

Measures to enhance data security at VSD



TRUNG TÂM LƯU KÝ CHỨNG KHOÁN VIỆT NAM
VIETNAM SECURITIES DEPOSITORY

Presenter: Trung Kien Chu (kienct@vsd.vn)

Senior Official of IT Division

ACG Cross Training Seminar 2022

Contents

1

Data security-facts and statistics

2

Data security mechanism overview

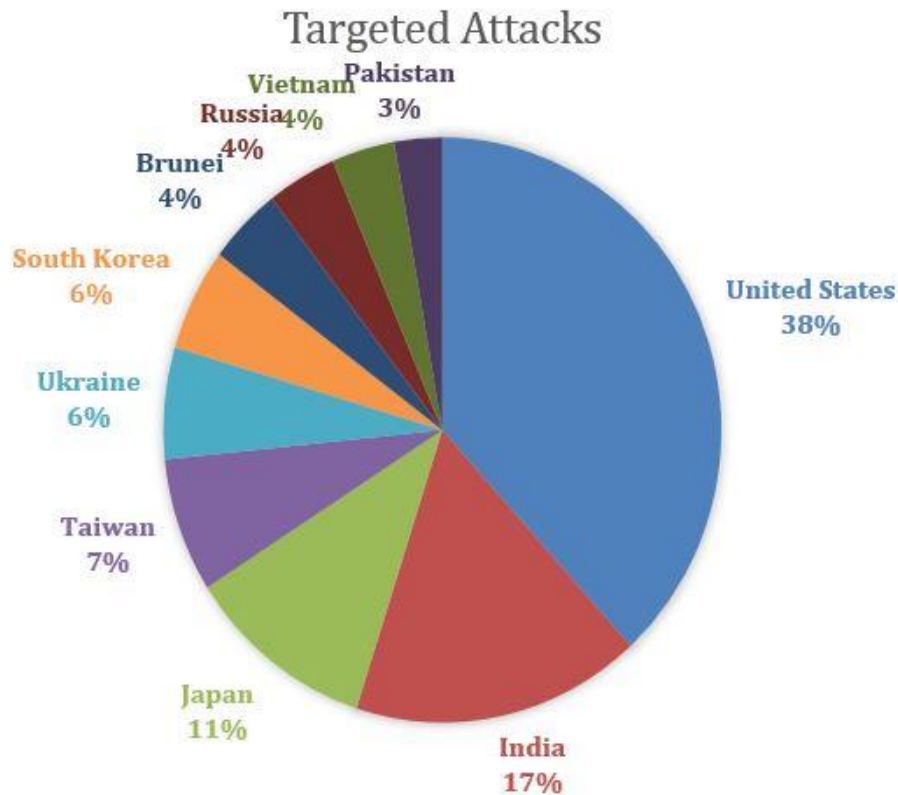
3

Legal measures & technical measures

4

Summary

1. Data security - Facts and statistics



- **The United States is No. 1 target for targeted attacks:** Targeted attacks are often state-sponsored, though some have been by private groups. The U.S. is the No. 1 target (38%), Vietnam (4%).
- **Attackers try to spy, disrupt, identity theft, sabotage, or rob from victims, especially companies in finance sector.**
 - Vietnam is one of most favorite targets for attacker!
 - VSD, a company in finance sector pays special attention to improve data security for the system by legal and technical measures.

2. Data security mechanism overview

- **Vietnam Securities Depository (VSD)** is only one CSD in Vietnam, which is in charge of saving securities investor information, balances, trading results
- Data is very important to VSD, therefore, VSD uses technical and legal measures to protect data.

1. Legal measures:

- To protect data, VSD promulgates *Regulation on data security at Vietnam Securities Depository* in Sept. 2017. This Regulation is checked, reviewed annually and updated if changes needed. The latest version was released in Feb. 2021
- This regulation specify information that should be kept confidential at VSD, for example:
 - + List of securities holders provided by VSD to the issuers
 - + List of securities owners exercising their rights provided by VSD to the member where the securities owner opens an deposit account information on
 - + Trading results sent by Stock Exchanges to VSD for clearing and settlement
 - + Information about the identity and ownership of investors and members on the VSD system, etc.

2. Technical measures:

VSD uses Database Firewall and Privileged Access Management System to control business database access incl. access from end-user via application and access from database administrator to monitoring database operation.

Legal measures

- ***Regulation on data security at Vietnam Securities Depository*** prescribes the principles of composing, storing, transporting and destroying documents and business data to ensure the principles of information security.
- **Information security principles to follow:**
 - **Security:** information should be encrypted as needed to ensure only authenticated recipient can read the information
 - **Authenticity:** Information from the sender needs to be verified to avoid receiving fake information
 - **Integrity:** Information needs to ensure the integrity of the data from the sender to the receiver to ensure that it is not modified during data transmission.
 - **Non-reputation:** An authenticated sender cannot reject submitted data if a legal dispute arises
- Expired data should be properly destroyed to avoid information leakage
- The access to business data through the application is authorized to each business staff
(Each officer is only authorized to access the data of members or issuers which managed by himself and take responsibility if information about that member or organization is leaked.)

Technical measures

- **Database access objectives:**
 - End-user (business user) access to database via application
 - Privileged-user (database administrator) access to database via Privileged Access Management System
- **Database access monitoring and controlling:**
 - End-user → Using Database Firewall
 - Privileged-user → Using Privileged Access Management System

Technical measures – Database firewall

- **Database Firewall to monitoring and controlling access from end-user to database via application**
- Identify 4W (Who-What-When-Where) + 1H (How)

WHO	Identify who access to database
WHAT	Identify which table or database record accessed
WHEN	Identify date/time of database access
WHERE	Identify database access from which Computer/IP address
HOW	Identify which tool is using to access database

Complete Audit Trail						
Event Date and Time	Source IP	User	Destination IP	Service	Source Application	Query
[-] User: erez (7)						
June 10, 2010 5:09:54 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	CREATE OR REPLACE FUNCTION MYFUNC
June 10, 2010 5:09:01 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	select * from table_users
June 10, 2010 5:08:51 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	SELECT ATTRIBUTE,SCOPE,NUMERIC_VAL
June 10, 2010 5:08:51 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	SELECT CHAR_VALUE FROM SYSTEM.PRO
June 10, 2010 5:07:22 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	SELECT ATTRIBUTE,SCOPE,NUMERIC_VAL
June 10, 2010 5:07:22 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	SELECT CHAR_VALUE FROM SYSTEM.PRO
June 10, 2010 4:58:55 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	SELECT "SPW LANGUAGE","SPW WORD","
[-] User: foo (18)						
March 31, 2010 10:44:49 PM	10.77.126.93	foo	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	drop table testpriv
March 31, 2010 10:44:41 PM	10.77.126.93	foo	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	truncate table testpriv

When?

Who?

Where?

How?

What?

*Source: Internet

Technical measures – Database firewall

Database access policy

- **Database access time interval (WHEN):** allowing access from 8 am to 5 pm on working days (if it is necessary to access the database outside of the above time, it must be approved by the VSD Manager)
- **Database access user (WHO):** only authenticated user can access to database via application
- **Database access source (WHERE):** only registered computer/ip address can access to database
- **Database access object (WHAT):** only registered business tables, view, function, procedures from database can be accessed via application.
- **Database access tool (HOW):** only registered tools can be used to access database

Technical measures – Database firewall

Mechanism to handle violations

- **Identify serverity of violation:**
 - Violation level 1 (low): under control and still allow access
 - Violation level 2 (medium): Alert relevant business departments to monitor and still allow access
 - Violation level 3 (high): Deny access
- **Identify violation by number of accessing database records per day (for example)**

	Violation level 1 (low)	Violation level 2 (medium)	Violation level 3 (high)
Request investor holding balance	Lower than 10 times	From 11 to 15 times	More than 16 times
Request depository member holding balance	Lower than 10 times	From 11 to 15 times	More than 16 times
Request investor information	Lower than 10 times	From 11 to 15 times	More than 16 times
Request depository member information	Lower than 10 times	From 11 to 15 times	More than 16 times

Technical measures – Database firewall

Mechanism to handle violations

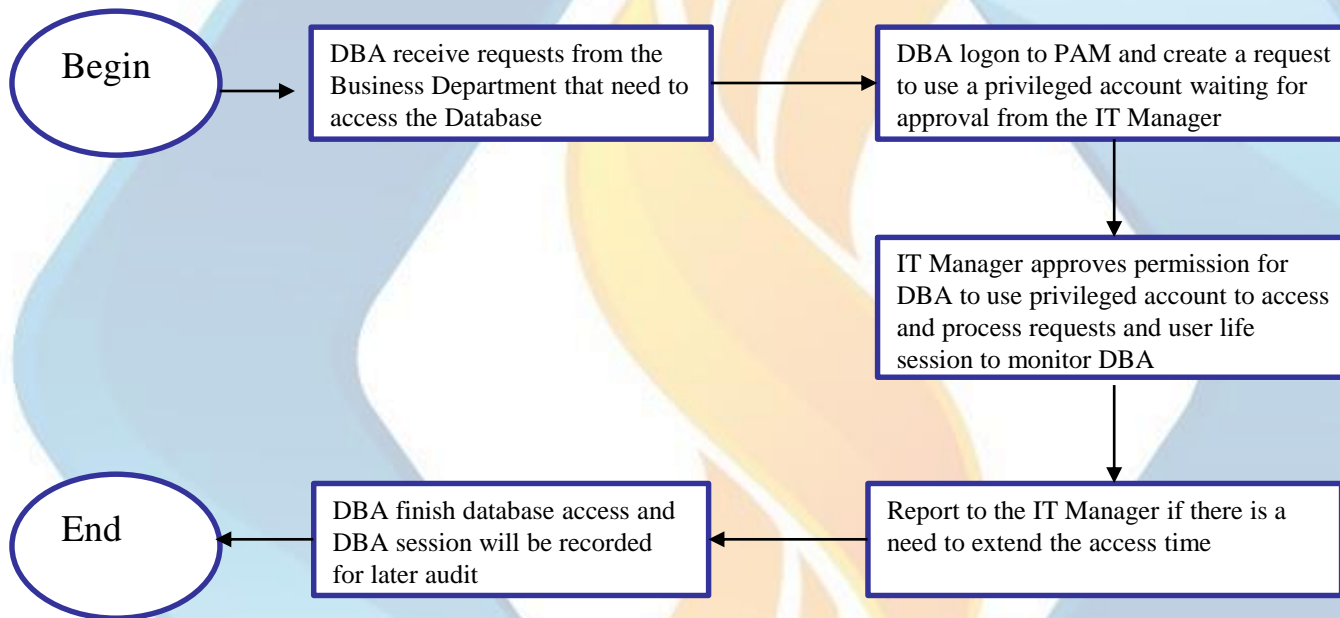
- **Identify violation by sensitive database commands:** Sensitive database commands like *drop database*, *drop table*, *truncate table*, etc. are listed to **Violation level 3 (high)** and access will be denied.
- **Identify violation by accessing database not from registered user or computer/ip address:** are listed to **Violation level 3 (high)** and access will be denied.
- **Access to Privileged account (database administration account)** only allowed via Privileged Access Management System (next slide)

Technical measures – Privileged Access Management

- **Privileged-Users are database administrators**, they are using privileged-account, which can monitor database process, insert/updated database record, therefore, accessing database of privileged-user must be monitored and controlled by another system.
- **Privileged Access Management System (PAM) to monitoring and controlling access from database administrator to database**
 - PAM allows storing passwords, managing sessions, and managing system policies on the same web-interface.
 - PAM record all privileged access sessions to database for later management and audit
 - PAM provide administrators with the most insight into the sessions that are connected to database by viewing life sessions, when violation detected, they can terminate the session.

Technical measures – Privileged Access Management

- **Workflow for database administrator (DBA) to access database via PAM**



Technical measures – Privileged Access Management

- **DBA must enter username/password + OTP to logon PAM system**
- **PAM uses technology to compress and store text and video session logs for later audit**
- **DBA only uses the account to log in to PAM, do not know the actual account of the database**
- **IT Manager uses statistics reports to detect misusing of privileged account database access.**








Technical measures – Privileged Access Management

PAM – Live stream of remote session

Remote sessions

Code Session ID Credential Device User Origin IP Protocol Proxy Session start until

Reason Justification Governance ID Prevent purge

Code	User	Origin IP	Credential	Device	Protocol	Proxy	Session ID	Start	End	Time	Prevent purge	Request	Action
59	Admin	192.168.	admin	192.168.	vnchttp	Proxy Web	e01f31d5d478325a24d680396efa02dleffda9d3	04/04/2022 3:07 PM		00:00:15	No		3 
60	Admin	192.168.	itsm	192.168.	ssh	Proxy Web	04f9cea01d5ec6fa7050a6f3f88afe752f3960bb	04/04/2022 3:07 PM		00:00:19	No		 
58	Admin	192.168.	itsm	192.168.	ssh	Jump Server	7d32a8239a423e1f350251b023feb78f8dc9f04f	04/04/2022 2:57 PM	04/04/2022 3:01 PM	00:03:37	No		 
57	Admin	192.168.	itsm	192.168.	ssh	Jump Server	8f911037f3ef2284a9823ae6f0635baldfd466a8	04/04/2022 2:56 PM	04/04/2022 3:01 PM	00:05:00	No		 

Total: 4 records

30 records 1 of 1

Technical measures – Privileged Access Management

PAM – audit text log

Session logs

Code	Start	End	Type	Host	Username	Error message
09a2d893942995273c6c985c2db0b349e6715208	01/16/2022 00:30:50	01/16/2022 00:31:35	ssh	192.	admin	

User info

User	User IP
demo01 (demo01)	10.

Session events

User	Date/Time	Event	Note
demo01	01/16/2022 00:33:07	Log viewer	
demo01	01/16/2022 00:31:35	Terminated	
demo01	01/16/2022 00:30:50	Started	

Session logs

Search term

Q Search

0 occurrences

```
1642267866010 | Sun, 16 Jan 2022 00:31:06 +0700 | system data | <Return>
1642267866010 | Sun, 16 Jan 2022 00:31:06 +0700 | friendly data |
1642267867917 | Sun, 16 Jan 2022 00:31:07 +0700 | system data | ena<Return>
1642267867917 | Sun, 16 Jan 2022 00:31:07 +0700 | friendly data | ena
1642267874441 | Sun, 16 Jan 2022 00:31:14 +0700 | system data | <Shift_L>Aer0hive<Shift_L>I<Return>
1642267874441 | Sun, 16 Jan 2022 00:31:14 +0700 | friendly data |
1642267879013 | Sun, 16 Jan 2022 00:31:19 +0700 | system data | show ver<Return>
1642267879013 | Sun, 16 Jan 2022 00:31:19 +0700 | friendly data | show ver
```

Screenshot

Technical measures – Privileged Access Management

PAM – audit video log

Video of session

Session info

Code	Start	End	Type	Host
09a2d893942995273c6c985c2db0b349e6715208	01/16/2022 00:30:50	01/16/2022 00:31:35	ssh	192.
Username	Error message			
admin				

User info

User	User IP
demo01 (demo01)	10.

Session

Size	Time
1.01 Kb	45s

▶ View

⚙️ Generate video for download

Summary

- **Data is very important to VSD, therefore, VSD uses technical and legal measures to protect data.**
- **To protect data, VSD promulgates *Regulation on data security at Vietnam Securities Depository* in Sept. 2017 This Regulation will be checked, reviewed annually and updated if changes needed. The latest version was released in Feb. 2021**
- **Database access monitoring and controlling:**
 - End-user → Using Database Firewall
 - Privileged-user → Using Privileged Access Management System



Thank You!