

Case Study: IT Security Objectives at Fun and Fitness Inc.

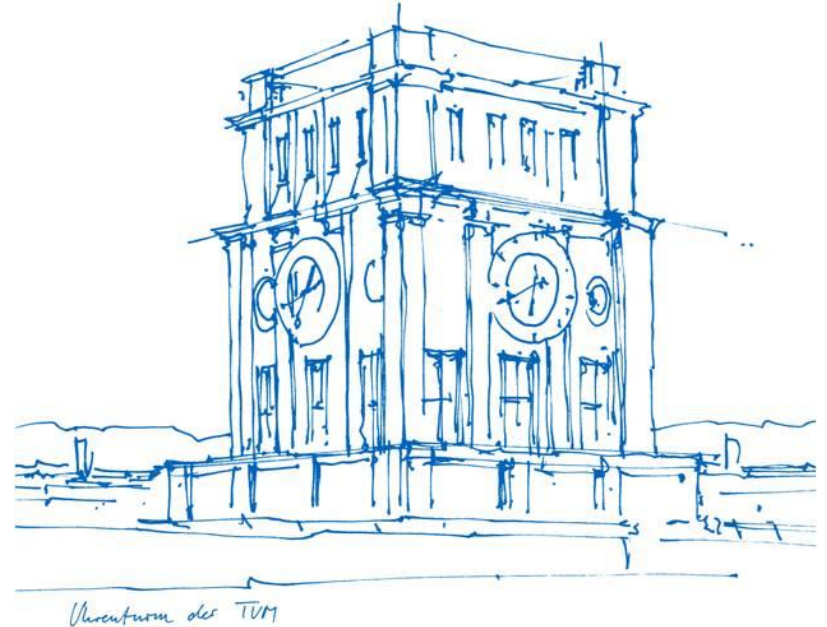
Group 19 (Münch et al.)

Technical University of Munich

Department of Informatics

Chair of Information Systems

Munich, 21.01.2020



Agenda



Case Study – Fun & Fitness Inc.



Definition IT Security and its Objectives



Examples and Methods from the Use Case


8	accountability						
5	data authenticity	6	non-repudiation	7	access control		
1	confidentiality	2	data integrity	3	authentication	4	availability

Fun & Fitness, Inc.

 **Product:** Instructor-led exercise classes (e.g. Zumba, Yoga, Pilates, etc.)

 **Infrastructure:**

- Website: Class Schedule & Class Registration
- Promotional Emails: pre-approved by CMO & “opt-out” possible

 **Payment:** Credit Card (Verification & Processing handled externally)

- Financial log & accounting information exported to *Fun & Fitness*

 **Information Storage:**

- Personal & payment information (currently only for members)

IT Security

Information Security



- Defending information from unauthorized access, use, modification, etc.

→ General term (regardless of the data format)

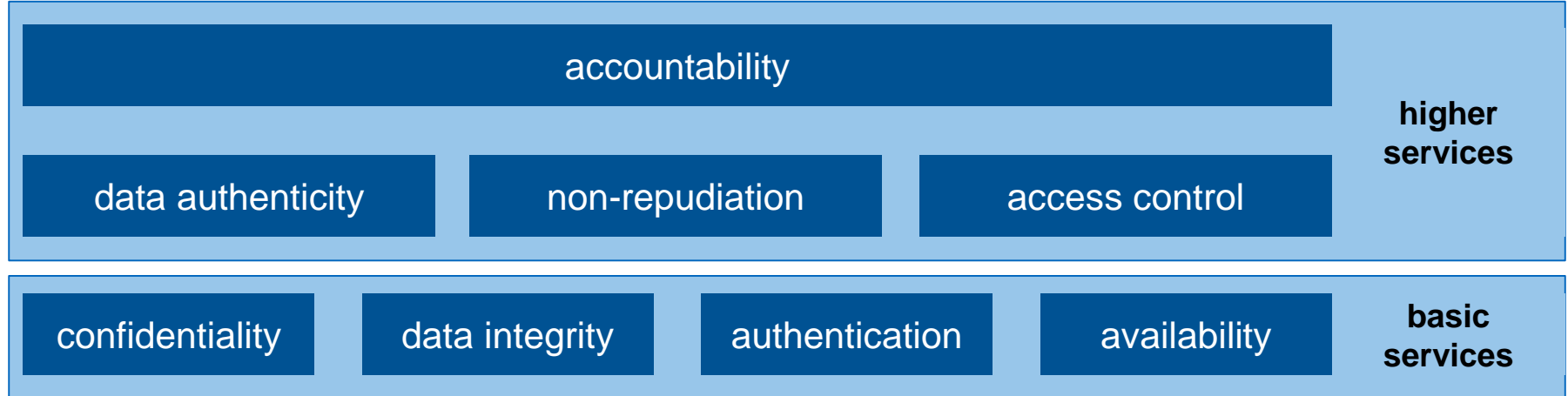
→ Today often electronic data in socio-technical systems

IT Security



- Shared networks, distributed services
- Organizations are even more vulnerable to security threats

IT Security Objectives



Confidentiality

accountability			
data authenticity	non-repudiation	access control	
confidentiality	data integrity	authentication	availability

Definition

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes



Source: Eckert 2009.

Confidentiality examples at Fun & Fitness, Inc.

- Protection of private data (by law, regulation)
- Protection of (business-) critical data
- Protection of transmission data

Violation

- ⚡ Unauthorised access private Information (Credit Card...)
- ⚡ Not yet released promo codes, revenue report
Employee is able to see salary of different employee
- ⚡ Attacker intercepts Email Transfer

Fulfillment

- Encryption of stored and transmitted Data
- Access Control
- Notifications in case of data breach



Data Integrity

accountability			
data authenticity	non-repudiation	access control	
confidentiality	data integrity	authentication	availability

Definition

The property that data has not been altered or destroyed in an unauthorized manner

Source: Eckert 2009, Rao & Nayak 2014.



Data integrity examples at Fun & Fitness, Inc.

- Hardware Fail Redundancy
- Data must only be modified by authorized actors
- Data must be secured from accidental changes

Violation

- ⚡ Hard disk fails, Bit Flip in File
- ⚡ Tampered Pricing, Credit Card Information
- ⚡ Accidental changed format of schedule

Fulfillment

- Redundancy (Backups), Hash-Codes
- Access Control, Email Signatures, Transmission Certificates
- Validating Inputs, Non-Repudiation



Authentication

accountability			
data authenticity	non-repudiation	access control	
confidentiality	data integrity	authentication	availability

Definition

The process of verification of an identity



Source: Eckert 2009, Rao & Nayak 2014.

Authentication examples at Fun & Fitness, Inc.

- Identification of Members
- Identification of Marketing Manager
- Identification of Credit Card Processor

Violation

- ⚡ Identity Theft, Access to Private Information
- ⚡ Access internal privileged Information
- ⚡ Selling course registrations without confirmation of credit

Fulfillment

- User's Access Credentials
- Credit Card Processor's Service identifies with certificate



Availability

accountability			
data authenticity	non-repudiation	access control	
confidentiality	data integrity	authentication	availability

Definition

The property of a reliable access at the right time on information and information systems.

Source: Eckert 2009, Rao & Nayak 2014.



Availability examples at Fun & Fitness, Inc.

- Course Registration is online
- Connection to Credit Card Processor Online
- Account information is online

Violation

- ⚡ Denial of Service Attacks, Website Downtime
- ⚡ Unverified Payment
- ⚡ Database Crash with Data loss

Fulfillment

- Data/Server Replication
- Load Balancing
- SLAs with external/internal Providers



Data authenticity

accountability			
data authenticity	non-repudiation	access control	
confidentiality	data integrity	authentication	availability

Definition

The property of data being genuine and being able to be verified and trusted;
confidence in the validity of data itself and its authorship



Source: Eckert 2009.

Data authenticity examples at Fun & Fitness, Inc.

- Send genuine promotion email
- Exercise class schedule
- Forward valid credit card information

Violation

- ⚡ Phishing email
- ⚡ Manipulated class schedule
- ⚡ Credit card fraud

Fulfillment

- Certificates for the website of the class schedule
- Keyed-Hash Message Authentication Code (HMAC)



Non-repudiation

accountability			
data authenticity	non-repudiation	access control	
confidentiality	data integrity	authentication	availability

Definition

Way of guaranteeing that the sender of message cannot later deny having sent that message

Source: BSI 2018, ISO/IEC 2018.



Non-repudiation examples at Fun & Fitness, Inc.

- Registrations and Payments can be traced back
- Uploaded trainings schedules can be traced back
- Promotional emails can be traced back

Violation

- ⚡ Unlimited registrations
- ⚡ Anonymous schedule tampering (→ dissatisfaction)
- ⚡ Anonymous spamming of customers (→ dissatisfaction)

Fulfillment

- Message Authentication Codes and Digital Signatures
- Auditing and Logging (e.g. Time-stamp and verify registrations)



Access control

accountability			
data authenticity	non-repudiation	access control	
confidentiality	data integrity	authentication	availability

Definition

Process of granting authorized entities the right to use information, while preventing access to non-authorized entities



Source: BSI 2018, ISO/IEC 2018.

Access control examples at Fun & Fitness, Inc.

- Members have access only to their own credit card info
- Only paying customers can register for a class
- Only F&F financial department can access transactions
- Only F&F employees can edit fitness schedule

Violation

- ⚡ Credit card info stolen, financial fraud
- ⚡ Financial losses for F&F
- ⚡ Disclosure of personal information
- ⚡ Customer dissatisfaction and confusion




Fulfillment

- Access Control through definition of **roles**, attributes or rules



Access control – RBAC

accountability			
data authenticity	non-repudiation	access control	
confidentiality	data integrity	authentication	availability

Role / Permission	 Class Registration	 Credit Card Information	 Financial Transactions
F&F Customer	Read & write	-	-
➤ Member	(Read & write)	Write	-
➤ Non Member	(Read & write)	-	-
F&F Employee	Read	-	-
➤ Financial Department	(Read)	-	(Read)

Accountability

accountability			
data authenticity	non-repudiation	access control	
confidentiality	data integrity	authentication	availability

Definition

The property of being able to trace activities on a system to individuals who may then be held responsible for their actions



Source: Eckert 2009.

Accountability examples at Fun & Fitness, Inc.

- Legal validity of bookings
- Legal validity of promotional offers
- Comply with legal standards (PCI DSS)

Violation

- ⚡ Customers can deny the contract
- ⚡ Marketing manager can deny promotional offers
- ⚡ Credit Cards' CCV2 code stored in F&F

Fulfillment

- Auditing and Logging
- Cross-department collaboration
- Cybersecurity Awareness Training on e.g. legal standards



Viele Dank für Ihre Aufmerksamkeit!

München, 21.01.2020



Sources

- BSI (ed.) (2018): IT-Grundschutz-Kompendium, Fassung vom Februar 2018, in: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2018.pdf?__blob=publicationFile&v=7 (Stand: 15. Januar 2020).
- Eckert, C. (2009). IT-Sicherheit: Konzepte - Verfahren - Protokolle. Munich: Oldenbourg.
- ISO/IEC (eds.) (2018): ISO/IEC 27000, version of February 2018, in <https://www.iso.org/standard/73906.html> (Last accessed: 15 January 2020).
- Microsoft (ed.) (2018): Internet of Things security architecture, in: <https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture> (Last accessed: 15 January 2020).
- Rao, U.; Nayak, U. (2014): The InfoSec Handbook, Berkeley 2014.
- Stouffer, K.; Pillitteri, V.; Lightman, S.; Abrams, M; Hahn, A. (2015): Guide to Industrial Control Systems (ICS) Security, in: <http://dx.doi.org/10.6028/NIST.SP.800-82r2> (Last accessed: 15 January 2020).
- (Bildquelle: <https://d1p2xdir0176pq.cloudfront.net/wp-content/uploads/cybersecurity.jpg>).