



Jak poskytovat řízené IT služby a vydělávat na nich

JAKÉ JSOU TRENDY V OBLASTI IT A IT INFRASTRUKTURY?

Jedním z trendů je akcelerující přechod podniků a organizací na nové modely **využívání informačních technologií ve formě služby**, namísto nákupu a provozování vlastní IT infrastruktury.

Mezi poskytovateli řízených služeb (MSP - Managed Service Provider) dochází v oblasti kybernetické bezpečnosti k dramatickému přesunu poptávky zákazníků od tradičního nákupu softwaru a hardwaru k předplatnému řízených služeb.



IT služby může poskytovat i vaše společnost

Tradiční model využívání IT je náročný jak finančně z pohledu vysokých nákladů na nákup a nasazení IT, tak z pohledu provozování a to personálně i organizačně.

Budeme svědky rozšiřování nabídky obvyklých IT služeb směrem k sofistikovanějším a komplexnějším službám typu kybernetické bezpečnosti. >>> segment s obrovským růstovým potenciálem.

Na jakých IT službách můžete vydělat?

Kybernetická ochrana jako SLUŽBA

Stále více firem si tváří v tvář koronavirové epidemii a množícím se kybernetickým rizikům uvědomuje, že **svou IT bezpečnost raději svěří do rukou profesionálů.**

Jaká je skutečnost na poli digitálních útoků?



31%

světových společností je nejméně jednou
denně napadeno kyberzločinci

50%

všech známých případů
představoval Maze ransomware



Po útocích
ransomwaru
došlo k úniku dat
ve více než

1000

společnostech

1000

chyb ve svých produktech
musel Microsoft opravit
za pouhých devět měsíců

Průměrná životnost malwaru je

3,4 dne

Firmy nekupují software nebo zařízení, **kupují si kompletní řešení**

„a že to bude fungovat!“

V rámci nového modelu využívání IT si pořizují poskytovatelé řízených služeb veškerou potřebnou infrastrukturu sami a následně ji formou IT služeb prodávají zákazníkům za pravidelný měsíční poplatek zahrnující náklady na hardware, software i údržbu.

Náš MSP partner pro prodej IT služeb kybernetické bezpečnosti:

„Nasadili jsme Acronis Cyber Disaster Recovery včetně cloudové instance například u výrobního zákazníka, jehož příjemně překvapila rychlost implementace a spolehlivost obnovy. V rámci pravidelné testovací obnovy, která se provádí několikrát ročně, je zákazník schopen provoz své kritické infrastruktury plně obnovit do 10 minut.“

Petr ČÁP ze společnosti



Budoucnost a trendy



92%

globálních organizací muselo k přechodu na model vzdálené práce nasadit nové technologie. Výsledkem byly zvýšené náklady na IT u 72 % společností během pandemie.



Exfiltrace dat
bude častější než šifrování dat

Ransomware
se bude zabývat novými cíli

1.

Jak na to **Krok první**

Budete potřebovat konkurenční výhodu:

Jak si zvolit dodavatele?

Na jednu stranu potřebujete obsloužit svého zákazníka, na druhou stranu chcete mít podporu pro prodávané řešení. Chcete mít řešení **“pro každého”**, protože tak můžete prodat více zákazníkům dle jeho okamžitých potřeb.

Co musíte zohlednit při výběru partnera?

A. UCELENOST ŘEŠENÍ a komplexnost nabídky pro vaše zákazníky

B. PODPORU poskytovanou jak vaší organizaci, tak vašim zákazníkům

A. UCELENOST ŘEŠENÍ

V naší nabídce naleznete hned několik řešení pokrývajících většinu podnikových požadavků na IT bezpečnost.

Dodavatelé našich řešení jsou lídry na trhu a průkopníky ve své oblasti.

Acronis

ucelené řešení kombinující ochranu dat a kybernetickou bezpečnost

GFI Software

produkty pokrývající různé oblasti kybernetické bezpečnosti od e-mailů až po ochranu sítě

N-ABLE
authorized distributor

řešení jednoduché správy a monitoringu koncových zařízení včetně jejich ochrany


CLOUDFLARE
PARTNER NETWORK

platforma zvyšující bezpečnost, výkonnost a spolehlivost internetových aplikací

Všechna naše řešení odpovídají těm nejmodernějším TRENDŮM a POŽADAVKŮM na zabezpečení.

B. PODPORA

Protože jsme svědky rozšiřování nabídky obvyklých IT služeb směrem k sofistikovanějším a komplexnějším službám typu kybernetické bezpečnosti, je potřeba mít nejen komplexní a moderní řešení, ale i podporu, díky které mají jak vy tak vaši zákazníci oporu.

OBCHODNÍ

- spolupracovat s námi znamená, že jako partner nemusíte investovat do uvedených technologií
- máte absolutní flexibilitu a kontrolu nad tím kolik, čeho a kdy odeberete
- nic nepředplácíte
- naučíme vás, jak tyto služby prodávat
- seznámíme vás s dílčími prodejními postupy a s informacemi, jaké to pro vás nese finanční benefity

TECHNICKÁ

- pomoc odborníků ze ZEBRA SYSTEMS při implementaci řešení
- seznámíme a naučíme, jak služby využívat a u svých klientů používat, implementovat
- ucelený systém školení v rámci akademie
- videa, tutoriály, whitepapery, znalostní testy
- certifikace

MARKETINGOVÁ

- s partnery spolupracujeme na případových studiích, které sdílíme do médií
- citujeme partnery v publikovaných tiskových zprávách
- jsme pravidelnými držiteli ocenění za naše případové studie
- účastníme se akcí našich partnerů, na kterých prezentujeme technologie a řešení
- společně s vendory oceňujeme nejlepší partnery účastí na celosvětových VIP akcích jako např. globální konferenci v Miami, závodech Formule 1 či fotbalových zápasech atp.
- již od roku 2015 předáváme naše vlastní ocenění Best for the best nejlepším partnerům

Poskytovatelé MSP řešení očekávají, že v příštích 2 letech vzroste jejich obrat v segmentu řízených služeb IT bezpečnosti v průměru o 89 %, cloudových řízených služeb o 51 %, přičemž poklesne obrat z přeprodeje softwaru o 20 % a hardwaru o 63 %.

Odpovědi na otázky v souvislosti s tématem: **“Jak funguje IT bezpečnost jako služba?”**

Můžete vy jako partner vydělat více?

ANO! Jako partner vyděláte více a to i přesto, že jednorázové výdaje vašich klientů jsou nižší.

Proč? Váš zákazník v souhrnu zaplatí více, a i přesto na to raději přistoupí.

Proč by na takovou nabídku koncový uživatel přistoupil?

Zákazník na tuto službu spíše přistoupí než aby zaplatil jednorázově jeden milion či „jen“ statisíce za nákup softwaru nebo jeho implementaci.

Jednorázové výdaje vašich klientů jsou tedy nižší, na což vaši zákazníci uslyší. Váš klient raději přistoupí na menší měsíční částky, než na jednorázový výdaj v mnohonásobně vyšší hodnotě.

Co je benefitem?

Neprodáváte “produkt”. Prodáváte ŘEŠENÍ a GARANCI, že to funguje. Váš klient má o svou digitální bezpečnost postaráno.

Co je ten “FÍGL?”

V ceně služby je zahrnut nejen samotný produkt (software), ale i s tím související služba (know-how a čas, který klientovi věnujete).

Vašemu klientovi poskytujete ten správný pocit péče o zákazníka (customer care) a to prostřednictvím nižších měsíčních položek oproti jednorázovému výdaji.

*Prodáváte-li službu na základě paušálu, váš zákazník nemá důvod přemýšlet, zda to vezme zase “od vás”.
Oproti jednorázovým nákupům, kdy bude v daný moment posuzovat vaši nabídku s několika dalšími.*

2.

Jak na to **Krok druhý**

Jak prodat služby kybernetické ochrany?

Získání jednoho nového zákazníka je mnohonásobně dražší než prodej stávajícímu.

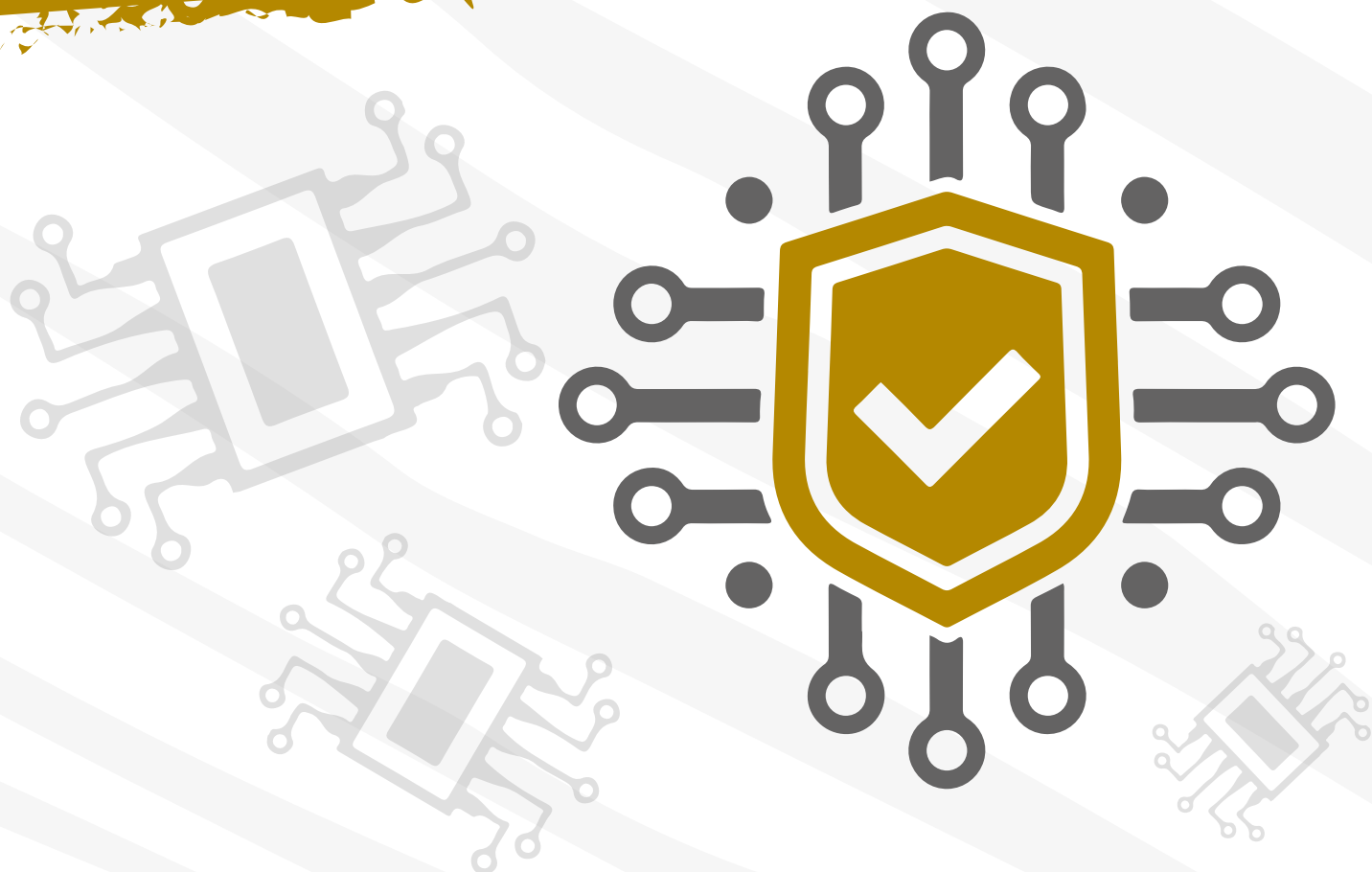
Poskytovatelé řízených služeb využívající moderní řešení ochrany dat mohou vydělat nejenom akvizicí nových zákazníků.

Nyní máte příležitost oslovit nové, ale i stávající zákazníky a odlišit se od konkurence. Odlišit se takovou úrovní ochrany dat, kterou všechny společnosti vyžadují pro své zabezpečení - svých počítačů, serverů, dat!

Moderní kybernetická ochrana je:

NADČASOVÁ | ŠPIČKOVÁ | KOMPLETNÍ

a taková, kterou si malé a střední podniky mohou dovolit.



Návod, jak prodat IT bezpečnost jako službu

První fáze - problém

I. Ukažte vašim klientům **PROBLÉM**

Definujte jejich ZTRÁTU v případě nefunkčnosti systémů.

Ukažte klientům, o kolik jejich firma přijde v případě nefungujícího IT.

II. Položte vašim klientům **OTÁZKU**

Máte spočítáno o kolik peněz vaše firma přijde, když se stanete terčem kybernetického útoku?

Co je vyšší? Náklady na ochranu vašich dat nebo případná finanční ztráta z jejich nedostupnosti?

III. Vypočtete ztrátu z **výpadku jejich IT**

K tomu vám dodáme tuto "kalkulačku".

Vzorový příklad

Cena produktivity zaměstnanců	
Roční výnosy	110 000 000,00 Kč
Počet zaměstnanců	20
Průměrný výnos na zaměstnance	5 500 000,00 Kč
Ztráta produktivity zaměstnanců za hodinu	55 000,00 Kč
Počet hodin nutných pro obnovení	36
ODHADOVANÉ NÁKLADY VÝPADKU IT	1 980 000,00 Kč

K této částce je také nutno připočítat cenu za obnovu, ve které může být zahrnut počet hodin nutných k obnově a tím i počet člověkohodin za každého, který se na obnově podílí. V případě potřeby je možné připočítat též cenu za nový hardware.

A nezapomeňte: Jaká bude reputace vaší firmy u zákazníků po úspěšném útoku hackera?

Druhá fáze - peníze

I. Ukažte vašim klientům **PENÍZE**

Jejich peníze - výdaje na zabezpečení. Namodelujte pro vaše klienty situaci jednorázových výdajů vs. měsíční operativní výdaje.

Nikdo nechce platit víc, než musí. Ale menší měsíční částky jsou pro firmy přijatelnější, než jednorázové investice bez garance fungování.

II. Uvedte vašim klientům **PŘÍKLAD**

Stejně jako váš zákazník platí měsíčně za telefon, elektřinu, plyn, teplo apod., tak bude platit za vaše služby. Zkuste vašemu klientovi vypnout, zabavit, znefunkčnit telefon - co by dělal? Co by dělal, kdyby v kanceláři přestalo fungovat topení v -15 °C ?

III. Vysvětlete klientům **ROZDÍL**

U služby je velmi důležitý rozdíl. Pro vaše klienty, ať už stávající či nové to znamená, že platí pouze za to, co aktuálně potřebují.

A navíc. A navíc službu můžete okamžitě přizpůsobit, např. počtu pracovníků, počtu koncových stanic apod.

IV. Ukažte **BENEFITY** a **ŘEŠENÍ**, které získají

Proč je to pro vás i vaše klienty tak atraktivní?

PŘÍKLAD Z IT SVĚTA

Jednorázový nákup MS OFFICE 2016:
Doživotní office 2016 (jen tuto verzi).

Pronájem Office 365:
K dispozici vždy ty nejnovější verze

PŘÍKLAD Z BĚŽNÉHO SVĚTA, KTERÝ JE VÁM DOBRĚ ZNÁM

Nákup nového auta vs. operativní leasing.

Třetí fáze - obchodní nabídka

I. Nabízejte klientům **ZÁŽITEK**

Nejlepší formou prodeje je zážitek!

Nechte vaše potenciální i stávající zákazníky produkt ZAŽÍT - tudíž vyzkoušet. A to ZDARMA!



*Ukažte vašemu
zákazníkovi,
jak je to skvělé*

*Nechte ho,
ať si na to zvykne,
ať si to otestuje*



Pak mu řekněte cenu

"A stejně tak to můžete mít od nás VY"

II.

Osvědčené postupy, které vám prodej usnadní

Zde máte od nás Osvědčené postupy - úspěšné modely nabízející MSP:

Ceny "a la carte"

Zákazníci si vyberou a zaplatí za konkrétní prvky služby, které potřebují.

Balíček / portfolio

Různé úrovně podpůrných balíčků, přístup do portfolia.

Paušální ceny

Hodnotový standardizovaný model, zákazník platí za celkovou „nabídku jídla“.

Ceny založené na uživateli

Paušální poplatek pro uživatele, kdy jsou pokrytá všechna jeho zařízení.

Ceny podle zařízení a koncových uživatelů

Paušální poplatek za každé zařízení, cena se liší v závislosti na typu zařízení.

VÝHODA PRO VÁS jako naše MSP partnery

Pro vás, jako potenciální MSP partnery je zde ještě další výhoda a to ŠKÁLOVATELNOST.

Co takhle, když vám to vysvětlíme na strategii "kafe denně". Zajímá vás to?



POJĎTE RŮST S NÁMI!

3.

Jak na to Krok třetí

Kolik můžeme na IT službách vydělat?

Jaký je celosvětový fenomén, na kterém se i vy můžete svést?

Podle výsledků průzkumu chtějí v oblasti zálohování MSP poskytovatelé vylepšit své nabídky o anti-ransomware ochranu (24 %), obnovu do odlišných prostředí (15 %), a rychlé RTO a RPO platformy (13 %).

Konkrétní příklad

Běžný stav:

- běžně partneři fungují se svými zákazníky projektově
- často jsou nuceni díky veřejným či neveřejným soutěžím jít z cenou jak za HW tak SW na naprosto minimální marži

Co je pak výsledek?

- dodávají projekt, na kterém mají jednorázový zisk typicky mezi 5 a 20%

Žádoucí stav - nabídka služby namísto projektů

- naši partneři využívají takové technologie, které jim umožňují flexibilitu a škálovatelnost
- v takovém případě nepotřebuje partner vydělávat na technologii, vydělává na svém know-how
- cena know-how je individuální a liší se dle konkurence v okolí a kvality partnera
- marže se pak pohybuje ve většině případů nad 50% a peněžní příjem z ní je ve většině případů stabilní, rostoucí a predikovatelný

Finanční porovnání tradiční varianty a varianty služby (neboli MSP):

Varianta tradiční

- 1 000 000Kč zobchodovaného objemu
- roční hrubý zisk 200 000Kč
- další rok je nutné hledat další zdroj příjmů

Varianta Partnera MSP

- 1 000 000Kč zobchodovaného objemu
- roční hrubý zisk 500 000Kč
- další rok pak typicky objem narůstá o 5-20% + je možné řešit získáním dalších klientů, kteří zisk dále zvednou

*Víte, proč každý rok narůstá objem? Podívejte se na škálovatelnost...
Jak můžete tyto služby využít pro svůj růst?*

Výhody služby **MSP**

Základem poskytnuté služby je:

- základní ochrana dat
- dohled nad infrastrukturou a notifikace
- dohodnutý objem servisních hodin

Jak můžete zvyšovat vaši ziskovost?

- garance SLA (Service level agreement) reakce, např. do hodiny 10/5, dražší pak 24/7
- přidáváním dalších služeb: antivirus / antimalware, posouzení zranitelnosti, patch management, možnost vzdáleného připojení na daná zařízení, cloudový prostor

Další možnosti vašeho růstu

- přidáváním dalších zařízení - pokud roste firma, rostete společně s ní
- datová náročnost neustále narůstá cca +20% ročně - díky tomu rostete podle trendu
- další garance klientovi umožní: dostupnost dat, obnovu zařízení kdykoliv a kdekoliv

Nejvyšším standardem je pak Business Continuity: garantování téměř neustálého a bezvýpadkového provozu, taková služba je pak nejdražší a generuje nejvyšší ziskovost



Existuje návod jak s těmito službami ZAČÍT?

5 jednoduchých způsobů jak snižovat fluktuaci zákazníků a začít RŮST

1. Vylepšete své základní (kotevní) produkty pomocí zálohy

- 50% podnikových uživatelů Office 365 přijme zálohovací řešení třetích stran.
- Téměř všechny podniky používají cloudová řešení, jako jsou poštovní schránky Office 365 nebo cloudové úložiště. Nástroje veřejného cloudu však nenabízejí komplexní zálohování. Zde přicházíte se schopností nabízet kompletní a pokročilá řešení BaaS.

2. Chraňte data zákazníků před ransomwarem

- Ransomware zaútočí na firmu každých 14 sekund.
- Ne všechna řešení jsou stejně efektivní – avšak ta s ransomwarovou ochranou umožňující automatickou obnovu infikovaných souborů poskytují MSP poskytovatelům významnou konkurenční výhodu.
- Díky integrované obraně proti ransomwaru poháněné umělou inteligencí s námi partneři získají nové možnosti.

3. Zajistěte, aby se zákazníci vyhnuli prostojům

- Průměrné náklady na jednu minutu neplánovaných odstávek činí cca 200 000,- Kč.
- Pokud jde o disaster recovery (dále jen DR), existuje jedinečná příležitost pomoci malým a středním podnikům, které nemají rozpočet ani odborné znalosti zaměstnanců IT, s implementací komplexního řešení DR. Nabídnout zákazníkům cenově dostupnou alternativu DRaaS znamená, že jsou připraveni na to nejhorší a přitom jim to nenabourá rozpočet.

4. Garantujte plnou kontrolu nad firemními daty

- Výzkum prokázal, že práce na dálku má VELKÝ VÝZNAM v produktivitě a úspoře nákladů.
- Vedoucí společnosti na trhu, jako je např. Dropbox, nabízí synchronizaci a sdílení pouze prostřednictvím jedné možnosti cloudového úložiště - jejich vlastní. Kromě funkcí synchronizace vyžadují zákazníci výběr, flexibilitu a kontrolu nad tím, kde jsou jejich soubory uloženy. Poskytněte jim to a odlište své podnikání pomocí řešení vytvořeného právě pro poskytovatele služeb.

5. Ověřte pravost obchodních údajů

- Očekávaný průměrný roční růst trhu s blockchainovými technologiemi činí 55,6 %.
- Poskytnout zákazníkům možnost ověřit svá klíčová obchodní data zmírňuje bezpečnostní rizika, zajišťuje transparentnost dodržování předpisů a eliminuje jejich potřebu dalšího řešení třetích stran. Se snadno nastavitelnou službou ověření postavenou na blockchainu, elektronickém podepisování a ověřování souborů můžete zvýšit jejich loajalitu k vám (a navíc tak zlepšit svou technologickou reputaci) poskytnutím specializované služby.

Nakonec se dostáváme k praxi

Lidé zodpovědní za podnikové IT systémy nechávali po celá léta finanční ředitele rozhodovat o tom, co je pro IT důležité. Vedení ignorovalo skutečné potřeby IT – návrhy na modernizaci systémů či zavádění moderních řešení. IT odborníci tak byli ve věcech plánování a rozhodování o IT odsunuti stranou. Kdy jsou požádáni o radu a pomoc? Až ve chvíli, kdy se celý systém společnosti zhroutí a přestane fungovat – buď kvůli zastaralosti, nebo následkem kybernetického útoku. V tu chvíli je jedno, že za to mohou finanční nebo generální ředitel, kteří ignorovali jakékoliv potřeby IT. Na vině jsou vždy pracovníci IT a ti musí vše opravit!

Každý ví, že pokud se olej v autě pravidelně nemění, motor jednoho dne přestane fungovat. Jak to, že není jasné, že IT systém potřebuje stejnou pozornost a údržbu?

Co pro to můžete udělat?

Věřte nebo ne, máme tipy, které vám pomohou vyhnout se takovým situacím.



**ZEBRA
SYSTEMS**

Opavská 6230/29A
708 00 Ostrava-Poruba
Czech Republic

Tel: +420 596 912 961
Fax: +420 596 912 963

info@zebra.cz
www.zebra.cz

IČ: 47675462
DIČ: CZ47675462

Acronis

GFI Software™

N-ABLE™
authorized distributor

CLOUDFLARE
PARTNER NETWORK

POJĎTE RŮST S NÁMI!
