# Presentation of the company

EY (Ernst & Young) is a worldwide known accounting firm and is proud member of the “Big four”. EY is spread around the world with more than 700 offices in more than 150 countries offering jobs to more than 200.000 employees. The Belgian offices are located in **Diegem** (office where the internship took place), Ghent, Antwerp, Bruges... For a total of twelve different locations in Belgium. The 1335 Belgian employees are spread between these locations. [1]



Figuur 1: Logo EY (2017) [6]

## History

Throughout the years EY was formed by merging with other organizations several times. The oldest originating partnership was founded in 1849 in England. In 1989 the fourth largest accountancy firm (Ernst & Whinney) merged with the fifth largest (Arthur Young) to create Ernst & Young. [2]



Figure 3: Logo Arthur Young [8]

Figure 2: Logo Ernst & Whinney [7]

At one point in time there were even plans to merge with KPMG (current member of the big four), but those plans were abandoned due to the difficulty of merging two diverse companies and cultures.

Today EY is still looking for opportunities to further expand and improve the quality of its services. One of the fastest expanding sectors is the cybersecurity, especially with the recent announcement of the General Data Protection Regulation (GDPR)[[1]](#footnote-1) [3]. These regulations are effective from May 2018. These are intended to unify data protection for enterprises within the EU. Organizations all over the EU are rushing to meet these requirement and ask companies like EY to accompany them in this process.

## Structure

### Geographical

EY groups their offices by geographical location into four areas. Each of these areas is then divided into more local areas. [2]

* **EMEIA (Europe, Middle East, India and Africa)**
  + Africa



Figure 4: EY’s company profile (EMEIA) [5]

* + **BeNe (Belgium and The Netherlands)**
  + CIS
  + CSE
  + FraMaLux
  + GSA
  + India
  + Ireland
  + Mediterranean
  + MENA
  + Nordics
  + UK
* Americas
* Asia-Pacific
* Japan

### Organizational

EY offers multiple services to companies world-wide. These services are grouped into four major service-lines:

* **Tax**: provide information about (global) tax infrastructure.
* **Transaction advisory services**: provides information regarding raising, investing, preserving and optimizing the organizations capital.
* **Assurance**: provides general financial information.
* **Advisory**: provide clients with information regarding risk management and performance improvement.

The advisory service-line facilitates the cybersecurity service in which this internship took place. The cybersecurity service is officially split into multiple services (business resilience, data privacy, cyber threat management) but members of the cyber security team can take assignments in any of these services.

Other services provided by the advisory branch are:

* IT Transformation
* Data Analytics
* Finance
* Supply Chain
* Customer & Strategy
* People Advisory Services
* Risk Management
* Internal Audit & Controls
* Risk Transformation
* **Cybersecurity**
  + Cyber Program Management
  + Cyber Threat Management
  + Identity & Access Management
  + Data Protection & Privacy
  + Business Resilience
  + Business Continuity
  + Incident Response (IR)
* IT Assurance

### Financial sector

EY has clients from very varying sectors, the financial sector covers the most part of the clients.

The whole above mentioned structure exists in duplicate. Once for clients in the financial sector (FSO) and once for clients of non-financial sectors (NON-FSO). This internship took place in the NON-FSO branch of EY.

### Summary

To get a better perspective where the internship took place within the complex organizational structure of EY the following flowchart was created.

## Big four

This is a group of the world largest professional service networks. EY is accompanied in this group by PwC, DeLoitte and KPMG. The group originally consisted of eight members but the group was reduced to four members after several merges and scandals. [4]

EY differs itself from the other members of the big four by being the most globally managed firm of the four. EY has defined a set of policies to assure consistency of services globally. This globalization is clearly visible in the daily working of the company. Desks are shared between colleagues of various nationalities, all employees get the chance to work together with colleagues with a complete different culture which results in a very dynamic, coherent and educational work experience.

## Students

EY invests a lot into the potential of students, throughout the year there are numerous internships offered in all the different services offered by EY. This is why EY is in the top of several rankings like: “best places to launch a career”, “Ideal employers” etc.

# Internship and thesis

Today more and more services are offered as a web applications and no longer as a software distribution (that has to be installed and configured by the user). Web applications are easier to develop, flexible, independent from the operating system of the user and can be accessed from everywhere. But it has one major pitfall, they are very susceptible to cyber-attacks. Attackers can perform a devastating attack (from everywhere) on a web application developed by a less experienced developer which didn’t implement all the required security measures. Inexperienced developers are the main source of web application vulnerabilities. This is where the web application firewall comes in. This device can protect (multiple) web applications from attacks. It does this by recognizing specific patterns in requests that could be part of an attack and preventing this malicious from reaching the web application. For example: requests that contain JavaScript code in the query string can be blocked to prevent XSS, requests that contain the MySQL ‘UNION’ statement can be blocked to prevent SQL-Injection.

The web application firewall looks like perfect solution in preventing web based cyber-attacks but it has its downsides. The biggest flaw is that they are really difficult to configure in order to function correctly. What if a certain application requires JavaScript code in the query string or the MySQL UNION statement? These are normally blocked by the web application firewall and thus will prevent the web application from functioning correctly. This frustration among developers can lead to full out disabling the web application firewall making all the web applications vulnerable again. This is a situation that the cybersecurity team of EY has encountered multiple times.

In order to eliminate the complex process of configuring the static rules, a web application firewall based on anomaly detection can be deployed. This type of firewall doesn’t need any static configuration but will “learn” what type of requests are safe/legitimate and which are malicious. It does this by first observing legitimate requests (profiling of the application) and then later comparing an incoming request with the profile of legitimate requests to determine if the request can be marked as legitimate. Malicious requests will be blocked because they show certain differences with the profiled (legitimate) requests. This kind of mindset will not only adapt itself when the web application changes but should also able to detect zero-day attacks.

During this internship an application profiler and anomaly detection engine will be developed in order to proof the power of this type of web application firewall. EY would like to gather information about this kind of firewalls before organizations start to deploy these.

The following flowchart will illustrate the working of the proof of concept.

Anomaly Detection engine

SAFE

REQUEST 1

MALICIOUS (Non numerical)

REQUEST 3

MALICIOUS (Non numerical)

REQUEST 2

MALICIOUS (Much more requests/hour)

REQUEST 5

MALICIOUS (Unfamiliar location)

REQUEST 6

MALICIOUS (Much longer than average)

REQUEST 4

Average length page value is 2

index.php

Page value is numerical

index.php

+/- 25 Request/hour

index.php

Traffic normaly originates from within BeNeLux

index.php

1000 x index.php

REQUEST 5

Index.php?page=a4e

REQUEST 5

index.php?page=4612356

REQUEST 4

From: Canada

REQUEST 6

Index.php?page=a4e

REQUEST 5

index.php?page=a4e

REQUEST 2

index.php?page=’OR1=1#

REQUEST 3

index.php?page=4

REQUEST 1

# References

|  |  |
| --- | --- |
| [1] | EY, „EY,” EY, [Online]. Available: http://www.ey.com/be/en/home. [Geopend 07 February 2017]. |
| [2] | Wikipedia, „Ernst & Young,” Wikipedia, 07 February 2017. [Online]. Available: https://en.wikipedia.org/wiki/Ernst\_%26\_Young. [Geopend 07 February 2017]. |
| [3] | Wikipedia, „General Data Protection Regulation,” Wikipedia, 24 January 2017. [Online]. Available: https://en.wikipedia.org/wiki/General\_Data\_Protection\_Regulation. [Geopend 08 February 2017]. |
| [4] | Wikipedia, „Big Four accounting firms,” Wikipedia, 06 February 2017. [Online]. Available: https://en.wikipedia.org/wiki/Big\_Four\_accounting\_firms. [Geopend 07 February 2017]. |
| [5] | EY, „EY Corporate Presenation,” May 2015. [Online]. Available: http://images.slideplayer.com/24/7228379/slides/slide\_3.jpg. [Geopend 1 March 2017]. |
| [6] | EY, „EY Logo,” [Online]. Available: http://www.ey.com/ecimages/EY.gif. [Geopend 1 March 2017]. |
| [7] | Erns & Whinney, „Erns & Whinney Logo,” [Online]. Available: http://userscontent2.emaze.com/images/86dbf6c2-1ab1-4300-b458-0e0c31ce5ac3/635348645831478302\_EWlogo.jpg. [Geopend 1 March 2017]. |
| [8] | Arthur Young, „Arthur Young Logo,” [Online]. Available: https://res.cloudinary.com/crunchbase-production/image/upload/v1457147586/eve4v8gr0liwkkhbvtqw.jpg. [Geopend 1 March 2017]. |

1. The primary objective is to give citizens back the control of their personal data. Enterprises that are not complied with this new regulations will risk a fine of 4% of their annual revenue. [↑](#footnote-ref-1)