O2 Next Generation Firewall

Popis služby

O2 Czech Republic a.s.,
IČ 60193336, DIČ CZ60193336, se sídlem Za Brumlovkou 266/2, 140 22 Praha 4 – Michle,
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze oddíl B, vložka 2322

1. Popis zákaznického řešení

Předmětem tohoto dokumentu je stručný popis služby O2 Next Generation Firewall (dále NGFW). Struktura služby je navržena tak, aby zákazník mohl jejich volbou realizovat zásady své bezpečnostní politiky.

Pro realizaci NGFW byla zvolena koncepce soustředění výkonných bezpečnostních HW prvků a centralizované bezpečnosti do jednoho místa, protože je ekonomicky, výkonnostně i z hlediska odolnosti lepším řešením než koncepce rozprostřené bezpečnosti. Pomocí centralizované bezpečnosti lze dosáhnout vyššího stupně zabezpečení s nižšími pořizovacími i provozními náklady.

Centrálně zajišťované služby nad komunikační infrastrukturou výrazným způsobem omezují možnosti průniku z vnějšího prostředí do interního IT prostředí zákazníka a vytvářejí podmínky pro koordinovaný postup zákazníka a poskytovatele proti potenciálním útočníkům.

NGFW je geograficky redundantní bezpečnostní infrastruktura, která je vytvořena zálohováním produkčních prvků ve dvou identických větvích umístěných ve dvou různých lokalitách, čímž se dosahuje vysoké spolehlivosti a dostupnosti poskytovaných služeb. Technologie NGFW je umístěna v hostingových centrech, která splňují vysoké bezpečnostní požadavky s vysokými ochrannými vlastnostmi a jsou certifikovány na Tier III dle Uptime Institutu.

Propojovací prostředí splňuje následující požadavky na oblast počítačové a komunikační bezpečnosti:

- redundantní datová konektivita min. 1 Gbps propojená do dvou nezávislých směrů zakončených na oddělené technologii v různých objektech,
- komunikační infrastruktura, na které jsou poskytovány služby, je technicky a geograficky redundantní,
- komunikační infrastruktura je umístěna v bezpečném prostředí hostingového centra, nebo v prostředí ekvivalentním,
- k systému správy prvků a služeb je řízený přístup (místní i vzdálený) v prostředí odděleném od prostředí zákazníka,
- správu infrastruktury provádějí odborně zdatní pracovníci, disponující odpovídajícími certifikacemi.

Požadavky na bezpečnost jsou garantovány a plněny po celou dobu plnění smluvního závazku.

Provoz je zajištěn v souladu s **ČSN ISO/IEC 17799:2005 Informační technologie – Soubor postupů pro řízení informační bezpečnosti.**

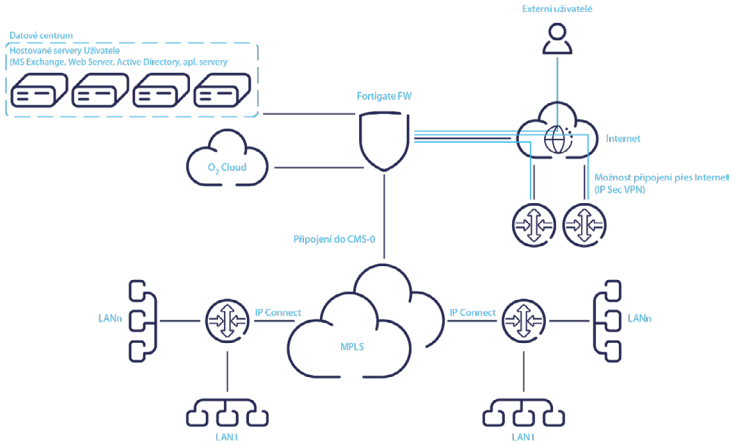
Poskytovatel má propracovaný a vyřešený systém bezpečnosti informací na základě normy **ISO/IEC 17799**, včetně bezpečnosti poskytovaných služeb.

Subdodavatelé poskytovatele splňují stejné podmínky jako poskytovatel.

1.1. O2 Next Generation Firewall

Koncepce NGFW je: nabídnout zákazníkovi komplexní bezpečnostní řešení formou služby. Na internetu je dnes nepřeberné množství různých ohrožení, zranitelností (vulnerability) datových sítí, souborů apod. Malware (tj. viry, trojské koně, spyware, atd.), nevyžádaná pošta (spam), sítě napadených počítačů (botnety), podvodné emaily a stránky (phishing a pharming), organizované hackerské skupiny, a další představuji potenciální ohrožení bezpečnosti pro firmy a jejich podnikání.

Služba NGFW je doplňkovou službou k MPLS VPN (IP Connect Internet) a k ICT službám. Jejím cílem je poskytnutí centrálně spravovaného bezpečného připojení do internetu.



Obrázek 1 – Schéma řešení O2 Next Generation Firewall

O2 Czech Republic a.s., Za Brumlovkou 266/2, 140 22 Praha 4 – Michle
IČ: 60193336, DIČ: CZ60193336, D-U-N-S: 366937597, Zapsaná v OR: MS v Praze, B.2322

Úkolem služby je ochrana a případná filtrace dat na internetovém připojení zákazníka. Ochrana je víceúrovňová a obsahuje:

- ochranu před útoky (firewall + IPS)
- ochranu nevyžádanými maily (antispam)
- ochranu před malware (antivir)
- obsahovou filtraci webu (webfiltering/content filtering/URL filtrace)
- řízení aplikací (application control)
- ochranu před únikem interních dat (DLP)
- VPN (IPSec i SSL, klientská i site-to-site)
- reporting

Služba NGFW je postavena na bezpečnostních produktech společnosti Fortinet. Konkrétně jde o UTM řešení FortiGate (využívá ASIC technologii), emailové bezpečnostní řešení FortiMail a nástroje pro reporting FortiAnalyzer. Společnost Fortinet patří k vedoucím společnostem v bezpečnostní oblasti.

O2 je certifikovaným partnerem společnosti Fortinet a disponuje řadou techniků, kteří mají certifikaci FCNSP = Fortinet Certified Network Security Professional.

Obrázek 2 – Firewall Fortigate

Zřízení služby nepředstavuje pro zákazníka instalaci žádného zařízení ani software. Pro implementaci služby NGFW k internetovému připojení v lokalitě zákazníka je nevýhodnějším řešením propojení koncového zařízení v lokalitě zákazníka s jeho dedikovaným virtuálním firewallem (VDOM) pomocí VPN spojení (IPSec, GRE) přes internet. Následně pak úprava nastavení koncového zařízení tak, aby komunikace zákazníka z / do internetu procházela tímto tunelem přes jeho virtuální firewall, kde bude možné provádět požadované bezpečnostní akce, dle jeho volby.

Díky konektivitě prostředí NGFW do MPLS (IP Connect) a propojení s infrastrukturními službami (Housing, Cloud) lze dále službu propojit i s těmito službami, nyní už bez nutnosti VPN spojení.

Veškerá příchozí i odchozí komunikace zákazníka prochází bezpečnostní platformou poskytovatele, který zajišťuje její ochranu a správu systémů zákazníka a dodržování definovaných bezpečnostních politik.

O2 Czech Republic a.s., Za Brumlovkou 266/2, 140 22 Praha 4 – Michle

IČ: 60193336, DIČ: CZ60193336, D-U-N-S: 366937597, Zapsaná v OR: MS v Praze, B.2322

1.2. Přehled variant NGFW

Tabulka 1 - Přehled variant NGF

NGFW	Varianty hlavní služby		Doplňkové služby	
	Advanced	Premium	Antispam	Správa 4h
Firewall	✓	✓	✗	✗
IPS	✓	✓	✗	✗
Antivirus a antimalware	✓	✓	✗	✗
Webfiltering	✓	✓	✗	✗
Application control	✓	✓	✗	✗
VPN	✗	✓	✗	✗
Data Los Prevention (DLP)	✗	✓	✗	✗
Reporting	✗	✓	✗	✗
Antispam	✗	✗	✓	✗
Správa	✗	✗	✗	✓

1.2.1. Nabízené služby

Firewall

Stavový firewall na síťové vrstvě (L3). V jeho nastavení je možné vybírat, které protokoly (TCP, UDP, ICMP apod.), na kterých portech a na kterých dotčených IP adresách a v jakém směru (příchozí, odchozí) se uplatní definované akce (základní akce ACCEPT, DENY a dále monitoring, traffic shaping, apod.)

IPS

IPS = Intrusion Protection System je systém pro prevenci narušení. Sleduje pomocí IPS senzorů síťový provoz na výskyt definovaných anomálií a signatur útoků Anomálie jsou to, když útočník používá síťovou komunikaci jako zbraň. Typicky se jedná o zahlcující (flood) komunikace, jejichž cílem je odepření koncové služby (DoS – Denail of Service). Není ochranou proti distribuované variantě (DDoS, kdy není schopen se vyrovnat s násobně většími toky, obranou proti těmto útokům je další bezpečnostní služba O2 – AntiDDoS). Druhým typem obrany je obrana založená na signaturách. Každý útok je charakterizován specifickou sekvencí v komunikaci, kterou lze odhalit a na základě toho blokovat daný provoz. Tento typ se používá pro ochranu systémů, na které není aplikován (případně dostupný) softwarový patch, který danou zranitelnost řeší (zero day útoky apod.).

Antimalware (antivirus)

Antivirová funkcionalita prohledává komunikaci na výskyt malwarových sekvencí v rozličných druzích komunikace: HTTP, FTP, IMAP, POP3, SMTP a NNTP, včetně šifrovaných variant. Skenuje na výskyt virů také souborové archivy (ZIP, RAR …) včetně několinásobně zanořených archivů (ZIP v ZIPu).

Pracuje se všemi druhy malware, tedy nejen viry, ale také trojskými koni, spyware, síťovými červy apod. Pro detekci využívá neustále aktualizovanou databázi signatur.

Web filter

Webová filtrace je nedílnou součástí NGFW. Její aplikace je vhodná jednak pro zajištění bezpečnosti (návštěvy nebezpečných stránek), ale stejně tak poskytuje možnost filtrace stránek s nevhodným pracovním obsahem a je potom nástrojem na zvýšení produktivity, či „zrychlení" linky díky odstranění nežádoucí komunikace.

Tři hlavní části webového filtru jsou následující:

- obsahový filtr (Web Content Filter)
- URL Filter
- a služba FortiGuard Web Filtering,

Poskytují maximální kontrolu nad tím, co je možné na internetu navštěvovat a kým. Obsahový filtr hledá definovaná slova (specifikovaná divokými znaky či regulárními výrazy), URL filtr používá databázi vyjmenovaných domén a služba FortiGuard Web Filtering definuje desítky kategorií a do těchto kategorií řadí jednotlivé domény na denní bázi.

O2 Czech Republic a.s., Za Brumlovkou 266/2, 140 22 Praha 4 – Michle
IČ: 60193336, DIČ: CZ60193336, D-U-N-S: 366937597, Zapsaná v OR: MS v Praze, B.2322

Opět je možné uplatnit několik akcí, co se má při návštěvě definované stránky stát, např. akce: **Allow** (povolit), **Monitor** (povolí návštěvu a provede záznam do logu, je možné využít ke kvótám), **Warning** (varování upozorňovací stránkou, po odsouhlasení je přesměrováno), **Authenticate** (před návštěvou stránky je nutné se autentizovat) a **Block** (zablokuje návštěvu).

Application Control

Jedná se o řízení síťových aplikací. Díky spojení se službou FortiGuard Applicaton Control, NGFW rozeznává na základě parametrů více než tisíc různých síťových aplikací, které jsou řazeny do kategorií. Tyto kategorie jsou například Hry (Games), Botnet, P2P apod. Na tedy základě identifikace aplikace provádět různé akce (obdoba funkcionality u web filteringu).

VPN

NGFW poskytuje možnost vytváření virtuálních privátních sítí (VPN) na bázi protokolu SSL a TLS. Podporuje různé verze těchto protokolů. VPN sítě je možné vytvářet v několika formách, tzv. bezklientské či pouze webové formě – pro vybrané protokoly (http, CIFS, FTP apod.) je vytvořen zabezpečený webový portál na který jsou tyto služby publikovány a přistupující uživatel nepotřebuje instalaci žádného VPN klienta. K přístupu stačí pouze webový prohlížeč podporující SSL a TLS.

Druhou formou je tunelový mod, kdy je potřeba klientský software (VPN klient). Podporovány jsou majoritní platformy (Windows, Apple Mac OS-X a Linux CentOS a Ubuntu).

U obou variant je možnost volby různých autentizačních mechanizmů, v případě doplnění o speciální zařízení (FortiToken) včetně dvou faktorové.

Kromě SSL VPN zařízení umožňuje vytváření i IPSec VPN, včetně site-to-site VPN.

Data Leak Prevention (DLP)

DLP zabrání odesílání citlivých informací zákazníka mimo společnost a tím úniku důvěrných informací. Umožňuje kontrolu odchozích i příchozích dokumentů na základě různých parametrů (obsah dokumentu, vodotisk, jméno souboru, specifický otisk – fingerprint apod.). Na základě shody s kontrolou je možné provést řadu akcí (nic, blokování, karanténa, logování). DLP se uplatňuje na e mailovou, http, ftp a IM komunikaci. Kromě standardní DLP funkcionality, je možné DLP využít také v archivačním módu, kdy je možné zaznamenávat aktivitu daných souborů.

Reporting

Na základě definovaných pravidel je vytvářen komplexní report v několika formátech (PDF, HTML apod.), který je možné zasílat emailem, případně si ho ze zařízení stahovat. Parametrizovatelný report v podobě grafů a tabulek popisuje využití služeb (např. četnost virů, provoz, uživatelé, blokované stránky apod.) za definované období.

Antispam

Antispam je doplňkovou službou, která využívá prvky FortiMail pro detekci nevyžádané pošty. Opět jde o geograficky redundantní cluster rozmístěný ve dvou datových centrech. Kromě vlastní antispamové funkcionality nabízí také karanténu pro zachycené zprávy (pro eliminaci tzv. false positive). Službu je možné implementovat také samostatně bez nutnosti ostatních komponent NGFW.

Správa

Konfigurační a konzultační podpora, kde zákazník nemá administrátorské oprávnění ke správě bezpečnostní platformy (VDOM), ale veškeré konfigurační zásahy provádí na základě požadavků zákazníka vyškolený personál poskytovatele. Tato podpora obsahuje 4 h pracovního času měsíčně.

1.3. Hlavní výhody a přednosti služby

Bezkonkurenční bezpečnost

- inteligence pro odhalování hrozeb je postavena na miliardách transakcí denně (FortiGuard).
- ochrana je zajištěna pro každý bajt webové transakce – příchozí i odchozí.
- nejmodernější a nejkomplexnější zabezpečení webu s garancí SLA.

O2 Czech Republic a.s., Za Brumlovkou 266/2, 140 22 Praha 4 – Michle
IČ: 60193336, DIČ: CZ60193336, D-U-N-S: 366937597, Zapsaná v OR: MS v Praze, B.2322

Vysoká dostupnost

- geograficky redundantní řešení v certifikovaných datových centrech

Jednoduchost a účinnost

- odstranění složitosti a konsolidace samostatných zařízení v lokalitách
- jednotný přístup ke globálnímu řízení bezpečnostní politiky a reportingu
- flexibilní a škálovatelné řešení dle rostoucích potřeb
- snadná a rychlá implementace
- místo investičních nákladů (CAPEX) má zákazník pravidelné měsíční náklady (OPEX), které lze snadno plánovat
- přináší prokazatelný efekt již od prvního dne
- konsolidované sledování provozu v reálném čase a reporting

1.4. FortiGuard

FortiGuard je celosvětová síť firmy Fortinet, jak ukazuje následující schematický obrázek.

Obrázek č. 3 - Celosvětová síť FortiGuard

Tato síť má za úkol sledovat a analyzovat aktuální dění na internetu a na základě jeho stavu připravovat a následně doručovat aktualizace do jednotlivých zařízení FortiGate, aby byly schopné čelit bezprostředním bezpečnostním rizikům a hrozbám.

Jednotlivé laboratoře jsou umístěny v Kanadě, Číně, Francii, Japonsku, Malajsii a ve Spojených státech, kvůli rozložení rizik a také pro snadné pokrytí všech časových pásem (laboratoře fungují v režimu 24×7×365). Tým specialistů FortiGuard spolupracuje také s vedoucími světovými organizacemi, které monitorují aktuální hrozby (např. je jedním z členů Cyber Threat Alliance).

Pro představu, během běžného týdne FortiGuard přidá nebo aktualizuje průměrně:

- přes sto tisíc antivirových definic (signatur)
- několik desítek IPS definic
- přes půl milionů URL zařazení do webfiltering kategorií (v 65 jazycích)
- okolo třiceti miliónů antispamových signatur

Na stránkách FortiGuard lze snadno dohledat aktuální signatury a nastavení pro všechny nabízené ochrany.

1.5. O2 Antispam

Služba O2 Antispam je navazující službou na službu NGFW, jenž nabízí Uživateli komplexní bezpečnostní řešení formou služby vzhledem k tomu, že na internetu je dnes nepřeberné množství různých ohrožení, zranitelností (vulnerability) datových sítí, souborů apod. Malware (tj. viry, trojské koně, spyware, atd.), **nevyžádaná pošta (spam)**, sítě napadených počítačů (botnety), podvodné emaily a stránky (phishing a pharming), organizované hackerské skupiny, a další představuji potenciální ohrožení bezpečnosti pro firmy a jejich podnikání.

O2 Czech Republic a.s., Za Brumlovkou 266/2, 140 22 Praha 4 – Michle
IČ: 60193336, DIČ: CZ60193336, D-U-N-S: 366937597, Zapsaná v OR: MS v Praze, B.2322

Služba NGFW a O2 Antispam jsou doplňkovou službou k internetovým službám (O2 Internet Business), k MPLS VPN (IP Connect) a k hostingovým službám (Hosting, Cloud). Jejím cílem je poskytnutí centrálně spravovaného bezpečného připojení do internetu. Službu O2 Antispam lze realizovat i jako samostatné řešení.

Úkolem služby O2 Antispam je:

- Ochrana před nevyžádanými maily (antispam)

Pro zřízení služby není nutné instalovat žádné zařízení ani software.

O2 Antispam je doplňkovou službou, která využívá prvky FortiMail pro detekci nevyžádané pošty. Jde o geograficky redundantní cluster rozmístěný ve dvou datových centrech. Kromě vlastní antispamové funkcionality nabízí také karanténu pro zachycené zprávy (pro eliminaci tzv. false positive). Službu je možné implementovat také samostatně bez nutnosti ostatních komponent NGFW.

1.5.1. Hlavní výhody a přednosti služby O2 Antispam:

Vysoká dostupnost

- geograficky redundantní řešení v certifikovaných datových centrech

Jednoduchost a účinnost

- odstranění složitosti a konsolidace samostatných zařízení v lokalitách
- jednotný přístup ke globálnímu řízení bezpečnostní politiky a reportingu
- flexibilní a škálovatelné řešení dle rostoucích potřeb
- snadná a rychlá implementace
- místo investičních nákladů (CAPEX) má Uživatel pravidelné měsíční náklady (OPEX), které lze snadno plánovat
- přináší prokazatelný efekt již od prvního dne
- reporting

1.6. Služba FortiMail

1.6.1. Popis služby

FortiMail je služba elektronické pošty, která ochraňuje cílové poštovní systémy zákazníka. Služba řeší požadavky na ochranu před spamem, zavirovanými zprávami a nedovoleným obsahem. Je provozována na hardwarové platformě Fortinet, kterou tvoří geografický cluster. Antispamová a antivirová databáze se aktualizuje každou celou hodinu.

1.6.2. Popis filtrů

Služba FortiMail má tři základní bloky filtrů – Antispamové, Antivirové a Content. Každý filtr je popsán svým profilem a návaznou akcí. Definice pravidel, profilů a akcí je v kompetenci poskytovatele služby a není přístupná zákazníkům. Případné změny konfigurace se provádějí na základě požadavku přes Service Desk poskytovatele. Zákazník má ve své kompetenci přístup do karantény, uvolňování zpráv z karantény a editaci black/white listu.

Antispamové filtry jsou zodpovědné za rozpoznávání spamových poštovních zpráv. Základním filtrem je filtr Fortiguard, který je spojen se stejnojmennou službou výrobce.

Antivirové filtry pracují na stejném principu jako antivirové programy. Lokální antivirová databáze je pravidelně aktualizována a každá přijatá zpráva a nezašifrovaná příloha je testována na přítomnost viru.

Content filtry nám umožňují definovat různé parametry pro přiložené soubory jako např.: přípony souborů, MIME typy, dokumenty Office, ochrana heslem dokumentu, práce s archivy a další.

1.6.3. Karanténa

Karanténa slouží jako uložiště spamových zpráv. Každý zákazník získá přístup do karantény přes webové rozhraní, které mu umožňuje editaci karantény a uvolňování uložených zpráv tj. přeposlání zpráv původnímu příjemci. Zprávy, které byly uloženy do karantény, jsou automaticky vymazány z této karantény po 14 dnech. Součástí služby je zasílání reportů se seznamem uložených zpráv jednotlivým příjemcům.

1.6.4. Black/White listy

Black/White listy slouží pro vytvoření seznamu odesílatelů na základě vlastního požadavku zákazníka. Přidáním odesílatele na black list znamená, že zpráva od tohoto odesílatele je systémem odmítnuta. Služba je nastavena s předvyplněným

O2 Czech Republic a.s., Za Brumlovkou 266/2, 140 22 Praha 4 – Michle
IČ: 60193336, DIČ: CZ60193336, D-U-N-S: 366937597, Zapsaná v OR: MS v Praze, B.2322

black listem, který lze libovolně modifikovat. Přidáním odesílatele na white list způsobí, že zpráva od toho odesílatele obchází blok antispamových filtrů. Každý zákazník získá přístup k vlastnímu black/white listu přes webové rozhraní.

1.6.5. Fronta

Přijaté zprávy jsou podrobeny kontrole a následně zařazeny do odchozí fronty. Není-li možné zprávu doručit okamžitě z důvodu překážky mimo vlastní systém, je zpráva ponechána v odchozí frontě a systém se ji snaží opakovaně doručit každých 15 minut. Pokud se to nedaří, je odesílatel zprávy po 1 hodině systémem informován pomocí NDR zprávy. Nepodaří-li se doručit zprávu do 24 hodin od prvního pokusu, je zpráva označena jako nedoručitelná a odesílatel zprávy je o této skutečnosti opět systémem informován.

1.6.6. Příchozí zpráva pro chráněnou doménu

Výchozí nastavení příchozích zpráv je následující:

- Maximální velikost zprávy 20 MB
- Počet adresátů 90
- Antispamové, Antivirové a Content filtry dle tabulky výše
- Na požádání je možné zapnout verifikaci příjemce proti LDAP serveru zákazníka

1.6.7. Odchozí zpráva z chráněné domény

Výchozí nastavení odchozích zpráv je následující:

- Odesílací server zpráv je selektivně povolen administrátorem systému
- Zprávy mají v poli From: chráněnou doménu zákazníka
- Maximální velikost zprávy 200 MB
- Počet adresátů 200
- Antivirový filtr dle tabulky výše
- Komunikace s SMTP serverem zákazníka je bez autentizace

1.6.8. Migrace

Základní konfigurace služby je spuštěna po podpisu smlouvy, jejíž součástí jsou názvy chráněných domén, kontaktní údaje administrátorů, kteří získají přístup ke karanténě a black/white listům chráněné domény a unikátní veřejná IP adresa / DNS záznam typu A pro odchozí provoz z chráněné domény. V rámci migrace na službu FortiMail je nutné nastavit MX záznam smtp.hosting-centre.cz pro chráněnou doménu na DNS serveru zákazníka a ponechat pouze tento jeden. Všechny další MX záznamy pro chráněnou doménu musí být smazány. Je-li zákazníkem využíván SPF záznam, pak je nutné jej doplnit příslušným údajem.

1.6.9. Podpora

Některá výchozí nastavení služby lze po konzultaci změnit, popřípadě message's flow doplnit o nová pravidla pro zohlednění specifických požadavků zákazníka.

2. Servisní, záruční a provozní podmínky

2.1. Zákaznická podpora – Service Desk

Poskytovatel poskytuje ke službě O2 NGFW zákaznickou podporu na první a druhé úrovni.

Service Desk poskytovatele je jednotným kontaktním místem pro žádosti o zákaznickou podporu.

Kontaktní údaje:

800 333 777 (volba 3 – ICT)

ict_sd@o2.cz

O2 Czech Republic a.s., Za Brumlovkou 266/2, 140 22 Praha 4 – Michle
IČ: 60193336, DIČ: CZ60193336, D-U-N-S: 366937597, Zapsaná v OR: MS v Praze, B.2322

Service Desk zajišťuje především:

- zakládání a evidence incidentů
- poskytování informace o průběhu řešení incidentu zákazníkovi (na vyžádání)
- eskalace incidentu při nedodržení SLA
- Service Desk řeší odpovědi na běžné dotazy typu:
    - nedaří se mi přihlásit se do administračního webového rozhraní
    - v případě sjednané doplňkové služby Správa:
        - nemohu se dostat na stránku, na kterou chci i přesto, že ji mám v pravidlech povolenu
        - nefunguje blokace na stránku, na kterou bych se podle nastavených pravidel neměl dostat

Požadavky na zákaznickou podporu jsou hlášeny pověřenými zástupci zákazníka (kontaktní osoby). Požadavky jsou v závislosti na jejich typu řešeny přímo poskytovatelem, nebo jsou postupovány dále na dodavatele / výrobce technologie.

Zákazník zajišťuje nultou úroveň podpory:

- provádí rutinní činnosti většinou spojené se správou uživatelů a definicí nových politik, monitoringem, reporty atd.
- poskytuje podporu vlastním uživatelům (zaměstnancům).

Zákaznická podpora poskytovaná ze strany poskytovatele zahrnuje:

- řešení nastalých provozních incidentů včetně případné eskalace na dodavatele nebo výrobce dané technologie.
- zajištění dostupnosti nabízeného řešení dle parametrů SLA pro jednotlivé poskytované služby včetně dohledů a pravidelné údržby těchto služeb na systémové a bezpečnostní úrovni.

Technická podpora nepokrývá žádné změnové požadavky zákazníka. Ty jsou řešeny vždy na základě objednávky a kalkulovány hodinovou sazbou.

O2 Czech Republic a.s., Za Brumlovkou 266/2, 140 22 Praha 4 – Michle
IČ: 60193336, DIČ: CZ60193336, D-U-N-S: 366937597, Zapsaná v OR: MS v Praze, B.2322