Surviving the security challenges in a SME

From a viewpoint of a security and data protection responsible

Miloš Božović, CISO
Zürich, 27.06.2022

Agenda

1
Brief intro of the company

2
Brief intro of me

3
What can happen

4
We all probably know, what has to be done

5
Why can’t we just do it

Brief intro of the company

localsearch helps to make Swiss SMEs successful in the digital world. As a company with its roots in the printed telephone book, we are now the established partner for Swiss SMEs in all matters digital. Our innovative solutions help you professionally present and establish your business and your products and services on the digital marketplace. In this way, your customers will find, view, book, buy and like what you have to offer.

> 600+ employees
> Internal developers for several platforms such as search.ch and local.ch but also external development through specialised companies
> Is a 100% daughter company of Swisscom (Schweiz) AG
> Handling a lot of personally identifiable information (PII)

Our platforms →

Platforms

local.ch
local.ch is Switzerland's No. 1 for finding detailed information about companies and services as well as telephone numbers.

search.ch
search.ch offers detailed company information and helpful functions such as route and leisure planners, public transport timetables and tickets, as well as weather information.

renovero
renovero is Switzerland's leading platform for tradespeople – the easy way to connect qualified tradespeople with clients!

Vergleich CH
Our universe of 55 comparison platforms encompasses over 140,000 providers from the beauty, health, crafts, lifestyle and business sectors.

Localcities
Localcities is Switzerland's most attractive and up-to-date platform for municipalities.

Third-party platforms

Brief intro of me

I've been interested in all tech things since my early years and so it came naturally that I chose to study and work in more or less tech related areas.

During my time at PwC, I discovered the interest for information security and started a post-diploma study in information security. From this point in time, I was only working in security related jobs, which eventually led to become the CISO of localsearch.

In my free time I enjoy my family life but I am still (what a cliché) an avid gamer, cyclist and classic car enthusiast, among other things.

> Lives in Zurich

> With Swisscom since 2013

> Studied Communications & Informatics in Winterthur and obtained Master of Studies in Information Security in Lucerne

> If you meet me on the bicycle, say hi! :-)

What can happen

Big company

Well, *everything* can happen. You just have to make sure that it does not. It's as simple as that.
And that's a problem, because you will *never* cover all of the threats.

Yeah, I know. This does not really help. So let's take a look at a bigger company.

Imagine what working for a big company *might* look like:

- Lots of defined processes
- Strong governance allowing or disallowing specific behaviour or connections to the outside world
- Maybe a big and strong IT department and in addition several people responsible for things like Information Security or data protection.
- Lots of operative security tasks such as monitoring and alerting with a SIEM-tool or maybe you have a SOC or even some automated solution, which helps you find the unknowns.
- Engineering or operations can assist in mitigating the risks

What can happen

Small company

Eventually, something *will* happen. The question is: Will you be able to detect it in the first place?
And will you be able to do something about it yourself?

Now, let's take a look at a small company.

Imagine what working for a small company *might* look like:

- Little to none defined processes or individuall processes for each department
- Weak governance allowing or disallowing specific behaviour or connections to the outside world
- Probably a small IT department (or outsourced IT) and in addition no dedicated responsibles for neither Information Security nor data protection.
- Lots of operative security tasks should be done, but there is noone to do them. Maybe, there are problems, but you are too «blind» to see what is currently going on in your network/cloud.
- Engineering or operations are busy with their own tasks or it is plainly too expensive to hire someone.

What can happen

How one incident happened

So let me tell you about an incident that we had some years ago.

- All of a sudden, mails started appearing, coming from an employee, asking other to open some document. It was classic phishing but from an internal address!
- Mail engineering noticed and alarmed me.
- By coincidence, I knew that the employee in question actually left the company some weeks prior.
- We started investigating, who might have clicked the link (review of logs and actions within O365)
- We started resetting these AD-passwords
- Soon, more mails appeared. We started resetting everyones AD-password.
- This seemed to work. For a day or two.
- Then the mails started coming again.
- We had to implement 2FA over night.
- This seemed to stop the issues but brought other issues like people who could not log in.
- Meanwhile, investigations were started to find the source of the problems and why it was possible.
- In parallel, we had to deal with announcing possible data leaks to the authorities (it seems like only a handful of people were affected)
- Mid-term solutions had to be found and implemented.

We all probably know, what has to be done

What we did

- After 2FA was in place, everything was rather quiet.
  - 2FA because accounts cannot be compromised as easily and we had several accounts compromised
- Nevertheless, we started **checking "risky sign-ins**" in O365 and reset the passwords of the users if they fall in this category
- We did a **hardening of the O365** environment
- We started building up internal "**Security Operations**"
  - Because before we lacked an organisation who could deal with such issues. Thus we had to hire expensive specialists
- We started building up a "**Centralised Logging**" solution
  - The specialists only found traces of several attack preparations and attempts but due to the **lack of logs (no logs, wrong logs, overwritten logs)** it could not be pinpointed to a specific source. We only know that all might have begun **up to four months prior to the incident** that we detected
- We conducted several audits and penetration tests of important systems and applications and started working on mitigating actions
- We conducted a ransomware check and started working on the findings
- We started building up a new inventory solution (with automated discovery functions)
- We are about to deploy a managed and automated security solution to help us find things within our network/cloud environment!
- All of these actions came to mind after the incident (and some more) but in a small company, it can take a lot of time to implement such measures. So we have been working on these things ever since, and will continue working
- Similar things have to be deployed for the diverse cloud solutions, too!

We all probably know, what has to be done

Some take aways from the incident (not sorted according to priority)

- Having some logs is better than having no logs at all
- Having external specialists is good, but it costs a lot. Establish a strategy of what you want to do yourself and what you want to hire others for.
- Participate in a bug bounty programme, if possible, because this can help you find issues with your external posture
- Try to scan your external perimeter for vulnerabilities (Check your DKIM/SPF/DMARC records ;)
- Activate 2FA for everyone (!) and make it mandatory (conditional access)
- Remove internet access for the server network (and your server admins)
- Test your online and offline backups
- Establish a communication process towards management (transparency, prioritisation)
- Establish emergency plans (or even better, do business continuity planning, have a business impact analysis)
- Maybe have a cyber insurance (they can help by sending specialists when you need them)
- Build up Security Operations or maybe buy it as a service
- Shift left – establish security checks while you are conducting projects or creating software/configs
- Establish security controls in project management or in HR processes
- Talk about the issues and let others challenge you and your decisions!

Why can’t we just do it?

What might hinder you in just establishing all of the things mentioned

- Time, money or knowledge might be limiting factors.
- The threats and risks are not understood correctly by management/decision makers
- There is no legal or contractual obligation to achieve a specific security maturity
- Challenging environment for the company (financial issues, lack of specialists, the pandemic) might lead to a shift of priorities towards surviving the said issues rather than information security issues
- The incidents in the past were handled (too) well, so management does not see a priority (no joke!)

So what can you do?

- Your job “is done” when you continuously collect the information on threats, translate this into risks, inform the management so they understand the risks and are able to make informed decisions.
- If taking a risk seems not appropriate to you, make the management aware of it. Fight for the chance to be heard and to avoid risks which might be disastrous for your company
- Learn from your mistakes. Let others challenge you. Exchange your experience with others.
- Look for new ways to improve what you already have achieved.
- Accept it, if management cannot put your ideas first.
- Prioritise, ask for money where you really need it, where it has the greatest effect for your company.

Let’s connect

You can find me here:

Threema: 7CZ9NBNR

Mail (private): owasp@bifroest.ch

Mail (work) milos.bozovic@localsearch.ch

Work address (for a coffee or so): Förrlibuckstrasse 62, 8005 Zürich

Linked-In: https://www.linkedin.com/in/milos-bozovic-6b6b0886/

Strava: https://www.strava.com/athletes/8051398 ;)

www.localsearch.ch