**TISKOVÁ ZPRÁVA**

Společnost Source Defense si zajistila 27 milionů dolarů růstového financování, aby urychlila ochranu proti kybernetickým rizikům na straně klienta

Fond Springtide Ventures rozšiřuje řady stávajících investorů ve společnost Source Defense. Ta je lídrem v oblasti ochrany webových aplikací na straně klienta, meziročně zvýšila počet instalací svých produktů u klientů o 240 % a upevnila svou dominanci v oblasti zmírňování rizik třetích stran. Jen v posledním roce vznikla v souvislosti s nedodržováním bezpečnostních zásad škoda ve výši 24 miliard dolarů.

**Rosh-Ha’ayin, Izrael, 27. dubna 2022 –** Společnost Source Defense, průkopník v oblasti ochrany webových aplikací na straně klienta, dnes oznámila, že si v rámci kola financování série B zajistila finanční prostředky ve výši 27 milionů dolarů. V čele tohoto kola stál nový investor [Springtide Ventures](https://kkcg.com/en/springtide-ventures) a zapojili se do něj i všichni stávající investoři, včetně fondů [Jerusalem Venture Partners (JVP)](https://www.jvpvc.com/), [Allegis Cyber Innovation](https://allegiscyber.com/), [Global Brain](https://globalbrains.com/en/), [Connecticut Innovations, Inc.](https://ctinnovations.com/), [NightDragon, LLC](https://www.nightdragon.com/) a [Capital One Ventures](https://growthventures.capitalone.com/). Vedle této investice se do představenstva společnosti Source Defense zapojí Karel Tušek, technický ředitel fondu Springtide. Nové finanční prostředky budou použity na plány urychleného rozvoje společnosti, včetně investic do prodeje, marketingu, tvorby aliancí a výzkumu a vývoje. Na další podporu tohoto růstu společnost koncem roku 2021 jmenovala svým marketingovým ředitelem Stephena Warda, veterána v oblasti start-upů zabývajících se kybernetickou bezpečností.

Společnost se zabývá závažným problémem spojeným s riziky třetích stran v digitálním dodavatelském řetězci, který měl v několika posledních letech nepříznivý dopad na tisíce společností. Jedno z největších a nejméně kvantifikovaných slabých míst z hlediska obchodu spočívá v používání JavaScriptu na webových stránkách. Kód na straně klienta, dodávaný v reálném čase partnery dodavatelského řetězce (třetí, čtvrtá, ale i n-tá strana), podporuje a zlepšuje uživatelský zážitek z webových stránek, zvyšuje zapojení uživatele a je základem pro analytické přehledy. Typické prvky webových stránek se spoléhají na desítky těchto partnerských skriptů. Současně však tyto skripty představují nechráněný a nikým nespravovaný stínový kód. V podstatě jde o snadný cíl pro protivníky na jakémkoli větším webu. Tento prostor pro hrozby a útoky, který nabízí útočníkům mnoho příležitostí k velkým ziskům, zaznamenal v posledních dvou letech stovky rozsáhlých útoků a vede měsíčně k více než 400 útokům na straně klienta (např. získávání přihlašovacích údajů, formjacking a útoky typu Magecart). Napadení některých velkých značek se dostalo na titulní stránky novin – jde například o Macy's, Ticketmaster, British Airways, Segway a mnoho dalších. To přimělo společnost Gartner, zabývající se průzkumem tohoto odvětví, aby rychle definovala novou kategorii [ochrany webových aplikací na straně klienta](https://sourcedefense.com/resources/the-dawn-of-web-app-client-side-protection-gartner-has-it-right/), která bude dle jejích předpokladů v příštích dvou letech vyžadovat masové tržní nasazení.

*„Společnosti vynakládají ohromné množství prostředků a času, aby jejich webové stránky před svým spuštěním byly dobře nadesignované, naprogramované a funkční, přesto však mnohé z nich ví velmi málo o tom, co se děje s jejich webovými stránkami poté, co kód stránky opustí servery společnosti (server-side) a zobrazí se ve webovém prohlížeči uživatele (client-side), a to přestože webové stránky z pohledu finanční hodnoty a hodnoty firemní značky patří k tomu nejdůležitějšímu,“* řekl Dan Dinnar, generální ředitel společnosti Source Defense. Společnost Source Defense nejenže brzy rozpoznala tuto oblast jako hlavní a stále rostoucí problém, ale rovnou se spojila s několika velkými a důvěryhodnými světovými značkami, aby v reálném čase zastavila jakékoli pokusy o digitální skimming, formjacking, clickjacking, ad injection, krádež PII a content defacement. *„Udělali jsme to způsobem, který nikdo nepovažoval za možný – se snadno testovatelným řešením, rychlým nasazením a prakticky bez další zátěže spojené se správou zabezpečení. Naléhavost řešení těchto útoků jen roste – o čemž svědčí nedávné předpovědi společnosti Gartner, že ochrana webových aplikací na straně klienta bude v příštích několika letech všudypřítomnou součástí bezpečnostních technologií,“ dodal Dinnar.*

Společnost Source Defense identifikovala tento vznikající problém, vybudovala si dominantní postavení na trhu a nadále rychle roste jako lídr dané kategorie. V posledních dvou letech vykázala více než 250% růst a do konce roku 2022 zvýší počet zaměstnanců o 70 %. Společnost v současné době chrání téměř 1,5 miliardy návštěv stránek měsíčně a zajišťuje transakce pro některé největší světové firmy – čímž čtvrtletně zabrání přibližně šesti miliardám porušení zásad zabezpečení.

*„Zatímco mnoho potenciálně zneužitelných slabých míst se nachází hluboko ve firemní infrastruktuře, webové stránky společnosti jsou něco jako její obnažený nerv – nebo v tomto případě spíše ohromný svazek obnažených nervů,“* poukázal Karel Tušek z fondu Springtide Ventures. *„Jako investor nechcete jen investovat do inovací, které posilují bezpečnost, ale chcete najít inovace, které mají příznivý, významný dopad na podnikání. Společnost Source Defense vyřešila obrovský problém; nyní může chránit firmy před milionovými ztrátami a pokutami a současně odříznout zločince od významného toku příjmů,“* doplnil

*„Útoky na webové stránky na straně klienta, související s dodavatelským řetězcem jsou na trhu nejrozšířenější, a přitom jsou nejméně vidět. Firmy podnikající online nemohou těmto útokům zamezit, protože škodlivý kód neprochází jejich servery a neustále se mění. To má za následek vážné riziko podvodu, krádeže informací, porušení předpisů, defacementu apod.,“* uvedl Yoav Tzruya, generální partner společnosti JVP. *„Source Defense jako jediná společnost nabízí přístup k řešení problému založený hlavně a především na prevenci. Source Defense chrání více než 100 předních značek – umožňuje organizacím zabezpečit transakce a informace o uživatelích a zároveň dosáhnout souladu s předpisy; rovněž poskytuje pracovníkům marketingu a vývojářům schopnost neustále se rozvíjet, působit proaktivně a udržet si konkurenceschopnost, což dramaticky snižuje rizika pro kybernetickou bezpečnost.“*

Platforma společnosti Source Defense řeší rizika pro všechny weby, které zprostředkovávají transakce či zpracovávají jiná citlivá data. Tím jsou minimalizovány hrozby a na druhé straně v mnohých případech dokonce dochází ke zvýšení výkonu webových stránek. Platforma nabízí plně automatizovaný přístup založený především na prevenci, který poskytuje kompletní řízení přístupu založeného na oprávněních nejen k výchozímu kódu, ale také k JavaScript nástrojům třetích stran. Source Defense chrání významné organizace v různých oborech, včetně finančních služeb, zdravotnictví, pohostinství a maloobchodu, a nabízí schopnost prevence kybernetické bezpečnosti, soulad s předpisy (např. PCI, HIPAA, GDPR) a také vyšší flexibilitu marketingových týmů a vývojářů.

**O společnosti Source Defense**

Source Defense je platforma pro zabezpečení a dodržování souladu s předpisy pro všechny webové stránky, které shromažďují citlivé údaje nebo se zaměřují na transakce. Zabývá se všudypřítomnými rezervami v řízení rizik digitálního dodavatelského řetězce na základě modelu nulové důvěry, který rozšiřuje zabezpečení do dalších částí sítě – na stranu klienta. Jako lídr na trhu ochrany webových aplikací na straně klienta poskytuje Source Defense detekci hrozeb v reálném čase a ochranu a prevenci slabých míst vytvářených JavaScriptem. Patentovaná platforma Source Defense Platform nabízí nejkomplexnější řešení pro hrozby a rizika vyplývajících z roustoucího využívání JavaScriptu, externích dodavatelů a open-source kódu na dnešních webových stránkách.

Řešení Source Defense používají významné společnosti z žebříčku Fortune 500 na trzích finančních služeb, maloobchodu, elektronického obchodování a zdravotnictví. Společnost Source Defense se sídlem v Izraeli a pobočkami po celých Spojených státech amerických je spolehlivým, důvěryhodným a inovativním partnerem v boji proti kybernetickým útokům na straně uživatele.

**O fondu Springtide Ventures**

Fond Springtide Ventures, člen skupiny KKCG, kterou založil Karel Komárek, se zaměřuje na podporu start-upů s globálními ambicemi, zejména B2B/SaaS společností v oblasti cloudové infrastruktury, kybernetické bezpečnosti, ML/AI a blockchainu. Od roku 2016 roste aktivita fondu Springtide v Izraeli, kde realizoval více než deset investic. Springtide těží z exkluzivního přístupu ke kapitálu, know-how a celosvětové působnosti KKCG. Díky svému vícestupňovému přístupu je fond Springtide připraven podporovat úspěšné projekty tím, že se účastní po sobě jdoucích investičních cyklů, od seed financování přes sérii A a B až po sérii C, daleko nad rámec počátečních investic.

**O KKCG**

KKCG Group, kterou řídí jeden z nejúspěšnějších českých podnikatelů Karel Komárek, je mezinárodní investiční společností s celkovou účetní hodnotou přesahující 9 miliard EUR. Skupina KKCG rozvíjí své obchodní aktivity v 38 zemích světa a mezi klíčové oblasti jejího působení patří zábavní průmysl, energetika, IT technologie a nemovitosti. Vlastní podíly v mnoha mezinárodních společnostech, mezi něž patří například Allwyn, ARICOMA Group, MND Group, KKCG Real Estate Group, Springtide Ventures a další. KKCG investuje také do amerického fondu Jazz Venture Partners (se sídlem v Silicon Valley), který se zaměřuje například na investice do technologií pro zlepšení lidské výkonnosti skrze neurovědu. Má vice než 9 tisíc zaměstnanců.

**Kontakt pro média:**

Dana Dvořáková

Ředitelka komunikace, KKCG a.s.

Vinohradská 230, Praha 10

T +420 225 010 399

M +420 602 372 834

E dana.dvorakova@kkcg.com