Martin Půlpán (net.pointers), Tomáš Budník (Thein): We envision hundreds of employees in our new security centre.

KAREL WOLF

4th December 2020

Author: Thein

Tomáš Budník and J&T Private Equity Group's investment fund is past its second successful acquisition. The Czech net.pointers, which focuses on cyber security, is the newest addition to the fund. What the fund plans to do with it?

Net.pointers s.r.o. operates on the market since 2010 and specialises in sensitive data-leak prevention, sophisticated cyber-attack defence, active DDoS attack protection and unknown malware detection. It also deals with implementation of security tools of well-known American and Israeli cyber security-focused companies. Its services are also used by government offices.

„We see a significant potential in providing security solutions for the government bodies, albeit it's not an easy thing to sell. The acquisition brought us capital to expand our business, but also to acquire more companies in the future," says MARTIN PŮLPÁN of net.pointers. We have discussed the fresh security acquisition made by J&T Thein SICAV investment fund with him, and the investor TOMÁŠ BUDNÍK.

How long were the preparations for the acquisition?

Martin Půlpán (MP): The first idea formed at the end of the last year, and we kept discussing it with Tomáš Budník. In the late summer of this year, we started to slowly work on it. A lot of other things had happened in the meantime – for example the fund establishment. Thus, the real acquisition process began in the fall.

Why has J&T Thein SICAV decided to focus on cyber security?

Tomáš Budník (TB): I think that cyber security is, especially in these "covid" times and the age of remote working, distant learning and cyber-attacks on hospitals, factories or banks, an extremely important and responsible topic. We want to be the pioneers of the segment and instil this competence in the future.

Author: Thein
Tomáš Budník

J&T Thein has completed its first two acquisitions. Can you give us an idea about the transaction values?

TB: We don't share any details about the transactions.

MP: It's not just about the money. It's about the synergy within the acquisition fund. These are things related to me becoming a shareholder and it's also a step forward in my career.

Are you going to have a strategic influence in the fund or is it just about being a shareholder?

MP: Yes, I've assumed the cyber security director role in the fund, for all activities, not just the acquisitions. I am responsible for the strategy when it comes to the selection of companies suitable for acquisition by the fund, but I also oversee the consolidation of cyber security-related activities across all acquired companies in the fund, with the goal to create a unified portfolio using the synergies between the companies.

A major advantage of the fund is that companies can mutually complete each other, share information and resources, which makes their operation significantly more effective. You create groups of specialists in pre-sale, deployment and service realisation, you can also share the sales know-how and other things. The hardest thing in cyber security is to know how to sell your services.

How much of your own resources does the fund have available and how much is through bank financing?

TB: The combination of our own resources and bank financing totals at approximately two billion CZK.

What does the acquisition mean for the net.pointers' business model and its future development?

MP: This acquisition is unusual due to my on-going involvement in the Thein J&T fund, in which I help Tomáš to create the security strategies for the whole fund. It's not just about the sale of my company, but it's a long-term co-operation, which has begun with the sale. The acquisition marks a new era for net.pointers, but it's also a stepping stone for the aggregate of companies, service portfolios, technologies and processes, where we try to see the cyber security as an ecosystem of intertwined services.

We want to cover the cyber security demand on the Czech and Slovak markets and later target the countries in the Balkan region. Tomáš has a similar idea outside the cyber security segment with his companies focused on ICT. Hence, the net.pointers acquisition is the first step. It also means I am becoming the fund's shareholder. We can focus on more acquisitions in the future and on filling in the portfolio, which we want to keep in line with the idea of a unified cyber security fund strategy.

It's more than just an investment though. Thein is not a traditional financial investor. It understands the principles of technologies, business and the market. It has a combination of know-how, market value and financial strength, all of which gives us an opportunity to start a host of new projects, which would have been limited by our lack of funds or would have taken a long time to realise if we were reliant on our own profits. We can now proceed with several such projects.

Can you elaborate?

MP: From the security point of view, we want to focus on five to six segments. First is a secure digital identity, meaning comfortable, secure, auditable access to critical systems, apps, services or data. This is followed by an area, which could be called „workplace security", which is essentially protection of the end devices. A zero-trust model is very popular today, through which the security of any and every device is taken in account (cell phone, computer, tablet…). The need for this soared due to the rise of home-office needs.

It has one big advantage over the classic VPN accesses, which is the option to control the content of the communication and the possibility to restrict the user access only where they have authorisation, which can also be controlled from one place. A classic VPN is problematic in situations, where you have an infected computer that you're using at home through which you spread the malware throughout the whole company network without control.

Other segment is related to OT networks, SCADA and IoT security. Today, the industrial systems are no longer separated as they used to be, but are connected with back-office apps, portal apps, and operate with data transfers – one way at least, but often two-way. These networks need good protection, because the production, production-line operation or the utility operational systems are reliant on them.

Also, the IoT devices, which are omnipresent nowadays, are very poorly protected. They are often cheap devices (e.g. cameras), which are connected to the internet, and thanks to the poor security setting can be easily used for massive volumetric DDoS attacks. Potentially at risk are city CCTV networks, surveillance devices within company enterprises and similarly also household devices.

Another segment can be called "advanced detection response", meaning the detection of sophisticated attacks, security incidents processing and the oversight on what is actually being transferred in the network. A lot of the enterprise customers are "blind" and don't see what's happening in their networks, or use tools with limited detection capability, for example from the net flow or behavioural analysis, that cannot see into the content.

The malware today is metamorphic, it can perform different APT attacks (Advanced Persistent Threat), where you don't know what exactly you should be looking for and you can only focus on the outside characteristic of the malware, which can change its structure and throughout its life can spread in different ways. In such cases the visibility, detection and reaction are crucial. It's a combination of know-how, technology providing you with detail information about the traffic (including the content) and tools, which can prevent sensitive data leaks.

Another area, which we want to focus on, is the cloud. It's a classic network security, the security of the individual cloud applications and instances, the security of public clouds such as Office 365, Google Apps and other services, where the company needs to evaluate the security in a bigger picture. You need certain tools to do that, so called "micro-segmentation", in which you use individual small firewalls already implemented in each separate container in the cloud, on which you run your company apps or other systems. A situation, where you communicate across the cloud within your own network needs to be

approached in a similar fashion. Additionally, you need to consider data centres, both internal (in your building) and external on the cloud.

We are connected with technology producers in the USA, where you can find very interesting and developed start-ups focusing on this problematic. That's something new that we want to bring to the domestic market. Then there is the traditional security from the point of data protection and governance, a system for sensitive data protection, risk analysis, the security politics and audits, penetration tests etc. You need to evaluate the way to protect the data, how are they cyphered, where are they stored, so your company complies with different demands, GDPR for example.

The digital identity is also about secure access to privileged accounts, auditable access, individual session recording, so you are aware what each individual system integrator does within your network, along with being able to check administrators with critical rights.

Do you think the composition of your customers will dramatically change with this specific focus?

MP: Our current customers are service providers, enterprise companies, utility companies and, to a lesser extent, the government administration. I see a big potential in relation to the government administration, although from the business point of view it's difficult to sell our services, and the contract negotiations always take a long time. But we want to focus on the top 100 companies in the Czech Republic and Slovakia, and then expand to Eastern Europe, which is the key segment in the future.

We are traditionally strong with service providers, but we see a big potential with the government administration, as they'll need to digitalise their services soon. Thanks to the current dismal state of the national budget, there is a motivation for the digitalisation to be implemented quickly. It will embody services operating on the cloud and tools for the data protection, because the government naturally needs to collect a vast array of sensitive data that needs to be protected and overseen. It's a part of the services we plan to offer.

We want to build a modern Security Operation Centrum (SOC). It's not only about the outsourcing though, but adding a value to our services and know-how, which we are able to offer through one existing SOC and hence provide only a specialised set of services.

We also want to focus on „data science", models of how the organisation should operate and compare them to reality while searching for weak spots not meeting the model. That can be applied to cyber security, company processes and other disciplines with large volumes of data.

Where is your security centre supposed to be located and how many people do you plan to employ?

MP: The headquarters will likely be located in Prague, but we'll have several branches both in the Czech Republic and in Slovakia. We'll share the resources, and once we expand abroad, we will be able to draw resources from there as well.

As for the recruitment, we plan to hire people for positions in Level 1, Level 2 and Level 3. We already have some people, especially for the Level 3 positions, but we plan to hire mainly skilled employees in the future, who already have the needed knowledge, which is not exactly simple these days. We plan an active co-operation with universities and organisations that are involved with security, and we want to nurture these talents. The SOC will operate in a recruitment mode at the beginning, during which we count on hiring dozens of people, but subsequently our plans envision several hundred new hires.

Do you already have any plans with the finances obtained through the acquisition?

MP: Yes, we do. We want to expand both through the know-how purchase, and acquisitions. All things can't be sorted through acquisitions though, there are certain projects, that will be financially managed and commenced by us, or we will work on them with other partners.

What's the turnover you'll finish this year with and what is your vision for the next year's profit?

MP: It's quite hard to say, because we have planned investments and acquisition strategies, that will negatively impact the projected profit. But let's say the next year could bring approx. 100 million CZK just through the security services. Naturally, it will be more within the whole group, because we'll subsequently consolidate these services. Hence, why it cannot be clearly measured, it will be a conjoined effort of the whole group, not a performance of one company.

And this year?

MP: Slightly below a hundred million CZK, maybe a bit more.

Are you not worried that with expanding your business you could become a competition for some of your current customers?

MP: Not so much customer, but naturally we will probably compete with companies that specialise on cyber security within the systematic integration segment. We plan to offer quite a lot of services through white-label solutions. Some services within different synergies can be sold by our customers under their own branding.

We want to co-operate with service providers across the region in the future on certain parts of the cyber security, which will allow them to have an interesting portfolio for their customers, while we provide the expertise in the background.

Can you please elaborate on the aforementioned expansion abroad?

MP: There will be a swift expansion to the market in Slovakia at the beginning of next year, then we are interested in the former Austria-Hungary region; Hungary, Serbia, Slovenia and Montenegro. Their markets are similar to the Czech one, and they will dynamically develop. It's a logical way from the Czech Republic outwards. We don't want to expand west; those are specific and saturated markets, heavily dependent on long-term relationships. The language barrier could be an additional factor.

You mentioned that the first acquisitions are quite close; can you at least give a hint on the sub-segment in which these companies operate?

MP: We can start talking about it after we pass a certain stage and only with the consent of the company owners. However, the segment is clear, it relates to things that will be helpful for building the know-how and intelligence for the SOC, the companies specialise in penetration tests and security audits. Further, we are talking about companies with know-how of certain advanced technologies, which fit like a missing puzzle piece in our portfolio. They are not necessarily large, we are after the know-how. There are a lot of small- and medium-sized companies with expert knowledge, which find it very hard to sell their experience and don't know how to approach corporate customers. We will offer the right platform for such companies, which will allow us to reach out to significant customers that take us seriously, and maximise their expertise at the same time. This way we can approach interesting customers from automotive, banks, government offices or armed forces.

Is it easier to hire specialists today than it was a year ago, at the peak of the economic conjuncture?

MP: The crisis in IT is generally not visible and it didn't affect the security segment at all. There are such a few people in this area that the demand is perpetually massive. We want to take advantage of the acquisition process, because it will bring us not only the know-how and the customers of each company, but also their employees. The business in cyber security is fully dependent on the people, thus it's an important source of specialists for us.

Do you offer home-office with the long-term positions?

MP: We are very flexible in this regard and we've started with this even before the coronavirus. We have colleagues, who are not from Prague, but perform a high quality work, who find the daily commute to work stressful

and complicated. We have implemented quite a laid back regime of remote working 4-5 years ago. However, we monitor how the work time is utilised. It's not always an attractive part of the job though, for example if you have small kids and no space to work alone, you prefer going in the office.

About the fund: J&T Thein SICAV fund

The fund was established in October 2020 and is focused on investments into the technological companies in the ICT infrastructure segment, cyber security area and cloud solutions-related app development in the Czech Republic and Slovakia. The fund was established through the partnership of technological expert Tomáš Budník, the 65% majority fund shareholder, and J&T Private Equity Group Ltd., which owns the remaining 35%.

How many people do you currently employ?

MP: In net.pointers, including external contractors, we employ around 20 people, in addition to which we co-operate with external subjects that are utilised for certain projects. The core of Thein is a team of 15 people, but it's constantly expanded, because we keep hiring people to fill specific positions and to meet the fund's acquisition strategy.

Before Thein's offer to acquire your company, have you considered entering the stock exchange to get the funding?

MP: That's a very complex matter, with a pretty arguable result, it may work and it may not. This is attractive for large companies with profit ranging in billions of CZK. Entering the stock exchange is expensive, and sensible only if you want to expand your services globally. Otherwise it's more reasonable to utilise some form of investment-based capital.

At the beginning the fund was split between you and the J&T group, is (or will be) the fund open to more outsider investors? If yes, what is the minimum investment capital necessary to enter?

TB: J&T Thein SICAV fund is open to other qualified investors; the distribution is handled by J&T bank. Both fund shareholders have already invested into the investment shares. The minimum investment is 4 million CZK.

How many acquisitions are currently under discussion in Thein?

TB: We are working on several other transactions which are at various stages of negotiation.