Security review

November 27th, 2009

Katarzyna Dziedziniewicz, CERN / IT-DM

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Review of database security

- Risks & vulnerabilities
- General security recommendations
- New reason to patch
- In-house solutions

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Risks

- Data loss / unauthorized change
- Data theft
- Downtime
- Negative press exposure

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Negative publicity

Common vulnerabilities

- **Software vulnerabilities**
  - Both database and applications
  - Most commons flaws widely known
  - Effective and widely available tools
- **Nonexistent or incomplete logging**
  - Difficult attack detection
- **Accounts with no passwords or weak passwords**
  - First and/or only defense line
- ***Nonexistent or incomplete backups***
- Default installs of operating systems
- Large number of open ports
- Not filtering packets

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

General recommendations

- Apply CPU patches ASAP
- Limit user privileges
- On installation revoke grants from packages known for security flaws
- Validate applications for vulnerabilities
- Secure DBA credentials
- Work closely with security, sysadmins and network teams
  - Attacker controlling server controls database too

User related recommendations

- Enforce strong passwords and their changes
- Urge users to user owner/reader/writer accounts
- Encourage users to protect applications with strong credentials
- Advise users on exposing sensitive information
  - Passwords and account names
  - Tnsnames
  - Setup information in Wikis/hypernews
- Alert your users to security risks and provide advice

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Patching

- Advertised by Luca in Barcelona
- New reason to patch: Metasploit
  - Framework for using and developing exploits
  - Allows people with no DB skills to gain DBA privileges
  - Tested in August – only latest patches removed all threats
  - New version contains build in support for Oracle exploits
  - New version is being tested now against October patches

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Deployed in-house tools

- Password scanner
  - Script searching for weak passwords on regular bases
- Locking mechanism for owner accounts
  - Very useful in streamed environment
  - Workflow:
    - Owner accounts are locked by default
    - Stored list of account owners
    - Unlock automatic based on an email from owner

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

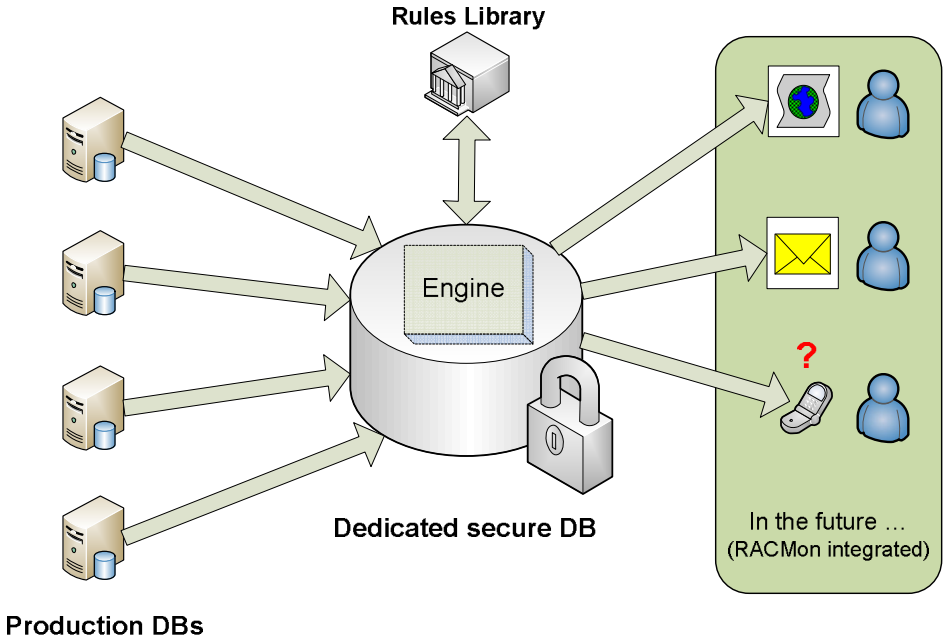
AUDITMON project

- Tool gathering and auditing logon data
- Phase: running prototype
- Can be customized for each experiment
- Uses sets of pre-defined rules to discover abnormalities in user's conduct
- Makes information available to DBA's trough a monitoring page
- Acknowledgments: Luca, David, Raul

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

AUDITMON architecture

- Data copied from each database's DBA_AUDIT_SESSION over a db_link
- Incremental copy of data done every hour
- After all data is transferred a set of jobs runs on the repository to check rules
- Per-database results are stored in the result table



CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

AUDITMON UI

CERN IT Department

Home

Operations
Events
Severity

Databases
TEST2
int9r
int2r
int6r

Select info from To Search
Today - Last 24h - Last Week
Selected dates: From '16-Nov-2009 00:11:00' To '25-Nov-2009 9:11:34'

int9r

DATABASE	EVENT	OCCURRENCES
int9r	No of Failed Logons Per Account	143
int9r	No of Failed Logons Per Account	0
int9r	No of Failed Logons Per Database	143
int9r	No of Failed Logons Per Database No restrictions	143

Home

Operations
Events
Severity

Databases
TEST2
int9r
int2r
int6r

Select info from To Search
Today - Last 24h - Last Week
Selected dates: From '16-Nov-2009 00:11:00' To '25-Nov-2009 9:11:40'

Severity

SEVERITY	OCCURRENCES
INFO	0
WARNING	1716
ALERT	286

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

AUDITMON future

- Broadening the set of rules
- Gathering additional data
  - User related information
- Integrating with DBA alert system
- Using gathered data as base for data-mining analysis
  - Goal: discover less obvious data correlation
  - Adjusting security policies according to discoveries
    - For example changes in profiles

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Conclusions

- Risks are known
- Vulnerabilities are multiplying
- Securing infrastructure is always work in progress
- In-house solutions provide measures tailored to our needs

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it