

Professional Skills
Agile Fundamentals
Jira
Git
Databases Introduction
Java Beginner
Maven
Testing (Foundation)
Java Intermediate
HTML
CSS
Javascript
Spring Boot
Selenium
Sonarqube
Advanced Testing (Theory)
Cucumber
MongoDB
Express
NodeJS
React
Express-Testing
Networking
Security
<div><div></div>Security Basics</div>
<div><div></div>Authentication and Authorization</div>
<div><div></div>Security Attacks</div>
<div><div></div>Passwords</div>
<div><div></div>Hashing vs Encrypting vs Encoding</div>
<div><div></div>Introduction to DevSecOps</div>
<div><div></div>Pen Testing, DAST & SAST</div>

Security Basics

Contents

- [Overview](#)
- [Need for security](#)
- [Case Studies](#)
 - [PlayStation Network - PSN \(2011\)](#)
 - [Yahoo! \(2014\)](#)
- [Impact of a security breach](#)
 - [Identity Theft](#)
 - [Financial Theft](#)
 - [Data Ransom](#)
 - [Illegitimate Sale of Data](#)
 - [Corporate Espionage](#)
 - [Reputation Loss](#)
- [Tutorial](#)
- [Exercises](#)

Overview

Security is defined as *the state of being free from danger or threat*. But what exactly does that mean for IT?
In this module we shall look at the need for security in the IT industry and the potential impacts of a security breach.

Need for security

IT is now a very large and profitable industry, making it more and more of an attractive target to criminals.
Even companies with very little to do with the industry will usually utilise computers, providing yet more insentive for cyber crime.

Inadequate security and security mistakes can be, and have been, used as oportunities for these cyber criminals.

Case Studies

Included below is some information about security breaches in two well known companies, and the consequences of them.

PlayStation Network - PSN (2011)

In spring of 2011, Sony's PlayStation Network was hacked and the personal details of around 77 million accounts were stolen.
Personal details included:


- Usernames
- Emails
- Passwords

In some cases credit/debit card information was also taken.

In the lead up to this event, Sony's PSN servers were repeatedly overwhelmed causing the PSN to crash. Shortly after, Sony voluntarily took PSN offline while they investigated the breach.

Sony estimates the total cost was in the region of £105m.

Yahoo! (2014)

 Introduction to OWASP
Cloud Fundamentals
AWS Foundations
AWS Intermediate
Linux
DevOps
Jenkins Introduction
Jenkins Pipeline
Markdown
IDE Cheatsheet

Yahoo! announced in September 2016 that two years earlier, there had been a breach in their security which lead to the theft of at least 500 million users' data.

Later that year they also annouced that in 2013 there had been a larger breach, in which between 1 and 3 billion accounts were affected.

The revalation of both breaches would lower the value of the company by nearly half a billion US Dollars, when they were eventually sold to Verizon in 2017.

Impact of a security breach

We have already seen that breaches in security can have a financial impact on companies. However, the impact of a security breach is not always financial and can affect individuals as well.

Identity Theft

The deliberate use of another person's identity, often, but not always, for financial gain.

The theft of any of the following pieces of data can be used for identity theft:

- Name
- Date of Birth
- Passport details
- Bank/card details

Sometimes the victim of this attack faces consequences for the actions of the thief.

Financial Theft

Accessing another person's bank account, or other financial accounts, to take money from them.

Financial theft can be obvious, if a bank account has been emptied, but it can be subtle too. Thieves sometimes take a small amount from an account each month, this is designed to look like a bill and remain undetected.

It can be difficult to prove that the withdrawals of money were not made by the account holder, this can leave people in a terrible financial situation.

Data Ransom

A fear-based form of extortion which aims to convince a victim to part with or services, to prevent the data from being released to the public.

Usually the information held to ransom is life changing, putting the victim in a desparate situation to extort as much from them as possible.

Illegitimate Sale of Data

After a victims data has been stolen, instead of being used, it can be sold on in an illegitimate sale of data.

This data can be sold to someone who intends to use it for one of the three impacts mentioned above, or used to send spam emails which aim to complete another data breach.

Corporate Espionage

The act of spying on, or stealing, confidential information for commercial purposes.

Stolen information can give a company's competitors an advantage when creating rival products.

Reputation Loss

After a major data breach, a company will undoubtedly have a worse reputation.

People are unlikely to store any personal details with a company who has lost

some of its data to an attack for fear of having their data lost or stolen.

In addition to the loss of reputation, the individuals who are affected by the data breach may need to be compensated.

This can damage a companies reputation even further if the compensation is not deemed to be enough.

Tutorial

There is no tutorial for the module.

Exercises

There are no exercises for this module.