Dokumenty EDRi

VYDÁNÍ 03


# JAK FUNGUJE INTERNET

Průvodce pro ty, kteří určují pravidla



EDRi

iure ...není nám to jedno

Tento text má těm, kteří se podílejí na vytváření pravidel, poskytnout základní přehled o internetu a s ním souvisejících technologiích. Jeho cílem je poskytnout přehledné základní informace o některých základních technologiích, které tvoří páteř internetu. Doufáme, že bude cennou referencí, pomůže vám vyznat se v žargonu a objasní, jak funguje otevřený internet, na kterém v současné době závisí tolik občanských svobod a takové množství ekonomických aktivit.

**Autoři:**
Joe McNamee, Kirsten Fiedler, Marie Humeau & Sophie Maisuradze

**Design:**
CtrlSPATIE

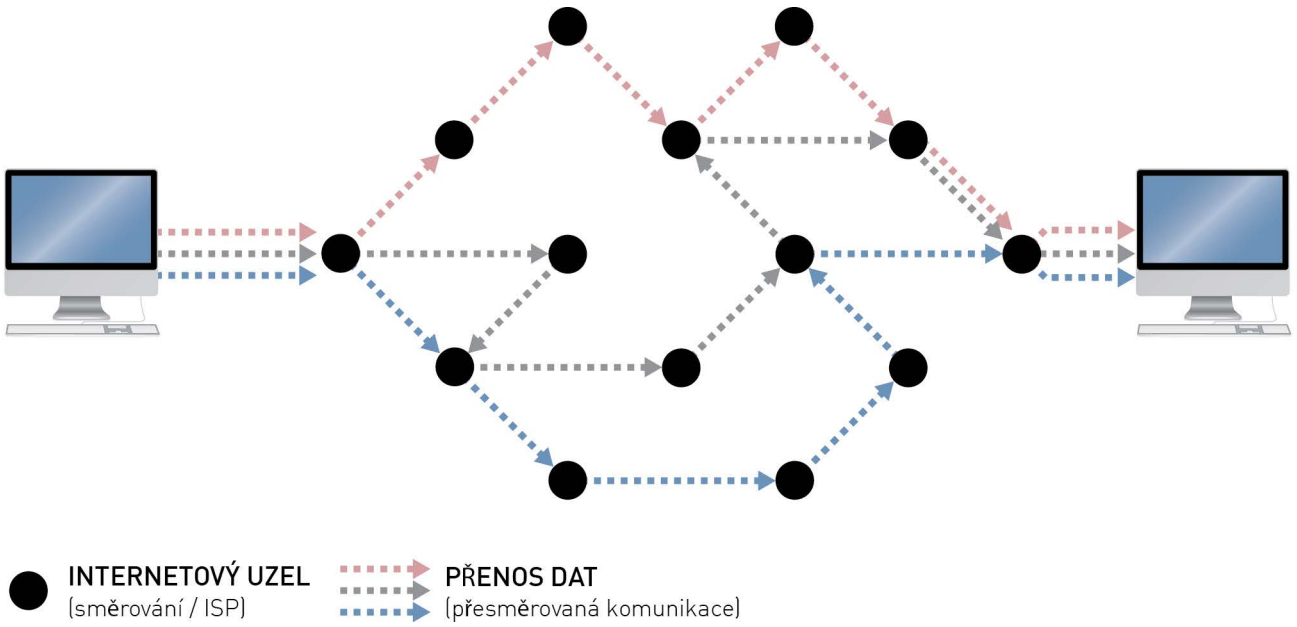
**Překlad do češtiny:**
Zuzana Veselá
Iuridicum Remedium, o.s.
Pplk. Sochora 40
170 00 Praha 7
tel.: +420 776 703 170
iure@iure.org

**European Digital Rights (EDRi) je asociace 36 nevládních organizací zabývajících se ochranou soukromí a digitálními právy z 18 zemí**

**European Digital Rights**
20 Rue Belliard
B-1040 Brussels
tel: + 32 (0)2 274 25 70
brussels@edri.org

# INTERNET

## SÍŤ POČÍTAČOVÝCH SÍTÍ




**Internet je celosvětový systém propojených počítačových sítí.**

Když se dvě nebo více elektronických zařízení (např. počítačů) spojí takovým způsobem, že spolu mohou komunikovat, stávají se součástí sítě. Internet se skládá z celosvětového propojení takových sítí patřících firmám, vládám i jednotlivcům, a ty umožňují všem k takovým sítím připojeným zařízením, aby spolu navzájem komunikovaly.

Aby spolu počítače mohly komunikovat, musejí si rozumět. Komunikace na internetu je možná díky tomu, že všechna zařízení užívají stejný „jazyk“, konkrétně internetový protokol (IP), „jednotný trh“ bez fyzických, technických či národních překážek. Ten představuje základ pro veškeré další systémy komunikace na internetu.

Vyslat jakoukoli komunikaci přes Internet prostřednictvím internetového protokolu je dost podobné, jako poslat stránky knihy poštou v mnoha jednotlivých obálkách. Všechny obálky budou mít stejnou adresu odesílatele a stejného adresáta. I když některé obálky bude přepravovat loď a jiné letadlo, všechny nakonec dorazí do stanoveného místa určení a knihu bude

možné zase poskládat dohromady. Nesejde na tom, že stránka 47 dorazila dřív než stránka 1.

Obsah takových obálek na internetu závisí na konvencích / protokolech (domluvených formátech), pro každý typ komunikace je jeden. Uveďme si několik příkladů takových konvencí, které se opírají o internetový protokol:

- SMTP pro zasílání e-mailů

- http pro přístup k webovým stránkám či

- BitTorrent pro sdílení souborů mezi rovnocennými uzly (tzv. P2P) (jedná se o způsob výměny datových souborů mezi velikými skupinami osob).

Kdokoli si může vymyslet vlastní konvenci / protokol a používat ho na internetu, pokud bude fungovat na bázi internetového protokolu. Jinými slovy, jediné omezení tvoří hranice lidské představivosti. Jediné pravidlo zní, že adresa na obálce bude ve standardním formátu. Právě otevřenost systému dělá z internetu celosvětový fenomén. Každé omezení otevřenosti snižuje jeho potenciál pro budoucí vývoj. Obecné používání jednoho protokolu pro veškerou komunikaci má mnoho zásadních výhod. Zařízení, která mají na starosti přenos internetových dat (zvaná routery), nemusejí být programována různě pro různé typy dat – dokonce ani nepotřebují žádné informace o přenášených datech, pokud je u všech z nich použit internetový protokol. Je to jako když pošťák doručuje tradiční poštu – podívá se pouze na obálku a je schopen zprávu doručit. Bez ohledu na to, jestli je v obálce složenka, nebo milostný dopis (na tom už záleží pouze adresátovi).

To s sebou přináší:

- Možnost neomezených inovačních možností ve smyslu nových protokolů a aplikací;

- „Privacy by design“: technologie je od počátku koncipovaná s ohledem na soukromí a není nutné cokoli vědět o obsahu komunikace;

- Flexibilní a rychlý tok dat.

Základní funkcí internetu je jedna jediná flexibilní služba: přenos dat od jednoho zařízení ke druhému bez ohledu na povahu takového zařízení, bez ohledu na to, jak a kde jsou zařízení na internet připojena, a bez ohledu na povahu a obsah dat.

Právě otevřenost a flexibilita je primární pro inovace a demokratický i ekonomický úspěch internetu.

**“Právě otevřenost a flexibilita je primární pro inovace a demokratický i ekonomický úspěch internetu.”**

# IP ADRESA

## DIGITÁLNÍ ADRESA

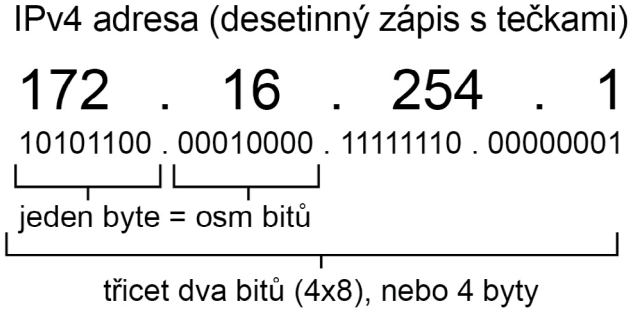
IP adresa je numerická adresa, která je přiřazena každému zařízení připojenému k internetu.[01]

V mnoha případech lze IP adresu využít pro identifikaci organizace nebo jednotlivce, který využil službu poskytovatele internetových služeb za účelem připojení jednoho nebo více zařízení k internetu.

V dalších případech, především ve společných sítích, veřejných či nechráněných bezdrátových připojeních, IP adresa ne vždy identifikuje konkrétního jednotlivce, který udělal něco digitálně dohledatelného.

Vzhledem k tomu, že běžný router v domácnostech a firmách často ukazuje pouze jednu IP adresu pro všechny osoby, které jsou k němu připojené, lze podle IP adresy určit spíše skupinu lidí než jednotlivce. V důsledku toho nebývá často jednoduché nebo dokonce ani možné pouze na základě IP adresy určit, kdo přesně co udělal.

Na druhou stranu velice často mohou IP adresy určovat jednotlivce, takže v souladu s principem základní prevence je k nim třeba takto přistupovat, dokud se s konečnou platností neukáže, že tomu tak není.

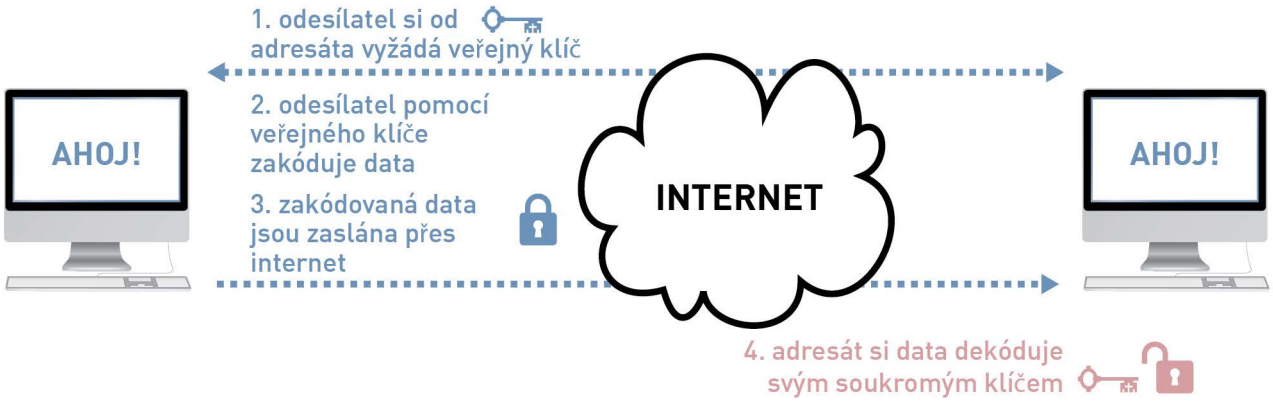



**“IP adresa ne vždy identifikuje konkrétního jednotlivce, který udělal něco digitálně dohledatelného.”**

01 Vzhledem k nedostatku stávající generace IP adres se především ve firemních sítích stále častěji IP adresy sdílejí – sdílejí je například všechny počítače v jedné kanceláři. Stávající nedostatek by měl pominout po zavedení IPv6 adres.

# ŠIFROVÁNÍ

## SOUKROMÍ NA VEŘEJNÉ SÍTI




**Jak může uživatel poslat zprávu s citlivými údaji tak, aby zůstala uchráněna před zraky „zvědavých očí“? Když posíláte dopis, mohou ho zachytit, otevřít, přečíst a znovu zavřít, aniž by po takovém zásahu zanechaly stopy. Telefonní rozhovor může být odposloucháván.**

Rychlý vývoj šifrování začal ve dvacátém století s vývojem počítačových technologií. Počítače umožňovaly nejen daleko rychlejší šifrování elektronických zpráv, ale také daleko rychlejší rozluštění doposud užívaných šifrovacích klíčů.

Šifrování není zázračný všelék a nezaručuje naprosté utajení. Častý způsob, jak obejít šifrování, je zachycení zprávy ještě předtím, než bude zašifrována – například pomocí utajeného programu, tzv. trojského koně, který je nainstalován na počítači odesílatele. Ten sleduje veškeré klávesy, které na klávesnici nebo dokonce na mobilním telefonu oběti někdo stiskne.

Dalším atributem, který téměř vždy musíte při šifrování zprávy chránit, je její integrita (tj. úplnost souboru). Jinak je možné se zprávou manipulovat i bez znalosti šifrovacího klíče. Uznávané šifrovací nástroje tohle udělají automaticky za vás.

Na obrázku vidíte fáze šifrování veřejným klíčem, celé to funguje na principu dvou klíčů, jednoho veřejného a jednoho soukromého:

1. Odesílatel si vyžádá kopii veřejného klíče.

2. Odesílatel pomocí odpovídajícího softwaru zašifruje zprávu podle příjemcova veřejného klíče.

3. Zpráva je odeslaná.

4. Adresát zprávu dešifruje pomocí veřejného i soukromého klíče společně.

# SYSTÉM DOMÉNOVÝCH JMEN

## (DNS, DOMAIN NAME SYSTEM)

### TELEFONNÍ SEZNAM INTERNETU


Když umístíte na internet webovou stránku, bude dostupná podle numerické IP adresy webového hostitelského serveru (v době přípravy tohoto textu byla například adresa EDRI.org 217.72.179.7). Ovšem IP adresy se lidem špatně pamatují. Používat je pro určování online zdrojů také není praktické, protože služby na internetu se občas musejí přestěhovat na novou IP adresu (například při změně poskytovatele služeb).

Protože používání IP adres není ani praktické, ani příliš výhodné pro uživatele, začaly vznikat „názvy domén“ (jako například edri.org). Celosvětový systém doménových jmen funguje tak trochu jako telefonní seznam pro internet.

Pokud znáte název domény webové stránky, kterou chcete navštívit, použije se pro nalezení odpovídající IP adresy webového serveru, kde je možné tuto stránku nalézt, systém doménových jmen – neviditelně a automaticky. Takže když napíšete http://edri.org, váš počítač z toho vyčte 217.72.179.7 a pošle konkrétní žádost na zobrazení naší webové stránky.

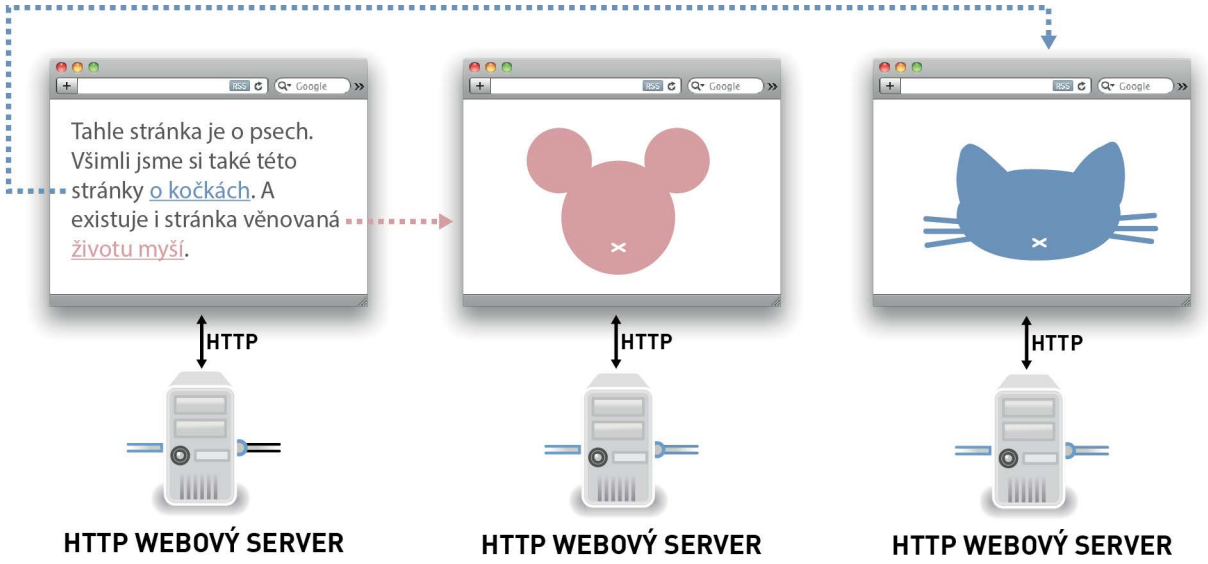
Systém vyhledávání názvů domén pracuje na základě hierarchie. Když napíšete http://edri,org, váš počítač se nejdříve spojí se serverem, aby se zeptal na adresu.[02] Přednastavený DNS server většinou provozuje váš poskytovatel internetu, můžete ale použít i nějaký jiný.

Pokud si někdo v nedávné době vyžádal přístup na http://edri.org, DNS server si bude „pamatovat“ detaily a dodá vám správnou IP adresu. Pokud ne, předá žádost na vyšší úroveň oprávnění, kde proběhne stejný proces. Na nejvyšším stupni oprávnění je třináct „základních serverů“, které nakonec shromažďují DNS servery. Je to třináct velice silných serverů s obrovskou kapacitou. A to takovou, že dokonce výkonně fungovaly i ve chvílích významných útoků (technikou tzv. rozloženého odmítnutí služby).

02 Pokud váš počítač nedávno na http://edri.org přistupoval, potom už IP adresu zná a nemusí ji kontrolovat s poskytovatelem služeb.

# THE WORLD WIDE WEB

## PROPOJOVÁNÍ INFORMAČNÍ SPOLEČNOSTI




Worl Wide Web, celosvětová internetová síť, staví na http, relativně mladém protokolu (jazyku), který je založený na internetovém protokolu (IP). http, HyperText Transfer Protocol, tedy hypertextový přenosový protokol, byl vytvořen pro stahování takzvaných hypertextových dokumentů (kterým se nyní říká webové stránky) a posílání základních informací zpátky na webový server.

Webové stránky se vytvářejí pomocí formátovacího jazyka HTML, HyperText Markup Language. Pravidla tohoto jazyka stanovuje konsorcium WWW (W3C) a konkretizují speciální značky, které označují typografii a formátování. Například tučnému textu bude předcházet  a **ukončí ho** .

Tato norma existuje v několika verzích (nejaktuálnější je HTML5), proces vývoje HTML se nezastaví a lze do něj vstoupit. Jakmile dojde ke stanovení standardů, neexistuje licence či poplatek za užívání HTML. Výhodou je, že všechny dostupné počítačové systémy instrukce v HTML chápou stejně – takže tento jazyk může používat každý (zdarma) a může si být jistý, že všechna zařízení zobrazí webovou stránku stejně. Web (a svět) by byl daleko chudší, kdyby lidé museli za vytváření stránek v jazycích různých druhů počítačů platit.

Tato otevřená a bezplatná povaha HTML je klíčová pro zajištění kompatibility webových stránek po nejrůznější druhy zařízení – stolní počítače, mobilní telefony, tablety, notebooky a další. Náležité používání specifikací HTML

při formátování webových stránek také zajišťuje přístup k takovým stránkám pro osoby s vadami zraku – jinak by systémy na čtení textu otevíraným stránkám nerozuměly.

Webové stránky se publikují na zařízeních známých pod označením „webové servery“. Webový server je počítač, který je možné dohledat podle unikátní IP adresy (jak bylo popsáno v předchozím textu). Většinou na stejné IP adrese najdete mnoho názvů domén (například www.edri,org a www.bitsoffreedom.nl), protože jsou uložené na stejném (hostitelském) serveru. Jeden webový server s unikátní IP adresou tedy

mezi počítačem koncového uživatele a webovým serverem, může získat přístup k veškerým informacím, které oběma směry proudí.

HTTPS do takového přenosu vnáší navíc i kódování, takže (teoreticky) může dešifrovat informaci proudící oběma směry pouze koncový uživatel a webový server. Je to založené na důvěře: Ten, kdo uveřejňuje webovou stránku, požádá někoho, komu důvěřuje, o přísně osobní certifikát, který je digitálně označený tak, aby potvrdil identitu toho, kdo stránku zveřejňuje. Je to podobné jako voskové pečeti, které se kdysi používaly


JAZYK VYTVOŘENÝ WWW KONSORCIEM W3C®

Tenhle TEXT je psán tučně.

JAK HO POUŽÍVAJÍ PROGRAMÁTOŘI


CO VIDÍTE VY

může hostit mnoho webových stránek. U komerčních společností, které se věnují tzv. webovému hostingu, mohou být na jednom webovém serveru stovky nijak nesouvisejících webových stránek. Pokusy „blokovat“ jednotlivé webové stránky podle jejich IP adresy tedy mají vždy katastrofální následky pro nesouvisející stránky na stejném serveru.

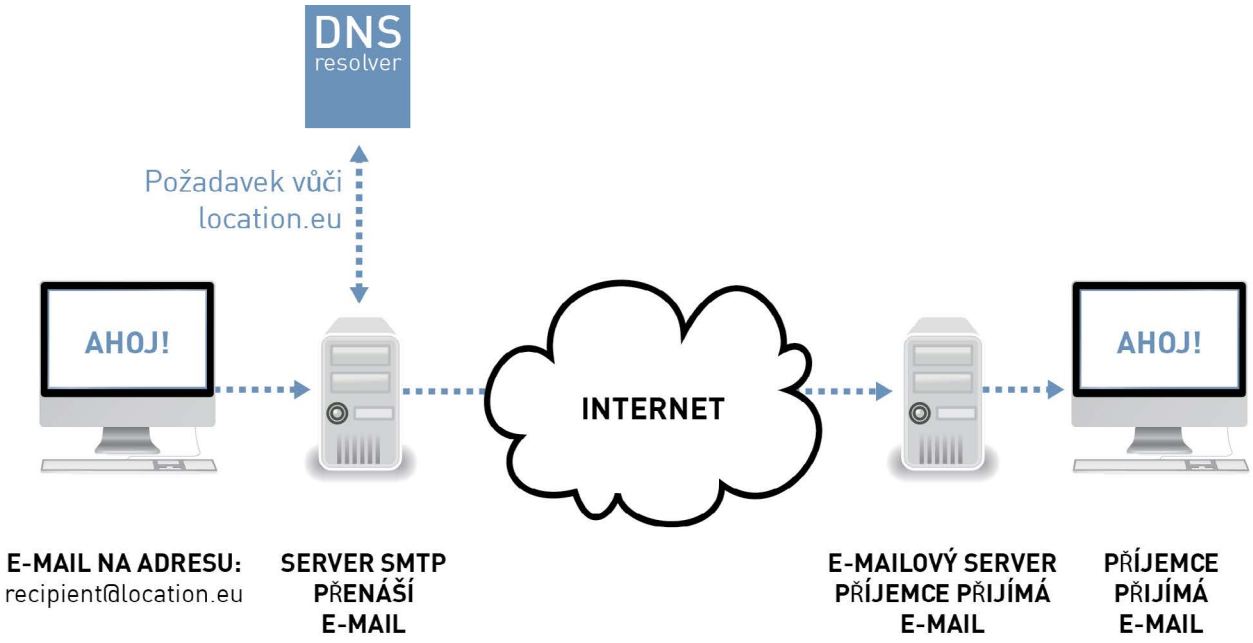
Vedle http existuje také zabezpečená varianta HTTPS. Přenos prostřednictvím http (a tedy následně i přenášené a stahované informace) nejsou zakódované a kdokoli, kdo má přístup ke kabelům sítě nebo zařízením

na pečetění dokumentů.

Když si uživatel koupí nový počítač nebo si nainstaluje nový prohlížeč, dostane standardní sadu důvěryhodných certifikačních autorit, bezpečný seznam subjektů, jejichž certifikátům udělovaným autorům webových stránek bude uživatel důvěřovat. Slabinou systému je důsledek tohoto předem definovaného seznamu – seznam obsahuje spousty jmen. Když se ukáže, že pouze jeden jediný subjekt není důvěryhodný, potom uživatelé důvěřují nespolehlivé službě.

# E-MAILY A JEJICH BEZPEČNOST

## POŠTA V DIGITÁLNÍM SVĚTĚ




Elektronická pošta neboli e-maily jsou zprávy, které zasílá jeden uživatel jednomu nebo více adresátům. Přenos těchto zpráv probíhá prostřednictvím SMTP (Simple Mail Transfer Protocol, jednoduchý protokol pro přenos pošty), který podobně jako HTTP staví na internetovém protokolu.

Po dopsání e-mailu na příslušné stránce nebo v e-mailovém programu dojde k přenosu tohoto e-mailu k odchozímu e-mailovému serveru pomocí SMTP. Poté dojde k přenosu z jednoho e-mailového serveru na další, opět za využití SMTP, dokud se nedostane k e-mailovému serveru, pro který je určen.

Odpověď na otázku, kam poštu poslat, hledají e-mailové servery pomocí již dříve popsaných informací ze systému doménových jmen (DNS). V tomto systému jsou také informace o tom, které servery mají na starosti e-maily té které domény. Doména se dá odvodit z té části e-mailové adresy příjemce, která následuje za značkou @.

Když zpráva dorazí k e-mailovému serveru, který se stará o veškeré e-maily adresáta, zůstane tam, dokud ji adresát nesmaže. Některé e-mailové softwary to dělají automaticky, protože se zprávy stahují do počítače nebo chytrého telefonu uživatele.

## Bezpečnost e-mailů

Vzhledem k tomu, že jsou e-maily zasílány z jednoho e-mailového serveru na jiný, může je zachytit třetí strana. Existují dva způsoby, jak tomu zabránit: Prostřednictvím zabezpečení komunikace mezi e-mailovými servery a kódování obsahu e-mailů. Zabezpečení komunikace mezi e-mailovými servery funguje stejným způsobem jako když protokol HTTPS zabezpečuje komunikaci http (jak bylo popsáno výše).

U e-mailů spočívá ovšem slabé místo v tom, že váš počítač nekomunikuje přímo s koncovým e-mailovým serverem. Pokud jeden prostřednický e-mailový server nepoužívá k přeposlání vaší zprávy kódování, může být na daném místě zachycena.

Kvůli téhle slabině je možná lepší zakódovat již samotné zprávy. Populární a zdarma dostupná kódovací metoda pro e-maily je PGP (Pretty Good Privacy, dost dobré soukromí), která existuje i v podobě OpenPGP a GPG.

# HLOUBKOVÁ KONTROLA PAKETŮ

## (DPI, DEEP PACKET INSPECTION)

PODÍVEJME SE NA VAŠI AKTIVITU NA INTERNETU

**Data se na internetu zasílají v paketech, což jsou v podstatě malé bloky dat. Každý paket má záhlaví, kde je popsán jeho původ a cílová destinace (jako obálka s adresou odesílatele a adresáta). Tato adresa umožňuje síťovým zařízením určit nejlepší cestu, kudy paket v danou chvíli poslat.**

Dříve síťová zařízení sledovala pouze informaci o původu a místu určení. Ovšem s dramatickým nárůstem zákeřných aktivit se majitelé sítí rozhodli, že je třeba sledovat u každého paketu i další detaily, aby bylo možné rozeznat „bezpečné“ pakety od těch, které jsou součástí hackerských pokusů, a zabránit útokům na služby.

Například síťové bezpečnostní programy, tzv. firewally, mohly zpočátku zablokovat pouze paket směřující z určitého místa do určitého místa určení a k dané službě. S pomocí těchto kritérií bylo možné blokovat veškeré příchozí požadavky na službu do vaší kancelářské sítě, protože žádnou službu neposkytujete široké veřejnosti. A přesto jste mohli dál využívat veškeré služby dostupné na internetu, pokud jste povolili veškeré žádosti o služby, které vzejdou z vaší kancelářské sítě.

Zároveň se například rozhodnete, že si ve své síti založíte webový server za účelem uveřejňování dokumentů. Budete muset upravit nastavení ochrany sítě, abyste povolili příchozí žádosti o službu, ale pouze pro webové služby. Ovšem existuje mnoho útoků na webové servery, které vypadají z pohledu firewallu celkem nevinně. Není možné rozlišit bezpečné pakety od těch nebezpečných pouze na základě informací o původu a místu určení.

Návrháři sítí si brzy uvědomili, že by se útoky snáze odhalovaly, pokud by síťová zařízení začala pakety zkoumat trochu více do hloubky. Teoreticky je to snadné – záhlaví paketů není „oddělené“ nijak jinak než logicky definovaným ohraničením. Je to pouze otázka analýzy o trochu více bytů, než kolik jich podléhalo kontrole doposud například pro účely směrování.  Nebo je možné jít ještě dál a podívat se do bloku dat v paketu.

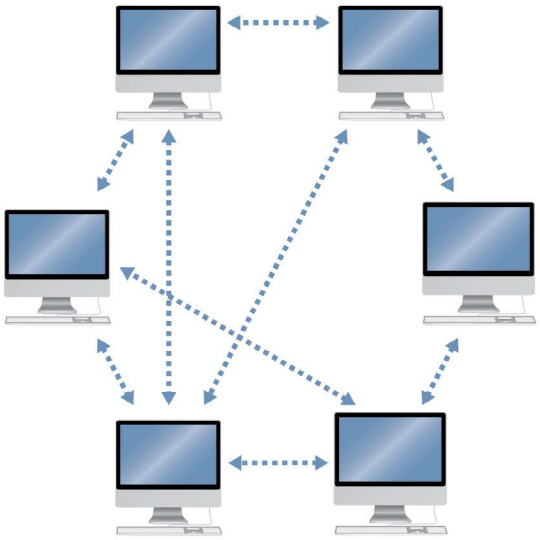
Zařízení, která se tímhle začala zabývat, se zpočátku jmenovala IPS (Intrusion Prevention System), systém prevence průniku, a tyto prvky byly brzy zavedeny do většiny síťových zařízení. Dokud se využívaly pro blokování hackerských pokusů, nebylo na nich nic kontroverzního.

Nicméně postupem času si začaly vlády, poskytovatelé obsahu i provozovatelé sítí uvědomovat, že jim tento postup, obecně nazývaný hloubková kontrola paketů (DPI, Deep Packet Inspection), poskytuje daleko větší kontrolu nad daty uživatelů sítě, než jaká byla dříve možná. Techniky hloubkové kontroly paketů se již používají k prosazování zákonů (dohled, blokování atd.), vytváření profilů na trhu a zacílení reklamy, vymáhání dohod o poskytování služeb a navrhuje se její využití pro vynucování autorských práv.

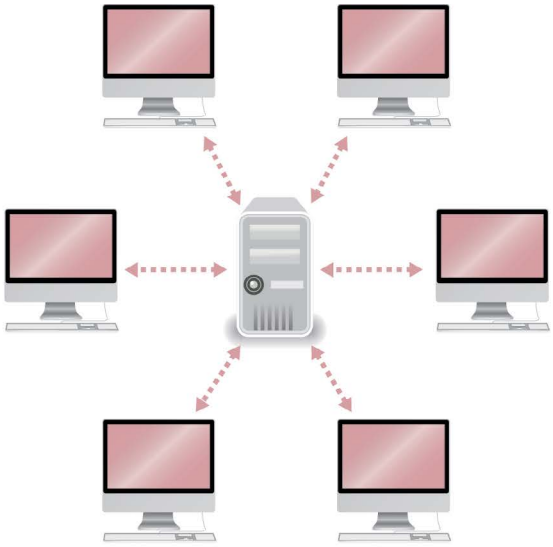
Z pohledu uživatele je možné techniky hloubkové kontroly paketů zablokovat pomocí kódování – „hloubkový“ obsah zakódovaného paketu pak zůstane provozovateli zcela nesrozumitelný.

# PEER-TO-PEER: PŘENOS MEZI ROVNOCENNÝMI UZLY

OD JEDNOHO PŘÍMO K DRUHÉMU, BEZ PROSTŘEDNÍKŮ



PŘENOS MEZI ROVNOCENNÝMI UZLY (PEER-TO-PEER)
SYSTÉM UZLŮ BEZ CENTRÁLNÍ INFRASTRUKTURY



CENTRALIZOVANÝ SYSTÉM
SERVISNÍ MODEL, KTERÝ JE POSTAVENÝ NA SERVERU (NIKOLI PŘENOSU MEZI ROVNOCENNÝMI UZLY)

**Peer-to-peer sítě sestávají ze zařízení (webových serverů nebo počítačů koncových uživatelů), která se daného typu komunikace účastní za jednotných podmínek. Každý uzel (tedy každé zařízení) může komunikovat s ostatními uzly, aniž by se rozlišovali „spotřebitelé“ a „výrobci“, klienti a servery, atd. Mnoho zařízení zkrátka komunikuje s mnoha zařízeními.**

Opakem tohoto systému je model klient – server neboli model jeden s mnoha, kde má jeden počítač na starosti žádosti mnoha klientů – například webová stránka, která poskytuje obsah mnoha uživatelům této stránky (tedy jedno zařízení komunikuje s mnoha jinými).

Aplikace peer-to-peer na internetu používají peer-to-peer protokoly, které jsou založené na IP, internetovém protokolu.

Sítě pro přenos mezi rovnocennými uzly mají celou řadu konkrétních výhod:

- Vzhledem k absenci centralizovaných entit neexistuje jedno jediné místo možné poruchy. Pokud v síti, kde komunikuje jedno zařízení s mnoha dalšími, dojde k poruše onoho „jednoho“ zařízení, naruší to celý systém. U systému komunikace mnoha zařízení s mnoha dalšími vzniká při poruše jednoho z nich minimální celková škoda.

- Mohou snadno růst, protože každý dodatečný uživatel přináší síti další zdroje (přenosovou kapacitu, paměť, výkon).

- Vzhledem k absenci centrální autority neexistuje správa.

- Selhání mívá minimální dopad, protože neexistují centralizované zdroje a zdroje jsou přirozeně do značné míry duplikovány.

- Takové sítě poskytují svým uživatelům svobodu. Nejen že jsou zařízení uživatelů rovnocenná, i zúčastnění uživatelé jsou na tom stejně.

Jedním z nejdůležitějších úkolů peer-to-per aplikací je organizace sítě a lokalizace zdrojů v síti.

E-mailové servery jsou do určité míry raným příkladem peer-to-peer aplikace.  Pomocí SMTP protokolu může jakýkoli server poslat jakémukoli jinému zařízení e-mail. V systému doménových jmen může být uvedeno také několik serverů, které jsou schopny zpracovat příchozí e-maily pro určitou doménu, čímž zvyšují spolehlivost systému.

Uzly v sítích na sdílení dat se ihned nedozvědí IP adresy ostatních uzlů zapojených v síti a nevědí, které uzly mají které soubory (nebo jejich části). O tohle se obvykle stará proces, ve kterém zúčastněné uzly sdílejí jim dostupné informace o obsahu ostatních uzlů. Soubory se identifikují pomocí tzv. hash keys, což jsou v podstatě otisky prstů, které umožňují, aby byly jednotlivé soubory specificky rozpoznatelné. Tabulky distributed hash tables (DHT) umožňují rovnocenným uzlům zjistit, které další uzly jsou dostupné za účelem stahování nějakého souboru nebo jeho části.

Uživatelé sítě rovnocenných uzlů musejí mít způsob, jak získávat informace o souborech, o které mají zájem. Některé se publikují na webových stránkách, například je možné stáhnout si verzi operačního systému Ubuntu. Existují slovníky, které pomocí těchto otisků mapují pro člověka čitelné popisy souborů tak, aby bylo možné v síti rovnocenných uzlů soubory vyhledávat.

Tyto slovníky jsou dostupné například na webových stránkách thepiratebay.org nebo mininova.org. Nicméně otisky se dají šířit také e-mailem, pomocí chatů a sociálních sítí – neexistuje tedy žádný centralizovaný systém.

Některé sítě rovnocenných uzlů ale poskytují zapojeným uzlům anonymitu.

# BEHAVIORÁLNÍ REKLAMA

## BUĎME TROCHU OSOBNÍ

**Behaviorální reklama (nazývaná také behaviorální cílování) je metoda založená na sledování aktivit uživatelů na internetu. Používá se k sestavování profilů uživatelů internetu. Těm se podle profilu poté zobrazuje reklama, která, pokud je profil správný, pro ně bude relevantnější, a tím pádem celkově účinnější.**

Behaviorální reklama využívá jednoduchý princip: Pokud uživatel nejdříve navštíví internetovou stránku věnovanou například fotbalu, uloží se v jeho webovém prohlížeči (jako např. Internet Explorer, Firefox či Chrome) malý soubor (tzv. cookie). Webová stránka se většinou skládá z obsahu pocházejícího z několika zdrojů, například text a obrázky jsou ze stránky, na kterou jste vstoupili ve svém prohlížeči, ovšem další obsah, jako například reklama, se stahují z jiných zdrojů (a to dokonce i ze zdrojů, které se samotnou stránkou nemají nic společného). Pokaždé, když dojde ke stahování obsahu, mohou být v rámci požadavku zasílána data zachycená pomocí cookies zpátky z vašeho počítače.

Pro účely behaviorální reklamy většinou cookies obsahují identifikační číslo. Pokud si potom uživatel přečte novinový článek o autech, budou schopny společnosti, které se behaviorální reklamou zabývají, odvodit předpoklady o člověku, který si čte články o autech a zároveň o fotbale. V tomto případě by se například mohlo jednat o primitivní domněnku, že se jedná o uživatele, který bude pozitivně reagovat na reklamy na pivo. Lze se také domnívat, že nejspíš nebude ten nejlepší nápad zobrazovat uživateli speciální nabídky na pojištění vozidel, protože se patrně jedná o mladého muže.

Čím více webových stránek, které jsou zařazeny do mapovací sítě služby behaviorální reklamy, jako například většinu novin a mnoho dalších, uživatel navštíví, tím více údajů přibude do jeho profilu. Za relativně krátkou dobu sledování internetových návyků nějaké osoby je možné vytvořit poměrně detailní profil – a „rozpoznatelnost“ těchto dat roste, ačkoli se teoreticky jedná o data „anonymní“.

Velké množství behaviorálních dat může zúžit velikost skupiny, do které daný jedinec patří, až na velmi malý počet lidí, kteří do ní

zapadají. Před několika lety zveřejnil jeden vyhledávač rozsáhlý soubor anonymních údajů o vyhledávání pomocí jeho služeb. Výsledkem analýzy těchto anonymních dat bylo, že se novinářům podařilo identifikovat konkrétní jednotlivce – a ukázat tak, že „anonymní“ údaje vlastně vůbec anonymní nejsou.

Jestli se pro behaviorální reklamu používají také další údaje z jiných zdrojů, to se neví. Mnoho firem, které se pohybují i v oblasti behaviorálního cílování, například Google a Yahoo!, poskytují i jiné internetové služby včetně vyhledávání. Spojením databází by došlo ke vzniku obrovského množství relativně snadno identifikovatelných dat.

Tvrdí se, že za ekonomickým úspěchem internetové reklamy posledních let stojí kromě jiného právě behaviorální reklama. Tato technika se také využívá ke zkušebnímu poskytování dalšího obsahu, například zpráv.

Na souhlas s takovým zpracováním osobních údajů se uživatelů nikdo neptá. Reklamní odvětví argumentuje tím, že je tento způsob sledování v zájmu uživatele, protože přispívá k tomu, že se k němu dostane pouze „relevantní“ reklama. Padl ale už i návrh tento systém zakázat, přičemž se ozývají hlasy, že takový postup naplňuje požadavky směrnice o soukromí na internetu (tzv. e-privacy).

Klíčovou otázkou je, zda samotné nastavení cookies (ochrana soukromí je ve výchozím nastavení jen málokdy zapnutá) v uživatelově vyhledávači představuje smysluplný projev souhlasu uživatele. Evropský inspektor ochrany údajů[03] tento názor nezastává.

Mnoho uživatelů internetu o cookies vůbec neví a nikdy jejich nastavení neměnilo. Navrhované řešení je ale problematické i z technického hlediska, protože možnost nepovolit tento proces se netýká všech inzerentů. A navíc stávající možnost nepovolit tento systém sám o sobě také používá cookies, takže jejich smazání smaže zároveň i možnost tohoto nastavení.

Kromě toho moderní prohlížeče a jejich rozšíření (tzv. plug ins jako je flash) nabízejí kromě tradičních cookies mnoho dalších způsobů ukládání a získávání dat. Tato další nastavení jsou pro běžného uživatele obtížná a nejsou vždy zahrnuta do nastavení cookies v prohlížečích.

V současné době mají Evropané sice evropské právo, které je chrání, ovšem zůstávají de facto nechráněni vzhledem k nedostatečné vůli toto právo implementovat.

03 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-01-09_ePricacy_2_EN.pdf

# VYHLEDÁVAČ

## INTERNETOVÝ INDEX

**Navigace v celosvětové síti www funguje pomocí hyperlinků (když na tyto texty nebo obrázky kliknete, otevře se jiná webová stránka).**

Všichni autoři na webu se mohou napojit na jakýkoli jiný obsah dostupný online. Díky takovému propojování pomocí linků pomáhají všichni uživatelé internetu organizovat online informace do sítě propojených zdrojů.

Podstatné je, že web neposkytuje centralizovaný index, kde by se sledovalo, co je na internetu k dispozici. Nejdůležitější službou jsou proto vyhledávače, které pomáhají uživatelům pohybovat se na internetu efektivněji.

Existují nejrůznější druhy služeb vyhledávačů. Nejvýznamnější model vyhledávače je vyhledávač založený na vyhledávacích robotech, tzv. crawlerech:

Využívá software (nazývaný crawler nebo spider) k vyhledávání toho, co je k dispozici online, a tento obsah systematicky indexuje. Sofistikovanost a efektivnost crawlerů je rozhodující pro velikost a aktuálnost indexu – přičemž obě tato kritéria jsou významná pro kvalitu vyhledávače. Jednoduše řečeno, spider / crawler sleduje všechny odkazy na všech stránkách, propojené stránky indexuje a potom sleduje odkazy na těchto stránkách, indexuje je a tak dále.

Nejdůležitější, co vyhledávač dělá, je přiřazení uživatelova požadavku na vyhledávání k informaci v indexu. Výsledkem tohoto přiřazovacího procesu je obvykle seřazený seznam odkazů. Tyto výsledky se obvykle skládají z názvu, úryvků daných informací a hyperlinků na stránky, které technologie vyhledávače vyhodnotila jako potenciálně relevantní.

Kromě „organických výsledků“ (tedy stránky, které nalezl vyhledávač), navrhují komerční vyhledávače sponzorované výsledky podle toho, jakou nabídku poskytnou na klíčová slova nabízející na trhu. Proces přiřazování v případě organických výsledků je složitý a komerční vyhledávače si chrání své přesné algoritmy pro třídění dat jako obchodní tajemství. Algoritmus řazení PageRank společnosti Google je jedním z nejznámějších algoritmů řazení pro vyhledávání na webu. Předpovídá relevantnost webových stránek v indexu na základě analýzy struktury odkazů na webu (tedy typů stránek, které jsou s danou stránkou propojené).

Mezi další důležité techniky pro lepší propojování indexu s tím, jakou informaci uživatel potřebuje, patří analýza obsahu webové stránky a analýza uživatelských dat. Komerční vyhledávače využívají cookies k ukládání požadavků uživatele na vyhledávání, klikání na odkazy a další, ukládají je v individualizované formě ve svých databázích na delší časová období.

„Vertikální“ neboli specializovaný vyhledávač se soustředí na vyhledávání určitého typu předmětu, například cestování, nákupy, akademické články, zprávy nebo hudba. Rozsáhlé vyhledávače založené na crawlerech nabízejí také zvlášť služby specializovaných vyhledávačů. Metavyhledávač je vyhledávač, který nevytváří vlastní index a výsledky hledání, místo toho využívá výsledky jednoho nebo více jiných vyhledávačů. V adresáři (directory) se ukládají odkazy roztříděné do nejrůznějších kategorií. Známými příklady je adresář Yahoo! a Open Directory project.

# CLOUD COMPUTING

## VAŠÍM POČÍTAČEM SE STÁVÁ INTERNET

**V poslední době se cloud computing stal marketingovým zaklínadlem. Na samotném konceptu není nic nového, ačkoli v poslední době jsme byli svědky obrovského nárůstu aplikací, které jsou jeho prostřednictvím dostupné.**

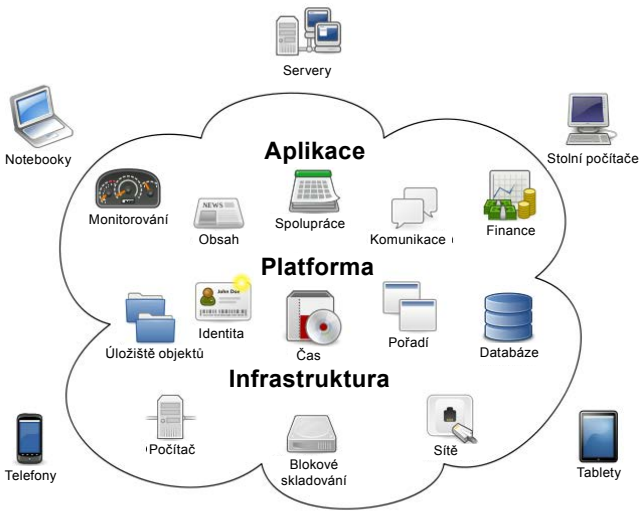
Na obrázku komunikační sítě označuje mrak (cloud) síť, která je vně sítě uživatele. Cloud computing tedy označuje jakoukoli službu počítače, která se odehrává v rámci sítě, nikoli v počítači koncového uživatele.

Jeden z prvních příkladů cloud computing je e-mail, který staví na webu (webmail). Uživatelé webmailu mají přístup ke svým e-mailům z jakéhokoli zařízení připojeného k internetu, nikoli pouze z jednoho přístroje. Mezi známé webmailové služby patří například Yahoo! Mail, Hotmail či Gmail.

S neustálým nárůstem rychlosti internetového připojení v posledních letech zaznamenala škála služeb, které je možné nabízet prostřednictvím cloud computingu, exponenciální nárůst. Nyní je například možné ukládat v „cloudu“ obrovské množství dat prostřednictvím virtuálních harddisků, jaké nabízí například Microsoft Live.

V nabídce je také stále větší množství online kancelářského softwaru, například programů pro práci s textem a technologie pro databáze.

Dalším krokem směrem ke cloud computingu je projekt společnosti Google, operační systém Chrome. Ten využívá webový prohlížeč Google Chrome a má za cíl automaticky zahrnout cloudové technologie mezi technologie výchozí, aby bylo množství softwaru v počítači minimální se značným důrazem na služby dostupné online – což je v mnoha ohledech postup zcela opačný od tradičních přístupů k informačním technologiím, kdy je prakticky veškerý software nainstalován v počítači a na cloud se spoléhá minimálně, či vůbec.




**Cloud Computing**

# SOCIÁLNÍ MÉDIA

MÍSTA, KDE SE SETKÁVÁME

**Sociální média představují sadu online komunikačních nástrojů, které umožňují vytváření a výměnu obsahu vytvořeného uživatelem.**

Sociální média se od běžných médií zásadně liší, protože nejen poskytují informace, ale interagují s vámi, zatímco vám tyto informace poskytují. Interakce může být prostá, například se vás budou ptát na váš komentář, nechají vás hlasovat o nějakém článku nebo se vás zeptají, zda se vám „líbí“ nebo „nelíbí“ něco, co udělali jiní uživatelé. Každý uživatel není pouhým konzumentem, ale zároveň i součástí tohoto média, protože ostatní uživatelé si mohou číst jeho komentáře či hodnocení.

Lidé si začínají zvykat, že mají možnost reagovat na to, co jiní lidé píšou, a projevit svůj vlastní úhel pohledu. To zvyšuje angažovanost komunity v probíhajících debatách. Počet uživatelů sociálních médií každoročně roste, a tím pádem roste i jejich vliv. Stávají se čím dál tím mocnějšími.

Jakoukoli stránku, která dává návštěvníkům možnost interakce s ní či ostatními návštěvníky, je možné považovat za sociální médium. Obecně vzato tady můžeme dělit šest různých typů:

1. Projekty založené na spolupráci (např. Wikipedia), kde dochází k interakci uživatelů tak, že přidávají nové články nebo upravují články již existující;
2. Blogy a mikroblogy (např. Twitter);
3. Komunity pro sdílení obsahu (např. YouTube, Flickr), kde k interakci dochází sdílením a komentováním fotografií či videí;
4. Sociální sítě (např. Facebook, Myspace, Hi5, google+), kde uživatelé interagují přidávání přátel, komentováním profilů, vstupem do skupin a diskusemi;
5. Virtuální světy her (např. World of Warcraft);
6. Virtuálními sociálními světy (např. Second Life).

Důležitou otázkou je ochrana uživatelů sociálních médií, především ochrana soukromí. Zatímco si uživatelé mohou většinou vybrat, zda budou svoje osobní informace sdílet, či zda zůstanou skryté, výchozí nastavení a doplňková ochrana dětí patří mezi témata značně kontroverzní. Navíc některé stránky, mezi jinými Facebook, jednostranně změnily nastavení soukromí svých uživatelů v minulosti již několikrát.

# ŘÍZENÍ INTERNETU

## DIGITÁLNÍ DEMOKRACIE

**První pokusy o definici řízení internetu (IG, internet governance) se objevily na přípravných jednáních Světového summitu Spojených národů o informační společnosti.**

První obecně uznávaná definice byla vytvořena v pracovní skupině zabývající se řízením internetu, skupiny více zainteresovaných stran vytvořené generálním tajemníkem Organizace spojených národů, a byla zahrnuta do tuniské agendy pro informační společnost. Řízení internetu podle definice představuje:

„vytváření a uplatňování společných principů, norem, pravidel, rozhodovacích postupů a programů, které utvářejí vývoj a užívání internetu, ze strany vlád, soukromého sektoru a občanské společností, podle jejich konkrétních rolí."

V této definici je zdůrazněn přístup mnoha zainteresovaných stran při diskuzi o postupech spojených s internetem: Zapojení všech hráčů otevřeným, průhledným a zodpovědným způsobem.

Pro dosažení tohoto cíle bylo založeno Fórum pro řízení internetu jakožto fórum pro mnoho zainteresovaných stran, kde má proběhnout diskuze o tématech z oblasti veřejné politiky týkající se základních součástí internetového řízení. Fórum v průběhu již šesti běhů (2006 až 2011) dalo popud k zakládání podobných národních a regionálních fór (např. EuroDIG – panevropský dialog o řízení internetu). Je důležité nastínit, že tato fóra přímo nerozhodují, ale ovlivňují politiky.

**Co všechno řízení internetu zahrnuje?**

- Infrastrukturu a standardizaci;

- Technické otázky spojené s fungováním internetu: telekomunikační infrastrukturu, internetové standardy a služby (např. internetový protokol IP, systém doménových jmen DNS), standardy pro obsah a aplikace (např. hypertextový jazyk HTML);

- Otázky týkající se zajištění bezpečného a stabilního provozu internetu: bezpečnost v kyberprostoru, kódování, spam;

- Právní otázky: národní i mezinárodní legislativa a regulace související s internetem (např. autorská práva, počítačová kriminalita, soukromí a ochrana dat);

- Ekonomické otázky: e-commerce, daňové otázky, elektronické podpisy, elektronické platby;

- Otázky rozvoje: digitální propast, všeobecný přístup k internetu;

- Sociálně kulturní záležitosti: lidská práva (svoboda projevu, právo hledat, získat a poskytovat informace), politiky týkající se obsahu, ochrany soukromí a dat, vícejazyčnost a kulturní rozmanitost, vzdělání, bezpečí dětí v online prostoru.

**Kdo se podílí na řízení internetu?**

- Vlády – ty vytvářejí a zavádějí veřejné politiky a regulace týkající se internetu;

- Soukromý sektor – poskytovatelé internetových služeb (ISP, internet service providers), poskytovatelé sítí, vedení rejstříku a zapisování doménových jmen, softwarové společnosti, společnost zabývající se obsahem;

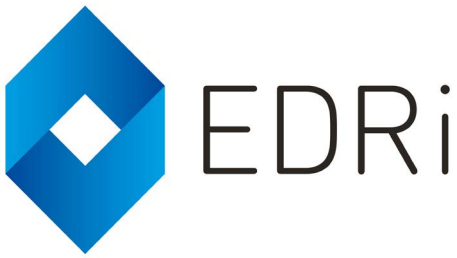
- Občanská společnost – nevládní organizace zastupující koncové uživatele internetu;

- Mezinárodní organizace: Mezinárodní telekomunikační unie, Organizace OSN pro výchovu, vědu a kulturu, Rozvojový program Organizace spojených národů;

- technická komunita – Internet Society, Internet Engineering Task Force, Internet Architecture Board, Internet Corporation for Assigned Names and Numbers.

Další informace:

Jovan Kurbalija, An Introduction to Internet Governance, Diplo Foundation, 2010.



EDRI.ORG/
PAPERS

Z anglického originálu
HOW THE INTERNET WORKS?

Přeložila pro Iuridicum Remedium,
o.s. Zuzana Veselá


Iuridicum Remedium, o.s.
Pplk. Sochora 40
170 00 Praha 7
tel.: +420 776 703 170
E-mail: iure@iure.org
www.iure.org
www.slidilove.cz

S finanční podporou programu Evropské unie Základní práva a občanství.