# Pomáháme rozumět logům

**S Filipem Weberem jsme mluvili o rostoucím zájmu o nástroj LOGmanager pro sběr a analýzu provozních a bezpečnostních logů, o jeho dalším vývoji a především o rozhodnutí přejít na distribuční obchodní model. Jaké partnery hledá a na čem mohou vydělat?**

**Jméno:** Filip Weber

**Pozice:** zakladatel a jednatel společnosti CompuNet, předseda správní rady společnosti Sirwisa

### Jak vznikl nápad vyvinout LOGmanager?

Jako síťaři jsme potřebovali nástroj na sběr a analýzu provozních a bezpečnostních logů. Vyzkoušeli jsme několik komerčních i open source variant, ale nebyli jsme spokojeni. Postupně se stejného nástroje začali dožadovat zákazníci, a to nás nakoplo k vytvoření vlastního systému. Začínali jsme na zelené louce, nesvazovala nás žádná historie, a tak jsme si mohli dovolit použít pro vývoj nejnovější technologie.

### Jak dlouho jste systém prodávali sami a proč jste se rozhodli změnit obchodní model?

LOGmanager jsme sami jako CompuNet prodávali necelé dva roky. Zájem byl obrovský a velice rychle jsme přestali stíhat implementace u zákazníků. Není to totiž jen o odvezení krabice, ale o pomoci s analýzou provozních a bezpečnostních logů, nastavením reportů a alertů a vůbec o pomoci správně rozumět informacím v lozích. To vytváří velký prostor pro práci partnerů, kteří mají se zákazníkem zkušenosti a znají podrobně jeho síť a zabezpečení. Tak přišlo rozhodnutí oddělit vývoj z **CompuNetu** do samostatné společnosti **Sirwisa**, která se soustředí jen na vývoj.

### Jaké máte referenční zákazníky?

Jsou to například Státní zemědělský intervenční fond, Ostravská univerzita, Městská část Praha 3, Státní veterinární správa, Státní pozemkový úřad, Krajská zdravotní a další.

### Potenciálním klientem je asi kterákoliv organizace používající více systémů, generujících logy. Kdo je však „zákazníkem“ uvnitř společnosti?

Především oddělení bezpečnosti IT a oddělení provozu IT. Ale také třeba oddělení vnitřního auditu, které se často zajímá o logy z aplikací, jako je SAP.

### Systém uchovává data v podobě pro potřeby shody s předpisy. Lze ho tedy nabídnout všem organizacím, pro které platí zákon o kybernetické bezpečnosti?

LOGmanager je ideálním a dostupným řešením požadavků § 21 a § 23 vyhlášky.

### Z jakých prostředků se LOGmanager financuje nejčastěji?

Obvykle z rozpočtu provozu IT, ale jak jsem již říkal, lze využít i prostředky IT bezpečnosti nebo vnitřního auditu.

### Jak vypadá váš licenční model?

Nemáme rádi složité licenční modely. Cena je tedy stanovena součtem appliance a softwaru, pak se platí roční poplatky za podporu, které zahrnují další verze systému a nové nebo upravené parsery. Žádné poplatky za EPS nebo za počet připojených zařízení.

### Na čem konkrétně vydělává partner?

Partner má marži na prodeji systému, ale především by měl vydělávat na implementaci a analytických službách. S tím mu samozřejmě můžeme pomoci školením techniků nebo zapůjčením našeho specialisty – analytika.

### Jakou podporu resellerům poskytuje Veracomp a jakou Sirwisa?

Veracomp je pro nás distributorem s přidanou hodnotou. Nabízí jim kompletní předprodejní podporu, zapůjčení dema i prezentaci u zákazníka. Sirwisa pak poskytuje resellerům hlubší detailní technickou analýzu uživatelského prostředí a vazbu na další vývoj appliance.

### Předpokládám, že vhodnými partnery jsou pro vás firmy, které nyní dodávají bezpečnostní a síťová řešení...

Partnerem je reseller, který považuje log management za základní pilíř každého bezpečnostního auditu a efektivní správy provozu. Ostatním se budeme snažit pomoci se v dané problematice zorientovat. Ideálním partnerem je pak reseller, který má pevnou vazbu s uživatelskou organizací a umí identifikovat, že v ní dozrál čas na implementaci systému pro sběr logů, případně SIEM systému. Dále jsou pro nás zajímaví partneři, kteří se specializují na řešení pro veřejnou správu, kde je vzhledem k novému zákonu o kybernetické bezpečnosti log management nezbytný.

### Co plánujete do budoucna?

Především kontinuální vývoj. Během příštího čtvrtletí se soustředíme hlavně na vývoj nového SIEM modulu, který posune LOGmanager do kategorie plnohodnotného SIEM nástroje. Chceme přistoupit k řešení problematiky zcela jinak než tradiční výrobci. Pokud se nám to povede, budeme mít výkonný SIEM systém bez omezení na počet zdrojů logů. ●

*Jan Mazal*