Use case diagram and Scenarios

Author:

Responsible:

Description: <https://learnit.itu.dk/mod/page/view.php?id=186444>

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Change | Author | Date |
| 0 | Added ChangeLog | Peter | 22/09 |
| 1 | Initial work on document, added scenarios, tasks | Peter, Cecilie, Luca, and Victoria | 03/11 |
| 2 | Added use case diagram | Victoria | 08/11 |
| 3 | Added more detailed descriptions of use case diagram, scenarios, actor table, actor descriptions, and use case descriptions | Luca, Cecilie, and Victoria | 09/11 |
| 4 | Added new scenarios based on discussions with Elda and changing lanes to go with an educational platform. | Cecilie | 10/11 |
|  |  |  |  |
|  |  |  |  |

Use case diagram and Scenarios

The purpose of the use case diagram is to understand how users interact with the system, it pertains to the application domain (Mathiassen, 2018). To start the process, we brainstormed a list of tasks and activities that users would likely encounter.

**Tasks/activities:**

* Taking a course
* Checking traffic on a file or folder
* Getting an overview of security status
* Read up on regulation changes
* Doing a phishing test
* See results of tests
* Notification of outside access
* Getting a certification
* Obtain information on security risks or considerations
* Feel safer
* Feel more confident
* Storing data in a secure way
* Regulating access to data

**Actor table**

For the actor table, we focused on narrowing down the tasks and activities to the most important ones.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Use case | Owner | Employee | Regulatory body |
| 1 | Take Course |  | x |  |
| 2 | Recognize breach | x |  |  |
| 3 | Reset access | x |  |  |
| 4 | Receive test email |  | x |  |
| 5 | Fail/pass test |  | x |  |
| 6 | Start phishing test | x |  |  |
| 7 | Check test result | x |  |  |
| 8 | Mandate course | x |  |  |
| 9 | Policy change |  |  | x |

**Description of actors**

As seen in the actor table above, we decided on three actors, Owner, Employee and Regulatory Body.

Owner

Goal: A person that owns a small business with 0-19 employees. The owner’s basic need is to keep their business safe from malicious attacks such as phishing attempts.

Characteristics: The owner uses our application to make sure they’re up to date on compliance and can educate themselves and their employees about security risks.

Examples:

Owner A is unsure if they comply with regulations. Owner A has difficulties understanding every aspect of the regulations they need to comply with. Owner A gives up trying to be correct as it is taking too much time and effort to be compliant.

Owner B pressed a link in phishing earlier this year. As they ended up losing a large amount of money, the owner wants to make sure this never happens again. They’ve decided to find an application that can help them stay on top of security threats.

Employee

Goal: A person who works in small business. The employee's responsibility is to not leak confidential information to people outside the business.

Characteristics: The employee are mandated from their bosses to take various security courses. The employee may be tested to make sure they live up to the security levels of the business.

Examples:

Employee A tries to get access to a piece of sensitive information. Their boss gets a notification about them trying to access. Employee A might need to retake a course about data availability.

Employee B is handling sensitive data, emails, of customers. Employee B has taken a course on secure handling of data. Employee B feels confident to not release this data publicly.

Regulatory Body:

Goal: A regulatory body creates and mandates regulations on which companies need to be compliant to. This is done to have a general ‘protective net’ for all customers.

Characteristics: The regulatory body affects and influences what the system may present as important to the SMB.

Examples:

Regulatory body A enforces a new regulation. This causes the system to be updated such that it is up to date with the latest regulations. The users of the systems get notified about the new regulation and possible changes which need to be made.

**Description of Use cases**

Take a course

Use case: Take a course is initiated by the employee. The employee taking the course takes their device such as phone or tablet and finds the application. At the applications interface they will find different types of courses. They click the course they want to take, and the course begins. During the course they learn all they need to know about the given subject. In the end they will be tested and earn a bache if they did well. When the employee is done taking the course, they can decide whether to take a new course or to close the application and lay down their device.

Object: Employee

Recognize breach

Use case: Recognize a breach is done by the owner. They receive a notification from the system informing them that there has been a breach, e.g. unrecognized user accessed the database. This startles the owner, but the system guides the owner with precise notation on what the next couple of steps are.

Object: Owner

Reset access

Use case: Reset access is initiated by the owner. If there has been a data breach, the owner will be notified through the application. The system will advise them to reset access and give a step-to-step guide in how to do so. The owner follows the guide and makes sure no one has unauthorized access to the company data. The access is reset.

Object: Owner

Report breach

Use case: Report breach is initiated by the owner. The system has recognized that customers data has been leaked. The system creates a report about it and informs the owner about it. The owner now has the responsibility to possible inform the affected customers about the breach as to stay on top of the issue and keep the trust of their customers.

Object: Owner

Receive test email

Use case: Receive test email happens to the employee. They receive an email detailing about a time sensitive issue from a supplier or company they have been in contact with. The email was sent by the system to test their capabilities to identity the malicious intent behind the email.

Object: Employee

Start/Fail test

Use case: Starting or failing a test is done by the employee. They either failed or succeeded to identity malicious intent in a test email or fail a test within the application. Their performance will be reported to the system and succeeded tests will be awarded.

Object: Employee

Start phishing test

Use case: Start phishing test is initiated by the owner. They want to test their employees to make sure they are not falling for phishing scams. Therefore, they log in to the system to deploy the test. The system sends out test emails to the employees. When the test is over the results are published to the owner.

Object: Owner

Check test results

Use case: Check test results are initiated by the owner. They look at the latest reports from the system indicating that some test on employees have been conducted. This report showcases which employees passed or failed a test. The system presents some possible actions the owner can take.

Object: Owner

Mandate course

Use case: Mandate course is done by the owner. They think it is time to upskill their employee's knowledge on cyber, therefore they go into the application to mandate a course on cyber security. The employees are notified that they have to take the course. The owner is able to see when the employees has finished the mandated courses.

Object: Owner

Policy change

Use case: A Policy change is done by a Regulatory Body which might change how the data handling for companies on customers’ data needs to be done. These policies need intervention for every company currently holding this type of data.

Object: Regulatory Body

**Scenarios**

For the scenarios it was emphasized to represent all actors and a subset of events. From our brainstorming there were multiple scenarios and groups of scenarios which would create a unified picture of education, security, and compliance.

For the chosen scenarios we decided on narrowing down the Actor to the Owner. As the goals of an owner can have the most impact on the SMB.

We decided on the following three scenarios which we based our use case diagram on.

*Actor: Owner*

*Goal: Owner wants to know if there has been a breach of data.*

*The owner goes to work in the morning and opens the app to check if anything remarkable happened tonight. The dashboard tells them that there was an outside access to files. After confirming the access was not warranted, Owner resets all access to the files and reports a data breach to the relevant authorities. (Perhaps add that the employee needs to regain access to files)*

Actor: Owner, employee(s)

Goal: Owner wants to test employees if they are up to date on phishing

Owner starts a phishing test. Employees receive a test email that looks legitimate but comes from an unknown source. They open the email and click the link. Owner gets notified and tells employee to take course.

Actor: Employee

Goal: The employee wants to complete a course on phishing

The employee has failed the phishing test their boss sent. They’re mandated to take a course on phishing. They successfully finish the course and get a badge.

Actor: Owner

Goal: To set up the application such that they can learn about security

The owner downloads the app. The initial set up of the app involve a set of questions that the owner has to answer. The owner provides the needed information and finishes the set up. The app shows personalized themes and courses for the owner based on their answers.

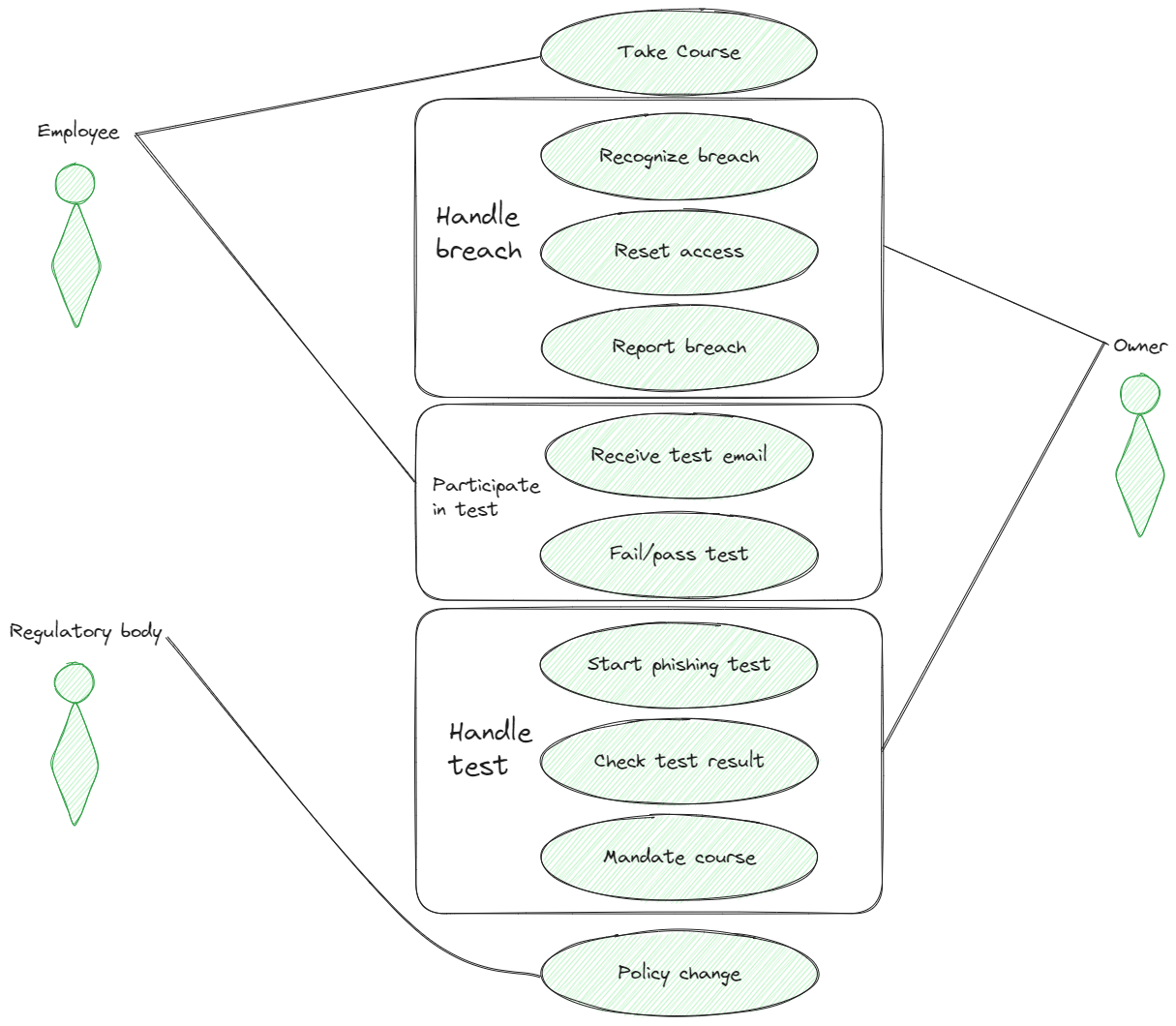
*Actor: Owner, regulatory body*

*Goal: To be compliant*

*Owner wants to check up on their compliancy. They notice that the EU regulations for data privacy has changed, so owner uses app to find relevant information and guides.*

**Use case diagram**

The use case diagram clearly shows all use cases and actors. When constructing the use case diagram, it was discovered that some use cases could be associated with each other. Recognize breach, reset access, and report breach can be described as a set of actions to handle a breach by the owner. Receive test email and fail/pass test are associated with the employee participating in a test. In principle the owner can also take tests and courses. The distinction between employee and owner is that the owner can handle test, through choosing what courses/tests should be deployed or mandated, they also have access to test results.



*Use case diagram*