N°03 - 2019
technická příloha
K-net Technical International Group

Vaše téma

BEZPEČNOST APLIKACÍ A DAT

Využijte bezpečnostní technologie v rámci K-net Cloud - netDispatcher

Vážení čtenáři,

V Loginu v roce 2017 jsme psali o technikách ochrany vnitřní sítě a webových portálů. Představili jsme proto zařízení typu Next Generation Firewall, Web Application Firewall a podobně.

Tato zařízení jsou pro zajištění ochrany sítě velmi účinná, ale také velmi nákladná na pořízení a náročná na správu. Nemalé peníze stojí roční aktualizace SW a databází a velmi podobné peníze stojí také jejich fyzická správa a monitoring.

Tato zařízení zachytávají velkou řadu událostí a je vhodné tyto události monitorovat, vyhodnocovat a případně dle potřeby upravovat nastavení.

Efektivním řešením může být pronájem těchto služeb v rámci cloudu, kde je možné se o náklady dělit s více subjekty a velmi tak snížit celkové náklady.

V tomto čísle bychom se podívali na možná řešení v rámci služeb K-net Cloud.

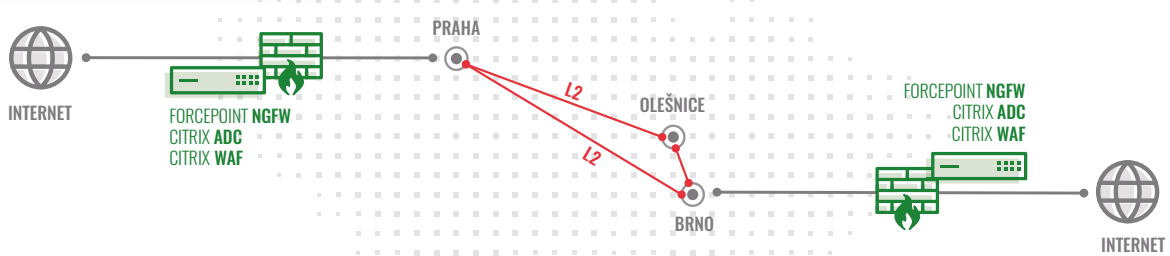
Ing. Petr Nepustil
IT konzultant K-net

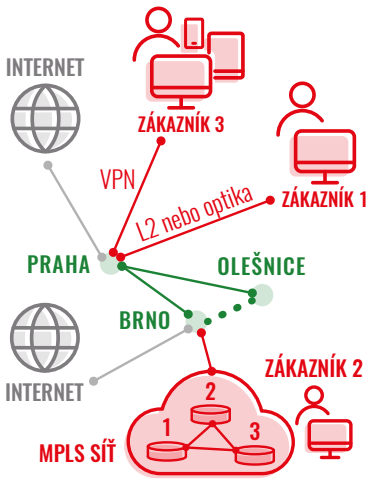
OBSAH TECHNICKÉ PŘÍLOHY:

BEZPEČNOSTNÍ INFRASTRUKTURA K-NET CLOUD

Jakým způsobem je postavená infrastruktura cloudového řešení?

K-net má v České republice 3 datová centra ve 3 lokalitách (Praha, Brno, Olešnice), která jsou vzájemně propojená L2 konektivitou od společnosti O2. Spojení L2 je vyhrazené a oddělené od internetu, čímž je bezpečnější, spolehlivější a rychlejší než běžné spojení přes internet. Připojení do internetu je ze dvou datových center (Praha a Brno). Díky tomu je možné při připojení do kteréhokoli z našich datových center využívat prostředků ostatních datových center K-net prakticky stejně, jako byste byli připojeni do každého z nich zvlášť. To je užitečné pro služby vyžadující vysokou dostupnost, kdy je možné např. využít rozšíření Global Load Balancing, které v případě výpadku internetové konektivity nebo serveru v jedné lokalitě umožní přístup ke službám přes druhou lokalitu. Přístup do internetu je chráněn enterprise-level bezpečnostními technologiemi Forcepoint Next Generation Firewall, Citrix ADC a Citrix WAF s možností dalších bezpečnostních rozšíření. V rámci K-net Cloud je možné využít ve všech lokalitách pronájmu cloudových služeb, jako je pronájem virtuálních serverů (PaaS), pronájem aplikací (SaaS), služby zálohování či disaster recovery a podobně.
Tématem dnešního článku jsou však možnosti využití našich nových cloudových bezpečnostních služeb netDispatcher v případě, že máte svoji serverovou infrastrukturu ve své serverovně, ale chcete ji chránit pokročilými bezpečnostními technologiemi formou pronájmu z cloudu.





JAKÉ JSOU MOŽNOSTI PŘIPOJENÍ DO **K-NET CLOUD**?

Pro využití bezpečnostních služeb netDispatcher v rámci K-net Cloud je nezbytné, aby klienti a síťové služby využívali přístup do internetu v rámci datových center K-net, které chrání bezpečnostní řešení.

Je tedy nutné místní infrastrukturu přesunout do cloudu nebo vlastní serverovnu propojit přímou konektivitou do některého cloudového centra K-net. Přístupových bodů, které je v tuto chvíli možné využít, je v České republice několik. Způsoby připojení jsou následující:

- Vyhrazený optický kabel
- Pronajatá L2 konektivita O2
- MPLS síť od O2 nebo jiného poskytovatele
- VPN

Nejlepším možným způsobem je samozřejmě pronajatý vyhrazený optický kabel do některého přípojného bodu v rámci K-net Cloud. To však není vždy technicky proveditelné a ve spoustě případů to ani nemusí být cenově dostupné. Druhou velmi dobrou variantou je pronájem L2 konektivity, která zajistí přímé propojení do některého datového centra K-net (většinou Praha nebo Brno). Cena se zde odvíjí už pouze od propustnosti linky, ale velkou výhodou je, že jde o spoj na druhé síťové vrstvě, linka tedy není zatížena další režií jako třeba u VPN. Třetí možností je začlenění některého přípojného bodu K-net Cloud do vlastní MPLS sítě od O2 či jiného poskytovatele a následná konfigurace internetové brány v rámci této sítě. Toto je varianta zajímavá v případě, že je na straně zákazníka rozsáhlejší síť lokalit (poboček), kde interní komunikaci zajišťuje i jiný operátor než O2. Poslední variantou, a také asi nejméně cenově náročnou, je konfigurace transparentní VPN z lokality zákazníka do datového centra K-net. Zde je však nutné počítat s režijními náklady v rámci propustnosti linky, kterou si vezme šifrování komunikace přes běžnou internetovou síť. Tato varianta je také o něco méně bezpečná, protože je komunikace sestavována přes internetovou linku a je vhodné mít dobrý router na straně lokality zákazníka (viz rozšíření služby netDispatcher NGFW). Tato varianta je tedy vhodná pouze v případech, kdy se neočekává velký datový provoz do internetu (případně mezi lokalitou zákazníka a datovým centrem K-net).

SLUŽBA **NETDISPATCHER NGFW**

netDispatcher NGFW je služba, která nabízí ochranu vnitřní sítě pomocí Next Generation Firewallu. Tato služba je postavená na technologii Forcepoint (dříve Stonesoft). Jedná se o robustní systémový firewall, který nabízí flexibilní řešení pro ochranu sítě před útoky zvenčí pro podniky všech velikostí.

Díky své hloubkové analýze datového provozu dokáže odhalit i ty nejskrytější hrozby internetového světa, včetně pokročilých metod útoku (tzv. AET - Advanced Evasion Techniques), které jsou aktuálně velkou hrozbou. Řešení nabízí také filtrování webového provozu, ochrany e-mailové komunikace a ochrany před únikem citlivých informací. Útočníci stále více používají techniky pokročilého útoku (AET), které jsou schopny obcházet většinu dnešních bezpečnostních síťových zařízení. AET například dostane malware mezi síťovými vrstvami nebo protokoly pomocí technik, jako je maskování. Toto vše dokáže Next Generation Firewall zastavit. Systém obsahuje antivirový systém, nebo i webový filtr. Vše je postavené na pravidelně aktualizovaných databázích škodlivých kódů a škodlivých chování, které jsou neustále aktualizovány. NGFW tak dokáže rozpoznat potencionální hrozbu a tu automaticky zablokovat nebo informovat bezpečnostního správce o případném potencionálním problému. Velmi efektivně je tak možné odstínit i hackerský útok pocházející z konkrétní lokality.

Příkladem může být jednoduché zablokování přístupu k serveru přes RDP protokol mimo lokalitu České republiky. Aktuálně se totiž jedná o velmi rozšířenou hackerskou aktivitu, kdy se útočník snaží přes tzv. «slovníkový útok» získat přístup k serveru a z něj pak přístup do celé sítě, ať už za účelem získání citlivých údajů či napadení sítě například kryptovirem.

Službu je také možné rozšířit o pronájem vlastního fyzického firewallu, který může být nasazen do vlastního datového centra či na pobočku. Toto rozšíření umožní například vytvoření VPN konektivity do datového centra nebo i bezpečný přístup do internetu přes vlastní internetovou přípojku.

NetDispatcher NGFW se dá takto velmi efektivně využít i v rámci tzv. «hybridních řešeních», kdy má zákazník část infrastruktury u sebe ve vlastním datovém centru a část infrastruktury v datovém centru K-net. Přístup do internetu pak může být směrován primárně přes vlastní internetový spoj, ale v případě výpadku této konektivity je komunikace nasměrována přes datové centrum K-net. Tato funkcionalita však už v případě výpadku nevyřeší přesměrování datové komunikace z internetu na servery zákazníka. Zde už je nutné použít další nabízenou službu, a tou je netDispatcher ADC.

Služba netDispatcher NGFW v sobě obsahuje následující:

- Přístup do internetu z datového centra K-NET dle pořízené datové propustnosti
- Pronájem výkonu sdíleného NGFW firewallu v cloudu (případně pronájem vlastního NGFW firewall zařízení)
- Pravidelně aktualizované databáze signatur, anti-malware, případně web filtru
- Monitoring a dohled nad systémem v režimu 24x7 včetně dostupnosti technika na telefonu
- Pravidelný reporting a informace o potencionálních síťových hrozbách.

SLUŽBA **NETDISPATCHER ADC**

Služba netDispatcher ADC (Application Delivery Controller) je velmi zajímavé řešení pro zvýšení dostupnosti, rychlosti a bezpečnosti vlastních či hybridních cloudových řešení. Služba je postavená na systému Citrix ADC a případně Citrix Gateway.

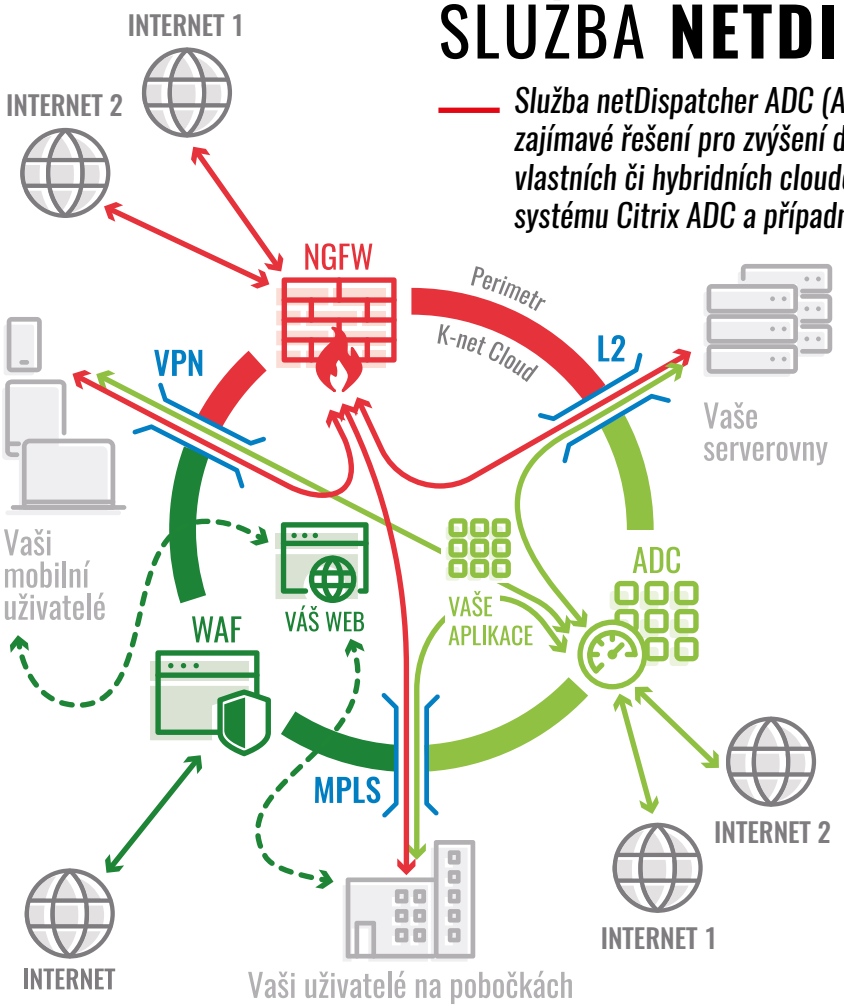
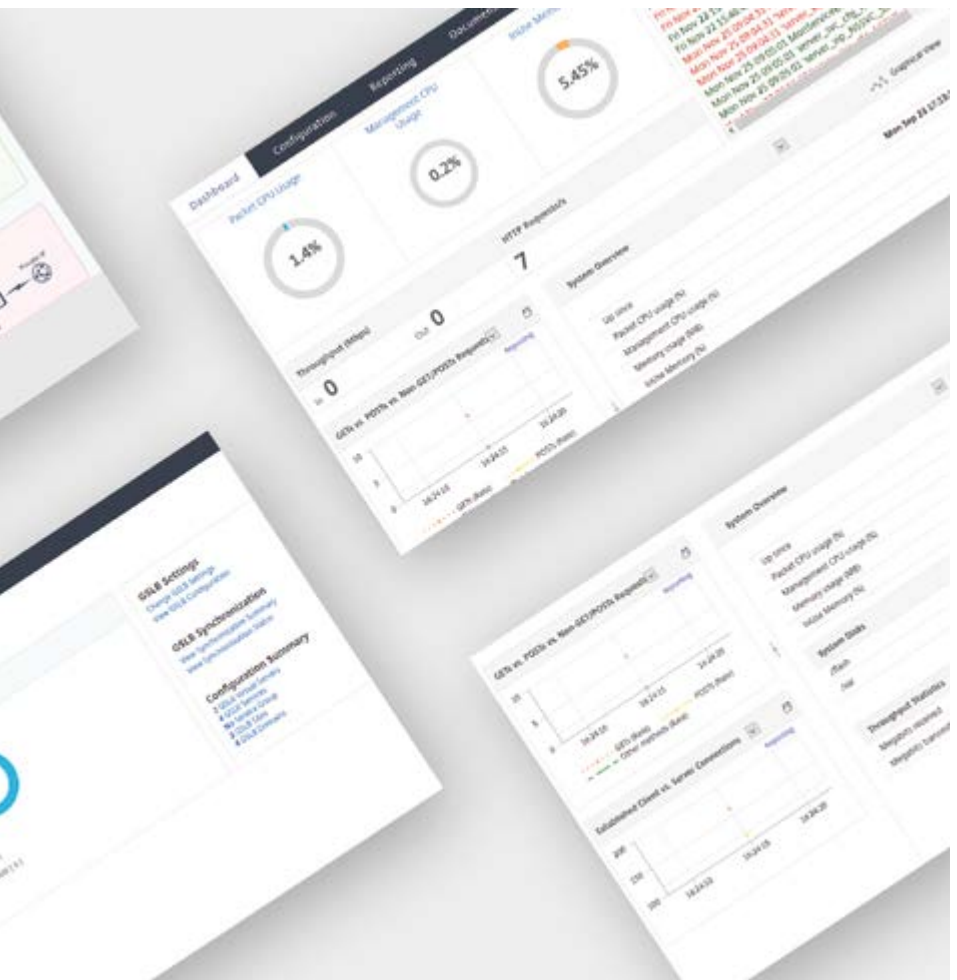


Schéma: služby netDispatcher na perimetru K-net Cloud (uvnitř kruhu) chránící vaše uživatele, aplikace a weby od vnějších nástrah.



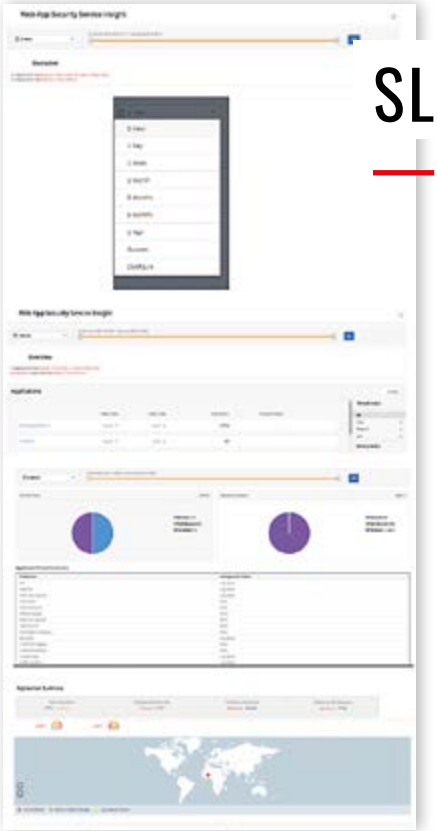
Velmi důležitou funkcionalitou celého řešení je možnost zajištění tzv. «Global Load Balancing» mezi různými datovými centry při přístupu z internetu. Tato funkcionalita zajistí, že v případě výpadku jednoho datového centra či jeho konektivity je provoz automaticky a bezvýpadkově přesměrován na druhé datové centrum. Systém umožňuje i například balancování výkonu některých služeb (například webových serverů), a tím zvyšuje i výkon a odezvu z pohledu uživatele.
ADC dále nabízí optimalizaci komunikačních protokolů pro rychlou odezvu aplikací, jako jsou HTTP/2 a TCP multiplexing, statický a dynamický web content caching, optimalizaci obrázků pro koncová zařízení, akceleraci protokolů TCP a HTTP a TCP optimalizaci pro mobilní sítě.
Umožňuje také velmi bezpečně řešit přístup ke špatně zabezpečeným aplikacím díky převzetí autorizace uživatele přes protokol HTTPS.

Příkladem může být protokol RDP, který tato služba dokáže zabezpečit přes protokol HTTPS. Funguje to tak, že uživatel se přihlásí přes webovou zabezpečenou stránku, systém provede autorizaci s interními autorizačními servery Active Directory a následně je komunikace propuštěna přes protokol RDP. Takto se dá efektivně odstranit problém s hackerskými útoky na otevřený RDP port. Pro další zvýšení zabezpečení je možné doplnit druhý faktor ověření (SMS kód, token v aplikaci, uživatelský certifikát).

Systém je možné rozšířit také o bezpečnostní ochranu webových portálů netDispatcher WAF (Web Application Firewall). Ten umožňuje ochránit interní aplikace před DDoS útoky, nastavit funkcionality jako TLS/SSL, content inspection, a rate limiting.
Služba dále umožňuje rozšířit funkčnost i o SSL VPN pro uživatele z internetu. Jedná se o velmi bezpečný a jednoduchý přístup uživatelů z internetu k interním aplikacím a datům společnosti.

Služba netDispatcher ADC v sobě obsahuje následující:

- Přístup z internetu do datového centra K-net (či infrastruktury zákazníka) dle pořízené datové propustnosti
- Pronájem výkonu Citrix ADC
- Zajištění Global Load Balancing v rámci internetových přípojek K-net Cloud (případně s internetovou konektivitou na straně zákazníka)
- Možnost rozšíření funkcionality o SSL VPN pro uživatele přistupující z internetu
- Monitoring funkcionality v režimu 24x7 včetně dostupnosti technika na telefonu
- Pravidelný reporting a informace o potencionálních kritických událostech.



SLUŽBA **NETDISPATCHER WAF**

Služba netDispatcher WAF (Web App Firewall) je specializované řešení ochrany webových portálů a aplikací. Je postavená na aplikačním firewallu Citrix WAF. Citrix Web App Firewall je jeden z nejlepších WAF firewallů, který chrání webové aplikace a webové stránky před známými i neznámými útoky, včetně celé aplikační vrstvy a «zero-day» hrozeb.

Hlavní vlastnosti Citrix WAF jsou:

- Hybridní bezpečnostní model zabezpečuje ochranu proti novým nepublikovaným hrozbám. Tzv. „positive-model policy engine" kontroluje přípustné interakce mezi uživateli a aplikacemi a automaticky blokuje veškerou komunikaci mimo tuto oblast. Jako doplněk je používán tzv. «negative model engine», který využívá databázi známých útoků a tím chrání weby proti známým aplikačním hrozbám.
- Ochrana XML blokuje nejen běžné hrozby, které mohou být přizpůsobeny pro útoky na aplikace založené na XML (např. cross-site scripting, command injection), ale také zahrnuje bohatou sadu specifických ochran pro XML, včetně komplexní validace schémat a schopnosti zabránit DoS útokům.
- Systém zajišťuje vícenásobnou ochranu dynamických prvků v rámci webových aplikací, jako jsou soubory cookie, pole formuláře a URL adresy, a tím potlačuje útoky, které jsou zaměřeny na vztah důvěryhodnosti mezi klientem a serverem (např. tzv. cross-site request forgery).
- Vyspělý automaticky se učící systém určuje očekávané chování podnikových webových aplikací a generuje doporučení pro politiky, které jsou čitelné pro lidi. Administrátoři pak mohou přizpůsobit bezpečnostní pravidla jedinečným požadavkům každé aplikace, aby se zabránilo detekování «false-positive» událostí.
- Citrix WAF umožňuje podnikům splnit požadavky na zabezpečení dat, jako je PCI DSS, který výslovně podporuje použití WAF pro aplikace orientované na veřejnost, které zpracovávají informace o kreditních kartách. Lze také generovat podrobné reporty, aby dokumentovaly všechny ochrany definované v zásadách firewallu, které se vztahují k mandátům PCI.
- Nejvýkonnější řešení zabezpečení webových aplikací na trhu poskytuje až 12 Gbps komplexní ochrany bez degradace doby odezvy aplikace.

Služba netDispatcher WAF je efektivní bezpečnostní webová brána, snadno použitelná a vysoce výkonná pro zabezpečení webu. Brána je použitelná pro webové portály běžící v rámci K-net Cloud nebo v infrastruktuře zákazníka. Systém umožňuje také sledovat a analyzovat chování uživatelů.
Zákazník tak v rámci služby dostává pravidelný report o bezpečnostních rizicích nejen ze strany případného napadení z internetu, ale také ze strany uživatelů.
NetDispatcher WAF je čistá webová proxy, tedy velkou výhodou je, že uživatel nekončí až na webovém serveru, ale už na tomto bezpečnostním zařízení.
V případě nějakého bezpečnostního incidentu se tak problém nedostane do vnitřní sítě, ale skončí někde v DMZ. Umí také řešit některé standardní bezpečnostní chyby v rámci webových aplikací.

Dobrým příkladem využití služby WAF je zabezpečení webů na populárních, avšak zranitelných a hackery oblíbených webových platformách Wordpress nebo Joomla. Systém dokáže například zablokovat pokus o změnu ceny v rámci objednávky na e-shopu, což je rozdíl oproti firewallu na 7. síťové vrstvě (jako je například i netDispatcher NGFW).

Služba netDispatcher WAF v sobě obsahuje následující:

- Přístup z internetu k webovým portálům dle pořízené datové propustnosti
- Pronájem výkonu Citrix WAF
- Ochrana webových portálu před útoky zvenčí
- Monitoring a dohled nad systémem v režimu 24x7 včetně dostupnosti technika na telefonu
- Pravidelný reporting a informace o potencionálních síťových hrozbách.

+

Máte zájem zvýšit bezpečnost vašeho IT bez velkých investic?
Kontaktujte nás pro nezávaznou konzultaci.
k.k-net.cz/nd-konzultace

K-net Technical International Group, s.r.o.
Olomoucká 170
627 00 Brno – Černovice
tel.: 548 220 150
GSM: 734 686 001
Pobočka: Rovečínská 16
679 74 Olešnice
tel.: 511 447 055

K-net Team Praha, s.r.o.
Sazečská 560/8
108 00 Praha 10 – Malešice
tel.: 734 686 014

K-net Team Ostrava, s.r.o.
Smetanovo náměstí 328/1
702 00 Ostrava
tel.: 734 686 012

facebook.k-net.cz
linkedin.k-net.cz
youtube.k-net.cz
info@k-net.cz

www.k-net.cz

Vysvětlení podtržených výrazů z Loginu a Technické přílohy najdete v glosáři IT pojmů na k.k-net.cz/glosar

Technická příloha časopisu LOGIN 3/2019, ročník č. 14 | *Připravili: Anaëlle Křečková, Petr Nepustil, Jan Knettig, Tomáš Kiedroň, Tomáš Knettig, Věra Staňková*
Vydala společnost K-net | Neprodejné | Uzávěrka čísla: 26. 1. 2020