DECROS NEWS

ŘÍJEN 2000 ČÍSLO 3/2000

Úvodník

Protože tento úvodník píši koncem září, mohl bych tvrdit, že za sebou máme tzv. okurkovou sezónu. Sice nevím, jak jste letní období prožívali Vy, ale já jsem léto vnímal jako poněkud hektickou dobu, nebo-li dobu plnou práce. Asi si říkáte - co teprve podzim. Nepochybuji o tom, že podzim nám přichystá nejedno další překvapení. Možná se ptáte jaká překvapení nás v létě zastihla? Podívejme se například na legislativní překvapení.

Myslím, že zákon o ochraně osobních údajů je dost velkým překvapením. Rychlost, s jakou vešel v platnost a termíny, které obsahuje, jistě předčily očekávání všech. Zřízení Úřadu pro ochranu osobních údajů nás jen utvrdilo v přesvědčení, že zákon opravdu vešel v platnost 1. června letošního roku. Můžeme se sice uklidňovat, že máme čas do konce roku, ale již nyní bychom měli začít něco dělat, minimálně proto, že sankce jsou velmi tvrdé.

Na druhou stranu se přijetím zákona o elektronickém podpisu moc neděje. Odborná veřejnost se rozdělila na dva tábory, z nichž ten první tvrdí, že přijetím tohoto zákona se udělal velmi důležitý krok, přičemž druhý tábor to nepopírá, ale skepticky dodává, že je to poněkud málo. Na otázku, v kterém roce si již budeme moci podávat daňové přiznání přes Internet, však nedostáváme rozumnou odpověď. Nechme se tedy překvapit.

Když píši o legislativě spojené s ochranou informací, nemohu samozřejmě opomenout ani zákon o utajovaných skutečnostech. Jeho termíny jsou také pevně spjaty s koncem roku. Skutečnost, že společnost DECROS uvádí několik produktů právě pro tento trh, jistě pomůže při plnění těchto termínů. Přesto subjekty, na které se vztahuje uplatnění tohoto zákona, nemají situaci vůbec jednoduchou.

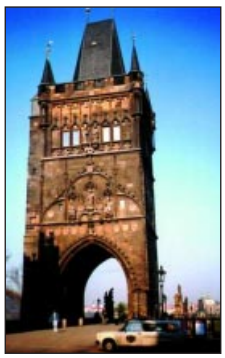
Máme tedy před sebou podzim, podzim plný práce, a to nejenom v oblasti informačních technologií. Věřím, že stejně jako každý rok dokážeme i letos vyvinout takové nasazení, abychom v závěru tohoto roku mohli úspěšně bilancovat. A to nejenom vzhledem k hospodářskému výsledku, ale například i k liteře zákona.

Josef Dvořák
j.dvorak@decros.cz

Chráníte či pracujete s osobními údaji?

Zákon o ochraně osobních údajů (zák. č. 101/2000 Sb.)

Tento zákon je zatím tak trochu neprávem ve stínu svých "velkých bratrů" - zákonu o ochraně utajovaných skutečností a zákonu o elektronickém podpisu, přestože bude mít přímý vliv na způsob práce v naprosté většině organizací. Vysvětlení, proč tomu tak je, se naskýtá hned několik:



Především nejde o zcela nový zákon. Dříve platný zákon 256/1992 Sb. řešil ochranu osobních údajů, zejména povinnosti související s ochranou informací, pouze při provozování informačních systémů nakládajících s osobními údaji. V případě manuálního nakládání s osobními údaji bylo nutné zákon přiměřeně aplikovat. Zákon také předpokládal ustavení orgánu, jehož posláním by byla ochrana práv jednotlivců na soukromí, resp. jejich osobních údajů tzv. datová inspekce. Tento orgán však nebyl nikdy zřízen.

Okrajovost řešení problematiky ochrany osobních údajů zákonem 256/1992 Sb. a absence inspekčního orgánu způsobily, že s jeho dodržováním si nikdo moc hlavu nelámal. Do podvědomí naší společnosti se tak bohužel dostal zkreslený názor, že si s osobními údaji a soukromím osob lze nakládat jakkoli a zcela beztrestně.

Zákon č. 101/2000 Sb. nabyl sice účinnosti již 1.6.2000, ale po určitou dobu budou platná přechodná ustanovení. Oznámení o zpracování osobních údajů je tedy nezbytné učinit po 1.12.2000 tak, aby bylo dosaženo registrace nejpozději do 31.5.2001 (v případě, že zpracování bylo zahájeno po 1.6.2000, vztahují se na ně plně povinnosti podle zákona). Takže se zdá, že je ještě dost času, ale opak je pravdou!

Většina lidí nebo organizací spoléhá na to, že se jich zákon netýká. Což by se jim v budoucnu nemuselo vyplatit. Kontrolní orgán je již ustanoven a sankce v zákoně také vymezeny. A to jak pro správce informací, tak i pro "pouhého" zpracovatele.

Nyní se podívejme trochu blíže na zmiňovaný zákon. Jeho plné znění je možno nalézt na www.uoou.cz, což jsou domovské stránky Úřadu pro ochranu osobních údajů. Na adresu info@uoou.cz můžete směřovat Vaše dotazy k této problematice.

Z čeho vychází zákon 101/2000 Sb.

Východisky pro zpracování nové právní úpravy ochrany osobních údajů se staly Listina základních práv a svobod, stávající zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, Směrnice č.95/46/EC Evropského parlamentu a Rady z roku 1995 o ochraně jednotlivců ve vztahu ke zpracování osobních dat a o volném pohybu těchto dat (dále jen

Obsah

"Směrnice") a Úmluva č. 108 Rady Evropy na ochranu osob ve vztahu k automatizovanému zpracování dat (dále jen "Úmluva") z roku 1981. Listina základních práv a svobod zaručuje nedotknutelnost osob a jejich soukromí. Tato nedotknutelnost může být omezena jen v případech stanovených zákonem. Listina dává každému právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno, právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života a právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě. Zároveň je každému dána možnost domáhat se stanoveným postupem svého práva u nezávislého a nestranného soudu a ve stanovených případech u jiného orgánu.

Proč bylo nutné přijmout nový zákon?

Dosud platný zákon o ochraně osobních údajů 256/1996 Sb., který stanovil základní právní rámec nakládání s osobními údaji, vzhledem k datu svého vzniku nevyhovoval mnohým ustanovením Směrnice. Neodpovídal také Úmluvě, proto k ní Česká republika nemohla doposud přistoupit. To komplikovalo činnost např. Ministerstvu zahraničí ČR, Ministerstvu vnitra ČR, protože přistoupení k Úmluvě je podmínkou spolupráce v rámci Schengenského informačního systému. Zákon dále neupravil či upravil pouze částečně řadu dalších oblastí, např. dostatečnou ochranu osobních údajů vypovídajících o osobnosti a soukromí, povinnost toho, kdo shromažďuje osobní údaje, informovat občana o jeho právech a o jiných pro něj významných skutečnostech, oznamovací povinnost nakládání s osobními údaji u kontrolního orgánu subjektem, který hodlá nakládat s osobními údaji, možnost zásahu kontrolního orgánu před zahájením takového nakládání s osobními údaji, které by z hlediska ochrany osobních údajů mohlo představovat určitá rizika, sankce za porušování zákona a předávání údajů do jiných zemí.

Co zákon řeší?

Zákon upravuje ochranu osobních údajů o fyzických osobách, práva a povinnosti při zpracování těchto údajů, stanoví podmínky, za nichž se uskutečňuje jejich předávání do jiných států, a sankce za porušení povinností stanovených tímto zákonem.

Dále zákon zřizuje se Úřad pro ochranu osobních údajů se sídlem v Praze (dále jen "Úřad").

Jaká je působnost zákona?

- **vztahuje se** na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby, pokud tento zákon nebo zvláštní zákon nestanoví jinak
- **vztahuje se** na veškeré zpracovávání osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky
- **nevztahuje se** na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu
- **nevztahuje se** na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány

Vymezení některých pojmů

Osobním údajem je jakýkoliv údaj týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze na základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho identitu.O osobní údaj se nejedná, pokud je třeba ke zjištění identity subjektu údajů nepřiměřené množství času, úsilí či materiálních prostředků (jde o tzv. depersonalizované údaje).

Citlivým údajem je osobní údaj vypovídající o majetku a majetkových poměrech, národnostním, rasovém nebo etnickém původu, politických postojích, členství v politických stranách či hnutích nebo odborových či zaměstnaneckých organizacích, náboženství a filozofickém přesvědčení, trestné činnosti, zdravotním stavu a sexuálním životě subjektu údajů.

Anonymním údajem je takový údaj, který buď v původním tvaru nebo po provedeném zpracování nelze přímo vztáhnout k určenému nebo určitelnému subjektu údajů.

Subjektem údajů je fyzická osoba, k níž se osobní údaje vztahují.

Zpracováním osobních údajů je jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.

Správcem je každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak.

Zpracovatelem je každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.

Práva a povinnosti při zpracování osobních údajů

Správce je povinen:

- stanovit účel, k němuž mají být osobní údaje zpracovány
- zpracovávat pouze pravdivé a přesné osobní údaje, které získal v souladu s tímto zákonem, je povinen ověřovat, zda jsou osobní údaje pravdivé a přesné
- zpracovávat osobní údaje pouze k tomu účelu, k němuž byly shromážděny
- zpracovávat k jinému účelu lze osobní údaj, jen pokud k tomu dal subjekt údajů souhlas
- shromažďovat osobní údaje pouze otevřeně, je vyloučeno shromažďovat údaje pod záminkou jiného účelu nebo jiné činnosti
- nesdružovat osobní údaje, které byly získány k rozdílným účelům
- citlivé údaje je možno zpracovávat, jestliže subjekt údajů dal ke zpracování výslovný souhlas. Souhlas musí být dán písemně, podepsán subjektem údajů a musí z něho být zřejmé, k jakým údajům je dáván, jakému správci údajů, k jakému účelu, na jaké období a kdo jej poskytuje. Souhlas může subjekt údajů kdykoliv odvolat. Správce je povinen předem subjekt údajů o jeho právech poučit. Tento souhlas musí správce uschovat po dobu zpracování osobních údajů, k jejichž zpracování byl souhlas dán
- je povinen včas a řádně subjekt údajů informovat o tom, že o něm shromažďuje údaje, v jakém rozsahu a pro jaký účel, kdo je bude dále zpracovávat a pro jaký účel a komu mohou být zpřístupněny či komu jsou údaje určeny. Součástí této informace musí být též údaj o jeho sídle, případně o sídle zpracovatele.

Jestliže zpracovatel zjistí, že správce porušuje povinnosti stanovené tímto zákonem, je povinen jej na to neprodleně upozornit a ukončit zpracování osobních

údajů. Pokud tak neučiní, odpovídá za škodu, která subjektu údajů vznikla, společně a nerozdílně se správcem údajů. Tím není dotčena jeho odpovědnost podle tohoto zákona.

Povinnosti osob při zabezpečení osobních údajů

Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.

Osoby, které zpracovávají osobní údaje, jsou povinny zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací.

Oznamovací povinnost

Ten, kdo hodlá zpracovávat osobní údaje, je povinen tuto skutečnost oznámit Úřadu před započetím zpracovávání osobních údajů. Oznámení je povinen učinit i správce, jestliže hodlá změnit zpracování osobních údajů. Oznámení musí být učiněno písemně.

Oznámení musí obsahovat následující informace (název správce, adresu jeho sídla a identifikační číslo, pokud bylo přiděleno, účel nebo účely zpracování, kategorie objektů údajů a osobních údajů, které se těchto subjektů týkají, zdroje osobních údajů, popis způsobu zpracování osobních údajů, atd).

Úřad je povinen do 30-ti dnů od doručení oznámení Úřadu oznamovateli sdělit, že jeho oznámení registruje, nebo vydat rozhodnutí podle § 17. Pokud Úřad oznámení zaregistroval, může dnem registrace oznamovatel zahájit zpracování osobních údajů.

Jestliže Úřad ve lhůtě stanovené v odstavci 3 oznamovateli nesdělí, že oznámení zaregistroval, ani nevydá rozhodnutí, má se za to, že oznámení zaregistroval. Zjistí-li Úřad, že oznamovatel nesplňuje podmínky stanovené tímto zákonem, zpracování osobních údajů nepovolí.

Postavení a působnost Úřadu

Úřad při provádění dozoru nad zpracováním osobních údajů postupuje nezávisle a řídí se pouze zákony a jinými právními předpisy, je nezávislý na vládě, jejich orgánech a ústředních orgánech státní správy. Do činnosti Úřadu lze zasahovat jen na základě zákona.

Dále Úřad provádí dozor nad dodržováním povinností stanovených tímto zákonem při zpracování osobních údajů, vede evidenci oznámení učiněných podle § 16 a registr povolených zpracování osobních údajů (dále jen "registr"), vykonává další působnosti stanovené mu zákonem.

Mezi další kompetence Úřadu patří projednávání přestupků a jiných správních deliktů a udělování pokut podle tohoto zákona.

Důležitým aspektem pro uvedení zákona do praxe je také skutečnost, že Úřad poskytuje konsultace v oblasti ochrany osobních údajů.

Sankce

Zákon obsahuje nejenom povinnosti všech zúčastněných stran, ale také rozsah sankcí a pokut, pakliže zákon není dodržován. Podívejme se na ty základní:

- Přestupku se dopustí a pokutou do výše 50 000 Kč bude potrestána osoba, která je ke správci nebo zpracovateli v pracovním nebo jiném obdobném poměru nebo pro něj vykonává činnosti na základě dohody, nebo osoba, která v rámci plnění zákonem uložených oprávnění a povinností přichází do styku s osobními údaji správce nebo zpracovatele, pokud poruší povinnost mlčenlivosti, uloženou podle tohoto zákona, nebo pokud poruší jinou povinnost stanovenou tímto zákonem bude potrestána pokutou do výše 25 000 Kč.
- Přestupku se dopustí a pokutou do výše 25 000 Kč bude potrestána osoba uvedená v odstavci 1, která poruší jinou povinnost stanovenou tímto zákonem.
- Pořádková pokuta bude udělena osobě, která neposkytne Úřadu při výkonu kontroly potřebnou součinnost, až do výše 25 000 Kč, a to i opakovaně.
- Pokutou do výše 10 000 000 Kč bude potrestán správce nebo zpracovatel, který poruší povinnost uloženou mu podle tohoto zákona.
- Pokud správce nebo zpracovatel do jednoho roku ode dne, kdy nabylo rozhodnutí o uložení pokuty právní moci, porušil povinnosti uložené mu tímto zákonem opakovaně, může mu být uložena pokuta do výše 20 000 000 Kč.
- Správce nebo zpracovatel, který maří kontrolu prováděnou Úřadem, může být potrestán pořádkovou pokutou do výše 1 000 000 Kč, a to i opakovaně.
- Porušení povinností projednává Úřad. Při ukládání pokuty podle tohoto zákona vychází Úřad zejména z povahy, závažnosti, způsobu jednání, míře zavinění, doby trvání a následků protiprávního jednání.

Závěr

Zákon č. 101/2000 Sb. vstoupil v platnost 1.6.2000. Protože naprostá většina našich současných informačních systémů (firemních dotazníků, knih návštěv, databází atd.) s ochranou osobních údajů příliš nepočítala, bude nutné věnovat určité úsilí na zapracování požadavků, které z tohoto zákona vyplývají.

Především je třeba přehodnotit, jaké osobní údaje organizace pro svoji činnost skutečně potřebuje, dále získat ke zpracování těchto informací souhlas, a to jak od subjektu

osobních údajů, tak Úřadu. Protože je nutné posuzovat případ od případu, kdy jde o zpracování osobních údajů ve smyslu tohoto zákona, bude určitě užitečné se nejdříve zeptat pracovníků Úřadu (info@uoou.cz), kteří mají povinnost ze zákona tyto konzultace provádět.

Podstatné je také uvědomit si, že v případě zpracovávání osobních údajů, musíte také zabránit neautorizovanému přístupu k těmto informacím! Investice do technologií, které zabezpečí zpracování těchto dat, jsou zanedbatelné ve srovnání s mnoha milionovými pokutami.

Pravidelným čtenářům DECROS News snad nemusím připomínat, že společnost DECROS nabízí technologie a služby, které spolehlivě Vaše data ochrání!

Radovan Pekárek
r.pekárek@decros.cz

Pro klid Vašich informací

Pod vlivem dnešního shonu, a to i mimo oblast informačních technologií, si uživatel běžného počítače (samozřejmě tak uživatel superychlé firemní sítě) často neuvědomuje cenu vlastních informací, které počítačová média obsahují. A co Vy?

Možná právě Vy patříte k té skupině uživatelů, kteří si "tvrdě" uvědomili, že informace mají cenu. Vynucené uvědomění je často příliš drahé, protože přichází s událostí typu:

- Došlo ke krádeži počítače (o to častěji mobilního)
- Došlo k vyzrazení dat, ať už nějakou chybou či útokem
- Havárie systému či počítače zničila data
- Virová infekce mi zničila (nevratně modifikovala) všechny informace
- a řada dalších

Je to prostě jako s pojištěním. Až do okamžiku první možné pojistné události, mnozí lidé často naprosto zavrhují pojistku. Po této události vše znovu zváží a často (patřím k této skupině i já :-)) si dodatečně zřídí pojistku, aby případné následující nepříjemné události mohli eliminovat. Existuje však celá další skupina uživatelů pojistek, která si nebezpečí uvědomuje a chce s tím něco dělat. Proto si pojistku uzavře dopředu; dříve, než k nějaké katastrofě dojde.

Potřebujete informační bezpečí?

Stejně tak jako není účelné uzavírat pojistku na luxusní automobil v případě, že jsem majitelem zánovní Felicie, je jistě i míra informační bezpečnosti, kterou nikdy nevyužiji. Ale pojďme se společně zamyslet nad třemi oblastmi, které se sami nabízejí.

Informace uložené na notebooku

Notebook je skvělá věc. Prostě se odpojím od sítě, zaklapnu a strčím do tašky. Cestuje se mnou na jednání k zákazníkům, domů, do kanceláře a … Co informace na něm? Mohu tvrdit, co chci, ale informace na něm jsou často používány na jednáních u zákazníků, na poradách ve firmě, dále obsahuje moji kompletní elektronickou komunikaci (poštu) s klienty, partnery i kolegy. Rád bych řekl: Nic zajímavého. Ale místo toho si pokládám otázku: Přál bych si, aby tyto informace někdo četl? Přál by si můj zaměstnavatel, aby se tyto informace dostaly na veřejnost? Odpovídám: Určitě ne.

Ne, opravdu na mém notebooku nemám utajované skutečnosti. Ale často, i když si to člověk neuvědomuje, pracuje s informacemi, které by mohly mít zásadní přínos pro konkurenci či které by mohly být nevhodně vysvětleny. Každopádně zde hrozí poškození dobrého jména společnosti.

Informace uložené na síti

Nevím, jak Vy, ale já mám velkou část dokumentů, se kterými jsem delší dobu nepracoval, uloženou na síti. Proč? Jednak je to kapacitou notebooku, jednak se nemusím starat o zálohování; zálohování serverů probíhá automaticky.

Ovšem musím dodat také relativní nevýhody práce s dokumenty či daty na síti, (samozřejmě kromě toho, že musím být připojený). Přestože na síti existují nějaká práva, nemohu mít pod kontrolou, zda někdo mé dokumenty prohlíží, modifikuje či kopíruje. Nechci v žádném případě nasazovat proti administrátorovi, ale vše záleží na hesle do Windows (a zároveň do sítě) a to prostřednictvím jednoduché utility z Internetu dokáže odchytit každý. Jeho zjištění se rovná jeho možnosti použití, a tak síť poskytne útočníkovi to, co mně. Musím navíc dodat, že zálohy sice jsou, ale v tom případě samozřejmě zase musím důvěřovat každému, ke komu se dostanou (byť i náhodou), ne pouze našemu administrátorovi.

Informace v servisu

No a potom přijde okamžik, kdy vzhledem k havárii grafické karty v notebooku musí být odvezen do servisního střediska. Ne že bych každého podezíral, to už bych nemohl vystrčit ani nos. Ale co se tam děje? Nemusí náhodou zálohovat můj disk, protože se obávají, že by mohli poškodit jeho data? Kde se potom taková záloha toulá? Určitě bychom našli spousty zajímavých otázek. Ale máme odpovědi?

Řešení bezpečnosti?

Ochrana informací na notebooku, v síti a jinde může být velmi jednoduchá. Je totiž možné použít aplikační nadstavbu PROTECT a bezpečnostní předmět, například DECROS Card PKI (bezpečnostním předmětům se věnuje samostatný článek na titulní straně). Co mi tato kombinace nabízí? Tyto dvě silné stránky:

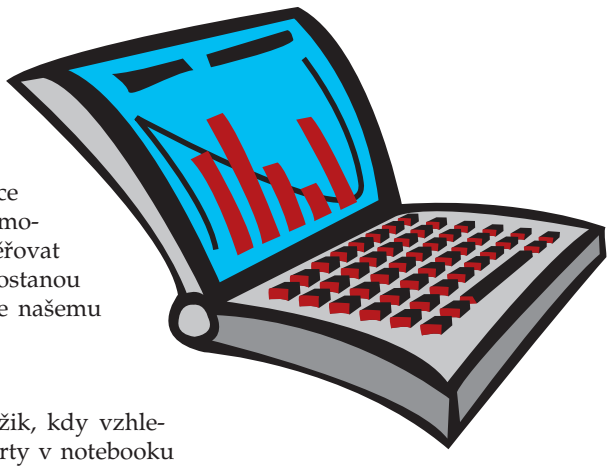
- kvalitní autentizaci uživatele
- silné transparentní šifrování

Jak ovlivní moji práci? Pojďme se podívat.

Kvalitní autentizace uživatele

Co se změnilo? Používám totiž nikoliv zápis hesla z klávesnice, ale po naběhnutí systému vložím čipovou kartu DECROS Card PKI (dále jen DC) do PCMCIA čtečky a po zapsání hesla k DC mne přihlašovací klient PROTECT Logon automaticky přihlásí do systému a sítě (pokud jsem připojen :-)).

Proč je to kvalitní? Protože heslo, kterým se přihlašuji, není jednoduché ani zapamatovatelné, tedy jinak řečeno, jeho prolomení je velmi obtížné. Jaké máte heslo dnes? Viděl jsem hesla typu : JANKA, JAMES007, 5309232713 (rodné číslo si každý pamatuje). Představte si však, že prostřednictvím DC se přihlásíte heslem M1D25EFL5:_PPO7ESX5S2S05. Líbí se Vám? Mně také.



Navíc díky technologii PROTECT Logon mohu okamžitě uzamknout notebook pouhým vytažením čipové karty DC ze čtečky. Velmi praktická funkce při odchodu na oběd či další jednání. Pokud zastrčím identickou, tedy mou, DC zpět do čtečky, tak se mi notebook odemkne a mohu pokračovat v práci s vědomím, že nikdo nezneužil mé nepřítomnosti.

Silné transparentní šifrování

Dle zkušeností nic bezpečnějšího než kvalitní šifrování neexistuje. Právě takové šifrování nabízí modul PROTECT Encrypt. Veškerou svou práci mám šifrovanou a to bez rozdílu, zda ji mám uloženou na notebooku, síti, disketě, firemní záloze či ftp serveru. Prostě všude, samozřejmě kam mohu v důsledku svých práv dosáhnout, si

mohu být jistý, že tady mám svou práci velmi dobře chráněnou.

Má práce po přihlášení vypadá tak, že v okamžiku, kdy chci pracovat s prvním dokumentem, který je šifrován, jsem dotázán na šifrovací klíč. Opět to samé jako s heslem - zapamatovatelný klíč se rovná špatný klíč. Proto ho nevypisuji na klávesnici, ale automaticky se mi načte z bezpečnostního předmětu, v mém případě z DECROS Card PKI. Zadám heslo k DC a je to. Mohu rázem pracovat se všemi daty, ke kterým jsem měl v DC uložený šifrovací klíč; vejde se jich tam až 31. Je to tak jednoduché.

Ještě pro pochopení, proč taková kapacita v DC. Já osobně například používám čtyři šifrovací klíče na notebooku: FIRMA, SECURITY, PRIVATE a TEMP. Klíč FIRMA používám na veškerou práci pro mého zaměstnavatele. Ne že by šlo o tak citlivé informace, ale práce se zašifrovaným dokumentem je naprosto stejná jako s nešifrovaným, a tak proč ne, co kdyby … Šifrovací klíč SECURITY zase využívám na vyloženě informace citlivé a nebo informace, které by mohly vést k citlivým informacím. Tak například tímto klíčem šifruji off-linové složky mailového klienta Outlook2000.

Šifrovací klíč PRIVATE pak využiji na ochranu soukromých informací a TEMP na šifrování všech pracovních adresářů, jako například Temp z Windows či Temporary Internet Files; ano, i to je vhodné šifrovat.

Správa bezpečnosti?

Pokud patříte mezi správce sítě, tak si jistě posteskněte, že další produkt do Vaší společnosti by byl poslední hřebíček do rakve Vaší IT, ale není tomu tak. Celý systém se totiž dá velmi dobře centrálně spravovat.

Společnost DECROS klade velký důraz na spravovatelnost, a tak nabízí řadu nástrojů, kterými lze vzdáleně centrálně spravovat nejen nastavení aplikace PROTECT for Windows pro každého uživatele, ale také spravovat bezpečnostní předměty.

Další zatížení uživatele?

Když se řekne bezpečnost, tak si uživatel představí celou řadu nepříjemných bariér, které ho otravují a zdržují od potřebné práce. Ano, i tak to může vypadat. Ovšem standardem společnosti DECROS je plné soustředění na to, aby uživateli nabídl míru bezpečnosti, po které touží, v takové formě, která jej nijak neomezuje.

Tak například heslo pro předmět (například DECROS Card PKI) se dá vypnout, takže PROTECT si toto heslo zapamatuje při přihlášení a všechny další činnosti provede bez nutnosti zadávat heslo. Ovšem je to určitá míra bezpečnosti.

To, co tuto míru nesnižuje, je pohodlí, které uživatel může získat kvalifikovaným nastavením. Například místo toho, aby si určoval, při každém odesílání zašifrovaných informací poštou, šifrovací klíč a algoritmus, má přednastavené tzv. Šifrovací šablony, které mu nabídnou dialog typu KOMU? a uživatel pouze vybere příjemce a odešle. Takových příkladů je samozřejmě více, ale není nad to si PROTECT for Windows vyzkoušet osobně. Proto neváhejte a stáhněte si jej z www.decros.cz či mi napište a demonstrační CD-ROM Vám rád zašlu.

Co říci závěrem?

Informační bezpečnost je oblast, která poměrně agresivně proniká do IT. Skutečnost, že samotné nainstalování výše popsané kombinace je přínosem pro uživatele, samozřejmě neznamená, že stejné řešení je právě to "pravé ořechové" pro Vaši organizaci. Proto neváhejte a pokud máte zájem o udržení Vaší informační bezpečnosti na patřičné úrovni, oslovte nás a tým našich specialistů se bude věnovat i Vám, protože jsme zde

... pro klid Vašich informací.

Josef Dvořák
j.dvorak@decros.cz

Otevřeno nové zastoupení Divize IT

V průběhu letošního léta bylo v Praze otevřeno nové zastoupení Divize informačních technologií.

Kontaktní místa Divize IT:

DECROS spol. s r.o.
Divize informačních technologií

V Olšinách 75
100 97 Praha 10

Tel.: 02-8100 2222
Fax: 02-8100 2244

DECROS spol. s r.o.
Divize informačních technologií

J.Š.Baara 40
370 01 České Budějovice

Tel.: 038-731 2808
Fax: 038-731 1480

e-mail: infoIT@decros.cz
http://www.decros.cz

PROTECT v novém kabátě

Ať již patříte k uživatelům aplikační nadstavby PROTECT či ne, jistě by Vás mohla oslovit nová verze tohoto produktu. Proč? Podívejte se na níže uvedený popis nových vlastností a pusťte se do testování osobně.

První, čeho si jistě povšimnete při instalaci, je skutečnost, že se PROTECT for Windows (dále jen Protect) skládá ze tří modulů Logon, Encrypt, Sign.

PROTECT Logon

Modul PROTECT Logon je velkým přínosem pro běžného uživatele tím, že s použitím bezpečnostního předmětu nabízí uživateli komfort v podobě přihlášení do Windows i sítí. Uživatel si tak nemusí pamatovat žádná jména a hesla pro přihlášení a tyto informace tak mohou být dostatečně kvalitní.

Využití bezpečnostního předmětu dále zajistí při odchodu od počítače jeho uzamknutí a při příchodu jeho bezpečné odemknutí.

Tento modul dále obsahuje vedení auditu. Jedná se o informace, které vypovídají o používání stanice a stavu bezpečnostních prvků na stanici.

Další součástí jsou tzv. Systémové ochrany, které umožňují nastavit uživateli určitý stupeň ochrany před neodbornými zásahy.

PROTECT Encrypt

Modul PROTECT Encrypt je se svou technologií symetrického šifrování je základem aplikační nadstavby PROTECT for Windows. Modul nabízí především kvalitní ochranu souborů šifrováním.

Šifrování, které využívá tento modul, využívá standardně symetrických šifrovacích algoritmů CAST, WinCros a Wincros II s délkou klíče až 160 bitů. Uživatel může využít dvou základních způsobů: transparentní šifrování (on-line) a chráněný archív.

Mezi další součásti patří také nevratné mazání souborů, které umožňuje velmi kvalitně smazat fyzické místo na médiu.

PROTECT Sign

Součástí modulu PROTECT Sign je také speciální knihovna DECROS CSP (Crypto Service Provider), která umožňuje díky CryptoAPI, rozhraní společnosti Microsoft, velmi kvalitní ochranu komunikačních kanálů; například v Microsoft Outlook 2000.

Pokud je na daném počítači nainstalován modul PROTECT Encrypt, pak modul PROTECT Sign doplňuje do systému možnost digitálního podepisování Chráněného archívu PROTECT. Chráněný archív PROTECT tak lze zároveň digitálně podepsat i kvalitně zašifrovat.

Protect for Windows 2000

Nástup Windows 2000 možná dnes nevidíte tak důležitý a aktuální jako já. Přesto může poměrně brzy nadejít den, kdy budete uvažovat, zda přejít na Windows 2000. Dobrá zpráva je, že Protect může přejít na tento nový operační systém s Vámi. Protect pro Windows 2000 přináší standardní bezpečnostní funkce jako pro ostatní Windows systémy.

Rozboru toho, proč a jaký to má efekt, budeme věnovat článek v dalším čísle DECROS News.

Grafické odlišení šifrovaných souborů

PROTECT od verze 3.0 přináší řadu vylepšení, která umožňují uživatelům i správcům lepší orientaci o tom, které soubory a adresáře jsou šifrované. Informace o této skutečnosti se zobrazuje na dvou místech: zaprvé ve Vlastnostech souboru/adresáře,

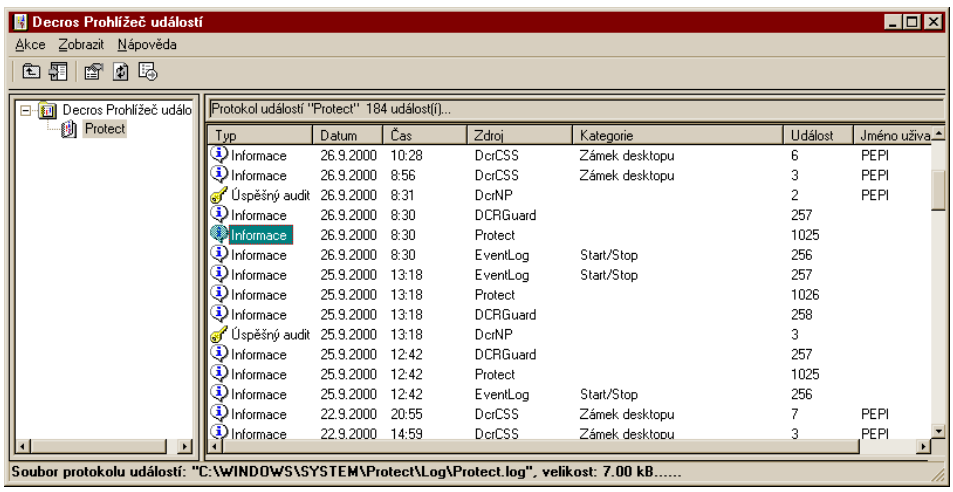
zadruhé, jak je patrné z obrázku, i v levé části Průzkumníka.

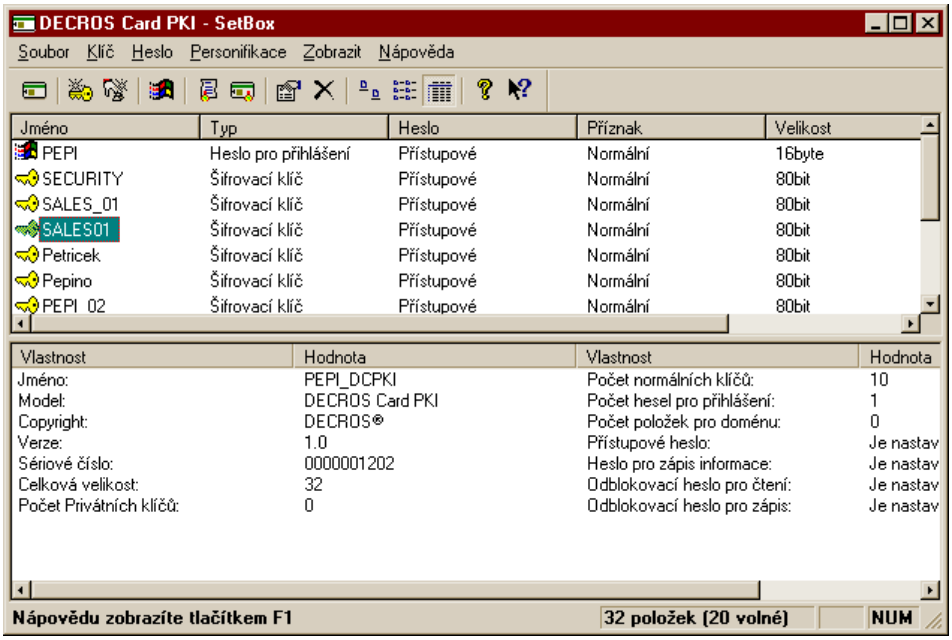
Další novinkou je skutečnost, že všechny soubory a adresáře, které jsou šifrované, mají ke své ikonce "přilepený" malý červený zámeček.

Záznam zvolených bezpečnostních operací

Prohlížeč událostí, jak byla tato funkce nazvána, je chápán jako prostředek k zaznamenání zvolených událostí, jako například přihlášení uživatele či uzamknutí stanice předmětem. Zaznamenané události by měly pomoci při hledání konfliktů, nejasností apod.

Každý modul má ve svých vlastnostech nastaveno, které operace se mají zaznamenávat. Tato nastavení jsou plně spravova-



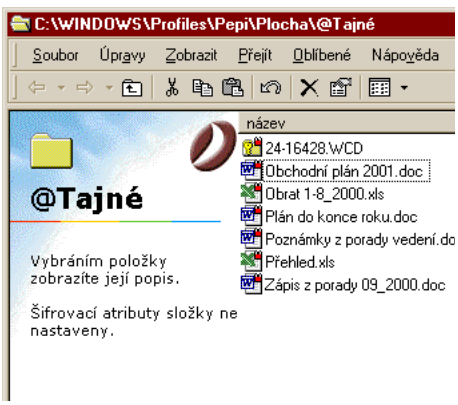


telná pomocí systémové politiky a dodávaných šablon pro systémovou politiku. Součástí každého záznamu je čas a jméno přihlášeného uživatele.

Do Prohlížeče událostí Protectu lze zaznamenávat:

- ukončení operačního systému
- start šifrovacího ovladače Protectu
- deaktivace/aktivace ovladače Protectu
- vypnutí/zapnutí šifrování
- uživatelem vyvolaná žádost o klíč při otevírání souboru (úspěch/neúspěch/jméno souboru/proces)
- záznam o otevření Protect.ini pro zápis
- načtení klíče/klíčů
- smazání klíčů - reset
- přihlášení (předmět, úspěch)/odhlášení
- zamknutí/odemknutí (předmět, úspěch) /automatické zamknutí (timeout)
- interní chyby, chybová hlášení

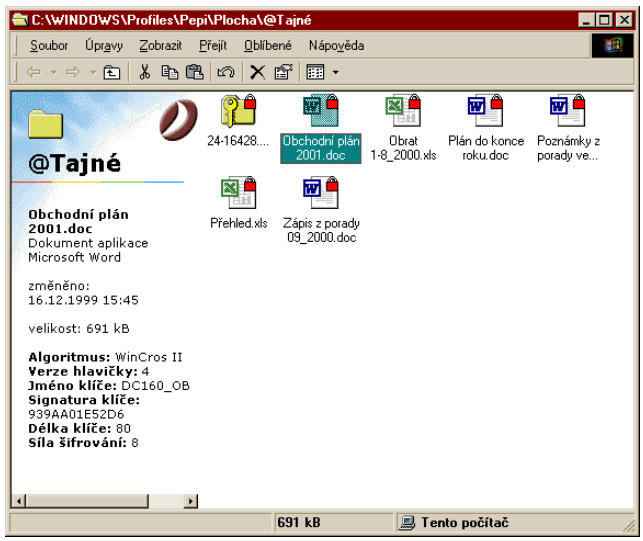
Všechny tyto události jsou zapisovány ve Windows 95 či Windows 98 do speciálního souboru, který je chráněn proti smazání a modifikaci uživatelem. Ve Windows NT či Windows 2000 se tyto záznamy zaznamenávají přímo do auditu systému.



DECROS SAPI Crypto Service Provider

Modul DECROS SAPI-CSP v systému pracuje jako poskytovatel prvotřídních kryptografických služeb, které mohou využít všechny aplikace kompatibilní s technologií Microsoft CryptoAPI. Mezi tyto aplikace v současné době patří komunikační nástroje Microsoft Outlook 2000, Microsoft Outlook Express a Microsoft Internet Explorer 5.0 a vyšší.

Pro plnou funkci DECROS SAPI-CSP je zapotřebí mít přístup k certifikační autoritě a další infrastruktuře PKI. Při využití např. v Microsoft Outlook 2000 je zapotřebí zaregistrovat osobní certifikáty CA a pak jednoduše pro další komunikaci zvolit možnost digitálně podepsat mail nebo zašifrovat mail či obojí. Příjemce takto zabezpečeného e-mailu pak použije pro dešifrování textu šifrovací klíč uložený v bezpečnostním předmětu. Jednoduchým kliknutím na ikonku v mailu si pak může ověřit platnost digitálního podpisu, jak je patrné z obrázku.



Podpora tenkého klienta

Ochranu dat šifrováním prostřednictvím PROTECT for Windows mohou využívati uživatelé tzv. tenkých klientů, kteří jsou připojeni k Citrix® MetaFrame™ for Microsoft® Windows® 2000 Servers. Díky nově použité technologii lze plně využívat modulů PROTECT i například prostřednictvím mobilních počítačů s operačním systémem Microsoft Windows CE či nově Microsoft PocketPC.

Systémové ochrany (pouze Windows 98/95)

Modul PROTECT Logon for Windows 98 umožňuje řadu zajímavých bezpečnostních funkcí prostřednictvím "Systémových ochran", které lze nastavit ve Vlastnostech disku či diskety nebo prostřednictvím Systémové politiky.

Na základě Systémových ochran správce dostává do ruky nástroj zajišťující:

- Ochranu zápisu či čtení z disket a pevného disku (kromě systémového)
- Ochranu vybraných souborů proti smazání, modifikaci či kopírování
- Ochranu adresářové struktury

Systémové ochrany mohou sloužit jako sekundární antivirová ochrana, jako ochrana dat před kopírováním na diskety bez zákazu čtení či jako prostředek pro uchování instalace programového vybavení na počítači v takovém stavu, v jakém jej obdržel od správce IT.

Jaký tedy je nový kabát

Nová verze nabízí další vlastnosti, které zvyšují nabídku bezpečnosti jak pro státní organizaci, tak i pro komerční sféru. Zpětná kompatibilita šifrování je samozřejmě zajištěna, a tak mohou zákazníci bez dalších prací přejít na verzi 3.x.

Vývojový tým společnosti DECROS připravuje další vylepšení do verze 3.1 koncem roku 2000. Nechme se překvapit, čím dalším nás technologie Protect ještě překvapí.

Josef Dvořák
j.dvorak@decros.cz

Bezpečnostní předměty I. díl

Série článků o bezpečnostních předmětech si klade za cíl nabídnout široké veřejnosti informace o této oblasti, o důvodech vedoucích k používání bezpečnostních předmětů (tzv. tokens) a dále pomoci orientovat se mezi jednotlivými typy předmětů.

Proč a jaké bezpečnostní předměty?

Bezpečnostní předměty se používají v zásadě z těchto důvodů:

- Bezpečná identifikace/autentizace
- Úschova šifrovacích klíčů
- Elektronický podpis (certifikáty)

Bezpečná identifikace/autentizace (I/A)

Proces přihlášení (tzv. logon) např. do operačního systému můžeme rozdělit na identifikaci, kdy systému říkám, kdo jsem (jméno uživatele), a autentizaci, kdy musím prokázat, že jsem to skutečně já. Autentizaci mohu provést heslem (něco jedinečného znám), předmětem (něco jedinečného mám), tím, čím jsem (biometrické metody), nebo kombinací předchozího.

S autentizací pomocí hesla se již asi setkal každý. Není však příliš bezpečná, ani uživatelsky příjemná. Vkládání hesla přes klávesnici vede k používání krátkých (a tím pádem nebezpečných) a snadno zapamatovatelných hesel. Takové heslo nepředstavuje pro útočníka žádný problém.

Autentizace předmětem zvyšuje bezpečnost přihlášení, ale i uživatelův komfort. Kvalitní přihlašovací heslo (dostatečně dlouhá, "nezapamatovatelná", náhodná kombinace alfanumerických znaků) je bezpečně uloženo v předmětu. Uživatel ho nemusí ani znát! Do systému se heslo automaticky načte po přiložení předmětu. Starosti s pamatováním hesla se tak redukují na střežení předmětu, který by mohl být v případě ztráty zneužit. V praxi se proto používají zejména ty, které jsou chráněny ještě svým heslem (tzv. PIN) nebo biometrikou (např. otisk palce) tak, aby znesnadnily použití předmětu v případě zcizení.

V reálném životě však pouze s bezpečnou I/A neobstojíme. Důvod je velice prostý. Výše popsané mechanismy (např. zmiňované přihlášení do OS) neochrání naše privátní data, jestliže útočník napadne systém jako takový (např. nahraje do počítače svůj OS, ukradne datový disk či disketu). V takovém případě má útočník přístupové mechanismy pod svojí kontrolou, protože nejsou použity žádné další ochranné mechanismy, a naše data mohou být kompromitována. Jak tomu zabránit? Data je nutné šifrovat. A tak se dostáváme k dalšímu důvodu, proč používat bezpečnostní předmět.

Úschova šifrovacích klíčů

Cílem šifrování dat (převod původních dat do nečitelné formy) je zajistit důvěrnost a soukromí informací před každým, kdo nemá oprávnění k jejich použití. Dešifrování je procesem opačným. Zašifrování a dešifrování vyžaduje od uživatele určitý tajný údaj, který se nazývá šifrovací klíč (řetězec alfanumerických znaků). Na kvalitu šifrovacího klíče (délku a náhodnost znaků) a jeho bezpečnost je kladena mnohem vyšší náročnost, než na přihlašovací heslo. Je to dáno jiným typem možného útoku na zašifrovaný text. Použití šifrování jako ochrany dat je v praxi spojeno s budováním klíčového hospodářství (soubor organizačních a technických opatření jako např. generování, distribuce, obnova, zneplatnění šifr. klíče). Vhodný HW předmět (s dostatečnou pamětí a inteligencí-mikroprocesorem na čipu) nám pak pomůže s řešením mnoha problémů.

Šifrováním tedy řešíme ochranu důvěrnosti dat. Ale co v případě, kdy nás spíše zajímá, kdo např. daný dokument vytvořil, zda nebyl měněn obsah atd. A tak se dostáváme k dalšímu zajímavému okruhu problémů, který se řeší tzv. elektronickým podpisem.

Elektronický podpis (EP)

Úkolem EP je zaručit autentičnost (původ autora), integritu (data nebyla úmyslně či neúmyslně změněna) a nepopiratelnost (podepisující nemůže později popřít, že dokument podepisoval) podepsaných dat. Jeho použití je podmíněno existencí infrastruktury služeb veřejného klíče tzv. PKI. Vlastní EP může být uložen mimo systém, přímo do bezpečnostního předmětu. V takovém případě je vlastní akt podepsání (pro ověření budeme stále potřebovat PKI) vázán pouze na použití předmětu, který můžeme nosit neustále u sebe jako např. občanský průkaz.

SCI-FI nebo blízká budoucnost?

Pokud se někomu z Vás zdá, že je to pořád málo, podívejme se někam, kde to dělají opravdu dobře. V Holandsku například již běžně používají elektronický občanský průkaz. Jde o Smart kartu, která zároveň slouží jako průkaz pojištěnce, kreditní karta, zdravotní karta a je připravena na další rozšíření nabízených služeb.

Bezpečnostní Předměty

Touch Memory (TM) - výrobce Dallas Semiconductor. Předmět podobné velikosti a vzhledu jako běžná knoflíková baterie do fotoaparátu nebo elektronického diáře a je obvykle vložena do plastikového pouzdra, které může být jednoduše navlečeno na svazku klíčů. K dispozici je mnoho různých druhů. TM 1990 obsahuje pouze vlastní sériové číslo (je levná, využívá se k identifikaci např. v docházkových nebo stravenkových systémech). TM 1991 a vyšší již obsahují zapisovatelnou paměť (128Byte - 8kByte). Mohou uchovávat identifikační a autentizační informace a také šifrovací klíče, stejně jako další informace. Reálné použití modelů s velkou pamětí však v praxi naráží na nízkou přenosovou rychlost přenosu TM.

Security Box (SB) - výrobce DECROS spol. s r.o. Krabička 4x4x1 cm obsahující mikroprocesor a paměť (360 Byte -1.5kByte). Je určen pro bezpečnou úschovu šifrovacích klíčů a přihlašovacích informací uživatele, dá se centrálně spravovat pomocí vzdáleného přístupu. Lze tak budovat i poměrně komplikované klíčové hospodářství ve velkých organizacích státní správy. Pro komunikaci slouží přímo sériový nebo infračervený port počítače (nepotřebujete žádné čtecí zařízení). SB je chráněn plnohodnotným heslem a navíc komunikace je šifrovaná tak, že ji nelze ani v případě odposlechnutí zneužít.

Čipová karta - výrobce např. Schlumberger, Gemplus, Plast, Siemens, karta o rozměrech vizitky se zapuštěným čipem. V případě, že čip není pouze pamětí (jako u telefonní karty), ale procesorem, mluvíme o tzv. Smart kartě (SK) . Na takovéto

kartě je možné provádět definované jednoduché operace, spouštět programy a na souborový systém karty lze také ukládat informace. SK lze použít pro bezpečnou úschovu šifrovacích klíčů a přihlašovacích informací uživatele. Na rozdíl od předchozích předmětů lze SK použít i pro uložení elektronického podpisu. V souladu s požadavky na využití elektronického podpisu je důležité, jakou kryptografickou podporu čip karty nabízí. Tedy zda a jaká asymetrie (zpravidla RSA) je přímo na čipu.

SK může kromě čipu obsahovat také pasivní zářič. Bezdotykové tzv. pasivní karty se používají převážně v rámci řešení systémů objektové bezpečnosti. Takže můžete používat jeden univerzální předmět.

USB token - dodává např. ALADDIN, Eutron, RAINBOW. Tvarově připomíná malý plynový zapalovač o rozměrech 5x1,5x0,5 cm. Funkční možnosti jsou totožné se Smart kartami. Záleží na čipu, kterým je předmět osazen. Na rozdíl od čipových karet nepotřebujete žádné čtecí zařízení, USB port je standardně na přenosných počítačích a dodává se i na pracovní stanice. Zatím je podporován pouze novými OS (Win 98 a Win 2000), i když výrobci tvrdí, že počítají i s podporou OS WinNT.

Předmět ano či ne?

Osobně používám bezpečnostní předmět již řadu let. V obsahu tohoto článku jsem se snažil stručně pojmenovat důvody, které vedou nejen mě, ale i další uživatele k tomu, že míru zabezpečení svých informací zvyšují používáním právě předmětů. V dalších číslech DECROS News se budeme této problematice věnovat podrobněji. Vývoj jde však dál a informací není nikdy dostatek.

Radovan Pekárek
r.pekárek@decros.cz

DECROS integruje D-DATA

Oznámení o integraci společností DECROS spol. s r.o. a D-data spol. s r.o.

Dovolte nám, abychom Vás touto cestou informovali o změnách, které na přelomu června a července t.r. proběhly v rámci vybraných společností sdružených v rámci skupiny ICZ.

Skupina ICZ působí na trhu informačních technologií od roku 1998 a během své krátké existence se stala významným a uznávaným subjektem. V současné době je ve skupině sdruženo 14 společností, které v loňském roce dosáhly obratu přes 600 mil. Kč, na jehož realizaci se podílelo našich 450 zaměstnanců.

V tomto seskupení firem působí i společnosti DECROS a D-data. Na základě analýzy se dohodlo vedení skupiny ICZ spolu s vedením společností D-data a DECROS na integraci obou společností, a to postupným začleněním činnosti společnosti D-data do Divize informačních technologií společnosti DECROS se zachováním právní subjektivity společnosti D-data.

Řízením společnosti D-data byl pověřen pan Petr Krůček, který nadále zůstává ředitelem Divize informačních technologií společnosti DECROS. Statutární orgány obou společností zůstávají beze změn.

Kontinuita stávajících vztahů s našimi zákazníky a partnery, stejně jako rozvoj našich aktivit směrem k Vám, jsou naší prioritou. Vzhledem k uvedené formě integrace garantujeme pokračování našich vztahů jak pod hlavičkou společnosti D-data, tak pod hlavičkou společnosti DECROS. Tam, kde to právní forma vztahu dovoluje, nabízíme po vzájemné dohodě převedení obchodních vztahů společnosti D-data do společnosti DECROS. Jsme připraveni dostát svým závazkům, jsme připraveni na rozvoj naší spolupráce.

Proces sjednocení řízení a činnosti společností D-data a DECROS je v pokročilém stádiu. Je definována jednotná strategie společnosti, jsou definovány obchodní cíle i produktové portfolio, je definován marketingový plán, stejně jako plán personálního rozvoje a organizační struktura. Vše uvedené odráží náš zájem a naši připravenost na plynulém pokračování a rozvoji všech aktivit.

Věříme, že i nadále budete ve společnosti DECROS i v celé skupině ICZ nalézat silného partnera s kompetencemi, které patří mezi ty nejlepší na poli informačních technologií. Děkuje Vám za důvěru.

Jiří Mifek
j.mifek@decros.cz

DECROS třikrát na Invexu

Přestože nemůžeme předvídat, zda čtete DECROS News před Invexem, po Invexu či otevíráte toto číslo právě na Invexu, rádi bychom Vás upozornili na naši expozici na tomto veletrhu informačních technologií v Brně. Opět po roce si Vás dovolujeme pozvat k návštěvě naší expozice na veletrhu INVEX 2000.

V letošním roce se společnost DECROS rozhodla přestěhovat do nové haly V, ve které se objeví hned na třech místech.

Divizi bezpečnosti letos naleznete v hale V, na stánku číslo C27. I tady se to bude "hemžit" novinkami. Novinkou číslo jedna bude zajisté nová verze technologie Protect for Windows 2000 s digitálním podepisováním. Ráda bych upozornila zejména na jednu z nových vlastností Protectu - modularitu. Protect for Windows se skládá ze tří modulů: šifrovací, podepisovací a identifikační/autentizační. Dalšími novými vlastnostmi jsou například: šifrování elektronické pošty, podepisování elektronické pošty, nová koncepce a rozšířené uživatelské rozhraní a mnoho dalších.

Kromě nové verze technologie Protect for Windows Vám představíme novou Security Card a mnoho dalších zajímavostí a služeb.

Kromě expozice divize bezpečnosti se zde představí i Divize IT, a to jako partner firem Microsoft (hala V, stánek B12) a Novell (hala V, stánek C24). Ve svých expozicích návštěvníkům nabídne hned několik zajímavých záležitostí jako jsou elektronický podpis ve státní správě, vysoká dostupnost systémů (Cluster Services), integrace platforem a aplikací pomocí NDS nové generace, jednotné uživatelské prostředí atd. O některých tématech budou diskutovat experti Divize IT ve svých přednáškách. O přesném programu přednášek Vás budeme včas informovat.

Těšíme se na setkání s Vámi, v Brně ve dnech 9. až 13. října 2000.

Denisa Mylbachrová
d.mylbachrová@decros.cz

Zákon o elektronickém podpisu

1. října 2000 vstoupil v platnost zákon č. 227/2000 Sb. o elektronickém podpisu. Tento zákon zrovnoprávňuje elektronický podpis s vlastnoručním podpisem[1] a umožňuje ho používat pro provádění právních úkonů. Sláva, můžeme ho začít používat. Můžeme?

Zákon říká, že můžeme použít zaručený elektronický podpis založený na kvalifikovaném certifikátu vytvořeném pomocí prostředku pro bezpečné vytváření podpisu. Pokud chceme elektronický podpis použít pro komunikaci s orgány veřejné správy, musíme použít kvalifikovaný certifikát vydaný akreditovaným poskytovatelem certifikačních služeb[2].

Zdá se Vám to lehce nestravitelné? Nejprve tedy …

Definice pojmů[3]

Zákon o elektronickém podpisu definuje dva termíny pro elektronický podpis: elektronický podpis a zaručený elektronický podpis.

Elektronickým podpisem je údaj připojený ke zprávě umožňující identifikaci podepsané osoby. To znamená, že elektronický podpis může vypadat třeba takto:

Petr Řehoř

nebo to může být naskenovaný obrázek vlastnoručního podpisu.

Na rozdíl od elektronického podpisu musí zaručený elektronický podpis splnit tyto čtyři podmínky:

- Musí být jednoznačně spojen s podepisující osobou
- Musí umožňovat identifikaci podepisující osoby
- Musí být vytvořen pomocí prostředků, které může udržet podepisující osoba pod svojí výhradní kontrolou
- Musí být ke zprávě připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat

Definici zaručeného elektronického podpisu vyhovuje beze zbytku digitální podpis založený na asymetrické kryptografii [1]. Zákon však umožňuje použít i jiné metody, pokud budou splňovat tyto čtyři podmínky.

Pokud tedy dnes někdo hovoří o elektronickém podpisu, ve smyslu zákona o elektronickém podpisu se jedná o zaručený elektronický podpis.

Zajímavá je i definice podepisující osoby. Podepisující osobou může být pouze fyzická osoba, která jedná jménem svým nebo v zastoupení jiné fyzické nebo právnické osoby, což odpovídá zvyklostem používání vlastnoručního podpisu.

Dalším termínem je kvalifikovaný certifikát. I zde Zákon o elektronickém podpisu

definuje dvě varianty: certifikát a kvalifikovaný certifikát.

Certifikát vydává poskytovatel certifikačních služeb a spojuje data pro ověřování podpisu s podepisující osobou a umožňuje ověřit její totožnost.

Kvalifikovaný certifikát je certifikát obsahující povinné atributy definované v Zákonu o elektronickém podpisu a musí být vystaven poskytovatelem certifikačních služeb splňujícím podmínky Zákona o elektronickém podpisu. Osobní údaje, s výjimkou jména, mohou být v certifikátu uvedeny pouze se souhlasem podepisující osoby, které je certifikát vydáván. Poskytovatel certifikačních služeb je povinen uzavřít na vydání certifikátu smlouvu a ověřit totožnost podepisující osoby.

Posledním důležitým pojmem je poskytovatel certifikačních služeb, který vydává certifikáty. Aby mohl vydávat kvalifikované certifikáty, musí splňovat požadavky Zákona o elektronickém podpisu. Jedná se zejména o prostředky pro bezpečné vytváření podpisu, které musí zajistit korektnost kryptografických operací při podepisování a požadavky na ověření totožnosti podepisující osoby.

Pokud poskytovatel certifikačních služeb splňuje požadavky Zákona o elektronickém podpisu, může požádat Úřad pro ochranu osobních údajů [2] o akreditaci a stane se akreditovaným poskytovatelem certifikačních služeb. Jeho certifikáty je potom možné používat při styku s orgány veřejné správy.

Zrovnoprávnění elektronického podpisu

Zrovnoprávnění elektronického podpisu s vlastnoručním podpisem bylo dosaženo doplněním této věty do §40 odstavce 3 Občanského zákoníku[4]:

Je-li právní úkon učiněn elektronickými prostředky, může být podepsán elektronicky podle zvláštních předpisů.

Na to navazují změny v dalších zákonech umožňující učinit podání v elektronické podobě podepsané elektronicky:

- Zákon č. 337/1992 Sb., O správě daní a poplatků
- Zákon č. 71/1967 Sb., O správním řízení
- Zákon č. 99/1963 Sb., Občanský soudní řád
- Zákon č. 141/1961 Sb., O trestním řízení soudním

Odpovědnost za škody

Zákon o elektronickém podpisu říká, že podepisující osoba je povinna udržovat data pro vytvoření podpisu pod svou výhradní kontrolou a zodpovídá za škody vzniklé jejich kompromitací podle Občanského zákoníku. Odpovědnosti však může být zproštěna, pokud prokáže, že ten, komu škodu způsobil, si neověřil platnost kvalifikovaného certifikátu u poskytovatele certifikačních služeb, který ho vydal (certifikát musel být samozřejmě již zneplatněn).

Z toho vyplývá, že osoba ověřující elektronický podpis, musí vždy ověřit platnost kvalifikovaného certifikátu u poskytovatele certifikačních služeb, který certifikát vydal.

Praxe

Zákon vstoupil v platnost 1. října 2000. Protože však Úřad pro ochranu osobních údajů teprve zahajuje svoji činnost, nebyly dosud vydány prováděcí vyhlášky, ve kte-

rých budou stanovena kritéria pro poskytovatele certifikačních služeb a pro prostředky pro bezpečné vytváření podpisu. Na sympóziu E-Fórum 2000 na začátku září slíbil ředitel Úřadu pro ochranu osobních údajů, RNDr. Neuwirt, že návrh těchto vyhlášek bude předložen k veřejné diskusi do konce letošního roku. Jejich vydání je očekáváno v první polovině příštího roku. Potom budou moci poskytovatelé certifikačních služeb začít vydávat kvalifikované certifikáty a požádat o akreditaci u Úřadu pro ochranu osobních údajů.

Druhým krokem pro uvedení Zákona o elektronickém podpisu do života bude nařízení vlády o používání elektronického podpisu v orgánech veřejné správy. Toto nařízení se podle PhDr. Dvořáka, poradce ministra Březiny, připravuje, nicméně nemůže být vydáno před prováděcími vyhláškami Úřadu pro ochranu osobních údajů, takže ho lze očekávat spíše v druhé polovině příštího roku. Toto nařízení by mělo, mimo jiné, obsahovat i metodiku pro vytvoření elektronické podatelny, která bude přijímat podání učiněná v elektronické podobě elektronicky podepsaná, protože orgány státní správy musí být schopné minimálně přijmout podání v elektronické podobě a ověřit platnost připojeného elektronického podpisu.

Petr Řehoř
p.rehor@decros.cz

Odkazy

[1] Články o kryptografii http://www.decros.cz/Security_Division/Crypto_Research/publikace.htm

[2] Úřad pro ochranu osobních údajů, http://www.uoou.cz

[3] Sdružení pro informační společnost, http://www.spis.cz

[4] CHIP 10/2000, strana 44-49, RNDr. Klíma, doc. Ing. Smejkal, Expres neujel - Otázky zůstávají

1 Náš právní řád zná pouze podpis. Abych lépe odlišil tento termín od elektronického podpisu, budu používat vlastnoruční podpis pro podpis na papíře

2 Pro poskytovatele certifikačních služeb se obvykle používá název certifikační autorita

3 Pojmy definované Zákonem o elektronickém podpisu a použité v podle této definice jsou v textu vyznačeny kurzívou

4 Zákon č. 40/1964 Sb. Ve znění pozdějších předpisů

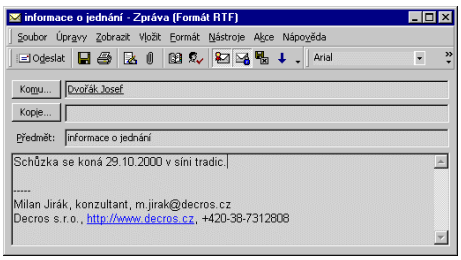
DECROS uvádí novou technologii!

Letos v létě společnost DECROS úspěšně dokončila vývoj DECROS SAPI-CSP (Crypto Service Provider). Opět se jí tak podařilo zařadit se do skupiny těch, kteří jsou na světové špičce v aplikaci nejnovějších trendů v oblasti bezpečnosti dat a kryptografie.

Modul DECROS SAPI-CSP v systému pracuje jako poskytovatel prvotřídních kryptografických služeb, které mohou využít všechny aplikace kompatibilní s technologií CryptoAPI společnosti Microsoft.

Jaké výhody přináší uživateli?

DECROS Crypto Service Provider je součástí jednoho z modulů nové verze technologie Protect for Windows, konkrétně se jedná o modul nazvaný PROTECT Sign. Tento modul je složen ze dvou základních částí - DECROS Crypto Service Provider a chráněný archiv.



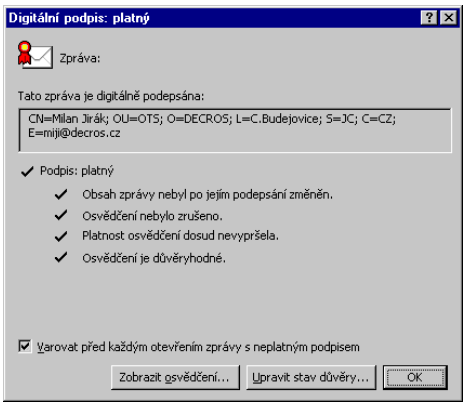
DECROS Crypto Service Provider poskytuje uživateli služby jako například elektronický podpis (RSA), asymetrické šifrování symetrických klíčů (RSA), symetrické šifrování (3DES, RC2, RC4), hašovací funkce (SHA -1, MD5, MAC) a generátor náhodných čísel. Znalce v oblasti kryptologie jistě bude zajímat, že délka klíče RSA modulu je 1024 až 4096 bitů s granularitou 64 bitů. Co se týče délky klíčů symetrických šifer, jsou to 3DES (efektivní délky bez paritních bitů): 112 bitů, 168 bitů, RC2: 128 bitů, RC4: 128 bitů. Módy blokových šifer jsou následující : ECB, CBC, OFB, CFB.

Mezi další bezpečnostní mechanismy patří například kontrola velikosti exponentu privátního klíče při jeho generování či možnost použití formátu dat EME_OAEP dle PKCS#1, v 2.0 pro šifrování symetrických klíčů. Módy OFB a CFB jsou povoleny pouze se zpětnou vazbou 64 bitů. RNG z rodiny Yarrow má speciální design odolný vůči SW útokům. Privátní klíč RSA je bezpečně chráněn fyzickým předmětem. Použití fyzického předmětu je vyžadováno před každou operací s privátním klíčem. Podezřelé události se zapisují do systémového logu. Přístup k otevřenému kontextu je dále povolen pouze tomu procesu, který jej otevřel - ochrana před útokem z nepřátelské aplikace.

Kromě kvalitní a bezpečné implementace osvědčených kryptografických metod se DECROS SAPI-CSP dále vyznačuje úzkou vazbou na fyzické předměty dostupné přes bezpečnostní subsystém SAPI (Security Application Programming Interface). Tyto předměty jsou zde využity k dosažení vysoké úrovně ochrany privátních klíčů.

Jak využít tuto technologii

V prvé řadě je zapotřebí upozornit, že DECROS SAPI - CSP funguje v operačních systémech Windows NT 4.0, Windows 95, Windows 98, Windows 2000. Rozhraní CryptoAPI společnosti Microsoft automaticky podporují aplikace jako například MS Outlook 98 a vyšší, MS Internet Explorer 4.01 a vyšší či MS Outlook Express a vyšší.



Ptáte se na využití? Nejprve je potřeba získat digitální certifikát (ať už prostřednictvím veřejné certifikační autority či prostřednictvím firemní infrastruktury). Pokud jej máte, není nic jednoduššího, než mít nainstalovaný modul PROTECT Sign (právě s ním nainstalujete DECROS SAPI-CSP) a vhodně si nastavit možnosti ochrany a digitálního podepisování e-mailové komunikace například prostřednictvím klienta Outlook 2000. Pak již pouze stačí, abyste při psaní „citlivého" mailu tento mail označili jako určený pro šifrování. Chcete digitálně podepsat? Označte mailovou zprávu i pro podepsání. A je to.

Snad bychom mohli parafrázovat jeden historický výrok na: "Malý krok pro DECROS, velký skok pro jeho zákazníky".

Denisa Mylbachrová
d.mylbachrová@decros.cz

Testovali jsme: NetWare Cluster Services

NetWare Cluster Services (NWCS) v 1.01 pro NetWare 5.1 je software, který umožňuje propojit několik samostatných NetWare serverů to skupiny - clusteru, čímž získají uživatelé téměř nepřetržitý přístup ke kritickým zdrojům sítě, jako jsou data, aplikace, softwarové licence a jiné služby.

Pokud jeden síťový server (uzel clusteru) selže, může jiný server automaticky převzít obsluhu aplikací a dat, které předtím obsluhoval havarovaný server. Přitom servery v clusteru si zachovávají velkou míru autonomie - například narozdíl od původního řešení pro zrcadlené spojení dvou NetWare serverů (SFT III) mohou být na serverech NetWare clusteru bez jakýchkoli omezení instalovány aplikace, které nejsou určeny pro práci v clusteru nebo toho nejsou schopny.

Architektura NWCS

Cluster je tvořen několika (nejméně dvěma, maximálně 32) servery NetWare 5.1, na kterých je nainstalován software NWCS. Alespoň některé ze serverů clusteru by měly obsluhovat NDS repliku, v níž je uložena konfigurace celého clusteru.

Komunikace mezi uzly clusteru je zajištěna pomocí speciálních protokolů nad protokolem TCP/IP. Těmito protokoly komunikují uzly clusteru mezi sebou po lokální síti. Mezi těmito protokoly je jedním z nejdůležitějších heartbeat protokol - "srdeční tep" clusteru. Pomocí tohoto protokolu hlásí neustále každý uzel ostatním uzlům clusteru, že je v pořádku. Tato komunikace probíhá po lokální síti, která slouží i pro přenosy dat mezi uživateli a servery clusteru. Stavové informace clusteru jsou takto dostupné z libovolného místa sítě, což umožňuje provádět z libovolné stanice sítě administraci clusteru. Stavové pakety clusteru nejsou při dnešní přenosové kapacitě pro síť nijak významnou zátěží, neboť například pakety heartbeat protokolu jsou vysílány z každého uzlu typicky jen jednou za sekundu.

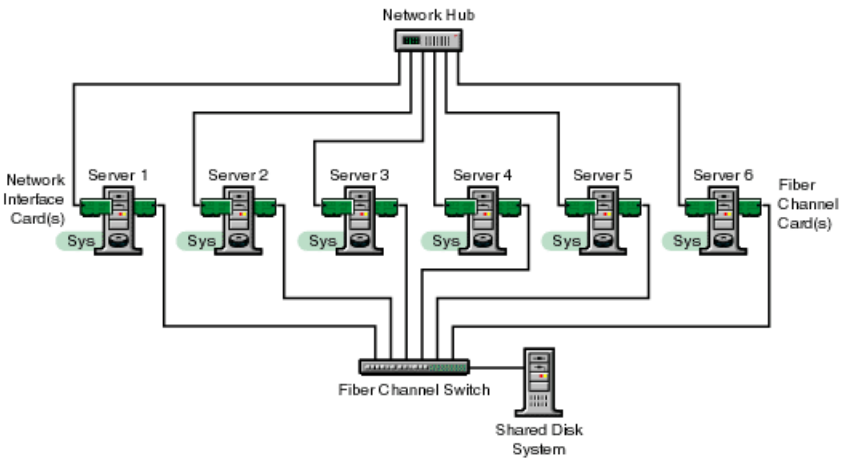
Doporučenou součástí clusteru je sdílený diskový subsystém. Teprve po připojení všech uzlů clusteru ke společnému diskovému subsystému lze plně využít všech výhod, které cluster nabízí. Na sdíleném diskovém prostoru si cluster vytváří při instalaci speciální služební svazek o velikosti cca 20 MB, který slouží, paralelně k síťovému propojení, jako další komunikační kanál mezi uzly clusteru. Sdílený svazek umožňuje mimo jiné předcházet takzvaným Split-Brain problémům, které nastanou, pokud selže síťové propojení mezi uzly clusteru a vznikne tak situace, kdy se několik nezávislých skupin uzlů clusteru (oddělených nefungujícím síťovým propojením) souběžně snaží obnovit činnost všech clusterových aplikací.

Připojením uzlů clusteru ke sdílenému diskovému systému vznikne takzvaná Storage Area Network (SAN). Sdílený diskový subsystém může být realizován jako diskové pole připojené přes rozhraní Fiber Channel nebo pomocí Serial Storage Architecture (SSA).

Pro propojení malých clusterů ke sdílenému diskovému subsystému lze také použít sdílených SCSI disků nebo diskových polí, u samostatných disků je však třeba nějakým způsobem zajistit jejich odolnost proti výpadkům, aby zde nevzniklo slabé místo, které by degradovalo spolehlivost celého clusteru.

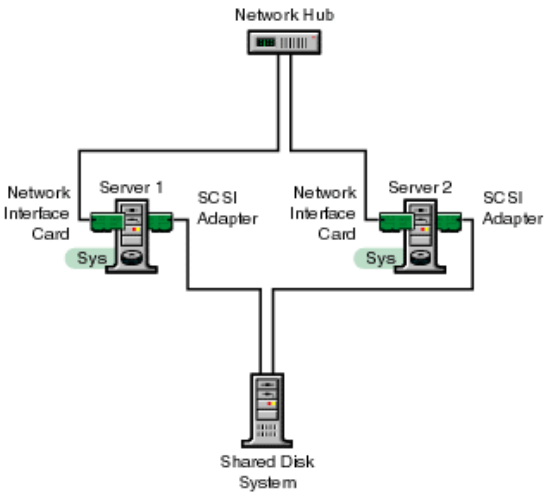
Pokud použijete SAN pro instalaci NWCS, můžete snadno přesouvat datové svazky mezi servery, aniž by došlo k výpadku přístupu. V případě, že některý uzel clusteru havaruje, musí zbylé uzly převzít jeho úkoly. S architekturou SAN má kterýkoli zbylý uzel clusteru přístup k datům, se kterými na sdíleném diskovém subsystému pracoval havarovaný uzel, a může tak snadno převzít veškerou agendu havarovaného uzlu. Podmínkou je, aby sdílené datové svazky clusteru byly instalovány ve filesystému NSS. V prostředí operačního systému NetWare totiž dokáže pouze NSS zajistit dostatečně rychlé montování datových svazků na serveru.

Zkušenosti ukazují, že při instalaci clusteru je třeba věnovat nastavení NSS filesystému mimořádnou pozornost, protože na konfiguraci NSS závisí většina ostatních výkonnostních parametrů clusteru. V některých případech (složitá struktura přístupových práv na svazku) může nevhodná konfigurace NSS prodloužit dobu, za kterou se přemontuje datový svazek z jednoho uzlu clusteru na druhý, až na desítky minut. Z hlediska budoucího vývoje je také vhodné konfigurovat NSS podle zvyklostí, jež zavede nová verze NetWare, očekávaná v příštím roce. Správně nakonfigurovaný NSS filesystém umožňuje minimalizovat dobu migrace clusterové aplikace z jednoho uzlu na druhý na méně než jednu minutu.



Princip instalace aplikací do prostředí NWCS

Do prostředí NWCS může být nainstalována prakticky libovolná aplikace pro server NetWare 5.X, která komunikuje s uživateli přes protokol TCP/IP, a která není vázána na specifický server sítě. V prostředí NWCS je možno přiřadit této aplikaci IP adresu, která bude v případě výpadku serveru přenesena spolu s touto aplikací na jiný server. Pomocí tohoto mechanismu se aplikace jeví, jako by běžela stále na stejném stroji. Při konfiguraci clusterové aplikace vytváří NWCS pro tuto aplikaci její virtuální server, u něhož jsou definovány dávky pro spuštění a pro ukončení aplikace na uzlu clusteru, připojení potřebných datových svazků a registraci IP adresy pro tuto aplikaci.



Jednoduchý způsob konfigurace aplikací do prostředí NWCS dovoluje převést do tohoto prostředí velké množství stávajících aplikací, včetně databázového serveru Oracle 8i, GroupWise, DHCP serveru, tiskových služeb, web serveru apod. Na druhou stranu doposud nejsou známy žádné aplikace, které by byly "programově vytvořeny" pro NetWare cluster (např. v tom smyslu, že by byly schopny monitorovat stav clusteru a samy reagovat na změny v jeho aktuální konfiguraci).

Sdílené datové svazky

Zvláštním druhem sdílených zdrojů NWCS jsou sdílené datové svazky. Ty jsou obsluhované virtuálními servery, které mají stejně jako aplikace clusteru přiřazenu vlastní IP adresu. Díky tomu se tyto svazky nacházejí neustále na stejné IP adrese nezávisle na tom, na kterém serveru clusteru jsou právě namontované.

IP adresy sdílených svazků a aplikací clusteru je vhodné registrovat v DNS, v souborech Hosts nebo použít speciální utilitu pro jejich registraci ve službě SLP, aby byly bez potíží viditelné všemi uživateli.

Konfigurace a administrace NWCS

Základní utilitou pro konfiguraci a administraci NetWare clusteru je známá ConsoleOne s instalovanými snap-iny pro NWCS. Většina konfiguračních informací NWCS je uchovávána v adresářové službě NDS. Pomocí ConsoleOne je možné konfigurovat servery clusteru a všechny clusterové zdroje - měnit jejich IP adresy, editovat příkazové dávky pro jejich spouštění a ukončování a určovat způsob, jakým budou zdroje clusteru migrovat v případě výpadku serveru na ostatní servery. Je zde také možné zobrazit aktuální stav clusteru a manuálně spouštět a ukončovat aplikace nebo je migrovat mezi jednotlivými uzly.

Jak nakoupit licence pro NetWare cluster

Každý server, který má být instalován do clusteru, musí mít k dispozici základní licenci NetWare 5.1 Server. Dále bude každý uzel clusteru vyžadovat jednu licenci pro NWCS 1.01 a uživatelé clusteru budou dále potřebovat uživatelské licence pro NetWare 5.1 a pro NWCS.

NetWare Cluster Services je také možné zakoupit s výraznou slevou v rámci zvýhodněných programů Novell Custpomer Connection nebo jako upgrade z následujících produktů: NetWare SFT III, Novell StandbyServer for NetWare a Novell High Availability Server.

Co říci závěrem? Pokud máte zájem o toto řešení, tak neváhejte. Napište nám a náš tým specialistů se Vám bude plně věnovat.

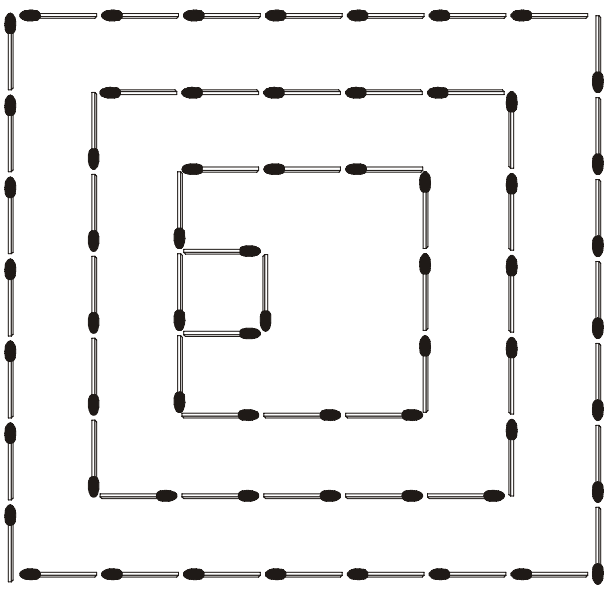
Štrobl Martin
m.strobl@decros.cz

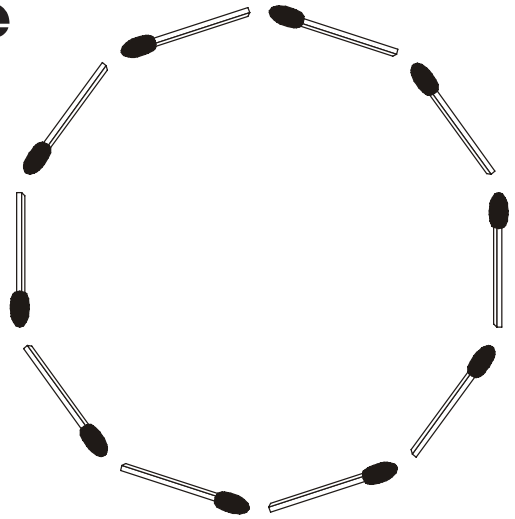
Hádanky pro volné chvíle

Opět jsme si pro vás připravili rébusy ze zápalek.

V dolním obrázku jsou vytvořeny ze 63 zápalek čtyři čtverce.
Přemístěte 5 zápalek tak, aby vznikl obrazec podobný spirále.

Ve druhém obrázku je zobrazen pravidelný desetiúhelník vytvořený z deseti zápalek. Přemístěte zápalky tak, aby vzniklý desetiúhelník měl tytéž strany (obvod), ale menší obsah.





DECROS NEWS

Informační bulletin pro zákazníky, partnery firmy DECROS a zájemce o informační bezpečnost.
Šéfredaktor: Josef Dvořák
Vydává: DECROS s.r.o., J.Š.Baara 40,
370 01 České Budějovice, tel.: 038-7312808,
fax: 038-7311480, http://www.decros.cz,
e-mail: dn@decros.cz, Vyšlo v říjnu 2000, zdarma

Podávání novinových zásilek povoleno Českou poštou, s.p., ředitelství odštěpného závodu Jižní Čechy v Českých Budějovicích, j.zn.: P-2901/99 ze dne 24. května 1999.
Registrační číslo: MK ČR 8230
Sazba a grafická úprava: © Martin Klíma, 2000

DECROS boduje ve Francii

Francie je pro společnost DECROS rozhodně jedním z velmi zajímavých zahraničních trhů a v poslední době jsme zde zaznamenali nemalé obchodní úspěchy.

Pro Francii jistě platí specifické podmínky, které je nutné splnit. Bezpochyby primární podmínkou je splnění dovozních pravidel vydaných francouskou vládou, která si tak zajišťuje kontrolu nad importem silných šifrovacích technologií do země. Tato podmínka byla splněna 15. června 1999, kdy francouzský státní institut SCSSI schválil a poté i vydal patřičnou certifikaci použitých symetrických algoritmů WinCross II (vlastní algoritmus společnosti DECROS; až 160-ti bitový šifrovací klíč) a CAST (veřejný šifrovací algoritmus; až 128-i bitový šifrovací klíč). Tímto byly splněny základní podmínky pro dovoz produktu Protect for Windows na francouzský trh.

Neméně důležité je také přizpůsobení se jazykovým požadavkům francouzských zákazníků. Rozhodně by nebylo možné úspěšně nabízet Protect for Windows bez francouzské jazykové mutace. S tímto bylo spojeno nemálo komplikací a námahy, ale nakonec vedle anglické, německé a japonské verze připravil náš vývojový tým ve spolupráci s francouzskými partnery i verzi ve francouzském jazyce.

Klíčem pro úspěšné působení rozhodně bylo nalezení vhodného francouzského partnera se znalostí trhu. V současné době úzce spolupracujeme s firmami Calyx Data Control Lyon a Informatique Development Paris. Obě firmy mají zkušenosti v oblasti bezpečnosti informačních systémů. Společnost Calyx navíc sází i na vlastní vývoj bezpečnostních řešení jako například produkt SpyKiller, který poskytuje možnosti autentizace pomocí předmětu (chipová karta, USB předmět).

Podobně jako u ActivCard, jednaly obě společnosti na základě zájmu o Protect for Windows o možnosti spojit oba produkty a lépe tak reagovat na poptávku francouzských zákazníků. Na základě obchodních a technických jednání byl zvolen podobný způsob integrace jako u ActivCard Gold, tedy využití autentizace spolu s HW předmětem (chipová karta) od společnosti Calyx a doplnění o možnost silného šifrování Protect for Windows. Počátkem září tohoto roku byla tato integrace úspěšně dokončena. Zároveň byla realizována i první dodávka nově upraveného a lokalizovaného produktu Protect for Windows.

ActivCard Digital Identity Award 2000

5. června 2000, konference partnerů společnosti ActivCard, Disneyland, Paris, Francie.

Společnost DECROS spol. s r.o. je oceněna mezi evropskými a asijskými partnery společnosti ActivCard. Ve stylovém prostředí Museée des Artes Forains bylo předáno ocenění "ActivCard Digital Identity Award 2000" za nejlepší integraci.

Této krátké zprávě předcházelo mnoho úsilí a jednání. Spolupráce společností DECROS a ActivCard začala v roce 1998, kdy společnost United Trade International (dále UTI; distributor společnosti DECROS) uspěl ve výběrovém řízení pro Národní banku Rumunska (NBR). NBR je největší a nejvýznamnější bankovní institucí v zemi (40 poboček). Vítězné bezpečnostní řešení společnosti UTI počítalo s kombinací silné autentifikace od ActivCard a silného šifrování implementované v Protectu. Obě tato řešení ActivCard Gold i Protect for Windows podporují technologii čipových karet - což bylo další podmínkou UTI resp. NBR. Podmínkou úspěšnosti bylo vhodně zkombinovat tyto požadavky a provést integraci dvou původně nezávislých řešení v jedno, které bude splňovat zákazníkovy podmínky.

Integrace byla uskutečněna ve společnosti DECROS. Jak již bylo uvedeno výše, bylo třeba spojit dva produkty v jeden, a to s jedním společným jmenovatelem - Smart Card. DECROS přizpůsobil Protect for Windows tak, aby podporoval čipovou kartu ActivCard (výrobce Schlumberger, 8kB pamět), a přes rozhraní PKCS#11 používá této karty pro uchování šifrovacích klíčů. Toto řešení využívá PC/SC standardu čteček čipových karet a samozřejmostí je také například možné využití PCMCIA čteček pro notebooky.

Výsledná integrace proběhla ve velmi krátkém časovém období a ve vysoké kvalitě. O tomto svědčí jednak zmiňované ocenění od společnosti ActivCard, ale hlavně spokojenost zákazníka, v tomto případě tedy Národní banky Rumunska. Spojení těchto silných řešení je pozitivní i pro další potenciální obchody a nabízí pro DECROS i ActivCard nové příležitosti.

ActivCard

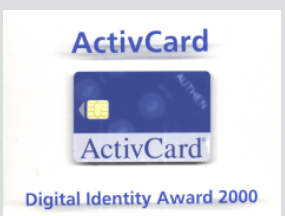
ActivCard je jednou z předních firem zabývajících se digitální identitou a elektronickými certifikačními technologiemi. Dodává jádra komponentů požadovaných pro zajištění komunikace a transakcí v e-Businessu. ActivCard technologie nabízí snadno použitelné ATM transakce s vysokou mírou bezpečnosti. Jejich řešení, v kombinaci s aplikační podporou veřejného klíče založeného na důvěrnosti a integritě umožňuje individuálnímu uživateli i firmám zajistit bezpečné on-line transakce přes Internet. Dnes, více než jeden milión lidí využívá produkty ActivCard pro bezpečný Internet banking, přístup k webu i vzdálenou správu k firemní síti. ActivCard sídlí ve Fremontu, USA; Suresnes, Francii a Singapuru.

Závěrem

Oba výše uvedené případy realizované s francouzskými firmami mají společný jmenovatel. Tím je zájem o technologickou spolupráci v oblasti kvalitní šifrovací technologie společnosti DECROS, které jsou obsaženy v produktu Protect for Windows. V obou případech se rovněž společnost DECROS podílela na přizpůsobení produktu. Obě integrace byly uskutečněny v relativně krátké době a na vysoké úrovni. Pro nás je to potvrzením o technologické úrovni produktu a vývoje, kdy můžeme reagovat na vysoké nároky v oblasti ochrany dat a to nejen u francouzských zákazníků.

Eduard Pitka
e.pitka@decros.cz

ActivCard
Digital Identity Award 2000



Přehled základních produktů firmy DECROS

Kompletní přehled je možné nalézt na internetové stránce http://www.decros.cz
Pokud byste uvítali informace o produktech firmy DECROS v tištěné podobě, kontaktujte nás. Rádi vám je zašleme.

Produkt		Popis		Verze
Protect for Windows 98		Komplexní řešení pro zabezpečení ochrany citlivých dat. Určeno pro OS Windows 95 i Windows 98. Tvořeno třemi samostatnými moduly.		3.0.20.
	MODUL	**Protect Logon**	Identifikační autentizační modul umožňující bezpečné přihlášení do OS pomocí osobního HW předmětu (Security Box, Touch Memory, Smart Cards). Tyto předměty jsou používány pro uložení uživatelského jména a hesla (domény).	
	MODUL	**Protect Encrypt**	Šifrovací modul - je silný souborově orientovaný šifrovací systém určený pro ochranu souborů/adresářů, archivů a elektronické pošty na lokálních nebo síťových discích. Je založen na výkonném transparentním on-the-fly souborovém šifrování implementovaném přímo do OS.	
	MODUL	**Protect Sign**	Modul digitálního podpisu - umožňuje kdykoli během archivace podepsat soubor systémem Protect a podporuje většinu běžně užívaných PKI standardů. Umožňuje ukládání certifikátů a tajných klíčů do HW bezpečnostních produktů (Security Box, Touch Memory, Smart Cards).	
Protect for Windows 2000		Komplexní řešení pro zabezpečení ochrany citlivých dat. Určeno pro OS Windows NT a Windows 2000. Tvořeno třemi samostatnými moduly.		3.0.35.
	MODUL	**Protect Logon**	Identifikační autentizační modul umožňující bezpečné přihlášení do OS pomocí osobního HW předmětu (Security Box, Touch Memory, Smart Cards). Tyto předměty jsou používány pro uložení uživatelského jména a hesla (domény).	
	MODUL	**Protect Encrypt**	Šifrovací modul - je silný souborově orientovaný šifrovací systém určený pro ochranu souborů/adresářů, archivů a elektronické pošty na lokálních nebo síťových discích. Je založen na výkonném transparentním on-the-fly souborovém šifrování implementovaném přímo do OS.	
	MODUL	**Protect Sign**	Modul digitálního podpisu - umožňuje kdykoli během archivace podepsat soubor systémem Protect a podporuje většinu běžně užívaných PKI standardů. Umožňuje ukládání certifikátů a tajných klíčů do HW bezpečnostních produktů (Security Box, Touch Memory, Smart Cards).	
Security Box		Je malé přenosné zařízení (cca 4x4x1 cm) pro bezpečnou úschovu šifrovacích klíčů a přihlašovacích informací uživatele. Je řízeno monolitickým mikroprocesorem. Dodává se ve dvou provedeních - Infrared a Seriál. Hlavním přínosem Security Boxu je značné zlepšení a zjednodušení správy šifrovacích klíčů a umožnění bezpečného přihlašování. Šifrovací klíče a hesla v Security Boxu jsou chráněna heslem. Problém zapamatování si klíčů se tedy redukuje na zapamatování jediného hesla. Další výhodou u tohoto bezpečnostního předmětu je možnost vzdálené správy.		
Touch Memory		Je kompaktní bezpečnostní předmět pro možnost uchovávání informací o uživateli a šifrovacích klíčů. Je podobné velikosti a vzhledu jako běžná knoflíková baterie a je obvykle vložen do plastikového pouzdra. Může uchovávat identifikační a autentizační informace pro identifikaci a autentizaci předmětem k Security Card nebo k operačnímu systému a také šifrovací klíče (zejména pro prostředky systému Protect), stejně jako další informace díky zapisovatelné paměti. Touch Memory je velmi vhodný předmět do náročného prostředí pro svoji fyzickou odolnost vůči okolním vlivům.		
DECROS Card		Je předmět velikosti a vzhledu jako běžná telefonní karta. Čip, který je zapuštěn do plastiku karty není pouze pamětí, jedná se o procesorovou kartu na níž je možné provádět definované jednoduché operace, spouštět programy a na souborový systém karty lze také ukládat informace. Lze ji tedy využít pro přihlašování, ovládání zámku stanice a ukládání a načítání šifrovacích klíčů programu Protect. Takové karty jsou souhrnně označovány jako Smart Card (ISO norma 7816-1,2,3,4) . Jsou určeny svými bezpečnostními vlastnostmi pro široké použití v oblasti bezpečnosti - od přístupových systémů, fyzické bezpečnosti až po kvalitní zabezpečení dat v PC.		
SBXadmin		Aplikace umožňující centrální vzdálenou správu obsahu bezpečnostních předmětů typu Security Box.		2.0.64.
Security Card Lite for DOS		HW ISA adaptér - karta, která umožňuje ochranu přístupu pro 8 uživatelů, nastavení práv přístupu k diskům, zákaz bootování z diskety, ochranu zavádění OS, audit na HW, podpora "Systémové ochrany" a podpora využití bezpečnostního předmětu Touch Memory.		3.x
Security Card for DOS		HW ISA adaptér - karta, která umožňuje ochranu přístupu pro 8 uživatelů, nastavení práv přístupu k diskům, zákaz bootování z diskety, ochranu zavádění OS, audit na HW, podpora "Systémové ochrany" a podpora využití bezpečnostního předmětu Touch Memory. Dále pak podporuje šifrování logických disků, uchovávání šifrovacích klíčů pro Protect for Windows 98 i 2000 a šifrování logických disků.		3.x
Security Card Lite for Windows		HW ISA adaptér - bezpečnostní karta rozšiřující bezpečnostní funkce vlastní systému Windows NT zejména o statistiku provozu a ochranu zavádění OS. Součástí karty je identifikační a autentizační modul dGINA umožňující přihlašování uživatele do Windows NT pomocí bezpečnostních předmětů (Touch Memory, Security Box, Security Card, Brain Card). Šifrování je zajištěno pomocí aplikací Protect for Windows 98 i 2000.		3.x
Security Card for Windows		HW ISA adaptér - bezpečnostní karta rozšiřující bezpečnostní funkce vlastní systému Windows NT zejména o statistiku provozu a ochranu zavádění OS. Součástí karty je identifikační a autentizační modul dGINA umožňující přihlašování uživatele do Windows NT pomocí bezpečnostních předmětů (Touch Memory, Security Box, Security Card, Brain Card). Šifrování je zajištěno pomocí aplikací Protect for Windows 98 i 2000. Dále pak podporuje šifrování logických disků, uchovávání šifrovacích klíčů pro Protect for Windows 98 i 2000 a šifrování logických disků.		3.x

Seznam autorizovaných partnerů firmy DECROS

DECROS®
Authorized Gold Partner

AutoCont CZ a.s. Ostrava
Kafkova 5
70200 Ostrava 2
069-6152111
069-6152128
Ing. Václav Kovář
kovar@autocont.cz
www.autocont.cz

AutoCont CZ a.s. pob.Brno
Česká 31
60200 Brno
05-42218617
05-422 130 16
RNDr. Jiří Kavan
kavan@brno.autocont.cz
www.autocont.cz

AutoCont CZ a.s., Praha
Běžecká 1
16900 Praha 69
02-51022111
02-51022999
Jiří Pašek
comments@praha.autocont.cz
www.autocont.cz

AutoCont CZ a.s.pob. Olomouc
tř. 1. Máje 29
77200 Olomouc 2
068-522 4781
068-522 4781
Josef Szturc
szturc@olomouc.autocont.cz
www.autocont.cz

DECROS®
Authorized Distributor

HITECCO s.r.o.
Pod Sokolicami 14
91101 Trenčín
00421-831-442565
00421-831-442513
Ing. Pavol Rieger
rieger@hitecco.sk
www.hitecco.sk

DECROS®
Authorized Business Partner

AUROTON COMPUTER spol. s r.o.
Prosecká 95
19000 Praha 9
02-6835311
02-83883150
Ing. Přemysl Ondra
premysl_ondra@auroton.com
www.auroton.com

DIGIP spol. s r.o.
Na Františku 32 - budova Min. prům.
11000 Praha 1
02-24852546
02-24852546
Ing. František Doušek
dousek@alef.mpo.cz

NOTES CS s.r.o.
Pod Višňovkou 25/1661
14000 Praha 4
02- 6130 0380
02- 4440 2035
Milan Černobila
mcernobila@notes.cz
www.notes.cz

SOFTWARE CZ spol. s r. o.
Podhorská 34
46601 Jablonec nad Nisou
0428-315 600
0428-315 600
Eva Barešová
softwarecz@volny.cz

DECROS®
Authorized Partner

AUTIS, a. s.
Šmejkalova 46
61600 Brno
05-41592492
05-742752
Ing. Jiří Kubálek
autis@autis.cz

CEDRUS spol. s r.o.
Národní 9
11000 Praha 1
02-22075340-1
02-24228273
Petr Dvořák
dvorak@cedrus.cz
www.cedrus.cz

DATOR3 spol. s r.o.
Stýblova 253/13
14900 Praha 4
602246064
Zdeněk Sazama
zdenek.sazama@dator3.cz

DELL Computer spol. s r.o.
Sokolovská 84-86
18600 Praha 8
02-22832711
02-22832714
Václav Vinkl
vaclav_vinkl@dell.com
www.dell.com/cz

ELIP - DataMarket s.r.o.
Pod soutratím 4
10100 Praha 10
02-71723559
02-71720317
Josef Hodač
elipsro@mbox.vol.cz

GETRONICS SERVICES s.r.o.
Křižíkova 69
18600 Praha 8
02-24890011
02-2313033
Daniela Trnková
daniela.petrova@getronics.com
www.getronics.cz

HESPRO spol. s r.o.
Gočárova 504
50002 Hradec Králové
049-5533041
049-5533241
Ing. Miloš Kormunda
kormunda@hespro.cz
www.hespro.cz

I.N.N. s.r.o.
Za potokem 46
10000 Praha 10
02-72767047
02-72764369
Tomáš Kudrna
kudrna@inn.cz

JANET spol. s r.o.
Koněvova 141
13000 Praha 3
02-6441502 l.231-2
02-127802
Ing. Lubomír Jankových
firma@janet.cz
www.janet.cz

JVB Engineering spol. s r.o.
Komenského 1173
40801 Rumburk
0413-333291
0413-333291
Ing. Václav Bače
vaclav.bace@jvbnet.cz
www.jvbnet.cz

MIUS a.s.
Masarykova 27a
41501 Teplice
0417-41228, 0417-42908
Ing. Robert Klotz
robert@mius.cz
www.mius.cz

PILSCOM s.r.o.
Houškova 16
30154 Plzeň
019-7431456
019-7431456
Ing. Stanislav Krásný
sales@pilscom.cz
web.telecom.cz/pilscom

POSAM spol. s r.o.
Holečkova 31
15000 Praha
02-5731 2091
02-5731 4096
Tomáš Olexa
tomas.olexa@praha.posam.cz
www.posam.cz

PROBIN s.r.o.
Táboritská 23
13087 Praha 3
02-67092476
02-67092473
Luboš Hurt
hurt@probin.cz
www.probin.cz

T-SOFT spol. s r.o.
Novodvorská 1010/14
14201 Praha 4
02-613 48 738
02-613 48 791
Tomáš Sekera
sekera@tsoft.cz
www.tsoft.cz

TACOMA s.r.o.
Staňkova 18
60200 Brno
05-4921 0388
05-4921 0387
Ing. Marek Hostaša
mhostasa@tac.cz
www.tac.cz

TECHNODAT CAE-SYSTÉMY s.r.o.
Třída T.Bati 3295
76001 Zlín
067-7218589
067-7210945 linka 24
Ivo Machač
ivo@tdat.cz
www.technodat.cz

TruconneXion, a.s.
S.K.Neumanna 449
29301 Mladá Boleslav
0326-711711
0326-24974
Robert Kleiner
robert@txn.cz
www.txn.cz

V-COMP
Renčova 28
62100 Brno
05-41246782
05-41246799 i zázn.
Ing. Luděk Vaníček
llvanicek@volny.cz

Aktuální seznam autorizovaných partnerů firmy DECROS najdete vždy na http://www.decros.cz