KRY LIVI

# Security at KRY/LIVI

## Guest lecture

Chalmers
29 April

**Carl Svensson**
Head of Security
carl@kry.se

# Agenda

## Biography: KRY/LIVI & I

Who am I? How did I end up here?

What do we do? How are we fast forwarding the future of healthcare?

## GDPR and friends

How did we work with GDPR and how do we keep up with compliance in a heavily regulated field?

## IT Security & appsec

How do we design and maintain systems and processes with the patient first while still being able to use data and stay competitive?

## Startup security

What does it look like to work with security at a small fast-paced company?

## Privacy by design

How do we design and maintain systems and processes with the patient first while still being able to use data and stay competitive?

## The next steps

Where are we heading?

Where are you heading? How do you become an expert?

# Bio: Carl

Who am I? What do I do here?

# Carl Svensson, Head of Security

- Programming
- Engineering physics @ KTH
- Security consultant @ Bitsec
- CTF, HackingForSoju

# Bio: KRY/LIVI

Who are we? What do we do?

Chapter 1b

# KRY/LIVI - Digital healthcare

- For patients, by patients
- See a clinician via video
- 1 000 000+ patients
- Five countries

# Startup security

Aka. wtf is an AnyJson object?

Chapter 2

# Initial steps - Fundamentals

## Centralized logging

Before: Logs were only stored on each respective server. Developers had to SSH into each machine to find the right log

After: Logs are accessible from CloudWatch

## Individual SSH accounts

Before: Developers used a single shared SSH account to log into servers.

After: Each developer uses their own account for improved access control and auditability.

## Typed code

Before: AnyJson doThing(AnyJson input) { ...

After: ClassA doThing(ClassB input) { ...

## Pentest follow-up

Before: Looks good but you have this XSS

After: Fix the same XSS in 20 places

I AM EMPLOYEE NUMBER

# 35

# Moving on - Recent projects

## Granular access control

Before: Everyone have access all the time

After: Access is requested and approved

## Audit tooling

Before: Look through logs manually to find suspicious behaviour.

After: Automated systems to help pinpoint areas of interest.

## Automated vuln mgmt

Before: Security team delegates tasks

After: Tool informs devs directly of vulnerable versions

# GDPR & friends

How I learned information security

Chapter 3

# Ugh, legal stuff...

Why and how does knowledge about neighbouring topics make you a better security professional?

# How to legal in 1 minutes

Laws and rules are kind of like code

Except it isn’t actually

Read! Don’t speculate

Reason, motivate, document

# 1 Country = 1 Framework

## Why the GDPR is such a gift

| Sweden | Norway | France | Germany | United Kingdom |
| --- | --- | --- | --- | --- |
| Patient data act | Norm for information security in the health sector | HDS/HADS | A lot of laws | ¯_(ツ)_/¯ |

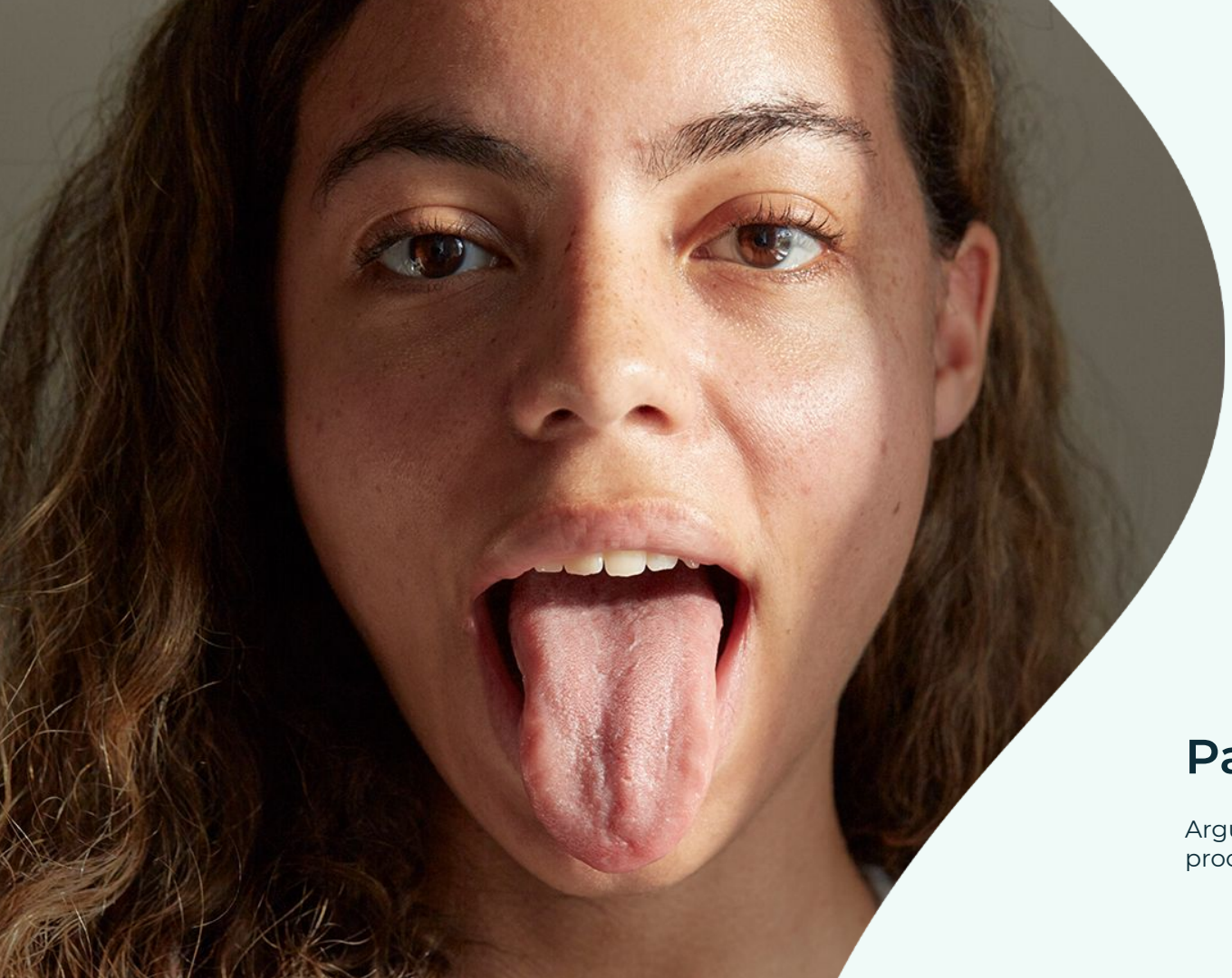
Not all failures are all bad

# R.I.P. VIDA

# Privacy by design

“Patient first” in practice

Chapter 4



# Patient data

Arguably the most sensitive data you can process. How can we do it in a safe way?

# Personal data

Basic information about a person

# Medical data

Sensitive personal data

# Medical records

Part of an electronic medical record, EMR

# IT security & appsec

“Patient first” in practice

Chapter 5

# Application security

Process - Plan, execute, review

Assurance - Types and/or tests

Architecture - Disassembling the monolith

Langsec - Full recognition before processing

# Incident response

How do we deal with issues and escalation?

# The next steps

The future for KRY/LIVI? For you?

Chapter 6

*Where do we go?*
*Where do we go now?*
*Where do we go?*
*Oh, oh*
*Where do we go?*
*(Where do we go now?)*

**Axl Rose**

NUMBER OF EMPLOYEES TODAY

# 500+

# Access controls

EVERY UNWARRANTED ACCESS IS A UNNEEDED LIABILITY

# Formalisation

THE COLLECTIVE KNOWLEDGE IS FRAGILE

# Monitoring

INSIGHT INTO A LARGE SYSTEM REQUIRES TOOLING

# How to get better

## Capture the Flag

PicoCTF.com - Beginner friendly CTF
CTFTime.org - Competition calendar & world ranking
https://gist.github.com/ZetaTwo/40976c9ed8b9abb81e44c872b3a68551 - Tools

## Blogs, articles, YouTube

https://youtube.com/LiveOverflowCTF
https://youtube.com/ZetaTwo
https://youtube.com/GynvaelEN

## Social media, Twitter

https://twitter.com/ZetaTwo
https://twitter.com/swiftonsecurity
https://twitter.com/cybergibbons
etc.

## Conferences and meetups

Security Fest
SEC-T
OWASP

# We are recruiting

We're on a mission to  build better and more accessible healthcare to alleviate the pressure that growing populations have on traditional medical support models. We are moving fast and we are doing this together. Care to join our journey?

https://career.kry.se
E-mail: carl@kry.se

- Full time positions
- Part time positions
- Master’s thesis
- Summer internships

KRY LIVI

# Thank you for listening

Good luck!

Chalmers
29 April

**Carl Svensson**
Head of Security
carl@kry.se