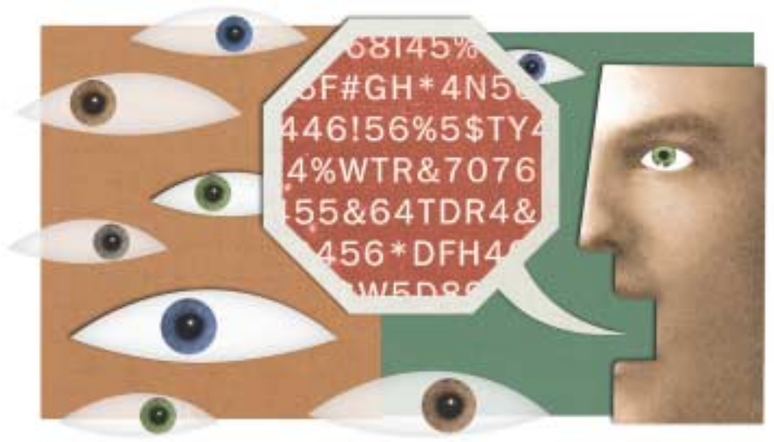
Prolamování hesel populárně

NÁSTROJE PRO PRÁCI S HESLY A JEJICH ODHALOVÁNÍ

MARTIN IGNJATOVIĆ



Hesla a šifry patří již dnes neodmyslitelně do světa počítačů. Hesla používáme všichni denně. Používáme je zpravidla k utajení dat a informací. Existuje mnoho nástrojů, které umí s hesly pracovat, a rovněž existuje mnoho nástrojů, které umí hesla odhalit. V tomto článku se podíváme na oba dva typy.

ALGORITMY

Pokud se chceme bavit o heslech a jejich luštění, musíme si alespoň v krátkosti říct něco o tom, na jakém principu fungují. Tato znalost není nezbytná, ale je vždy lépe vědět, s čím pracujeme, než slepě spoléhat, že to za nás vyřeší nějaký nástroj.

V principu lze šifrování dělit na symetrické a asymetrické. Mezi oběma je diametrální rozdíl. Princip symetrického šifrování spočívá v použití stejného klíče k šifrování i dešifrování dat. Naopak asymetrické šifrování používá dvojici klíčů, a to klíč veřejný a klíč soukromý. Důležitý jako způsob šifrování je rovněž použitý algoritmus. Algoritmů existuje velké množství, ale nejznámější a nejpoužívanější jsou jen některé. Jako příklad uveďme DES, 3DES, MD5. V krátkosti si o každém z nich něco povíme.

DES

Stále se jedná o jeden z nejpoužívanějších šifrovacích algoritmů (spíše však jeho „potomků"). Byl vyvinut a patentován firmou IBM začátkem 70. let. Postupně však byly objeveny různé slabiny, které logicky vedly ke vzniku dalších verzí. S využitím dnešního hardwaru lze tento algoritmus prolomit prostým vyzkoušením všech hesel. Proto vznikly další algoritmy, vycházející z DES, avšak řádně vylepšené a bezpečnější.

3DES

Triple DES je algoritmem, jenž vychází z algoritmu DES, je však výrazně bezpečnější. Pracuje na principu tří šifrovacích operací.

Postup při zašifrování nějaké zprávy je následující:

1. Šifrování klíčem 1
2. Dešifrování klíčem 2
3. Šifrování klíčem 3

Postup při dešifrování je opačný:

1. Dešifrování klíčem 3
2. Šifrování klíčem 2
3. Dešifrování klíčem 1

MD5

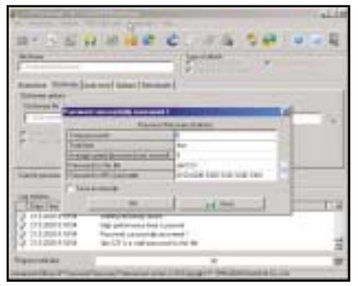
Toto je jeden z nejrozšířenějších algoritmů používaných ke generování kontrolního součtu. Distribuuje jej společnost RSA a navrhl jej Ronald Rivest. Princip tohoto algoritmu je poměrně jednoduchý. MD5 generuje z libovolně dlouhého vstupu 128bitový výtah. Jeho jedinou nevýhodou je snížená rychlost, ale při výkonu dnešních počítačů již není tento problém aktuální. Tento algoritmus se používá na největších unixových systémech v souvislosti s uživatelskými hesly. Odpadá tak nutnost heslo uchovávat v systému. Při jeho zadání v programu login se provede „pouze" kontrolní součet tohoto hesla, porovná se s kontrolním součtem uloženým v systému, a pokud souhlasí, je uživatel „vpuštěn" do systému. Tohoto principu lze využít i v jiných aplikacích. Problém je v případě, kdy heslo zapomeneme, neboť z kontrolního součtu, který je uložen v systému, bychom teoreticky nikdy neměli vygenerovat zpět původní heslo. Nicméně existují programy, jež generují náhodné součty a zkouší je porovnávat s těmi „pravými". Proto je důležité dodržovat princip silných hesel. Předchůdci MD5 jsou algoritmy MD2 a MD4, ve kterých však byly v polovině 90. let minulého století objeveny závažné nedostatky, a proto se nedoporučuje tyto algoritmy používat.

METODY ÚTOKU

Poté, co jsme se seznámili s algoritmy používanými k šifrování, řekneme si nyní, jaké druhy útoků na tyto algoritmy existují, kdy se používají a jaký je jejich princip. Pokud se setkáme s kvalitním algoritmem, těžko můžeme počítat s tím, že se nám podaří nějakým zázrakem odhalit heslo, jak je tomu ve většině filmů, kdy hlavní hrdina po několik úderech do klávesnice hrdě oznámí, že má heslo nebo že ho bude znát do 10 minut. Tak to v reálném světě naštěstí nechodí. Musí použít mnohem prozaičtějších metod. Tyto metody si hned popíšeme. Nutno ještě zdůraznit, že pracujeme s kvalitním algoritmem. U neznámých a neověřených algoritmů může dojít k prolomení hesla velice snadno, ale takové algoritmy jistě za použití nestojí. Proto pokud chcete šifrovat, vždy si dobře zjistěte, jaký algoritmus bude použit. Tím se vyhnete spoustě nepříjemností a ochráníte tak svá data.

ÚTOK HRUBOU SILOU

Tento způsob útoku je poměrně primitivní, časově náročný a ne příliš účinný. Bývá použit až jako poslední možnost, když všechny ostatní metody selžou. Jeho princip spočívá ve zkoušení všech možných i nemožných kombinací různých čísel, písmen a ostatních znaků. Vezmeme-li v úvahu, že abeceda bez českých znaků obsahuje 26 písmen, k tomu přičteme 10 číslic, plus nějaké ty speciální znaky jako hvězdička, podtržítko nebo plus, a budeme počítat s tím, že neznáme přesnou délku hesla, musíme logicky dojít k závěru, že tímto způsobem nemůžeme heslo prakticky rozluštit. Úkol nám může usnadnit, pokud víme, jak dlouhé je heslo a z jakých znaků se skládá. Pokud tedy víme, že někdo používá 6místné heslo složené jen z číslic, je otázka prolomení hesla opravdu záležitostí několika milisekund (například prolomení čtyřmístného číselného hesla k souboru MS Word trvalo na stroji Celeron 1,1 GHz 6 milisekund, prolomení hesla složeného ze 4 písmen trvalo 1,2 sekundy).



Z čehož logicky vyplývá potřeba použití složitých a delších hesel. K tomu se dostaneme v závěru článku.

SLOVNÍKOVÝ ÚTOK

Slovníkový útok je jedním z nejčastěji používaných útoků, a je také jedním z nejúčinnějších. Základem úspěchu tohoto útoku je kvalitní slovník, na jehož základě se útok provádí. Slovníků je k dispozici velké množství a nutně musí patřit do výbavy každého, kde se pokouší nějaké heslo prolomit. ***http://www.phreak.org/html/wordlists.shtml*** – na této adrese najdete zhruba 120 slovníků, které mohou být použity pro útok. Najdete zde slovníky z nejrůznějších jazyků a oborů, afrikánštinou počínaje a slovy ze seriálu Star Trek konče. Takže pokud si myslíte, že vaše heslo nemůže být uhodnuto, zkuste ho porovnat s touto databází. V UNIXu pak jednoduše *grep heslo **. Pokud bude nalezena nějaká shoda, máte špatné heslo a je třeba jej změnit. Jak, to si povíme ke konci. Nyní se zaměříme na konkrétní operační systémy a ukážeme si problémy v oblasti hesel specifické pro jednotlivé z nich. Začněme systémy založenými na UNIXu.

UNIX/LINUX

Jelikož jsou systémy UNIX poměrně staré a časem odzkoušené, není zde situace kolem bezpečnosti hesel tak aktuální, jako je tomu na platformě Windows. Většina kryptografických algoritmů byla vyvinuta na těchto systémech a používají se zde jen ty ověřené a bezpečné (zpravidla, ale ne vždy). Systémy UNIX jsou ale převážně síťovými operačními systémy, a proto se zaměříme spíše na problémy jednotlivých síťových služeb, i když lokální bezpečnost nevynecháme.

PASSWD, SHADOW

Systémový soubor s hesly je cílem většiny útočníků na tyto systémy. Jsou v něm uložena hesla všech uživatelů systému. Ta mohou být pro útočníka velmi užitečná. Dříve používala většina unixových systémů jako soubor s hesly soubor /etc/passwd, který byl čitelný každému uživateli systému. V některých systémech je tomu tak dodnes (SCO atd.). Jelikož bezpečnost těchto systému spočívala na silných heslech, byl vyvinut mechanismus, který měl zabránit volné dostupnosti hesel, byť v zašifrované podobě. Tímto mechanismem jsou takzvaná stínová hesla a dnes je používá většina systémů (Linux, BSD). Princip je poměrně jednoduchý. V souboru /etc/passwd jsou uloženy informace o uživatelích, ne však jejich heslo. Hesla jsou uložena ve speciálním souboru, zpravidla /etc/shadow, kde je jejich zašifrovaná podoba. Tento soubor je však přístupný jen uživateli s UID 0, tedy pouze uživateli s právy správce systému (root). I kdyby se útočníkovi podařilo získat práva správce systému, stále ještě nemá vyhráno, protože hesla v souboru jsou šifrována jednocestným algoritmem, jako například MD5 či crypt, a nejsou tudíž čitelná. K jejich prolomení bude potřebovat útočník speciální nástroj. Jedním takovým je John the Ripper, který můžete získat na adrese ***http://openwall. com /john/***.

Existuje verze pro UNIX, DOS i Windows. Jde o nástroj pro příkazový řádek a je považován za nejlepší nástroj pro luštění unixových hesel. Zvládne toho ale mnohem více. Zde je přehled algoritmů, se kterými John umí pracovat:

DES (Kerberos, BSDI, Standard, NTLM)
MD5
Blowfish

John umí pracovat v mnoha modech. Můžete tak na soubor s hesly útočit hrubou silou či slovníkovým útokem. Rovněž můžete specifikovat pravidla, jaká budou použita, ať již jde o rozsah znaků či různé přesmyčky atd. Existuje rovněž program djohn (distribuovaný), který funguje jako služba naslouchající po síti a můžete zátěž rozložit na několik počítačů, a zkrátit tak čas potřebný k prolomení hesla. Na obrázku vidíte, jak rychle byla odhalena špatná hesla uživatelů.

LOKÁLNÍ SOUBORY

Pokud budete chtít zašifrovat nějaký soubor na lokálním disku, použijte k tomu kvalitní software typu PGP či GNUPG. Tyto programy používají kvalitní algoritmy a rozluštění takto zašifrovaných souborů není vůbec snadné, ne-li nemožné, pokud používáte delší a ne příliš známou frázi. Rozhodně nepoužívejte pochybné nástroje, jejichž původ či použitý algoritmus není známý nebo je nejasný.

SÍŤOVÉ SLUŽBY

Jak již bylo řečeno, systémy UNIX jsou převážně síťovými systémy, na kterých běží spousta služeb. A právě na prolamování hesel k těmto službám se podíváme nyní. Zde je situace pro útočníka mnohem složitější, neboť nemůže plně využít výpočetního výkonu svého počítače. Je to z toho důvodu, že prolamování probíhá po síti, a je tedy potřebný určitý čas mezi zasláním hesla a obdržením odpovědi. O útoku hrubou silou na tyto služby ani nemluvě. Nyní již k jednotlivým službám a nástrojům.

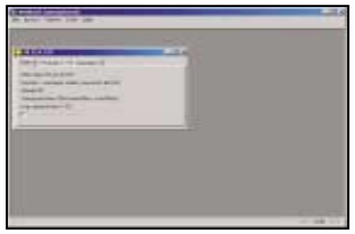
FTP, POP, TELNET

Útoky na tyto služby nejsou tak časté, přesto se s nimi můžeme setkat. Je to jednak z důvodu časové náročnosti, zanechání spousty stop a vzbuzení pozornosti. Jen opravdu neschopný administrátor si nevšimne, pokud se mu v rozmezí několika minut objeví upozornění o stovkách až tisících neúspěšných přihlášení. Dalším důvodem, proč nejsou tyto útoky příliš oblíbené, je to, že tyto služby posílají hesla po síti v textové podobě, tudíž je pro útočníka jednodušší hesla odchytit na cestě k cíli, než se pokoušet je prolamovat. I přes to však existují dostupné nástroje. Jedním takovým je například brutus, což je perlovský skript. Existují však desítky dalších. Na obrázku vidíme, jak pomocí nástroje brutus odhalíme špatná hesla k FTP serveru.

Obdobně můžeme postupovat i proti serveru POP či Telnet. Teď se zaměříme na platformu Windows, kde je situace pro člověka, který se snaží zjišťovat hesla, skutečným rájem na zemi.

HTTP

Http autentizace je v prostředí webu velmi rozšířená. Bohužel to s bezpečností této služby není nijak slavné. Za prvé mohou být tato hesla odchycena na síti, neboť jsou posílána v textové podobě, a za druhé existuje množství nástrojů na prolamování těchto hesel. A pro mnoho začínajících útočníků není lákavější cíl, než získat heslo k nějaké stránce s tajným obsahem. Proto je lepší tento způsob autentizace nahradit nějakým bezpečnějším řešením. Takovým je například SSL. SSL implementuje bezpečné algoritmy a šifruje veškerou komunikaci. Http autentizaci používá i spousta síťových prvků, jako například různé huby a switche. Na obrázku vidíte, jak snadno bylo prolomeno špatné heslo k přepínači 3com. U síťových prvků je nesnadné, dokonce někdy i nemožné, nahradit stávající systém například SSL, proto vždy zvolte silné heslo.



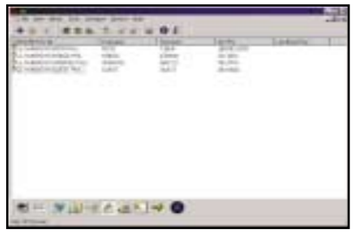
WINDOWS

Při psaní tohoto článku jsem byl v rozpacích, z které strany začít. Na platformě Windows je toho k prolamování opravdu dost, a ne vše mohlo být pokryto. Začněme tedy systémovými hesly k systému Windows.

PWL, SAM

Na systémech Windows 9x je soubor *.pwl souborem, kde jsou uložena hesla uživatelů k systému. Nebudeme si zde namlouvat, že systémy 9x jsou bezpečné. Každý z vás ví, že jakmile sedíte u počítače se systémem xp, máte nad ním plnou kontrolu. Hesla uložená v souboru pwl mohou být pro útočníka zajímavá například proto, že velké množství uživatelů používá jedno heslo k mnoha systémům nebo službám. Pokud se tedy útočníkovi podaří získat toto heslo, může tak mimoděk získat heslo například k poště uživatele, k jeho webovým stránkám nebo k účtu na ftp serveru. Na obrázku vidíte, jak snadné je získat hesla systému Windows z pwl souboru.

K získání těchto hesel byl použit nástroj Cain, který můžete získat na adrese ***www.oxid.it***. Tento nástroj je zdarma a umí toho



opravdu hodně. Na platformě Windows je to jeden z nejlepších bezpečnostních nástrojů. Vyjmenujeme si, co všechno Cain umí:

- Odkrýt heslo spořiče obrazovky (lokálně i z registru)
- Zobrazit heslo schované pod hvězdičkami
- Zobrazit hesla od lokálních sdílených prostředků
- Zobrazit uložená hesla
- Útočit na vzdálené sdílené prostředky
- Útočit na hesla od databáze Access
- Sniffovat po síti a zachytávat SMB hashe, poté je prolamovat

Pokud se tedy musíte nebo chcete přihla-

šovat do systému 9x, použijte k tomu nějaké heslo, které si snadno zapamatujete, ale nebudete ho používat nikde jinde. Rovněž mějte na paměti, že toto heslo může zjistit každý, kdo má přístup k vašemu počítači, a že toto heslo NEslouží k ochraně vašich dat či čehokoliv jiného, ale pouze k ochraně vašeho profilu (barvy, schéma, spořič atd.), a proto na toto heslo nespoléhejte.

Soubory sam jsou systémovými soubory s hesly u systémů w2k, xp. Zde je v heslech diametrální rozdíl. Na těchto systémech slouží hesla opravdu k ochraně vašich souborů a citlivých informací. Navíc tento soubor není jen tak lehce přístupný komukoliv a používá silné algoritmy. Proto heslo do systému Windows 2k, xp dobře vybírejte a střežte. Heslo by nemělo být stejné jako k jiným službám, ale nebezpečí je zde jistě nižší než na systémech 9x. Existuje však i program na hádání hesel do systémů 2k, xp a k luštění souboru sam. Tento program se jmenuje L0phtcrack a můžete jej získat na adrese ***www.astake.com***. Zmíněný program by měl být ve výbavě každého správce systému a systémová hesla by měla být pravidelně kontrolována.

SDÍLENÍ

Sdílení je další problematickou částí systémů Windows. Pokud jste uživateli sítě Windows, pravděpodobně pracujete se sdílenými položkami velmi často. Bohužel, s bezpečností těchto sdílených prostředků to není tak jednoduché a hesla k těmto prostředkům mohou být poměrně snadno získána. Nejjednodušší pro útočníka je zjistit si tato hesla lokálně. K tomu mu stačí přístup k počítači se systémem 9x. Zde má hesla jako na dlani. Může k tomu použít například již zmiňovaný nástroj Cain, který umí

nejen zobrazit všechna lokální sdílení, uložená hesla ke vzdáleným sdílením, ale umí vzdálená sdílení napadat a hádat hesla, stejně dobře jako hesla odchytávat. SMB relace jsou rovněž pro útočníka důležité i z jiných důvodů, a to zejména tím, že poskytují spoustu informací o systému a uživatelích. Pokud tedy sdílení výslovně nepotřebujete, snažte se jej zakázat a nahradit jej jinou vhodnou alternativou, pokud je to možné (například FTP). Pokud to možné není, tak používejte silná hesla, neukládejte si při jejich zadávání a příliš na zabezpečení heslem nespoléhejte. Na předešlém obrázku vidíte útok slovníkovým útokem na sdílený prostředek.

ARCHIVY

Mnoho uživatelů používá k šifrování svých souborů nějaký archivační program. Není to ale příliš šťastné řešení, protože algoritmus těchto souborů není příliš silný a lze jej poměrně snadno prolomit útokem hrubou silou. K prolomení hesla byl použit nástroj Advanced Archive Password Recovery. Zkušební verzi toho ná-

stroje můžete získat na adrese ***www.elcomsoft.com***. ElcomSoft je firma, která vyvíjí software na prolamování hesel. Na jejich stránkách můžete získat nástroje, které ve světě Windows prolomí téměř vše. Na obrázku vidíte, jak rychle bylo odhaleno heslo k archivu zip. Základem pro útok byl kvalitní slovník. Na druhém obrázku vidíte výsledek benchmarkového testu na stroji Celeron 1,1 GHz.

Rychlost je opravdu velká, a tím se snižuje i čas potřebný k prolomení hesla hrubou silou. Pokud chcete nějaký dokument opravdu chránit,

nespoléhejte na tuto metodu a raději sáhněte po nějakém kvalitním nástroji, jako je například PGP, neboť ten umí šifrovat lokální data stejně dobře, ale za použití velmi silného algoritmu, který může být prolomen jen velmi obtížně. Pokud chcete archiv chránit heslem, používejte silné heslo, tak jak bude uvedeno dále.

MS OFFICE

MS Office, jako nejrozšířenější kancelářský balík, nabízí možnost ochrany souboru heslem. Můžete dokument chránit pro čtení nebo pro zápis. I tato ochrana se dá však celkem snadno obejít. K tomu nám slouží nástroj od ElcomSoftu, jímž je Advanced Office XP Password Recovery. Tento nástroj je opravdu špičkou ve své oblasti. Jeho zkušební verzi lze získat na adrese ***www.elcomsoft.com***. Zmíněný nástroj umí pracovat se soubory následujících aplikací:

- MS Word
- MS Excel
- MS Access
- MS Outlook
- MS Money
- MS Schedule+
- MS Backup
- MS Visio
- MS Project
- MS Power Point

Sami vidíte, že záběr programu je velmi široký. Pomocí něho můžete na soubory útočit hrubou silou, slovníkovým útokem, přičemž si můžete různě nastavovat, jaké podmínky a znaky budou při luštění použity. Program je rovněž velmi rychlý, jak můžete vidět na přiloženém obrázku, kdy byl spuštěn benchmark, který je součástí programu.

DALŠÍ HESLA

Neexistují však hesla pouze pod systémem Windows či UNIX. S hesly se můžete setkat i u kapesních počítačů, u BIOSu počítače a v dalších oblastech IT. Hesla používají různé algoritmy a schémata. Od primitivních až po ty složité a bezpečné. Vždy lze najít nástroj, který umí nebo se pokusí heslo prolomit. Proto je volba hesla velmi důležitým prvkem bezpečnostní strategie. Nyní si uvedeme několik rad a doporučení, jak by mělo správné heslo vypadat.

TVORBA HESLA

Existuje několik obecný rad a postupů, jak vytvořit dobré heslo. Zde uvedeme několik bodů, jak by správné heslo mělo vypadat, a čeho se naopak při tvorbě hesla vyvarovat.

Co by heslo nemělo obsahovat:

- Jakékoliv slovo
- Jakékoliv jméno
- Kombinaci slova (jména) a číslic
- Datum narození kohokoliv
- Rodné číslo kohokoliv
- Telefonní číslo, číslo dveří, bytu atd.

Naopak, co by heslo mělo obsahovat:

- Malá a velká písmena
- Číslice
- Interpunkční znaky
- Min. 6 znaků

Nyní si předvedeme postup, jak vytvořit dobré heslo. Vyberete si nějaký oblíbený citát, výrok z filmu, jakoukoliv větu. My si vezmeme jako příklad Senecův citát: „Nikdo se nerodí moudrým“. Máme teď dostatek prostoru k tvorbě hesla a k hraní si s čísly. Existují tisíce variant, a záleží jen na vaší tvořivosti a nápaditosti. Vezmeme například z každého slova první písmeno. Dostaneme tedy nsnm. Pokračujeme dále. Nyní místo mezer mezi slovy doplníme číslice. A nebudeme začínat jedničkou, ale například pětkou. Výsledek bude n5s6n7m. To už je celkem slušné heslo. Kombinací by šlo vymyslet několik tisíc. Místo číslic bychom mohli doplňovat speciální znaky, z každého slova vybrat ne první, ale druhé, třetí písmeno atd. atd. Důležité je, abychom byli schopni z fráze heslo rekonstruovat bez pomoci tužky a papíru. Fráze slouží k tomu, abychom si heslo snadno zapamatovali a nebyli nuceni si jej někam poznamenávat. Frázi si poznamenat můžeme v případě, že máme jistotu, že se nikomu nepodaří heslo z fráze odhalit. Jistě, mohli byste si například z hlavy vymyslet heslo 6s&5@df, ale takové se velmi špatně pamatuje. Navíc musíte brát zřetel na jedno ze základních pravidel, které říká, že byste neměli jedno heslo použít dvakrát. Pokud tedy máte zřízeno několik e-mailových adres, měli byste u každé z nich použít jiné heslo. Mohlo by se stát, že by bylo vaše heslo prozrazeno (například pomocí snifferu), a útočníkovi byste tak poskytli přístup do mnoha jiných systémů.

ZÁVĚREM

Tvorba hesel je zábavný proces. Proto heslo vždy vybírejte pečlivě a mějte na zřeteli základní bezpečnostní pravidla. Pokud je pro vás bezpečnost systému důležitá, musí začínat a končit silnými hesly. Ovšem jen silná hesla váš systém neochrání. Je-li však systém velmi dobře zabezpečen, stávají se hesla jedinou branou do systému, a proto je důležité volit a vyžadovat silná hesla, která nemohou být snadno prolomena.

Nápady, dotazy, návrhy témat, jež vás zajímají a připomínky zasílejte na adresu igm@centrum.cz. Na vaše dotazy k této problematice se pokusíme najít odpovědi. 3 0373/FEL ❑