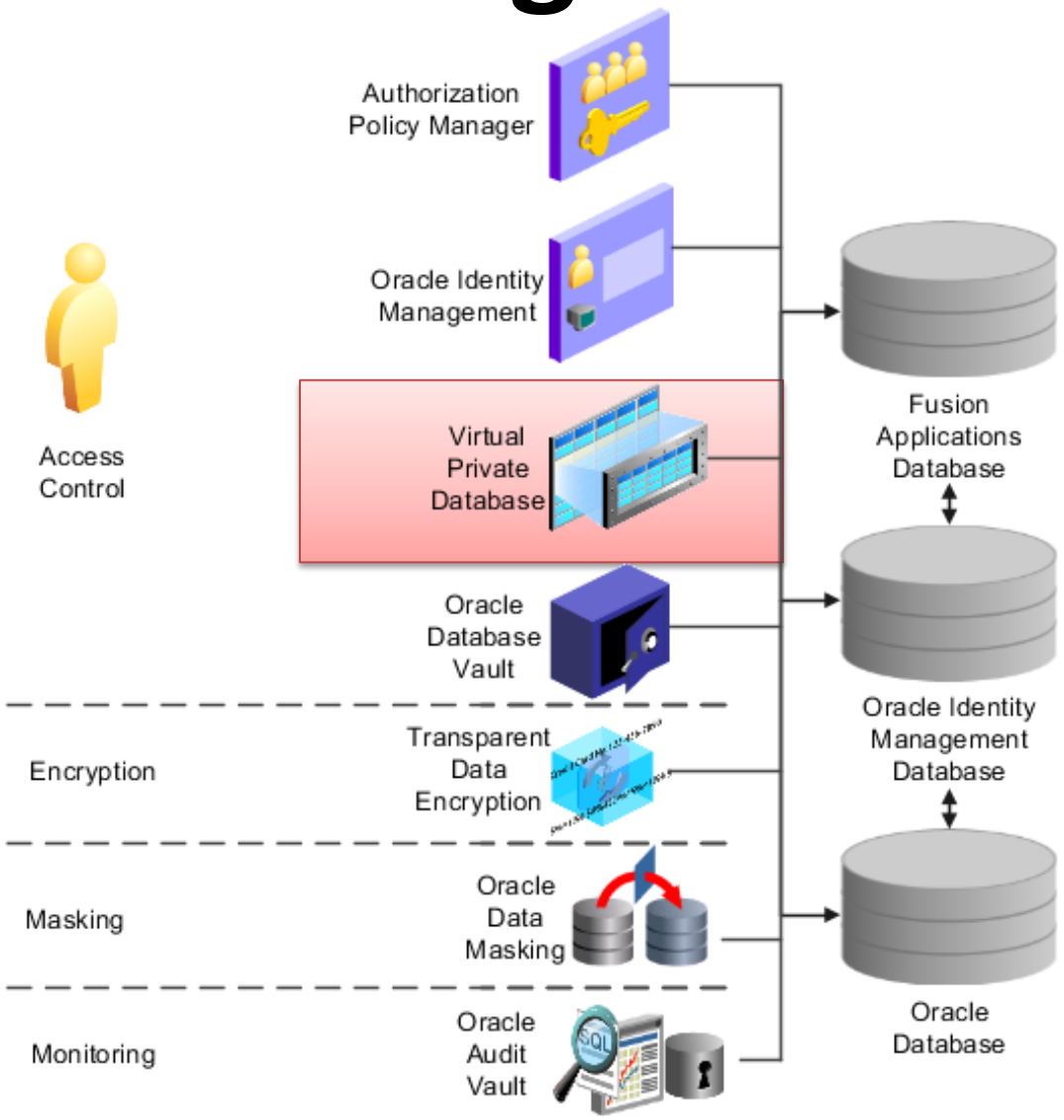
1. Privilegios Excesivo (Cont.)

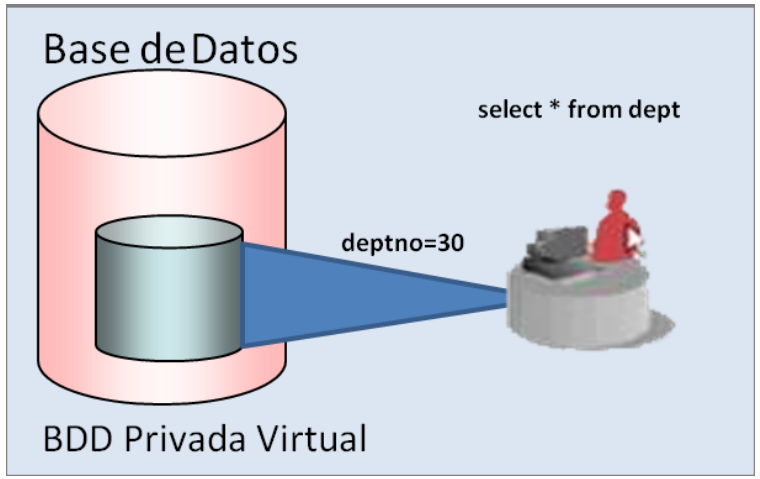
- El abuso de privilegios legítimos puede considerarse una vulnerabilidad de la base de datos.
- **Contramedidas incluye:**
  - **Política de control de acceso:** no se debe otorgar privilegios innecesarios al usuario.
  - **El abuso de privilegios legítimos puede detenerse** para realizar una buena pista de auditoría.

1. Privilegios Excesivo (Cont.)



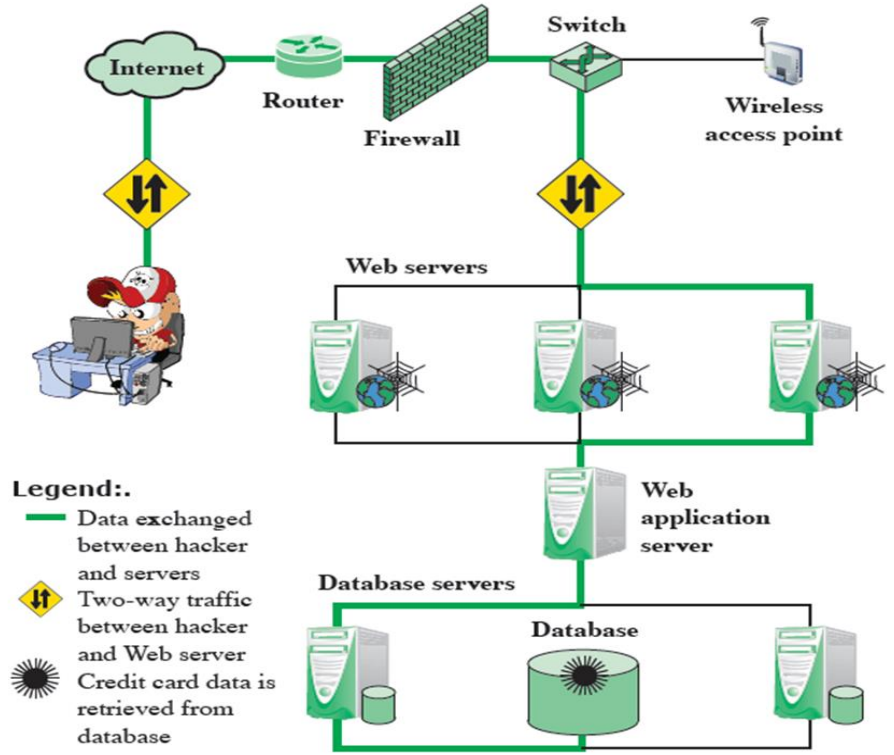
1. Privilegios Excesivo (Cont.)





2. SQL Injection

- Es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente de las entradas para realizar consultas a una base de datos.
- Tipos:
  - **SQL Injection:** objetivo BD tradicional
  - **NoSQL Injection:** objetivo plataformas big data



2. SQL Injection (Cont.)

- Tanto en ataque de inyección SQL o NoSQL exitoso puede dar acceso sin restricción al atacante a toda la base de datos.
- **Contramedidas incluye:**
  - Uso de **procedimientos almacenados** en lugar de implementar consultas directas.
  - Implementación de una **arquitectura MVC**
  - Use funciones que **elimine caracteres especiales** (como comillas) de las cadenas

2. SQL Injection (Cont.)

```
Usuario login(String uname, String pass) throws SQLException {
  Connection conn = null;
  try {
    //Supongamos que se encripta el password con un MD5
    String sql = "SELECT * FROM usuario WHERE username='" + uname + "' AND password='" + pass + "'";
    conn = //obtener una conexión a base de datos
    Statement st = conn.createStatement();
    ResultSet rs = st.executeQuery(sql);
    Usuario u = null;
    if (rs.next()) {
      //Creamos un usuario a partir de la info en el primer registro
      //del ResultSet
    }
    rs.close();
    st.close();
    return u;
  } finally {
    if (conn != null) {
      conn.close();
    }
  }
}
```

Para secuestrar una cuenta específica simplemente en el password se puede enviar ' OR username='admin y con eso podriamos entrar como el usuario admin.

La idea es que si pasamos por ejemplo juan y clave como parámetros, la cadena SQL queda así:
SELECT * FROM usuario WHERE username='juan' AND password='clave'
Pero, ¿qué pasa si pasamos como parámetros x en username y ' OR ''=' en password? Pues la cadena de SQL quedaría así:
SELECT * FROM usuario WHERE username='x' AND password='' OR ''=''

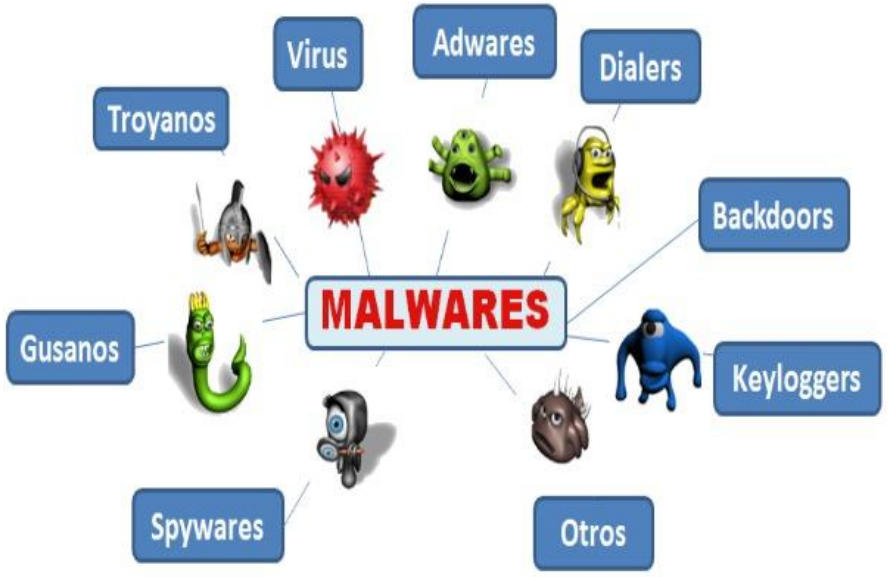
2. SQL Injection (Cont.)

```
Usuario login(String uname, String pass) throws SQLException {
  Connection conn = null;
  try {
    //Supongamos que se encripta el password con un MD5
    conn = //obtener una conexión a base de datos
    PreparedStatement ps = conn.prepareStatement(
      "SELECT * FROM usuario WHERE username=? AND password=?");
    ps.setString(1, uname);
    ps.setString(2, pass);
    ResultSet rs = ps.executeQuery(sql);
    Usuario u = null;
    if (rs.next()) {
      //Creamos un usuario a partir de la info en el primer registro
      //del ResultSet
    }
    rs.close();
    st.close();
    return u;
  } finally {
    if (conn != null) {
      conn.close();
    }
  }
}
```

Con este simple cambio, ahora si mandamos **x** y **' OR username='admin** como usuario y password, se va a buscar exactamente eso, y solamente se tendrá entrada al sistema si existe un usuario llamado **x** y su password es **' OR username='admin**.

3. Malware

- Los ciberdelicuentes, los hackers patrocinados por el estado y los espías usan ataques avanzados.
- Lanzan correos electrónicos de **phising** y **malware** para penetrar a las corporaciones y robar datos confidenciales.
- Un malware desconocido que infecta un dispositivo de un usuario legítimo, éste se convierte en un conducto para que accedan a sus redes y datos.



3. Malware (Cont.)

- **Contramedidas:**
  - Habilite una protección de **firewall**
  - Instalar un **antivirus**

4. Auditoría de pistas débil

- La *tecnología y política de autoría débil*, es un riesgo en cumplimiento, disuasión, detección, análisis forense y recuperación.
- La mayoría de mecanismos de auditoria *desconocen quien es el usuario final*, toda su actividad está asociada a una cuenta de la aplicación web.
- Los informes, la visibilidad y el análisis forense se ve obstaculizado porque no existe enlace con el *usuario responsable*.
- Los usuarios con acceso administrativo a la BD, obtenidos de forma legítima o maliciosa, *pueden desactivar la auditoría de la BD para ocultar su actividad fraudulenta.*

4. Auditoría de pistas débil (Cont.)

- Las capacidades y responsabilidades de *auditoria deben estar separadas de los DBAs* para asegurar una separación de las políticas de derecho.
- **Contramedidas**
  - **Soluciones de auditoria basadas en red**. Estas soluciones no tienen impacto en el desempeño de la base de datos, operan independientemente de todos los usuarios y ofrecen una gran colección de datos.

4. Auditoría de pistas débil (Cont.)

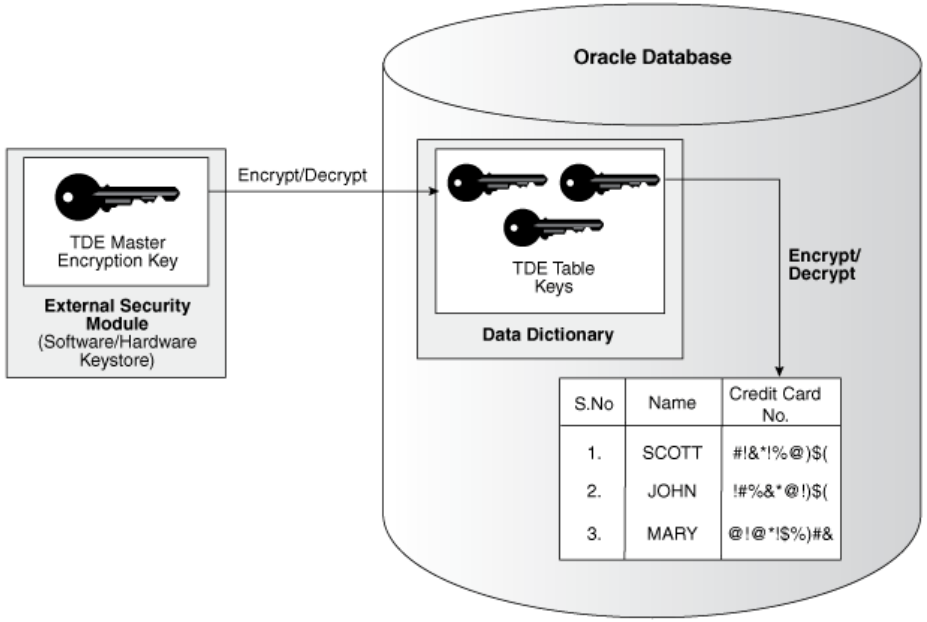
- Generación de Informes de eventos de seguridad
- Informes de conformidad integrados
- Vista global de políticas de seguridad

5. Exposición de respaldos

- Los discos y cintas son a menudo desprotegidos de ataques.
- El hecho de no auditar ni monitorear las actividades de los administradores pueden poner en riesgo los datos.
- Proteger las copias de seguridad y monitorear a sus usuarios con privilegios de administración es una buena práctica.

5. Exposición de respaldos (Cont.)

- **Contramedidas**
  - **Encriptación de la base de datos:** los datos almacenados en forma encriptado permite asegurar las base de datos de producción y copias de seguridad, para luego auditar y controlar el acceso a los datos confidenciales de los usuarios que acceden a la BD a nivel de OS y almacenamiento. Ej. Oracle Advanced Security (cifrado TDE), Oracle Data Masking and Subsetting y Oracle Data Redaction



5. Exposición de respaldos (Cont.)

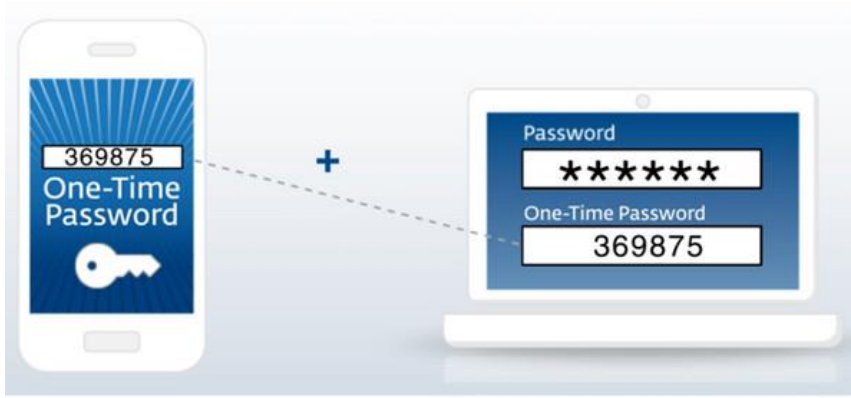
- Ej. Encriptación de datos en Oracle:
- SQL> alter system set key identified by “password”;
- SQL> select column_name, table_name, data_type from dba_tab_cols where column_name like '%SOCIAL%‘ or column_name like '%SSN%‘ or column_name like '%SECNUM%‘ or column_name like "%SOC%‘ and owner='<owner>';
- SQL> alter table customers modify (credit_card encrypt);
- SQL> create table billing_information (first_name varchar2(40),last_name varchar2(40), card_number varchar2(19) encrypt using 'AES256');
- CREATE TABLESPACE seguro_tbs DATAFILE '/oradata/seguro_ts01.dbf.dbf' SIZE 1M ENCRYPTION USING 'AES256‘ DEFAULT STORAGE(ENCRYPT);

6. Autenticación débil

- Permiten a los atacantes asumir la identidad de los usuarios legítimos de la base de datos.
- Estrategias de ataque incluyen: fuerza bruta, ingeniería social, etc.
- Es necesario una implementación de contraseña o autenticación de doble factor.
- Para escalabilidad y fácil uso, la autenticación debe integrarse con infraestructuras de administración de directorios/usuarios de la corporación.

6. Autenticación débil (Cont.)

- **Contramedidas**
  - **Endurecimiento de contraseñas** de los usuarios finales de la base de datos. Ej. Habilitar la función de complejidad de contraseñas en Oracle.
  - **Autenticación doble factor**



7. Mala configuración y vulnerabilidad de BD

- Bases de datos *sin parches de seguridad*
- Cuentas de *usuarios predeterminados*
- Requerimientos complejos y largos para probar parches, difícil encontrar una ventana de mantenimiento para trabajar *sin detener los servicios* críticos de una corporación. Esto puede tardar meses, durante las cuales la base de datos permanece vulnerable.

Oracle » Database Server : Vulnerability Statistics

Vulnerabilities (420) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules

Related OVAL Definitions : Vulnerabilities (24) Patches (0) Inventory Definitions (1) Compliance Definitions (0)

Vulnerability Feeds & Widgets

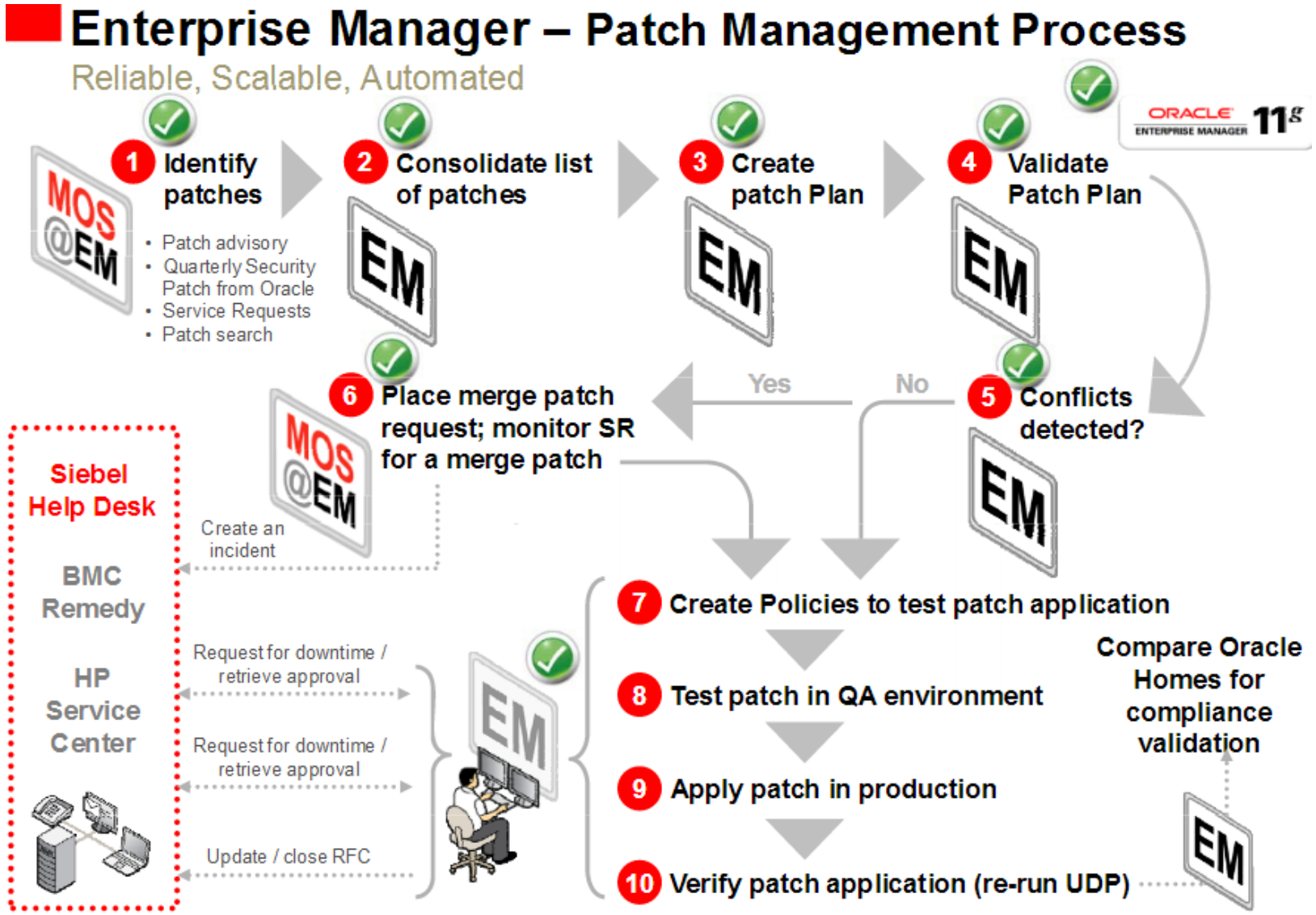
Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
1999	1											1			
2001	9	2	3	2											
2002	6	2	3	2			1			1					
2003	4	1	3	4											
2004	4	1	2	1		1					1	1			
2005	18	1	3	1		2	1	1		1	1	1			
2006	63		5	3		27				2					
2007	54	5	9	15		9	3	1		1	1	2	1		3
2008	30	1	1	2		4						1			
2009	31		1			1	1					1			
2010	31														
2011	49		1												
2012	25		2			1					1				1
2013	13														
2014	40										1				
2015	29	1	1	1											
2016	13										3				
Total	420	14	34	31		45	6	2		5	8	7	1		4
% Of All		3.3	8.1	7.4	0.0	10.7	1.4	0.5	0.0	1.2	1.9	1.7	0.2	0.0	

7. Mala configuración y vulnerabilidad de BD (Cont.)

- **Contramedidas:**
  - No debe tener **cuentas por defecto**. Las cuentas deben crearse de nuevo así como nuevas contraseñas.
  - Existen herramientas para **monitorizar las base de datos y aplicación automáticas de parches**. Ej. McAfee Vulnerability Manager for Database, vPatch Erizo, OEM, etc.

7. Mala configuración y vulnerabilidad de BD (Cont.)



8. Datos sensibles no administrados

- Existen *base de datos olvidada*s que contienen información sensible y que pueden generar una nueva base de datos, por ejemplo, en entornos de desarrollo y prueba, no tienen visibilidad para el equipo de seguridad.
- Los datos confidenciales *están expuestos a amenazas* sino se implementan los controles y permisos necesarios.

8. Datos sensibles no administrados (Cont.)

- **Contramedidas:**
  - Encriptar los datos sensibles de la base de datos
  - Aplicar controles y otorgar permisos necesarios a la base de datos.

9. Denegación de Servicios

- Es el que se realiza cuando una cantidad considerable de sistemas atacan a un objetivo único, provocando la denegación del servicio.
- Las técnicas mas comunes: *desbordamiento de búfer*, *corrupción de datos*, *inundación de la red* y el *consumo de recursos*.

9. Denegación de Servicios (Cont.)

- **Contramedidas:**
  - Endurezca la pila del TCP/IP aplicando la configuración del registro apropiado para **aumentar el tamaño de la cola de conexión TCP/IP, disminuir el periodo de establecimiento de la conexión**, y emplear un mecanismo de registro dinámico para garantizar que la **cola de conexión nunca se sature**.
  - Use un **IDS/IPS** (también wireless) de la red porque estos pueden detectar automáticamente y responder a los ataques SYN (saturación del tráfico de la red).

9. Denegación de Servicios (Cont.)

- En Linux: /etc/sysctl.conf
  - Primer paso, **activar las SYN cookies**:
  - # sysctl -w net.ipv4.tcp_syncookies="1"
  - Segundo paso, **aumentar el 'backlog queue'** (es decir, dar mas holgura al sistema para procesar peticiones entre-abiertas)
  - # sysctl -w net.ipv4.tcp_max_syn_backlog="2048"
  - Tercer paso, **hacer que el sistema minimice el tiempo de espera en la respuesta al SYN+ACK**. En principio un sistema Linux 'por defecto' esperará 3 minutos (valor 5), nosotros lo vamos a dejar en 60 segundos
  - #sysctl -w net.ipv4.tcp_synack_retries=2

10. Educación y experiencia limitada en seguridad

- La seguridad no técnica juega un papel importante.
- Los controles internos no siguen el ritmo del crecimiento de los datos y muchas corporaciones están mal equipadas frente a violaciones de seguridad.
- Falta de experiencia para implementar controles de seguridad, aplicar políticas o contar con procesos para responder a los incidentes.

10. Educación y experiencia limitada en seguridad (Cont.)

- **Contramedidas:**
  - Educación y conciencia de los usuarios
  - Cultivar profesionales en Experiencia de Seguridad

Resumen

- La seguridad de los datos es critico
- Se requiere seguridad en diferentes niveles
- Muchas soluciones técnicas
- El entrenamiento de la persona es vital