Data Privacy for **Individuals in the Digital World**

11th Edition of The Bengal Chamber's Annual Business IT Conclave

Welcome

4th December 2020

INTRODUCTION – Who are we?

Sarbajit Das

Snr. Defendeer Partner

Technology Center & SOC
Kolkata, India

Konstantin Stassinakis

Snr. Defendeer Partner

Technologie & Operations
Zug, Switzerland

Charly Graf

Snr. Defendeer Partner

Architecture & Solutions
Zug, Switzerland

Defendeer: Data Centric Security Solutions

- We provide solutions to counteract **internal threats**
- We're experts on **security service orchestration**
- We integrate and orchestrate security solutions for disciplines such as **Activity Monitoring, Encryption & Dynamic Masking, Data Loss Prevention and Security Incident & Event Management**
- We provide Security as a Service and Managed **Security Operations Center** Services

We're Swiss based but work globally!

Defendeer is a cyber security service company that believes in **quality, performance and reliability.**
Being highly driven by the **Swiss culture**, we put a lot of emphasis on the innovative approaches that push the boundaries of Cyber Security. Our honesty and dedication has helped us achieve extensive experience and track record that ensures your **sensitive data is safe**.

AGENDA – Introduction Data Centric Security

- **Topics of Today**
  - Sensitive Data are exposed to internal threats
  - DCAP as an effective technical measure
  - Life Demo of a DCAP solution

THREATS – Insiders are a key risk factor for sensitive data

Quelle: https://www.veriato.com/resources/whitepapers/insider-threat-report-2018

90% of organizations
consider themselves vulnerable towards insider risks

57% stated,
to be most vulnerable for the loss of sensitive business data

Key risk facts from the survey (> 400k responses)

- **37 %** of employees have excessive permissions to sensitive data (despite existing RBAC on target systems
- **56 %** of employees' behavior or business routine led to a data breach (intentional or **unintentional**)
- **53 %** of respondent stated that they have recorded insider offenses within the last 12 months in their organization

51% are concerned
about negligent behavior of employees

TECHNICAL & ORGANIZATIONAL MEASURES – Example GDPR EU

GDPR-EU requires,

that all (proportional) measures must be taken to ensure an appropriate level of protection during the collection, processing and storage of the data until deletion (Art. 7, 17, 32)

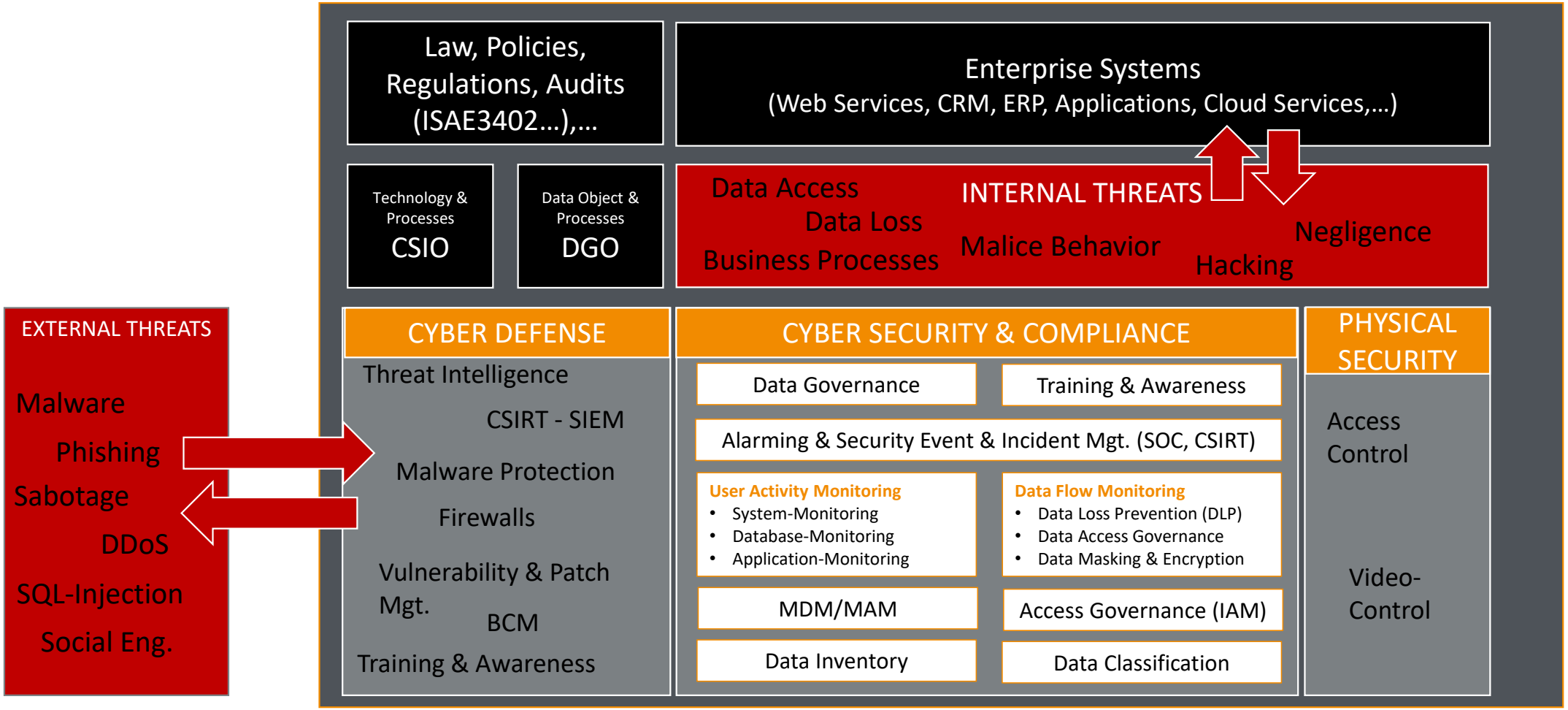
Potential Technical Measures

- Monitor processing of sensitive data
- Ensure transparency while processing sensitive data (Records of Processing)
- Pseudonymize or encrypt sensitive data and reduce access privileges
- Identify and track data breaches fast and effective

Data Privacy Regulation for INDIA?

Indian Personal Data Protection Bill 2019 and GDPR have many things in common but also some differences. But basic principle is to protect personal sensitive data from disclosure and abuse.

TECHNICAL & ORGANIZATIONAL MEASURES – Security Architecture



SENSITIVE DATA – Focus Personal Identification Data

Why is this important?

- Personal data are super sensitive
- Owner of the data is is always the human being
- Disclosure & abuse have a direct impact to the individual's life

What are the latest trends?

- Cashless Payments – digital currency
- Digital Identification (ID) – digital identity
- eHealth - Electronical medical records
- eGovernement – voting & services
- eTransportation – geo movements
- Digital Marketing - Data mining and profiling
- IoT – Smart home (Behavior models)

SENSITIVE DATA – more than just Personal Identification Data

Point of view for organizations

- Legal requirements
- Regulatory requirements
- Ethical & moral responsibility
- Corporate guidelines
- …

External Datasubjects	Internal Datasubjects	Cat.
• Customer information • Health-, credit rating-, criminal-information • Personal preferences • Social information • Geolocation information	• Employee information • Health-, credit rating-, criminal-information • Working conditions(salaries) • Social information • Performance evaluation	Personal data
• Contractual conditions • Commissions payments • Customer recipes & formulas • Customer Process Technologies • Purchases / consumptions • Financial transactions (Bank, Credit cards) • Communication connections (CDR)	• Internal concepts • Purchasing lists • Recipes & Formulas • Process technologies • Construction plans & Designs • Intellectual properties (patents, trademarks)	Feature data

Be aware:

Internal company data must be protected as well as they represent your enterprise assets!


DCAP Use Case:
Dynamic Masking
Protect Personal Data
in Business Applications

DCAP – Why is DCAP very effective

Data-Centric Audit and Protection (DCAP) is a term, that is used by Gartner Group, a known industry research company, to group and compare solutions that cover all DCAP related disciplines.

The main purpose of DCAP is to protect sensitive Data in an organization and to apply the measures on highly sensitive data subjects only and not on the entire data collection of the organization.

DATA-CENTRIC
AUDIT & PROTECTION

Disciplines

- **Real-time Monitoring & Auditing**
- **User Behavior Analytics (Anomaly detection)**
- **Dynamic Data Masking and Data Encryption**
- **Data Access Governance (Consent Control)**
- **Data Discovery & Classification**
- **Logical & Physical Deletion**

THREAT MODELLING – Security Use Cases are the key to success

Scenario Group I: Use Cases Access Patterns

- Access from unusual roles or users (unusual permissions)
- Access from unusual sources (IP, Systems, Countries etc.)
- Access at unusual times ((e.g. outside of business hours)
- Access to huge amount data sets (customer lists or similar)

Scenario Group II: Use Cases Business Processes

- Abnormal frequent access to the same data set (e.g. specific customer) within a defined period
- Unauthorized access to data without approval (e.g. ticket, consent etc.)
- Execute unusual or suspicious business transactions (credit notes, functions etc.)
- **Access to special sets of data (e.g. VIP-customers)**
- Role or function-based masking of not required data within business processes (need to know principle)
- Logical deletion of data sets on behalf of the data owner (e.g. right to be forgotten)
- Decryption of data that needs to be available in the clear for the process (least privilege principle)

Scenario Group III: Use Cases Encryption, Exfiltration & Exports of Data

- **Execution of an allowed function „Export“ from an application while encrypting the data during the export process (e.g. MS-AIP)**
- Encrypt data at source or at transport (e.g. system processes, data warehouses, big data etc.)
- Physical deletion of data


SecuPi
Example
Dynamic Masking with DCAP
Use Case: VIP Customers

DCAP – Security Use Case “Dynamic Masking of VIP customers”

Procedure «Secure in Motion»

- Data remain unchanged (in the clear) at the data source
- Fully tailored presentation of data ensured (role-based model)
- NO changes of the current business process required
- System-driven data transfers are considered in the security model
- Need to know and least privilege principles are fully covered
- In case of a failure of the en-/decryption engine, no business process are impacted
- If case of a loss of the encryption key, the data integrity is not impacted as the source is still available
- Potential risks on data privacy and potential loss could only occurs in case of a failure of the security component

DCAP – Security Use Case “Dynamic Masking of VIP customers”

DCAP – Demo Summary

DCAP offers multiple capabilities out of one suite

We protected sensitive data from unwanted access and loss

- We protected the application with minimally invasive changes (agent installation)
- We dynamically masked data for non authorized users
- We differentiated users from accessing data even they have the same user role
- We encrypted the data export even though the file contains masked data

We monitored all transactions with sensitive data

- We logged all access and transaction activities with sensitive data
- We added the activities in the records of processing

We created security alerts

- We created security events or incidents based on the Use Case for further actions

Questions & Answers

and how can we support your organization?

DEFENDEER
Data Centric Security Solutions
a bluecoons group LLC division
Pilatusstrasse 3
6300 Zug
Switzerland

Phone: +41 41 552 02 95
Mail: office@defendeer.com
URL: defendeer.com

Official Partner of

SecuPi stealthbits