BRIAN VERMEER (@BRIANVERM)

DON'T BE A TROJAN

J2D

DATA IS THE NEW GOLD

Google Analytics

Sign out

Account My Store

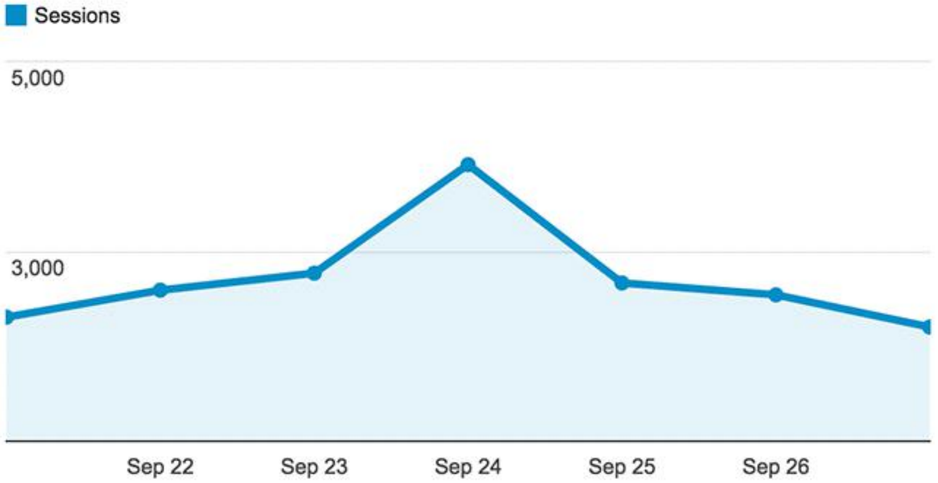
Property My Store

View All Web Site Data

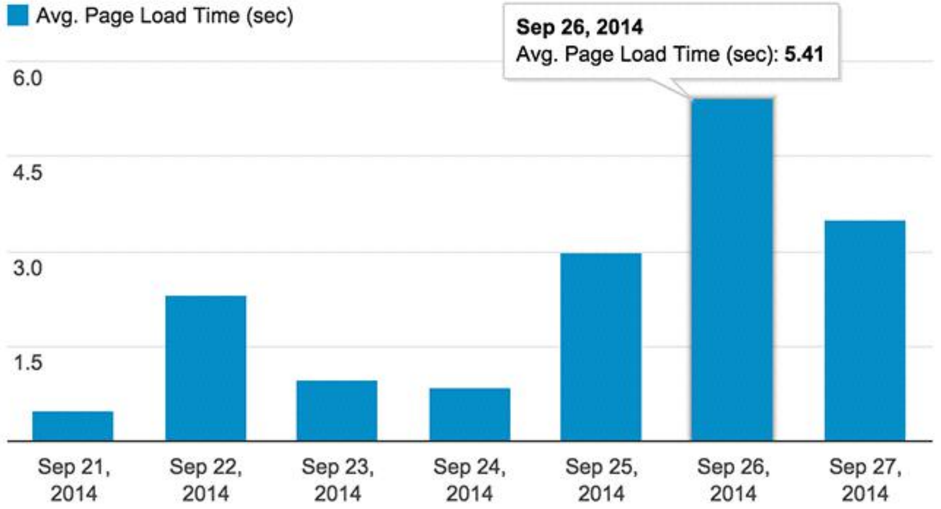
Start Date 09/21/2014

End Date 09/27/2014

Site Traffic

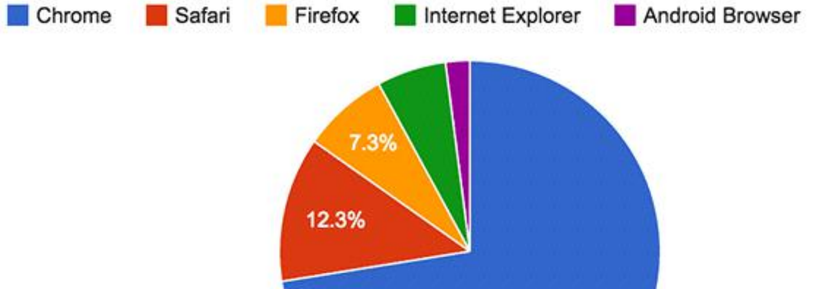


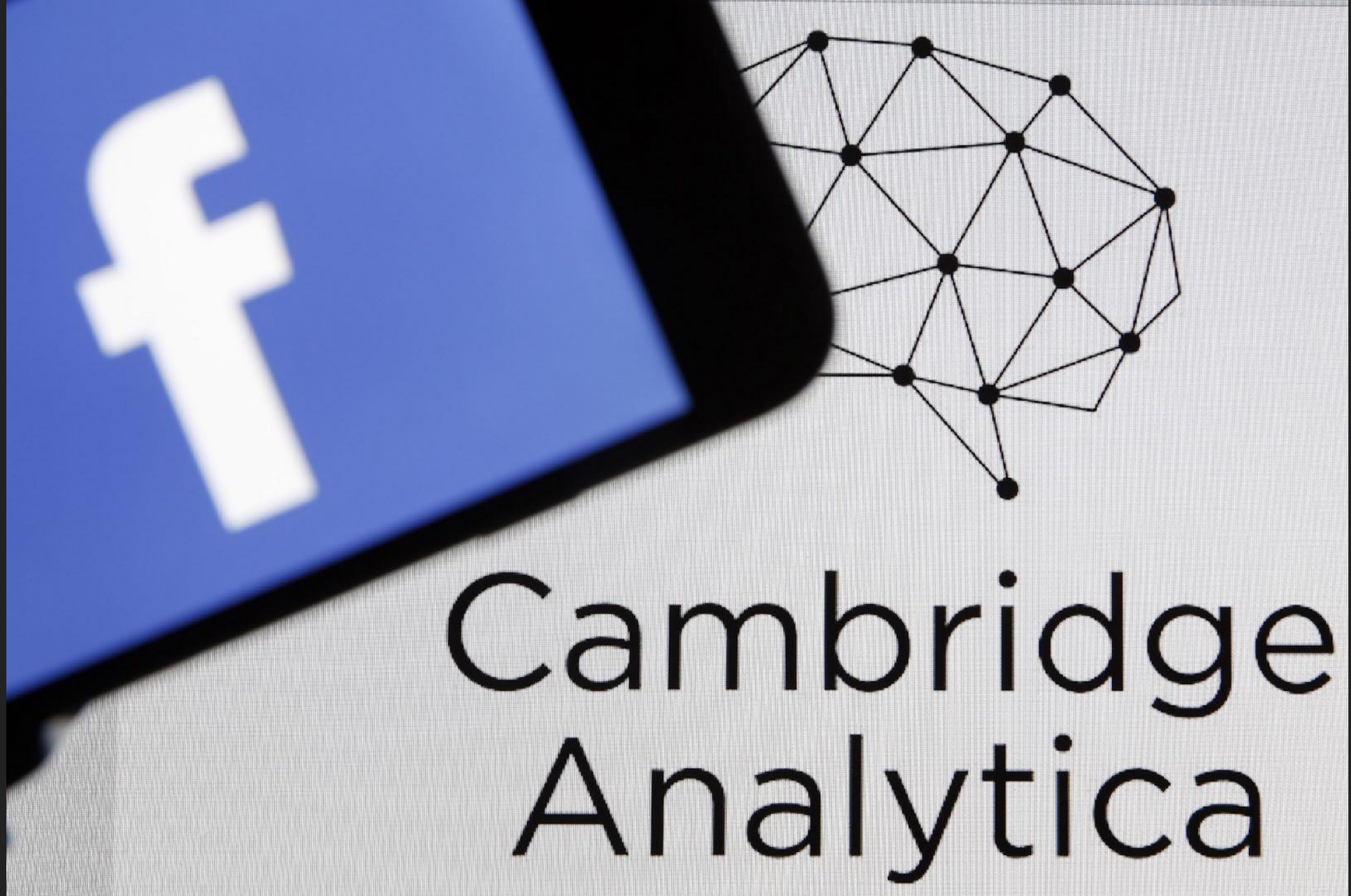
Average Page Load Times



Users by Country

Pageviews by Browser




Cambridge
Analytica

blue4IT

BRIAN VERMEER

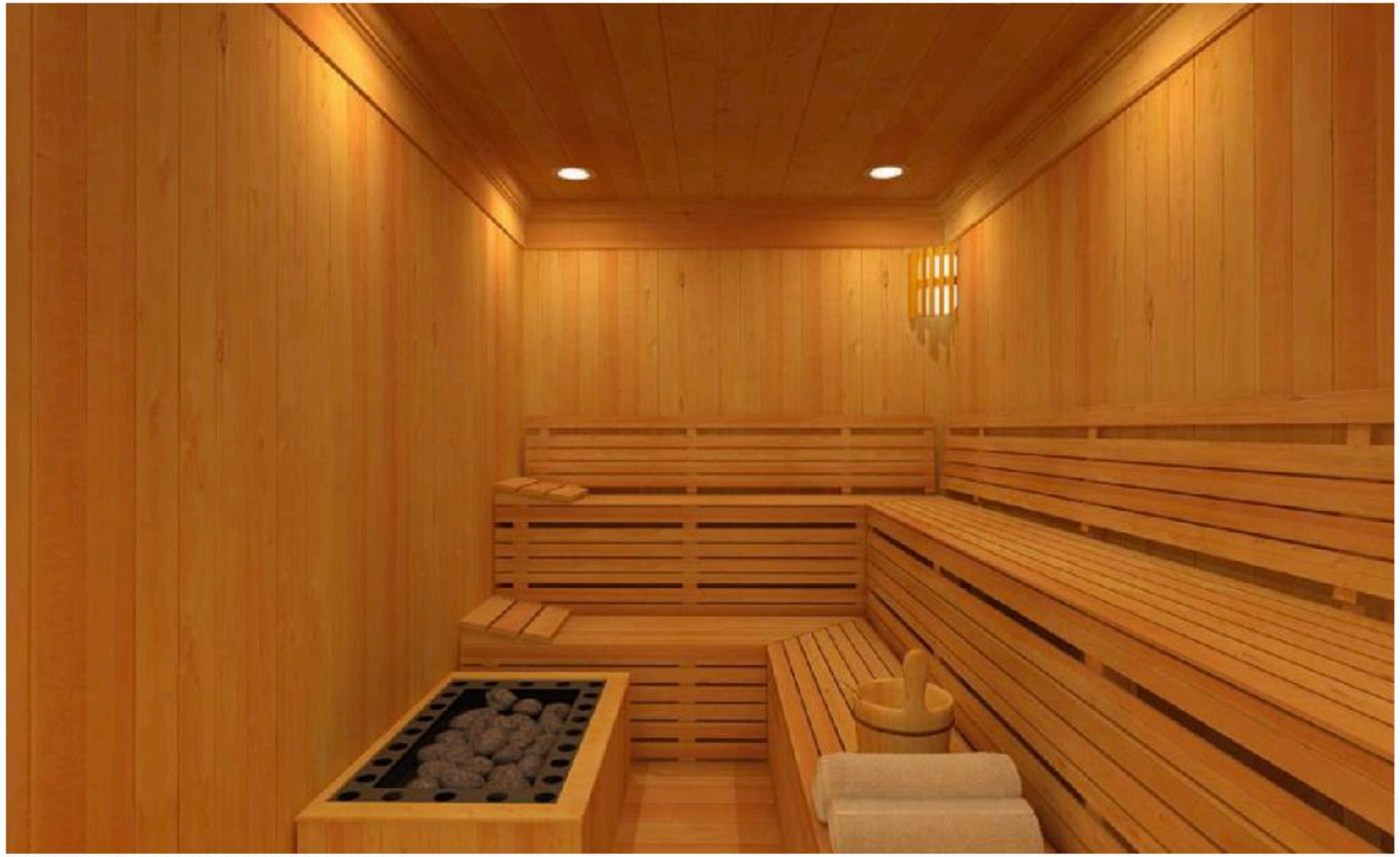
SOFTWARE ENGINEER

ORACLE
Developer
Champion

BUT I GOT NOTHING TO HIDE . . .

NUDE VIDEOS OF DUTCH HANDBALL TEAM LEAK ONLINE AFTER SAUNA CAMERA HACK

By Janene Pieters on March 8, 2018 - 09:41

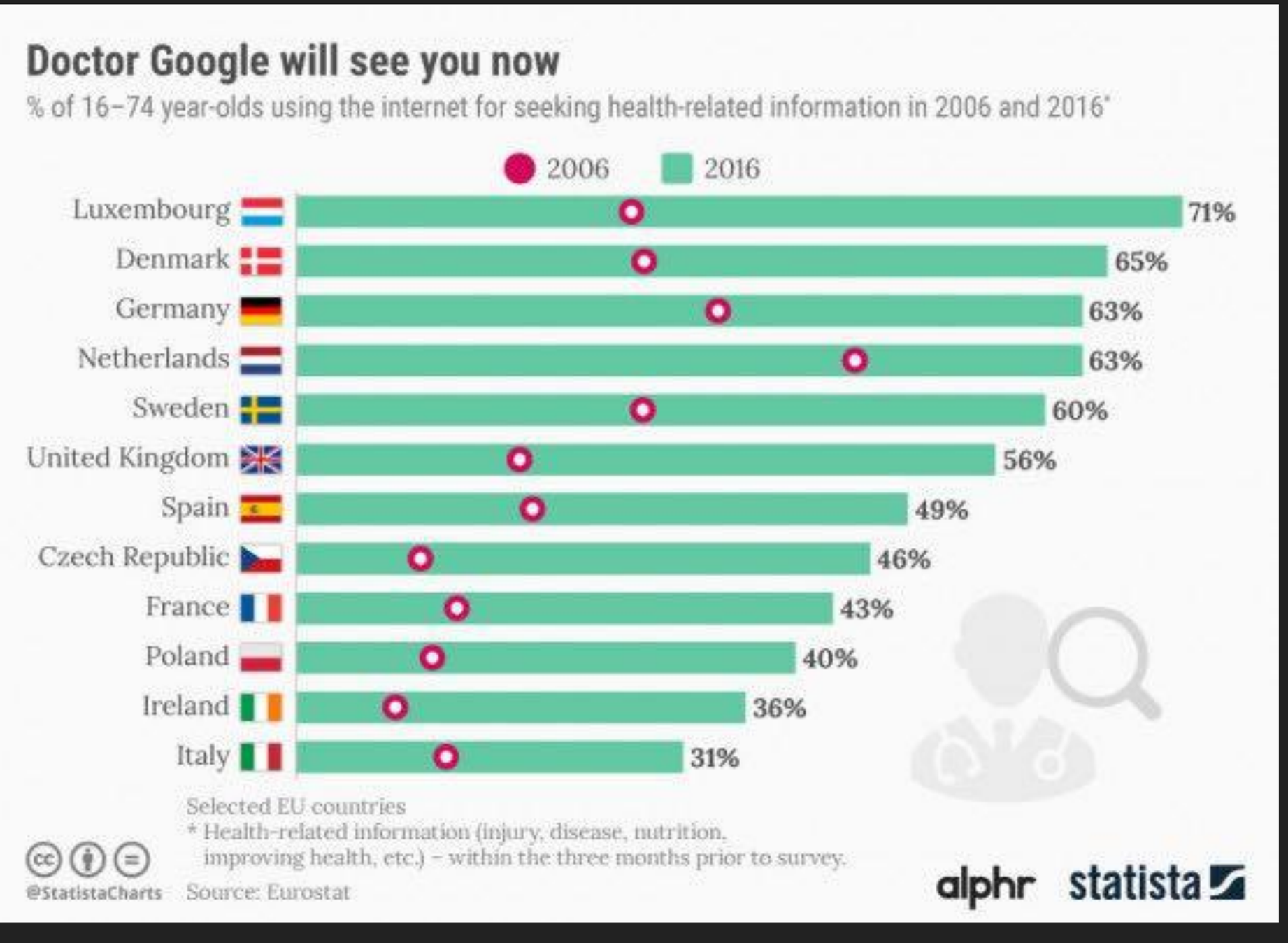


Sauna. Photo: Todtanis / Wikimedia Commons

Videos of the Dutch women's handball team naked in a dressing room of sauna Oase in Nederasselt, were posted on a popular porn website for several hours in December. According to sauna owner Erik van Ingen Schenau, the surveillance cameras were hacked, the Gelderlander reports.

Criminals hacked the surveillance cameras in 2015, but only posted the footage online late last year. The hackers immediately told the owner that the cameras were hacked. "I received a mail containing a photo, a still from a video of one of the security cameras", he said to the newspaper. "With the warning that the

HTTPS://NLTIMES.NL/2018/03/08/NUDE-VIDEOS-DUTCH-HANDBALL-TEAM-LEAK-ONLINE-SAUNA-CAMERA-HACK



HTTP://WWW.ALPHR.COM/HEALTH/1005587/THE-NUMBER-OF-PEOPLE-ASKING-GOOGLE-FOR-MEDICAL-ADVICE-HAS-SKYROCKETED-IN-A-DECADE

SOCIAL RANKING CHINA

CYBERCRIME

REAL THREAT
AND IT IS GROWING

ORGANISED AND PROFESSIONAL
IT'S A BUSINESS

RISKS ARE LOW

WE ARE NOT READY

LOT OF MONEY INVOLVED

HOW PROFITABLE IS CYBERCRIME?

Bank of Iraq Heist (2003)
1 Billion dollars

US Military and Defence Expanses (2015)
600 Billion dollars

Cyber crime damage world wide (2016)
3 Trillion dollars


CONFIDENTIALITY
AVAILABILITY
CIA
TRIAD
INTEGRITY

BUT NOW WE HAVE GDPR...RIGHT?!

HTTPS://FUSION.TV/STORY/281543/REAL-FUTURE-EPISODE-8-HACK-ATTACK/?CURATOR=TECHREDEF KEVIN ROOSE - 24 FEB 2016

Nice to Kn

Naomi Surug

Inbox

Dear Beloved Frier
I know this messag
business relationsh
I am Miss Naomi S
murdered during th
was a strong suppo
Meanwhile before
USD4, 200,000.00
West Africa for safe
I am here seeking
trustworthy person
my parent`s and I v
purpose.
Please I will offer y
transfer the fund u
country due to the
medical student be
email:missnaomisu
Remain blessed,
Miss Naomi Surugaba.

Bank of America

nline Banking account,

ccount indefinitely, as
tion in this manner.

Onderwerp: Reset iConnect WiFi instellingen

Rabobank

RaboWeb
Mens & Middelen IT Portaal

Beste Simon ,
Vanwege onderhoudswerkzaamheden zijn jouw inloggegevens gereset. Om ook in de toekomst gebruik te kunnen blijven maken van Wifi vragen wij je om de inloggegevens binnen 48 uur te updaten. Maak daarvoor gebruik van de volgende link: iConnect WIFI Access Point Setup .
Met vriendelijke groeten,
ITN Infra Support

==========

Rabobank disclaimer: http://www.rabobank.nl/disclaimer


Toshiba Personal Computer (R1400GR)
Copyright 1984,85 Toshiba Corporation
MS-DOS Ver 2.11
Copyright 1983,84 Microsoft Corp.
Command Ver 2.11
A>echo off
Bitte etwas Geduld,
bin nicht mehr der Jüngste...

LAPTOP

PASSWORDS


DEVOPS


TEST DATA

THE “NEW GUY”

SCENARIO

DEVELOPMENT

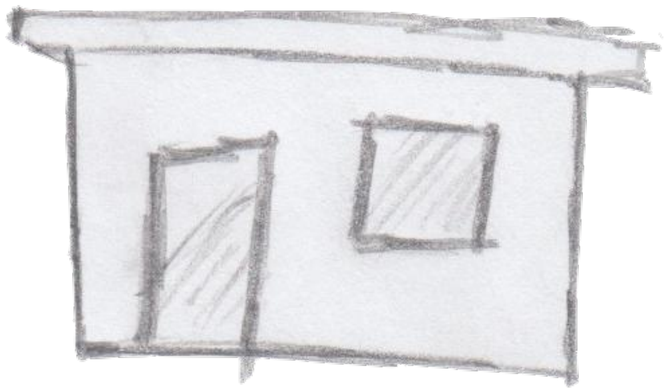
SECURITY BY DESIGN

DATA STORAGE

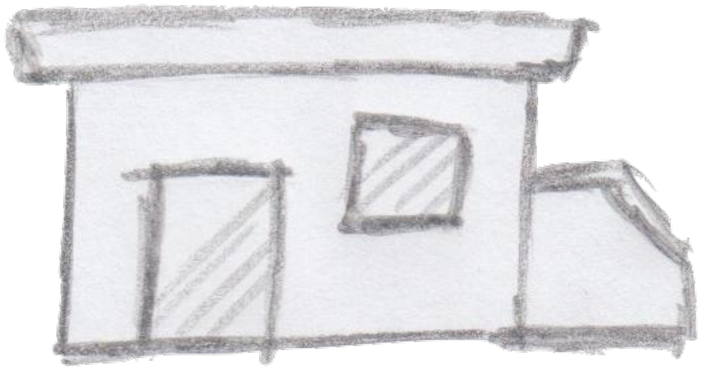
- WHAT DATA DO WE STORE?
- WHAT DATA DO WE NEED?
- HOW LONG DO WE NEED TO KEEP THIS DATA?
- HOW DOES THIS DATA TRACE BACK TO AN INDIVIDUAL?
- WHO HAS ACCESS TO THIS DATA

SOFTWARE DEVELOPMENT OVER TIME

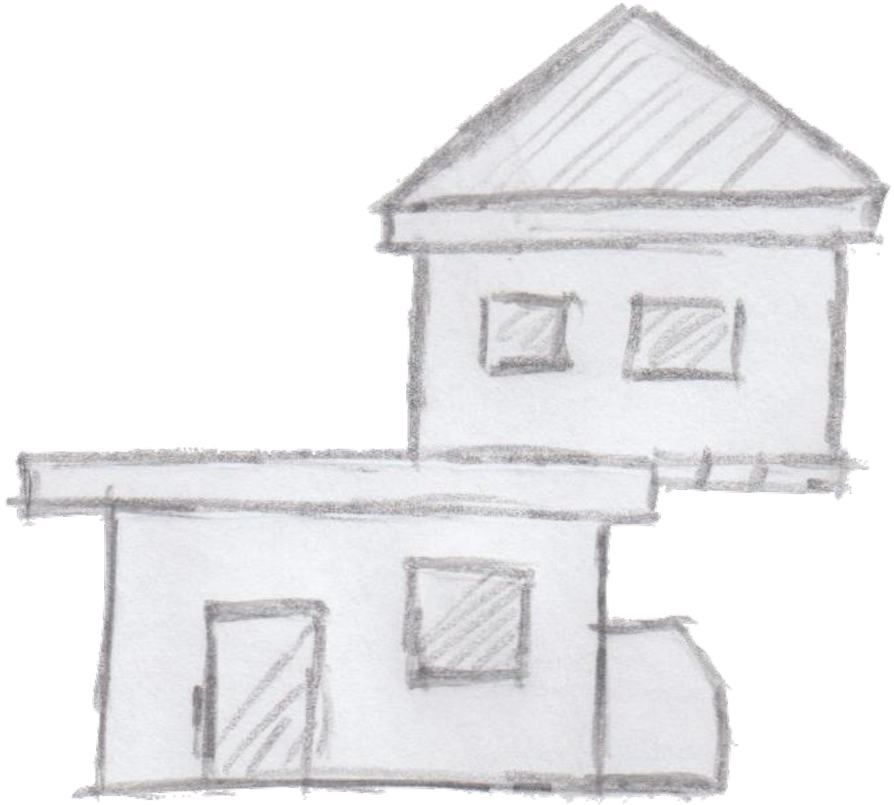
STAGE 1 – BUILD A NICE CLEAN SYSTEM



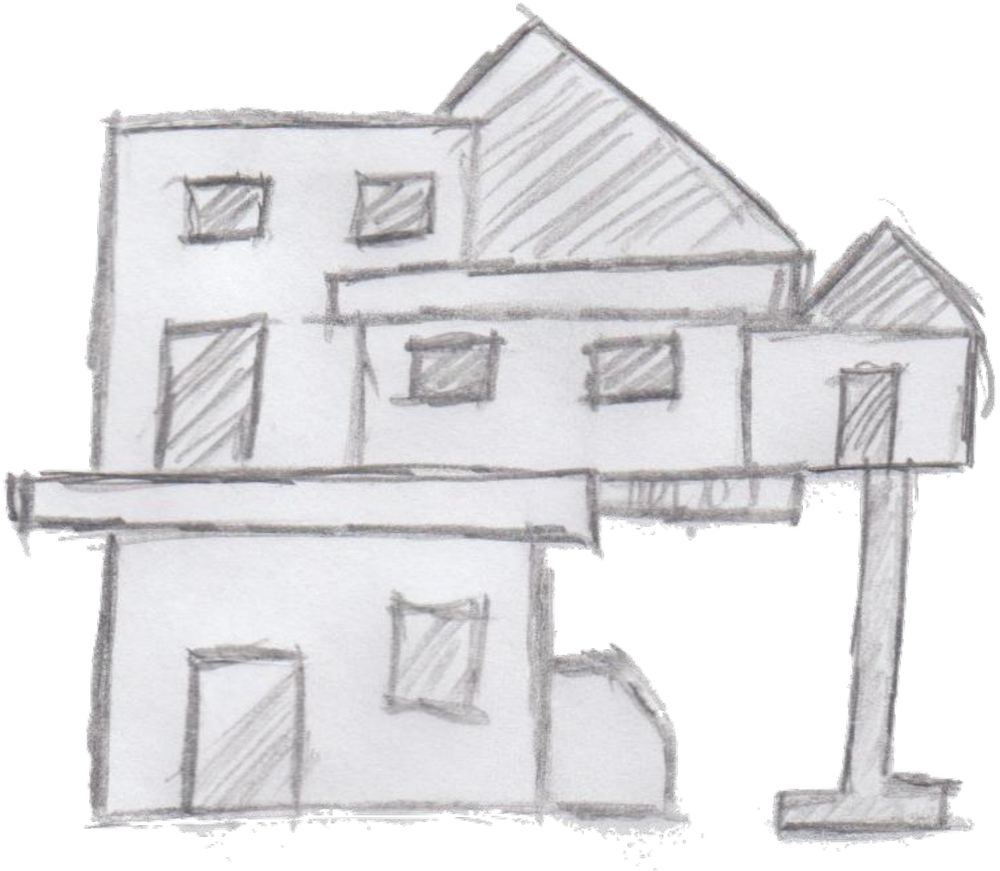
STAGE 2 – A LITTLE ADDITION



STAGE 3 – A COMPLETE NEW FEATURE ON TOP

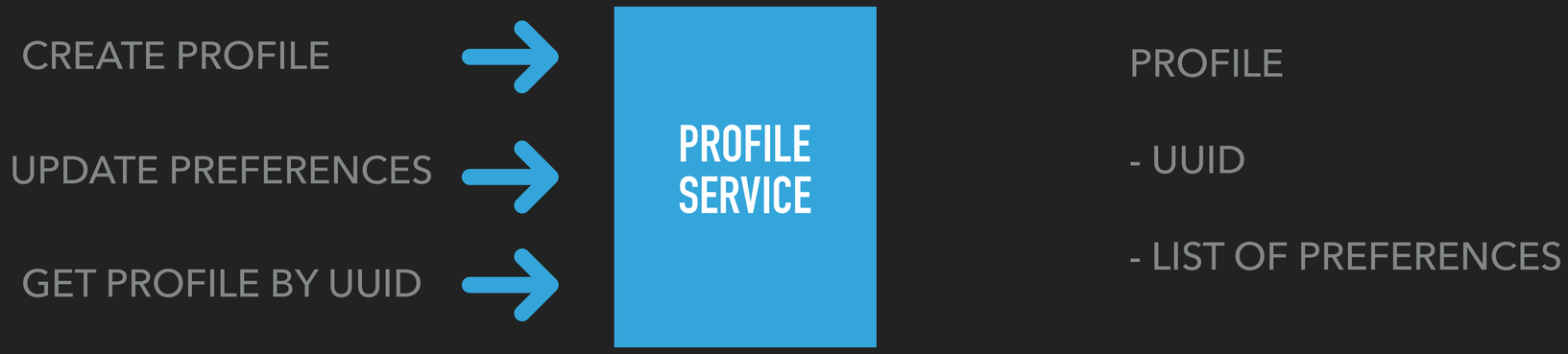


STAGE 4 – EXPANDING WITH A NEW SCOPE



STAGE 5 – AND NOW WE WANT TO RULE THE WORLD

EXAMPLE


CREATE PROFILE
UPDATE PREFERENCES
GET PROFILE BY UUID
PROFILE SERVICE
PROFILE
- UUID
- LIST OF PREFERENCES

EXAMPLE

CREATE PROFILE

UPDATE PREFERENCES

GET PROFILE BY UUID

SECURED LOGIN

PROFILE SERVICE

PROFILE

- UUID
- EMAIL
- LIST OF PREFERENCES

CLAIM A HOUSE

UPDATE YOUR HOUSE

FIND ALL HOUSES

MYHOME SERVICE

MyHOUSE

- UUID
- HOUSE ADDRESS
- HOUSE PICTURES

EXAMPLE

GET PROFILE BY UUID

PROFILE SERVICE

PROFILE

- UUID
- EMAIL
- LIST OF PREFERENCES

FIND ALL HOUSES

MYHOME SERVICE

MyHOUSE

- UUID (EXPOSED)
- HOUSE ADDRESS
- HOUSE PICTURES

WHAT DATA IS EXPOSED TO THE OUTSIDE WORLD

DATA LEAK?

WHO WAS EXPOSED?

HOW LONG WAS IT THERE?

WHAT WAS THE IMPACT?

WHAT KIND OF DATA IS LEAKED?

AM I A VICTIM?

LOG EVERYTHING

BUT WHAT ABOUT CI/CD ?

AUTOMATED SECURITY TESTS

```
977             <exclusions>
978                 <exclusion>
979                     <groupId>commons-logging</groupId>
980                     <artifactId>commons-logging</artifactId>
981                 </exclusion>
982                 <exclusion>
983                     <groupId>commons-beanutils</groupId>
984                     <artifactId>commons-beanutils</artifactId>
985                 </exclusion>
986             </exclusions>
987         </dependency>
988         <dependency>
989             <groupId>net.sf.dozer</groupId>
990             <artifactId>dozer</artifactId>
991             <version>5.4.0</version>
992             <!-- 5.5.0: separate dozer-spring artifact -->
993             <exclusions>
994                 <exclusion>
995                     <groupId>org.slf4j</groupId>
996                     <artifactId>slf4j-log4j12</artifactId>
997                 </exclusion>
998             </exclusions>
999         </dependency>
1000        <dependency>
1001            <groupId>javax.ws.rs</groupId>
1002            <artifactId>jsr311-api</artifactId>
1003            <version>${jsr311-api.version}</version>
1004            <scope>provided</scope>
1005        </dependency>
1006        <dependency>
1007            <groupId>javax.ws.rs</groupId>
1008            <artifactId>javax.ws.rs-api</artifactId>
1009            <version>${rs-api.version}</version>
1010        </dependency>
1011        <dependency>
1012            <groupId>org.glassfish.jersey</groupId>
1013            <artifactId>jersey-bom</artifactId>
1014            <version>${jersey.version}</version>
1015            <type>pom</type>
1016            <scope>import</scope>
1017        </dependency>
1018        <dependency>
1019            <groupId>org.hibernate</groupId>
1020            <artifactId>hibernate-validator</artifactId>
1021            <version>${hibernate-validator.version}</version>
1022        </dependency>
1023        <dependency>
```

DEPENDENCIES

WHATS IN IT

CODE REVIEW

CODE REVIEW

```
@GetMapping(path="/all")
public List<MyHouse> getAllHouses() {
   return MyHouseRepository.findAll();
}

public class MyHouse {
   @Id private String id;
   private Date creationDate;
   private Date modificationDate;
   private String userId;
   private String street;
   private Integer number;
   private String zip;
   private String city;
}
```

CODE REVIEW

```
@GetMapping(path="/all")
public List<MyHouse> getAllHouses() {
   return MyHouseRepository.findAll();
}

public class MyHouse {
   @Id private String id;
   private Date creationDate;
   private Date modificationDate;
   @JsonIgnore private String userId;
   private String street;
   private Integer number;
   private String zip;
   private String city;
}
```

DESIGN TO BE COMPROMISED

PASSWORD PROTECTION

- Use a password policy
- Use a cryptographically strong credential-specific salt
- Use a cryptographic hash algorithm (e.g. PBKDF2 / bCrypt)
- Use a HMAC (keyed-hash message authentication code), HMAC-SHA256
- Review algorithms

CENTRALIZED LOGGING AND ALERT ON IT

WORK TOGETHER WITH SECURITY DEPARTMENT

BRIAN VERMEER

@BRIANVERM

BRIAN@BRIANVERMEER.NL

blue4IT