Text a foto: Pavel Vokáč, Tibor Szabó

Z průzkumu Asociace malých a středních podniků a živnostníků ČR (AMSP ČR) vyplývá, že pouze 40 % dotázaných firem hodnotí rizika spojená s kybernetickou bezpečností nejméně jednou za čtvrt roku, již téměř třetina se setkala s kyberútokem, a z odvětví obchodu je to dokonce 42 % firem. V reakci na nárůst kyberútoků a vyvíjející se digitální prostředí vznikl program Kyberobrana.cz, za nímž stojí AMSP ČR a IT společnost inQool. Cílem programu, který vznikl v rámci projektu Rok nové energie 2024 (RNE 2024), je chránit a edukovat malé a střední podniky v Česku v kyberbezpečnosti. Hovoří o něm Pavel Vokáč z AMSP ČR a Tibor Szabó ze společnosti inQool.

Kdy program Kyberobrana.cz vznikl a co k němu AMSP ČR vedlo?

Pavel Vokáč: Program vznikl na konci loňského roku. Jeho primární ambicí je pomáhat čelit novým výzvám v kyberbezpečnosti statisícům malých a středních podniků v Česku. Nezvládnutý kyberútok totiž může

Jak se chránit před kyberútoky

Program Kyberobrana.cz má pomoci malým a středním podnikům čelit výzvám v kyberbezpečnosti, říká Pavel Vokáč z AMSP ČR a Tibor Szabó ze společnosti inQool.

mít pro podnikatele fatální dopady, čemuž chceme předcházet. Digitální gramotnost velké části malých a středních firem není nejlepší, proto hledáme cesty, jak omezit rizika v jejich podnikání, a kyberbezpečnost je jedním nich.

Co program nabízí?

Pavel Vokáč: Budujeme a provozujeme unikátní edukační koncept a platformu v kyberbezpečnosti, aby se zvýšila informovanost a připravenost firem a živnostníků čelit kyberhrozbám. Program zaštítila AMSP ČR, jelikož jde o klíčový prvek projektu Rok nové energie 2024. Hlavním partnerem programu se stala společnost inQool, jejíž výkonný ředitel Tibor Szabó vystupuje na akcích, na nichž předává informace a know-how z kyberbezpečnosti.

Tibor Szabó: Program přispívá k budování bezpečného a moderního Česka tím, že chrání a edukuje malé a střední podniky v kyberbezpečnosti, protože právě ty patří mezi nejzranitelnější v důsledku malé vyspělosti v IT. Poskytuje

jim odborné know-how a připravuje je na efektivní obranu před kyberhrozbami. Edukaci v kyberbezpečnosti totiž potřebuje každý. Není nic horšího než zjistit, že se vás to týká, až když může být pozdě.

Jak se jako zástupce programu Kyberobrana.cz stavíte ke spolupráci s pojišťovnami a poskytování pojištění proti kybernetickým rizikům? A jak by taková spolupráce mohla přispět k ochraně malých a středních podniků v Česku?
Pavel Vokáč: Jednoznačně zde navazujeme na tradici spolupráce s pojišťovnami a s jejich službami pro malé a střední podniky. Mohu zmínit dnes již klasické „pojištění odpovědnosti členů orgánů…“, ale zde hovoříme o nové zkušenosti – jak vnímat kybernetickou bezpečnost v bezpečném ekosystému firmy (kybernetické útoky reálně mohou zcela ochromit core business firmy s dopady až do její existence). A podobně jako ve všem co děláte – i kybernetická bezpečnost je dobrá, platná, funkční – pokud uznáváte pravidla, doporučení, máte určitou, řekněme aspoň taktickou strategii, jak je třeba ve firmě, ve vašem IT, směrem k zaměstnancům atd…postupovat. Jelikož se však jedná o ne zcela běžnou znalostní kompetenci právě u malých a středních firem, naše pozice se dlouhodobě soustředí na doručování povědomí a připravenosti, odborní partneři (pojišťovny) pak realizují vlastní službu, dodávají svůj produkt.

Pavel Vokáč, CSc., MBA

Místopředseda představenstva AMSP ČR
Vice-Chairman of the Board at AMSP ČR

Mgr. Tibor Szabó

Předseda představenstva inQool a.s.
Chairman of the Board at inQool a.s.

> *„Nezvládnutý kyberútok totiž může mít pro podnikatele fatální dopady, čemuž chceme předcházet.“*

Tibor Szabó: Řekl bych, že všichni členové programu Kyberobrana.cz se staví ke spolupráci s pojišťovnami a poskytování pojištění proti kybernetickým rizikům velmi pozitivně. Prostřednictvím Asociace malých a středních podniků plánujeme informovat nejen členy, ale i širší veřejnost, o možnosti pojištění proti kybernetickým hrozbám. Tato spolupráce by mohla významně přispět k ochraně malých a středních podniků v Česku tím, že poskytne další důležitý nástroj v boji proti kybernetickým útokům. Pojištění proti kybernetickým rizikům by se tak stalo dalším pilířem ochrany, který podnikatelům a organizacím umožní lépe se chránit a minimalizovat potenciální finanční i reputační ztráty v případě kybernetických incidentů. Tímto způsobem bychom chtěli podporovat osvětu o kybernetických hrozbách a zdůraznit význam prevence a zabezpečení dat ve firemním prostředí.

Plánuje program Kyberobrana.cz nějakou formu spolupráce s pojišťovnami v rámci pojištění proti kybernetickým rizikům? Jaký je význam této informace pro malé a střední podniky v Česku a jakou roli v tom hraje přímo AMSP ČR?
Tibor Szabó: Ano, určitě, aktuálně chystáme edukativní sekci přímo na našich webových stránkách s podrobnými informacemi o pojištění proti kybernetickým rizikům. Také připravujeme workshopy a školení nejen pro členy AMSP ČR, aby mohli lépe problematiku pochopit, odborně se připravit na podmínky kladené pojišťovnami a zvládnout tak případná rizika spojená s kybernetickými hrozbami.

Jak souvisí RNE 2024 s programem Kyberobrana.cz?
Pavel Vokáč: RNE 2024 je hlavním letošním projektem AMSP ČR a inspiruje všechny, kteří chtějí posunout své podnikání, vydat se novým směrem a být součástí inovací na trhu. A tou program Kyberobrana.cz je.

Jaká jsou hlavní témata programu Kyberobrana.cz?
Tibor Szabó: Edukace v oblasti auditu a řízení rizik, hrozeb souvisejících s umělou inteligencí, penetračních testů, ochrany sítě a provozu, zátěžových testů aplikací a infrastruktury, bezpečnostních operací a auditu dodavatelů. Nabízíme také praktická bezpečnostní školení a pomáháme zájemce nasměrovat i na další školení, přičemž spolupracujeme s dalšími odbornými subjekty.

Považujete AI pro firmy za hrozbu, nebo za příležitost a přínos?
Tibor Szabó: O tom jsem přednášel na jedné z akcí, kterých jsem se zúčastnil jako zástupce programu Kyberobrana.cz, konkrétně šlo o AI Open Day, který pořádala AMSP ČR a Evropské centrum pro digitální inovace při ČVUT v Praze. Začal jsem hrozbami, protože si je mnohem méně uvědomujeme. Zaměřil jsem se na hrozby umělé inteligence v oblasti kyberbezpečnosti firem a rozebral například zátěžové útoky, pokročilé sociální inženýrství nebo deepfake videa či fotky.

Co do programu přináší společnost inQool? Proč se stala se jeho součástí, co si od něho slibuje a jaký má pro ni význam?
Tibor Szabó: Společnost inQool do programu přináší dlouholeté zkušenosti a odborné znalosti v kyberbezpečnosti. Působíme v segmentu kyberbezpečnosti, která se týká softwarového vybavení, informačních systémů, portálů, mobilních aplikací, obecně digitalizace byznysu i společností. Do programu vstupujeme jako odborný prvek, který se členy i nečleny AMSP ČR konzultuje a radí jim, kde mohou být jejich systémy chybné nebo zastaralé a jak tyto nálezy řešit. Význam kyberbezpečnosti pro tak velkou členskou základnu podnikatelů, jako má AMSP ČR, je pro nás nosným tématem. Jedním z komponentů, na který se mohou členové AMSP ČR v rámci programu Kyberobrana.cz těšit, je mobilní aplikace od společnosti inQool. Slouží jako kontaktní místo a komunikační kanál. Postupně budujeme a plníme edukativním obsahem také portál www.kyberobrana.cz, kde se zaměřujeme na interakci s členy.

> *„Program přispívá k budování bezpečného a moderního Česka tím, že chrání a edukuje malé a střední podniky v kyberbezpečnosti, protože právě ty patří mezi nejzranitelnější v důsledku malé vyspělosti v IT."*

Jaké další subjekty podporují program Kyberobrana.cz?
Pavel Vokáč: Evropské centrum pro digitální inovace, zde konkrétně EDIH CTU (Praha, ČVUT) v oblasti umělé inteligence (AI) a strojového učení (ML). Tento subjekt se zaměřuje na transfer důvěryhodných řešení, produkty a služby právě do oblasti malých a středních podniků, a to ve specifickém spojení AI a kybernetické bezpečnosti. Je to velmi významný trend poslední doby, bohužel také často využívaný na straně útočníků. Většina toho, co v rámci této spolupráce nabízíme, je k dispozici v prvních stupních (tj. získání povědomí a připravenosti pro kvalitní řešení kybernetické bezpečnosti) i zcela zdarma.
Shodnou smlouvu a podporu v projektu Kyberobrana.cz máme i s dalším EDIHem: Cybersecurity Innovation Hub (CIH) a organizací CzechInno. Zcela prakticky zde jde opět o škálu konkrétních služeb od testování kyberbezpečnostní odolnosti sítí a zařízení, vzdělávací aktivity pro běžné uživatele i cvičení pro kyberbezpečnostní specialisty až po konzultace s cílem vyhodnotit aktuální kyberbezpečnostní úroveň firem i organizací a navrhnout její zlepšení. CIH ve spolupráci s AMSP ČR má tak v nabídce přes 50 typů služeb pro malé a střední podniky.
Ještě si dovolím poznamenat, že naše aktivity jsou samozřejmě realizovány s podporou Národního úřadu pro kybernetickou a informační bezpečnost a v souladu s ním, a také se zákonem o kybernetické bezpečnosti, který postupně reaguje na situaci v této oblasti i v souladu se strategií EU.

Pánové, děkujeme Vám za rozhovor.

How to Protect Yourself from Cyber Attacks

The Cyber Defense Program (Kyberobrana.cz) is designed to help small and medium-sized enterprises (SMEs) tackle cybersecurity challenges, says Pavel Vokáč from AMSP ČR and Tibor Szabó from inQool.

According to a survey by the Association of Small and Medium-Sized Enterprises and Crafts of the Czech Republic (AMSP ČR), only 40% of the surveyed companies assess the risks associated with cybersecurity at least once every quarter. Nearly a third have encountered a cyber attack, and in the trade sector, this figure is as high as 42%. In response to the increase in cyber attacks and the evolving digital environment, the Cyber Defense Program (Kyberobrana.cz) was established by AMSP ČR and the IT company inQool. The program, created within the framework of the "Year of New Energy 2024" (RNE 2024) project, aims to protect and educate SMEs in the Czech Republic about cybersecurity. Pavel Vokáč from AMSP ČR and Tibor Szabó from inQool discuss the program.

When was the Cyber Defense Program (Kyberobrana.cz) established. What led AMSP ČR to create it?

Pavel Vokáč: The program was established at the end of last year. Its primary ambition is to help hundreds of thousands of SMEs in the Czech Republic face new cybersecurity challenges. A poorly managed cyber attack can have fatal consequences for entrepreneurs, which we aim to prevent. The digital literacy of many SMEs is not the best, so we are looking for ways to mitigate risks in their businesses, with cybersecurity being one of them.

What does the program offer?

Pavel Vokáč: We are building and operating a unique educational concept and platform for cybersecurity to increase awareness and preparedness of companies and entrepreneurs to face cyber threats. The program is sponsored by AMSP ČR as a key element of the Year of New Energy 2024 project. Our main partner is inQool, whose CEO Tibor Szabó participates in events where he shares information and know-how about cybersecurity.

Tibor Szabó: The program contributes to building a safe and modern Czech Republic by protecting and educating SMEs about cybersecurity, as they are among the most vulnerable due to their low IT maturity. It provides them with expert know-how and prepares them for effective defense against cyber threats. Everyone needs education in cybersecurity. It's crucial to realize this before it's too late.

> *"A poorly managed cyber attack can have fatal consequences for entrepreneurs, which we aim to prevent."*

How do you, as a representative of the Cyber Defense Program (Kyberobrana.cz), approach collaboration with insurance companies and providing cyber risk insurance? How could such collaboration contribute to the protection of SMEs in the Czech Republic?

Pavel Vokáč: We definitely build on a tradition of cooperation with insurance companies and their services for SMEs. I can mention the classic "liability insurance for members of statutory bodies," but here we are talking about a new experience – understanding cybersecurity within a secure company ecosystem (cyber attacks can realistically cripple a company's core business, affecting its very existence). Just like in everything you do, cybersecurity is good, valid, and functional if you follow the rules, recommendations, and have at least a tactical strategy for your company, IT, and employees. Since this is not a common knowledge competency among SMEs, we focus on delivering awareness and preparedness. Our expert partners (insurance companies) then implement their service, delivering their product.

Tibor Szabó:I would say that all members of the Cyber Defense Program (Kyberobrana.cz) are very positive about collaborating with insurance companies and providing cyber risk insurance. Through the AMSP ČR, we plan to inform not only members but also the wider public about the possibility of cyber threat insurance. This collaboration could significantly contribute to the protection of SMEs in the Czech Republic by providing an additional important tool in the fight against cyber attacks. Cyber risk insurance would become another pillar of protection, enabling entrepreneurs and organisations to better protect themselves and minimise potential financial and reputational losses in case of cyber incidents. This way, we want to promote awareness of cyber threats and emphasise the importance of data security and prevention in a business environment.

Does the Cyber Defense Program (Kyberobrana.cz) plan any form of collaboration with insurance

companies regarding cyber risk insurance? What is the significance of this information for SMEs in the Czech Republic, and what role does AMSP ČR play in it?
Tibor Szabó: Yes, definitely. We are currently preparing an educational section on our website with detailed information about cyber risk insurance. We are also preparing workshops and training sessions not only for AMSP ČR members, so that they can better understand the issue, be professionally prepared for the conditions set by insurance companies, and manage the risks associated with cyber threats.

> *"The program contributes to building a safe and modern Czech Republic by protecting and educating SMEs about cybersecurity, as they are among the most vulnerable due to their low IT maturity."*

How does the Year of New Energy 2024 (RNE 2024) relate to the Cyber Defense Program (Kyberobrana.cz)?
Pavel Vokáč: RNE 2024 is AMSP ČR's main project this year and inspires everyone who wants to advance their business, explore new directions, and be part of market innovations. And the Cyber Defense Program (Kyberobrana.cz) is part of that.

What are the main topics of the Cyber Defense Program (Kyberobrana.cz)?
Tibor Szabó: Education in audit and risk management, threats related to artificial intelligence, penetration testing, network and operations protection, application and infrastructure stress testing, security operations, and supplier audits. We also offer practical security training and help direct interested parties to further training, and cooperating with other professional entities.

Do you consider AI a threat, an opportunity, or a benefit for companies?
Tibor Szabó: I gave a lecture on this topic at one of the events I attended as a representative of the Cyber Defense Program (Kyberobrana.cz), specifically the AI Open Day organised by AMSP ČR and the European Digital Innovation Center at CTU in Prague. I started with the threats because we are much less aware of them. I focused on AI threats in the cybersecurity field, such as stress attacks, advanced social engineering, and deepfake videos or photos.

What does inQool bring to the program? Why did it become part of it, and what does it expect from it? What significance does it have for the company?
Tibor Szabó: InQool brings years of experience and expertise in cybersecurity to the program. We operate in the cybersecurity segment related to software, information systems, portals, mobile applications, and the general digitalization of business and companies. We join the program as a professional element, consulting with and advising AMSP ČR members and non-members on where their systems may be faulty or outdated and how to address these findings. The importance of cybersecurity for such a large member base of entrepreneurs, like AMSP ČR, is a key topic for us. One of the components that AMSP ČR members can look forward to as part of the Cyber Defense Program (Kyberobrana.cz) is a mobile app from inQool. It serves as a contact point and communication channel. We are also building and filling the www.kyberobrana.cz portal with educational content, focusing on interaction with members.

What other entities support the Cyber Defense Program (Kyberobrana.cz)?
Pavel Vokáč: The European Digital Innovation Center, specifically EDIH CTU (Prague, CTU), in the field of artificial intelligence (AI) and machine learning (ML). This entity focuses on transferring trustworthy solutions, products, and services to SMEs, specifically in the connection of AI and cybersecurity. This is a very significant trend recently, unfortunately also often used by attackers. Most of what we offer in this cooperation is available in the initial stages (i.e., gaining awareness and preparedness for quality cybersecurity solutions) for free. We have similar agreements and support in the Cyber Defense Program (Kyberobrana.cz) with another EDIH: Cybersecurity Innovation Hub (CIH) and the organization CzechInno. Practically speaking, this involves a range of specific services from testing the cybersecurity resilience of networks and devices, educational activities for regular users, exercises for cybersecurity specialists, to consultations to assess the current cybersecurity level of companies and organizations and suggest improvements. CIH, in collaboration with AMSP ČR, offers over 50 types of services for SMEs.

I would also like to note that our activities are, of course, carried out in compliance with and with the support of the National Cyber and Information Security Agency and in accordance with the Cybersecurity Act, which is gradually responding to the situation in this area in line with the EU strategy.

Thank you for the interview.