Lekis

MAGAZÍN | ČTENÍ PRO ČESKÉ LÉKÁRNY | PODZIM 2018

Obsah

4 Protipadělková směrnice (Falsified Medicines Directive)
9 Harmonogram finálního zprovoznění nových agend, zákonných norem a povinností v lékárenských informačních systémech v ČR na přelomu roku 2018/2019
10 Zálohování dat do cloudu
12 Moderní hrozby IT bezpečnosti a jak se proti nim chránit
14 Systém měření teplot
16 Lekis pro Windows v Nemocnici Havlíčkův Brod, p. o.
17 První ročník veletrhu Obchodní dny pro lékárny
18 Výherní křížovka
19 Pohotovostní servis

Redakce, grafické zpracování a tisk:
KNM Agency s.r.o., Krnovská 63,
Opava 746 01. E-mail: info@knm.cz

Vážení čtenáři,
připravili jsme pro vás další vydání našeho úzce specializovaného magazínu, který se věnuje dění na českém farmaceutickém trhu. Předchozí vydání se zaměřilo na hlavní událost roku 2018, tedy zavedení GDPR do každodenního života lékáren. Z informací od našich uživatelů vím, že se toto nařízení Evropské unie úspěšně podařilo zvládnout. Jsem rád, že jsme vám v tomto legislativně nelehkém úkolu významně pomohli. Jako jediný poskytovatel lékárenského informačního systému jsme pro vás připravili set materiálů, které se staly východiskem pro zvládnutí celé problematiky. Potěšil mne každý děkovný e-mail, který jste nám zaslali. Je to pro mě významný signál, že naši práci děláme dobře a jsme pro vás důvěryhodnými partnery.

Jak to tak bývá, jen co se jedna komplikace vyřeší, žene se na nás další a mnohem náročnější. Opět v podobě legislativního nařízení Evropské komise, tzv. protipadělková směrnice (FMD – Falsified Medicine Directive). Osobně ji považuji za největší zásah do provozu lékáren od zavedení počítačů a povinné evidence léčivých přípravků. Mnozí z vás zatím asi netuší, co toto nařízení od 9. 2. 2019 přinese, a proto se v aktuálním vydání našeho magazínu tomuto tématu obsáhle věnujeme. Zeptal jsem se našeho hlavního analytika, Ing. Tomáše Budila, na několik otázek, které by mohly pomoci k prvotnímu seznámení se s tím, co nás čeká. Pro nás v Lekisu toto nařízení znamená s předstihem celou legislativu pochopit a následně upravit náš informační systém tak, aby vše zvládl. Osobně vnímám lékárenský software jako pomyslné srdce lékárny, které když nefunguje, není lékárna schopna provozu. Jelikož považuji celou událost za zcela zásadní pro chod lékáren, připravili jsme pro vás semináře a následně i praktická školení nových funkcí v programu týkajících se FMD. Chceme být pro vás oporou a partnerem při zvládnutí těchto komplikací.

Dalším velkým tématem posledních měsíců a hlavně budoucnosti je bezpečnost dat. Kde jsou ty časy, kdy pro zajištění ochrany dat stačilo nainstalovat antivir nebo zálohovat do jiného adresáře, popř. na jiný počítač v síti. Zaznamenali jsme desítky útoků na data námi spravovaných sítí v lékárnách a mnoho z nich skončilo katastrofálně s následnou nucenou inventurou. Cílem hackerů už dávno nejsou jen velké instituce či bankovní servery, ale cílem se stal sektor malých podniků, lékárny nevyjímaje. Je na odpovědnosti každé lékárny, jak zabezpečí svoje data. My přicházíme s nabídkou moderního funkčního řešení kompletní ochrany dat, včetně zálohování do cloudu. Pozorně si přečtěte další článek v tomto vydání, který se snaží jednoduše naše řešení vysvětlit.

Svět moderních technologií přináší mnoho výhod, ale zároveň se s ním rodí nové hrozby, kterým je nutno předcházet. Systémy jsou propojené, otevřené a to nabízí příležitosti pro nekalé úmysly hackerů z celého světa. Abychom těmto hrozbám mohli čelit, kontinuálně budujeme tým profesionálů, kteří se snaží držet krok s rostoucí technologickou náročností těchto útoků. Nic však není zadarmo a tento fakt nás přinutil poprvé po 10 letech upravit naše ceny. Věříme, že pokud jste s naší prací spokojeni, tak tento krok pochopíte. Přeji nám všem pevné nervy při zvládnutí FMD.

Ing. Petr Hála, ředitel společnosti Lekis s.r.o.

PROTIPADĚLKOVÁ SMĚRNICE
(Falsified Medicines Directive)

Vážení čtenáři, převážně uživatelé informačního systému Lekis pro Windows, od února 2019 dopadne na lékárníky v celé EU včetně ČR další zcela zásadní povinnost. Při výdeji léčivých přípravků se bude muset ověřovat jejich pravost. V této souvislosti jsem požádal našeho hlavního analytika, Ing. Tomáše Budila, aby nám všem odpověděl na několik otázek týkajících se této významné problematiky.

Protipadělková směrnice (FMD – Falsified Medicines Directive) má začít platit od 9. února 2019. Je nějaká šance, že platnost tohoto nařízení bude ještě odsunuta?
Povinnosti vyplývající ze směrnice EU č. 2011/62 a návazného delegovaného aktu (č. 6601), kterým se doplňuje směrnice Evropského parlamentu a Rady 2001/83/ES stanovením podrobných pravidel pro ochranné prvky uvedení na obalu humánních léčivých přípravků, skutečně začínají platit i na území ČR přesně 9. 2. 2019 a odsunout její platnost je de facto nemožné. Dá se říci, že vyjma nějakých obecnějších a více méně nereálných scénářů, a to s danou problematikou a nařízením FMD nesouvisejících, přes tento termín nejede vlak.

Co tedy naplnění této směrnice bude pro lékárníky v praxi znamenat?
Lékárna bude mít povinnost při výdeji léčivého přípravku načíst snímačem 2D kód, pokud takový bude na krabičce vytištěn, a zkontrolovat, že je vydávané balení neporušené. K tomu musí být lékárny zcela nevyhnutelně vybaveny vhodnými snímači.
Po načtení kódu lékárenský systém vykomunikuje s národním systémem („HUBem"), zda je daná krabička výrobcem určena k prodeji, případně upozorní lékárníka na problém. Po ukončení výdeje lékárenský systém zneplatní dané balení v národním HUBu, a znemožní tak opakující se výdej téhož balení.

Znamená to, že všechny krabičky s registrovanými léčivými přípravky vydávané po 9. 2. 2019 budou muset obsahovat speciální 2D kód, o kterém mluvíte?
Tak to úplně přesně není. 2D kódem (jedinečným identifikátorem konkrétní krabičky, také se označuje jako FMD kód) musí být označeny až ty léčivé přípravky, které se vyrobí v období od 9. 2. 2019. Balení vyrobená a na trh dodaná před tímto datem jedinečný identifikátor obsahovat nemusí. Vzhledem k běžným exspiracím léčivých přípravků lze předpokládat, že takové přechodné období, kdy lékárník bude ověřovat jenom část vydávaných balení, bude trvat několik let.

Bude existovat nějaký seznam nebo obecnější pravidlo, podle kterého se budou moci lékárníci orientovat, kdy mají na krabičce hledat 2D kód a kdy ho hledat nemusí, protože bude dopředu jasné, že tam není?
Opět to takto jednoduché nebude. Jedna z největších komplikací při zavádění celého systému bude pro vydávajícího lékárníka v tom, že u stejného léčivého přípravku, se shodným kódem SÚKLu, může mít na skladě některé šarže bez a jiné s 2D kódem. Celá šarže, tedy všechna balení ze stejné šarže, budou nebo nebudou 2D kód z výroby obsahovat. Výdej v lékárně se tomu bude muset přizpůsobit.

V Lekisu pro Windows máme připraveno řešení, které vydávajícího upozorní při výdeji z konkrétní šarže (resp. položky skladové karty), jestli musí 2D kód načítat, nebo ne. Aby takový mechanismus byl účinný, musí se při příjmu na dodacím listu léčivé přípravky označit, zda FMD kódy obsahují, nebo ne, protože žádný seznam 2D kódy označených šarží v celém systému FMD neexistuje a ani se nepočítá s tím, že by někdy existoval. Napomoci by měla spolupráce s distributory, kteří pokud takovou informaci budou mít k dispozici (obsahuje 2D kód, nebo ne), uvedou ji na dodacím listě, jehož elektronický formát byl z tohoto důvodu rozšířen.

Existuje alespoň nějaký obecný seznam registrovaných léčivých přípravků, kterých se tato povinnost týká, nebo se týká i jiných přípravků vydávaných nebo prodávaných v lékárnách?
V principu se tato povinnost ověřovat pravost a také neporušenost balení, na co se mnohdy při vysvětlování praktické aplikace směrnice FMD zapomíná, týká všech přípravků vydávaných na recept. Naopak netýká se volně prodejných přípravků. Konkrétní výjimky z tohoto pravidla jsou uvedené na tzv. black and white listu, ale těch je skutečně jen omezený počet a platí pro celou EU.

Vypadá to celé moc komplikovaně a hlavně pro lékárny pracně...
A to záměrně zatím neříkám všechno, abych to ještě více nekomplikoval.

Uvádí se součinnost lékárenského informačního systému s národním HUBem. To je předpokládám nějaké společné úložiště všech 2D kódů určených výrobcem k prodeji. Kdo ho vytvořil, udržuje a platí vývoj?
Existuje Evropská organizace pro ověřování léčiv (EMVO), což je nezisková organizace založená evropskými zájmovými sdruženími za účelem ochrany legálního dodavatelského řešení před padělanými léčivými přípravky. Jejím cílem je správa společného evropského úložiště (evropský HUB). Podobně existují na národní bázi neziskové právní subjekty, tzv. Národní organizace pro ověřování léčiv (NMVO), které byly založeny za účelem vytvoření a správy národního úložiště dat. V ČR se tato organizace jmenuje NOOL (Národní organizace pro ověřování léčiv) a její zakládající členové jsou AIFP, ČAFF, AVEL, AEDL a ČLnK.
Když se vrátím k první části vaší otázky, úplně přesně to funguje tak, že výrobce zapisuje 2D kódy do společného evropského úložiště dat (HUBu) a ten potom přepošle kódy do národního úložiště, podle toho, pro který trh, resp. členský stát EU jsou jednotlivá balení určena. A protože existují i balení určená pro společný trh (např. ČR a SR), musí být součástí řešení i společná komunikace národních HUBů, která se ale v praxi realizuje vždy přes společnou evropskou centrálu (HUB). Budiž nám nadějí, že tyto „složitější" a časově jistě náročnější komunikace by u nás (v ČR) měly

být zajištěny bezproblémově, protože dodavatel našeho národního řešení je stejný jako dodavatel společného evropského úložiště – společnost Solidsoft Reply Ltd, která byla původně (Solidsoft) založena v roce 1993 ve Velké Británii.

Kdo to celé financuje?
Realizaci národního a evropského HUBu platí zmiňované neziskové organizace, a to příspěvky jednotlivých MAHů (držitel rozhodnutí o registraci léčivých přípravků), v ČR je to prostřednictvím registračních (jednorázových) a uživatelských (ročních) poplatků za připojení k NSOL (Národní systém ověřování léčiv). Je ovšem jisté, že část úprav v systému na straně lékárenských informačních systémů a také jednoznačně zvýšené organizačně-pracovní náklady zaplatí beze zbytku majitelé lékáren.

Vraťme se k lékárníkům a jejich novým povinnostem. Lékárník bude muset 2D kód zneplatnit v úložišti při výdeji, ale co když bude chtít výdej stornovat a krabičku vrátit na sklad k dalšímu prodeji, lze to vůbec?
Lze. Balení lze znovu aktivovat pro výdej, a to maximálně do 10 dnů od zneplatnění, čili od původního výdeje. Uplyne-li od výdeje více jak 10 dní, tak reaktivaci FMD systém neumožní. Lékárník bude muset takovou krabičku odepsat se ztrátou, neboť ani distributor balení ji zpět nepřijme. Mimochodem distributor si u všech balení vracených vratkou z lékáren,

která budou obsahovat FMD kód, bude ověřovat jejich stav v úložišti a přijme zpět pouze ty v aktivním stavu, které lze znovu vydat, nebo ty, které jsou v úložišti v předem definovaných stavech, které budou umožňovat lékárně balení vrátit distributorovi. Rozhodně to ale nebudou stavy všechny. Takže i v tomto lze předpokládat minimálně v úvodu projektu nejasnosti a částečné komplikace.

Nemohla by si lékárna zjednodušit situaci tím, že by jednotlivá balení zneplatnila v úložišti již při příjmu zboží, čímž by si jednak ověřila, že dodaná balení distributorem jsou v pořádku, a jednak by si zjednodušila výdej, protože by na skladě měla jenom balení, která již žádnou „komunikaci s HUBem nepotřebují“?
Tak to možné není. Směrnice přesně hovoří o tom, že ke zneplatnění daného balení (krabičky) musí dojít až při výdeji koncovému zákazníkovi v lékárně. Nicméně k ověření aktuálního stavu v úložišti může lékárna přistoupit, kolikrát chce, a to i opakovaně. Toho budeme v našem lékárenském systému využívat i při běžném výdeji, neboť samotné zneplatnění bude probíhat dvoufázově. Po načtení 2D kódu z balení dojde k ověření balení v úložišti a k samotnému zneplatnění načtených identifikátorů dochází až po ukončení zákazníka a uložení účtenky. Tím se dle našeho názoru vyhneme problémům při dodatečném zpětném „lovení“ zákazníků s neověřeným balením v tašce, ale i zvýšené míře výskytu incidentů, které budou systémem zaznamenány a předávané SÚKLu k řešení. Lze také ověřovat stav balení při příjmu (například z důvodu kontroly dodávky DL), načítání 2D kódu při výdeji se tím ovšem lékárna stejně nevyhne. Pro zajímavost: zneplatňovat 2D kódy v úložišti kromě lékáren budou v jistých výjimečných případech i distributoři (pokud zjistí na balení „vadu“ nebo při dodávkách LP do ordinací, veterinárním lékařům atp.).

Stejně to bude fungovat i v nemocniční lékárně, která zásobuje oddělení vlastní nemocnice?
V nemocničních lékárnách navržený systém (na základě FMD směrnice) umožňuje zneplatnit balení již před „převozem na oddělení“, protože sama lékárna je již zástupce konečného příjemce, a to kdykoliv, pokud bezpečně ví, že balení bude spotřebováno v rámci nemocničního oddělení (např. samostatný sklad léčiv). Lze si také představit složitější opakovaný výdej téhož balení mezi nemocniční lékárnou a odděleními nemocnice v rámci jediné organizace (např. vratky nespotřebovaných léčiv z oddělení do nemocniční lékárny) a to bez komunikace s úložištěm, nelze se ovšem v takovém případě vyhnout riziku blokování vytvoření vratky distributorovi. Ten totiž balení, které je ve stavu „již vydáno“ jistě od lékárny nepřijme.

Řešení výdeje balení, která byla opatřena 2D kódem ještě před 9. 2. 2019 a nejsou výrobcem zapsaná v úložišti atp. Jsou to všechno scénáře, na které se při přípravě lékárenského systému pro FMD systém snažíme již dopředu myslet. Předpokládám ovšem, že i praxe a ostrý provoz celého systému si vynutí další dílčí úpravy v lékárenských systémech z pohledu konkrétních řešení povinností lékáren ve FMD projektu.

Jakým způsobem má vydávající označit balení, které mu systém FMD teoreticky označí za padělek a co s ním má provést, vrátit distributorovi?
Při komunikaci lékárenského informačního systému s HUBem může dojít k tzv. incidentu nebo též alertu. Alert je událost, při které je zjištěno porušení pravidel, například při pokusu o zneplatnění FMD kódu, který je již v HUBu zneplatněn, vyřazen nebo není v systému vůbec zaveden. Lékárna bude muset takový problém nahlásit SÚKLu prostřednictvím zvláštního nového typu agendy – Hlášení OP. Což bude jistě další komplikace v celém koloběhu a to už z toho důvodu, že na přesnou specifikaci zadání ze strany SÚKLu teprve čekáme a o nějakém testování si můžeme nechat jenom zdát. Odpovědný MAH potom informuje SÚKL o vyřešení incidentu. Zatím to vypadá, že balení, u kterých bude prostřednictvím komunikace s HUBem zamezeno výdeji, bude lékárna oprávněná vrátit distributorovi, alespoň v některých případech.

Co když celý systém nebude nějakou dobu funkční? Budou moci vydávající vydávat i bez on-line zneplatnění daného kódu v úložišti, tj. jak vy říkáte v národním HUBu? I u e-receptu jsme toho již byli svědky.
Při tomto scénáři se předpokládá, že zneplatnit balení, tedy označit je v úložišti jako vydané, půjde i dodatečně. Předpokládá to ovšem, že lékárenský systém musí znát jednoznačné identifikátory u vydaných balení, aby mohl všechna taková balení označit jako vydaná v úložišti dodatečně. Povinnosti snímat 2D kódy při výdeji se tak vydávající nezbaví ani při výpadku FMD systému.
Obecně platí, že lékárník může léčivý přípravek vydat vždy, pokud nemá pochybnosti o původu, kvalitě a neporušenosti balení.

Zdá se mi, že moc optimismu ve vašich odpovědích neslyším. Existuje tedy vůbec něco, co vy sám považujete za výhodu pro vydávajícího nebo pacienta v celém zaváděném systému?
Domnívám se, že kromě zpřesnění skladové evidence, protože 2D kód – jedinečný identifikátor musí obsahovat kromě vlastního sériového čísla balení, také kód přípravku, číslo šarže a datum použitelnosti, může systém přinést drobnou výhodu např. při stahování šarží z trhu, neboť lékárník by mohl být systémem při výdeji na takový problém u konkrétního balení upozorněn. Pak zde existuje možnost nějakých nadstavbových funkcí při komunikaci lékárenského systému s národním HUBem, které by mohl vydávající obdržet. Ty však nebudou součástí systému ihned od jeho spuštění.

Původní smysl směrnice, ověřování pravosti léčiv při výdejích v lékárnách, ve smyslu ochrany pacienta, bych si dovolil příliš nekomentovat. Přesto při pohledu na celý systém si svým „selským rozumem" myslím, že těžko může mít reálný smysl pokusit se bránit něčemu, k čemu nikdy v historii nedošlo, a to ještě ke všemu tak robustním a nákladným způsobem. Leda by se předpokládalo, že k tomu v budoucnu s jistotou docházet opakovaně má. Pravděpodobně tak někdo ví něco víc, nebo mi něco uniká, nebo někdo neříká celou pravdu o smyslu takového řešení.

Můžete nám prosím ještě sdělit, kdo bude celý proces dodržování směrnice v lékárně kontrolovat a zda lze za porušování pravidel při výdeji udělit nějakou pokutu?
V ČR bude národní autoritou pro kontrolu dodržování směrnice SÚKL. Rozsahy možných pokut budou nebo již jsou definovány v českých zákonných normách a jsou nemalé. Stejně tak SÚKL bude tím správním orgánem, který bude s lékárnou řešit systémem FMD hlášený incident. Incident přitom bude muset lékárna řešit nejen proto, že sama chce, jelikož jí to směrnice nařizuje, ale i proto, že může být vyzvána SÚKLem, který bude mít automaticky k dispozici všechny „podezřelé" pokusy o výdej v lékárně ze systému FMD samotného. Zároveň pak pravděpodobně budou lékárny v budoucnu nuceny své aktuální výdeje (Lek13, e-recept) doplnit o jednoznačný identifikátor balení, takže SÚKL informace nutné ke kontrole dodržování pravidel FMD tak či tak mít bude.

Závěrem se chci zeptat na dvě věci. Za prvé, jakým způsobem se lékárna do celého systému (FMD) připojí? Jestli ji někdo někdy k připojení vyzve?
První podmínkou pro připojení lékárny do systému FMD je to, že dodavatel jejího lékárenského informačního systému musí projít se svým systémem certifikací u dodavatele národního řešení. Lekis pro Windows takovou certifikaci získal již na jaře 2018. Dále je dobré vědět, že pilotní projekt FMD systému v ČR již běží, přibližně od června roku 2018. Pilotní prostředí je totožné s tím, které bude v provozu od 9. 2. 2019. Takže část lékáren, které jsou v pilotu zapojeny, již má své připojení vyřešeno. Bohužel pilot samotný se jen velmi pomalu rozjíždí a v systému je jen minimum balení LP. Pilotní provoz tak slouží spíše k testování komunikace mezi systémy než k testování a zkoušení skutečných souvisejících činností v lékárně v plném rozsahu a objemu. Navíc u finální verze samotného systému v národním úložišti je plánováno nasazení až v prosinci 2018. Takže testování na všech frontách se dá dle mého předpokládat skutečně až do 8. 2. 2019.

Co se týká většiny do pilotu nezapojených lékáren, vím, že ČLnK připravila procesní schéma postupu přihlášení se do systému FMD, který řeší podpis smlouvy s NOOL, získání přihlašovacích údajů, připojení lékárenského systému atd. V této souvislosti bych chtěl požádat všechny provozovatele lékáren, aby se do systému FMD přihlásili co nejdříve to půjde. Nic tím neztratí, povinnost ověřování se vztahuje až k datu 9. 2. 2019, nikoliv k datu přihlášení se do systému FMD. Získají tím naopak čas na vyzkoušení všech procesů a našim konzultantům se tím jistě lehce uleví v očekávaném tlaku ke konci ledna 2019.

Za druhé, jelikož vidím, že nový systém přinese pro lékárníky mnoho novinek, komplikací a práce navíc, zda by bylo přínosné, abychom buď my, Lekis s.r.o., nebo ČLnK, připravili nějaké semináře, na kterých bychom celý systém lékárníkům vysvětlili a představili. Možná by vedle teorie bylo vhodné udělat i školení, kde by se lékárny prakticky naučily všechny nové funkce, které FMD přináší do Lekisu pro Windows?
Co se týká druhé otázky, tak víme, že ČLnK pro své členy organizuje k problematice FMD sérii webinářů, ale také my v Lekisu připravuje pro zájemce z řad svých zákazníků cyklus seminářů o FMD. Semináře s praktickými ukázkami řešení jednotlivých situací v Lekisu pro Windows by měly proběhnout v lednu 2019.

Děkuji za rozhovor a přeji celému našemu vývojovému a konzultačnímu týmu Lekis pro Windows mnoho úspěchů v další, jistě ne zcela jednoduché práci. A lékárnám, aby zvládly tuto novou povinnost, se kterou se jim budeme snažit maximálně pomoci.
Já také děkuji a všem lékárníkům přeji při zavádění FMD směrnice ve svých lékárnách především pevné nervy.

Ing. Petr Hála
ředitel společnosti Lekis s.r.o.

HARMONOGRAM finálního zprovoznění nových agend, zákonných norem a povinností v lékárenských informačních systémech v ČR na přelomu roku 2018/2019

1. 12. 2018 – nové řešení SÚKLu – agenda LEK13 (podle verze Lek13v6)
- pro lékárnu bude znamenat nutně novou verzi (UPG) stávajícího LIS;
- mimo jiné rozšíření hlášení výdejů o výdeje na žádanky;
- lékárna již nebude používat ROUTER dodávaný SÚKLem

1. 1. 2019 – změna vykazování Signálního výkonu, nově na položku receptu (14 Kč)
- pro lékárnu bude znamenat nutně novou verzi (UPG) stávajícího LIS;
- změna vykazování signálního výkonu ve výdeji na recept;
- změna datového rozhraní dávek pro ZP

1. 1. 2019 – povinné použití e-Receptu při preskripci LP (pod sankcí pro lékaře), se stávajícími výjimkami pro možné použití listinného receptu stanovenými nižší právní normou
- pro lékárnu zatím pravděpodobně nebude znamenat nové povinnosti hrozící např. při zadávání „papírového" receptu do systému

9. 2. 2019 – povinnost evidence a ověření výdejů dle evropské „protipadělkové" směrnice EU č. 2011/62 z 8. 6. 2011 (FMD)
- pro lékárnu bude znamenat nutně novou verzi (UPG) stávajícího LIS, pravděpodobně již v průběhu roku 2018;
- pro lékárnu bude znamenat nutně investice obsažené v nákupu nových 2D snímačů (nejlépe již v průběhu roku 2018);
- pro lékárnu bude znamenat nutně povinnost ověření 2D kódu na každé krabičce registrovaného RX přípravku, který bude do systému zařazen

9. 2. 2019 – nové řešení SÚKLu – agenda hlášení OP (ověřování přípravků)
- pro lékárnu bude znamenat nutně novou verzi (UPG) stávajícího LIS;
- hlášení bude obsahovat problémy při ověření jedinečného identifikátoru i při zjištění porušení obalu;
- každý problém se bude hlásit samostatně, hlášení při ověření FMD bude obsahovat mimo jiné ID výstrahy a ERROR kód z FMD systému (NSOL), pokud se záznam nebude týkat zjištění porušení obalu;
- přihlášení, identifikace lékárny a způsob komunikace bude probíhat na stejných principech jako u jiných aktuálních agend SÚKLu

ZÁLOHOVÁNÍ dat do cloudu

Vážení uživatelé, v minulých číslech našeho magazínu jsme vám představovali problematiku ransomware útoků. V roce 2017 došlo k nárůstu ransomware útoků o 328 %. Útoky jsou vedeny na velké nadnárodní společnosti, drobné podnikatele i domácnosti. Běžná částka výkupného u běžného uživatele se pohybuje do 500 USD, nicméně ani po uhrazení výkupného nemáte jistotu, že svá data skutečně získáte zpět.

V drtivé většině případů jsou po napadení počítačové sítě zašifrována všechna dostupná data na stanicích, serverech a všech připojitelných zařízeních, která byla ve chvíli útoku dostupná. Moderní ransomware se umí šířit počítačovou sítí velmi rychle a **zašifrování všech dat je otázkou několika sekund (nebo několika desítek sekund).**

Zkuste si představit situaci, kdy přijdete ráno do práce a zjistíte, že máte zašifrovaná data a musíte lékárnu uzavřít. Najednou budete vystaveni ekonomickým ztrátám plynoucím z uzavření lékárny. Ztráty na tržbách, ztráty na platech zaměstnanců, kteří nebudou moci pracovat a budou pouze čekat na zprovoznění systému, a pravděpodobně platba za obnovení systému. V ideálním případě budete mít k dispozici nezašifrovanou zálohu dat a zprovoznění systému zabere několik hodin. Ovšem i takové „hodinové" ztráty se mohou vyšplhat během jednoho dne na desítky tisíc korun.

Pokud by se jednalo o kompletní ztrátu dat včetně všech záloh informačního systému, lékárnu bude nutné uzavřít na několik dní. Po takovém útoku musíte systém znovu zprovoznit, zadat do něj všechna data, zejména skladové položky včetně všech cen, exspirací, šarží apod. Začnete přemýšlet nad tím, odkud data pro zadání do systému získáte. Pravděpodobně oslovíte všechny dodavatele, aby vám poslali zpětně všechny dodací listy, a **začnete vše manuálně zadávat do systému.**

V závislosti na velikosti lékárny může zprovoznění lékárny zabrat i pět pracovních dnů. Jaké budou ztráty? Obrovské? Likvidační?

Po takovémto napadení se uživatel začne pídit po zálohách informačního systému, které jsou uloženy ve většině případů pouze lokálně v lékárně. V drtivé většině případů jsou ovšem i tyto zálohy zašifrované.

Základním pravidlem zálohování je, že kromě vytváření lokálních záloh je třeba zálohovat i mimo provozovnu. Ideálně do virtuálního úložiště, které dnes nazýváme cloud. Naše společnost se rozhodla využívat produkt Acronis Backup Cloud renomované společnosti Acronis, která má v této oblasti mnohaleté zkušenosti a patří v daném segmentu mezi leadery. Zálohy jsou z lékárny do cloudu přenášeny pomocí šifrované komunikace a navíc jsou data v cloudu šifrována z důvodu ochrany osobních údajů, takže nikdo se nemusí obávat jejich případného zneužití.

Zálohování je stále řadou uživatelů podceňováno, ti si chybně myslí, že antivir je v dnešní době naprosto dostačující. Toto je bohužel tragický omyl, neboť ransomware se objevuje v mnoha modifikacích a během dne je podniknuto až 200 000 útoků novými ransomwary po celém světě. Běžné antiviry se spoléhají na detekci pomocí signatur (znám hrozbu, mám na ni lék), čímž jsou v dnešní době nepoužitelné, neboť než je k dispozici signatura, objeví se další řada nových modifikací ransomwarů. Antivirové společnosti musí přecházet na nový způsob detekce, kterým je sledování běžících procesů a v případě detekce nebezpečného chování zastavení procesu. Ovšem i v případě úspěšného zastavení procesu může dojít k částečnému zašifrování dat. V našem magazínu se rovněž dozvíte i o nabídce pokročilého zabezpečení stanic a serverů pomocí nových technologií společnosti Sophos, která přináší zcela nové technologie a nový pohled na správu a zabezpečení počítačových sítí.

I v případě sebelepší ochrany stanic a serverů NIKDY NEZAPOMÍNEJTE NA ZÁLOHOVÁNÍ SYSTÉMU DO CLOUDU!

V případě zájmu o zálohování dat do cloudu prosím kontaktujte svého konzultanta, který vám vše velmi rád vysvětlí.

Ing. Petr Ficek,
provozní ředitel regionu Morava

ZÁKAZNÍCI SPOLEČNOSTI LEKIS S.R.O. S PLATNOU SMLOUVOU O SOFTWAROVÉ A DATOVÉ PODPOŘE

Zálohování do CLOUDu – lékárna *Pouze pro jednu lékárnu jednoho majitele.* *Limit zálohovaných dat činí 100 GB / lékárnu*	390,-	Kč/jednu lékárnu/ měsíc bez DPH
Zálohování do CLOUDu – lékárna + výdejna *Pouze pro jednu lékárnu a výdejnu jednoho majitele.* *Limit zálohovaných dat činí 100 GB za lékárnu a výdejnu*	490,-	Kč/jednu lékárnu a výdejnu/měsíc
Zálohování do CLOUDu pro ostatní zákazníky	dle individuální kalkulace	
Podmínkou zálohování dat do cloudu je vysokorychlostní připojení k internetu. Doporučený upload je minimálně 2 Mbps.		

Moderní hrozby IT bezpečnosti a JAK SE proti nim CHRÁNIT

JAKÉ HROZBY NÁS DNES NEJVÍCE OHROŽUJÍ?

Svět IT je již od devadesátých let plný nejrůznějších hrozeb. Od zprvu jednoduchých virů, které se šířily, zpomalovaly počítače a případně bylo nutné reinstalovat systém, se hrozby vyvinuly v obrovský byznys s mnohamiliardovými obraty. S rozvojem internetu je také daleko snazší šíření jednotlivých hrozeb a hlavně útočníci našli ideální oběť, jež je ochotna zaplatit za data – je to jejich majitel. I proto jsme v posledních letech stále častěji svědky opravdu velkých útoků s obrovským finančním dopadem.

A jaké hrozby jsou dnes nejaktuálnější? Nebudu daleko od pravdy, pokud budu tvrdit, že každý z Vás zná pojem **Ransomware**. Jedná se o techniku, kdy útočník nějakým způsobem zablokuje data uživatele, například je zašifruje, a požaduje výkupné (z angl. ransom) výměnou za obnovu dat. Někteří útočníci celou operaci pojímají jako obchodní případ, což znamená, že postiženému uživateli poskytují nápovědu jak platit v bitcoinech, nabízí důkaz odblokováním například dvou nebo tří souborů, či provozují technickou podporu. Dokonce již byly zaznamenány případy, kdy poskytli slevu na výkupném, protože zrovna byly Vánoce. V poslední době se ojevuje varianta šifrování zaváděcího sektoru disku, tzv. MBR. Je to velmi nepříjemný útok, neboť v okamžiku útoku uživatel nic nezpozoruje, disk pracuje, data jsou stále na něm, zdánlivě je vše v pořádku. Bohužel jen do prvního restartu PC, kdy systém disk zahlásí jako vadný a zobrazí výzvu útočníka k zaplacení výkupného.

Dalším kandidátem na nejaktivnější hrozbu současnosti je takzvaný **Cryptojacking**, česky bychom mohli přeložit jako Kryptodolování. Útočník po úspěšně provedeném útoku začne počítač oběti využívat na těžbu kryptoměn, například Bitcoin nebo Ethereum. Podmaní-li si řádově desítky či stovky počítačů, může poměrně rychle zbohatnout. Možná se ptáte, jak vás toto ohrožuje? Odpověď je jednoduchá – jste to vy, kdo nesete náklady, ať již ve formě spotřebované elektrické energie, jejíž spotřeba roste, nebo sníženým pracovním výkonem, protože počítač se věnuje hlavně těžbě, nikoliv běžným úlohám, jako je vydání léku či komunikace s úřady. Hrozby typu Cryptojackingu napadají nejen pracovní stanice, ale také servery nebo chytré mobilní telefony.

A jak je možné, že se podobné hrozby dostanou do počítače? Většinou používají kombinaci více různých technik, velká část z nich využívá různých **zranitelností** (angl. vulnerability), což jsou chyby v různých programech nebo operačních systémech. Pochopitelně, že výrobci se tyto chyby snaží odstraňovat tím, že vydávají **záplaty** (angl. patch), ale čas hraje ve prospěch útočníků, protože ne každý z nás stihne záplaty instalovat. Na využití zranitelnosti pak útočníci využívají **Exploity**, což jsou nástroje, které pomocí různých technik mohou takové zranitelnosti využít a ovládnout napadený systém, například v něm spustit nějaký svůj kód, jenž pak vykoná „špinavou" práci, například zašifruje soubory. Někdy však jen využije svého hostitele k nepozorovanému šíření případně ke krádežím citlivých informací.
V souvislosti s Exploity se také zmiňuje pojem **Exploit kit**, jde v podstatě o sadu nástrojů, které si útočník může online zakoupit na dark webu, nechat upravit pro své potřeby a podniknout například cílený útok na konkrétní uživatele či servery. Jak vidíte, jedná se celkem o velmi dobře propracovaný byznys.

ZÁKAZNÍCI SPOLEČNOSTI LEKIS S.R.O. S PLATNOU SMLOUVOU O SW A DATOVÉ PODPOŘE

Central Intercept X Advanced for Server	390,-	Kč/server/měsíc
Central Intercept X Advanced for Server	3650,-	Kč/server/rok
Central Endpoint Intercept X/Advanced	dle individuální kalkulace	

JAKÝ VLIV MÁ LIDSKÝ FAKTOR?

Dříve tradovaný názor, že postačí být na internetu opatrný a neotevírat anglicky psané maily, bohužel dnes již neplatí. Naopak, je nutno zkombinovat vhodné a obezřetné chování s dalšími technickými prostředky.

Co můžeme ovlivnit naším chování je odhalení tzv. **Phishingu**, v angličtině jde o zkomoleninu slova fishing, tedy rybaření. Tato zvukově velmi podobná slova přesně vystihují podstatu phishingu – vydávat se za něco velmi podobného a takto oklamat oběť (a pak zaseknout háček). Nejčastěji se phishing vyskytuje ve formě podvržených emailů, kdy se útočník vydává za někoho jiného a obvykle s velmi urgentní žádostí o rychlou reakci, například otevření přílohy, spuštění nějakého kódu, přihlášení ke svému mailu, do své banky a podobně. Problém je ten, že pokud uživatel podlehne klamu, tak svým přičiněním velmi útočníkovi pomůže. Buď mu přímo spustí kód ve svém počítači, nebo mu naopak vyzradí své přihlašovací údaje, třeba i ke svému bankovnímu kontu. Následky mohou být nedozírné, proto opatrnosti není nikdy nazbyt. Často se jedná o drobnosti, například záměna písmen v adrese odesílatele, nebo odkazy v mailu, které vedou na neexistující stránky. (Tip: než na odkaz kliknete, najeďte na něj myší a od se Vám ukáže) Existují dokonce i nástroje, které Vás otestují, jak jste odolní proti Phishingu a pokud zjistí, že nikoliv, tak Vás rovnou proškolí.

NENAVŠTĚVUJI PODEZŘELÉ STRÁNKY, JSEM TEDY V BEZPEČÍ?

Bohužel ani věta z nadpisu již dnes neplatí. Útočníci dnes napadají přímo webové servery, případně servery s proužkovou reklamou, na které infiltrují své Exploit kity a pak už jen čekají, až si danou stránku otevře uživatel s nedostatečně zabezpečeným počítačem. Proto někdy postačí i návštěva naprosto neškodné stránky, kde však majitel podcenil zabezpečení. Nezbývá, než kromě obezřetnosti vzít na pomoc další technické prostředky.

NÁSTROJE, JEŽ NÁS MOHOU OCHRÁNIT

Každý z nás má jistě v povědomí, že bez kvalitního antivirového programu se neobejdeme. Vzhledem k vývoji na poli malware však dnes již musíme hledat mezi takzvaným „Next-gen" antimalware, který je schopen detekovat a hlavně eliminovat i zcela nové formy útoků. Zatímco klasický antivir spoléhá na znalost již objevených virů, produkt nové generace je schopen detekovat i zcela nové a neznámé hrozby na základě chování jednotlivých částí kódu v paměti. Nejmodernější verze též zapojují umělou inteligenci Deep Learning, což je obdoba neuronových sítí. Díky nim jsou schopni ve velmi krátké době ohodnotit neznámý kód, zda je či není škodlivý a to při velmi nízké míře falešných poplachů.

Z pochopitelných důvodů se i společnost Lekis snaží nabídnout svým klientům řešení, které by data v lékárnách ochránilo. S tímto záměrem jsme se obrátili na společnost Sophos, jejíž specialisté mají s ochranou dat zkušenosti v celosvětovém měřítku. Pro lékárny jsme tak připravili nabídku, která významně snižuje rizika spojená s možností ztráty dat. Nabídka spočívá v instalaci Sophos Intercept X Advanced for Server. Co je Sophos Intercept X Advanced for Server? Je to unikátní nástroj pro pokročilou ochranu uložených dat, který se sám učí bránit se hrozbám a napadením a co je důležité – dovede je zastavit před tím, než poškodí nebo zašifrují data na serveru.

Ochrana serveru je primárním a základním úkonem pro to, aby lékárna o svá data nepřišla a aby se nevystavovala riziku jejich obnovy ze záloh, pokud vůbec existují. Dalším stupněm pro zajištění bezpečí údajů může být ochrana pracovních stanic. Ani jim se pozornost vývojářů a analytiků společnosti Sophos nevyhýbá a mají i pro ně připravená adekvátní řešení, jmenovitě Central Endpoint Intercept X nebo Central Endpoint Advanced. Do třetice se dá škodlivému softwaru postavit do cesty překážka v podobě firewallu, což je laicky řečeno zeď, která se podílí na ochraně celé sítě v lékárně. Podrobnosti k uvedeným produktům i konkrétní cenovou nabídku lékárně zpracuje její konzultant. Žádný z nás nemusí být geniálním matematikem a ekonomem jakým byl třeba John Nash, aby si dokázal spočítat, kolik stojí den, kdy je lékárna z nějakého důvodu zavřená. Nyní vedle této částky postavte 10 Kč, za které vám Sophos denně data na serveru pohlídá a ochrání. V těchto 10 korunách denně je obsaženo celoroční předplatné Sophos Intercept X for Server. Je zde samozřejmě i možnost měsíční platby.

SYSTÉM MĚŘENÍ TEPLOT

Historie používání automatizovaného systému měření teplot (dále jen Symet) dodávaného naší společností sahá do roku 2003. Od tohoto roku jsme Symet instalovali zhruba ve 100 provozovnách po celé České republice.

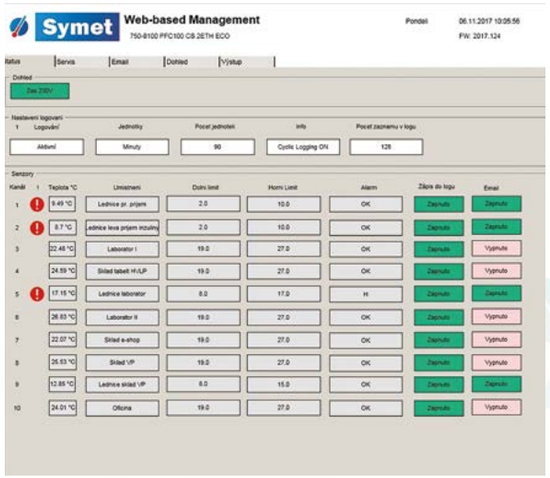
Symet se skládá z certifikovaných a kalibrovaných čidel umístěných v lednicích a z datové kabeláže, která čidla spojuje s ústřednou „srdcem" tohoto systému. Ústředna naměřené hodnoty z čidel zaznamenává a dále je připravuje k následnému zpracování v lékárenském informačním systému Lekis pro Windows.
Vzhledem k radikálnímu rozvoji v oblasti řízení a automatizace jsme se v roce 2017 rozhodli ke kompletní modernizaci Symetu. Po několikaměsíčním testování v ostrém provozu pilotních lékáren vám nyní můžeme oznámit, že systém je plně funkční a nabízí mnohem více než původní řešení. Srdce Symetu tvoří zcela profesionální ústředna společnosti WAGO. Společnost WAGO patří od roku 1951 ve svém oboru řízení a automatizace mezi jedničku na trhu. Jejich systémy jsou celosvětově využívány k řízení komplikovaných staveb a budov. Součástí nového systému Symet jsou rovněž zcela nová teplotní čidla, která jsou certifikovaná a kalibrovatelná.

Systém tedy jako celek vyhovuje všem požadavkům Státního ústavu pro kontrolu léčiv.

VÝHODY NOVÉHO SYSTÉMU JSOU:

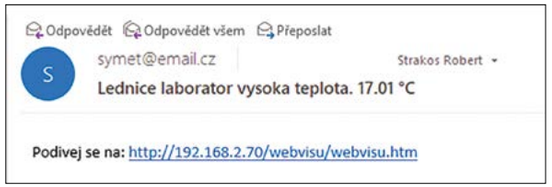
1. Symet **hlídá, zda jsou monitorované lednice napájeny z elektrické sítě** 230 V.
2. Nově je součástí ústředny i SD karta, která slouží k **zálohování naměřených hodnot**.
3. **Systém je zcela automatizovaný** a k jeho činnosti není vyžadována uživatelská interakce. **Naměřené hodnoty se automaticky importují do lékárenského informačního systému Lekis pro Windows.**
4. Symet nabízí **okamžitý náhled na aktuální teploty** v lednicích **pomocí webového prohlížeče**. Přístup přes webový prohlížeč je chráněn jménem a heslem.
5. Symet nabízí **rychlý přístup** k samotné administraci systému pomocí webového prohlížeče. Přístup přes webový prohlížeč je chráněn jménem a heslem.
6. Do webového rozhraní můžete rovněž přistupovat pomocí chytrého telefonu nebo tabletu.
7. Do webového rozhraní můžete přistupovat odkudkoliv, kde máte k dispozici kvalitní internetové připojení.
8. Symet nabízí pro lepší orientaci vlastní pojmenování lednic a měřených zařízení.
9. V případě překročení limitních hodnot je uživatel informován pomocí e-mailové notifikace. Předmět a obsah odesílané zprávy lze definovat z konfiguraci Symetu.
10. V případě překročení limitních hodnot může být uživatel informován pomocí SMS odesílané na mobilní telefon uživatele.
11. Při obnovení dodávky elektrické energie a spuštění ústředny je uživatel o této skutečnosti informován e-mailem.
12. Symet nabízí přehled o počtu nestažených naměřených hodnot uložených na SD kartě ústředny.
13. Symet nabízí uživatelskou definici časového intervalu snímání teplot.
14. Tisky naměřených hodnot provedete pohodlně z Lekisu pro Windows.
15. Systém lze použít rovněž v lékárnách, které nepoužívají Lekis pro Windows. V takovém případě dodavatel konkurenčního informačního systému musí zabezpečit zpracování dat exportovaných z ústředny ve vlastním lékárenském informačním systému.

Náhled webového rozhraní:

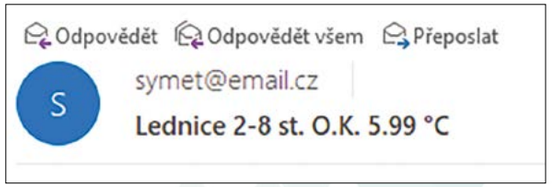


E-mailová notifikace uživatele:
Symet nabízí možnost notifikace uživatele v případě překročení limitních hodnot e-mailem a volitelně i SMS. Abychom zabránili zasílání planých poplachů, které mohou vznikat např. v době doplňování lednic apod., systém používá tzv. paměťový efekt nazývaný rovněž hystereze. Pokud by tedy v lednici došlo pouze ke krátkodobému navýšení teploty, nedojde k odeslání varovné notifikace uživateli. Naopak při navýšení mimo definované podmínky a toleranci dojde k odeslání notifikace okamžitě. Četnost zasílaných „planých" varovných hlášení se takto snížila na minimum.

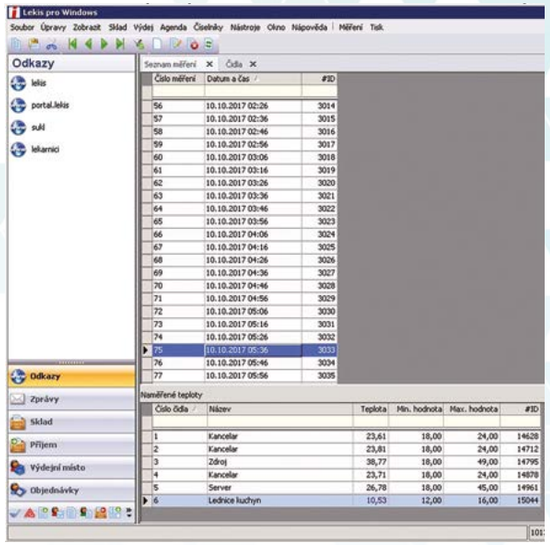
Ukázka e-mailové notifikace:



Po obdržení varovného e-mailu se uživatel může podívat na aktuální stav teplot pomocí webového prohlížeče, případně počkat zhruba 30 minut na další e-mail, zda nedošlo k navrácení teploty v lednici k normálu. Níže následuje ukázka e-mailu související s odvoláním poplachu:



Náhled naměřených hodnot v Lekisu pro Windows



Symet je ideální volbou pro automatizované měření a zaznamenávání teplot ve vaší lékárně. V případě vašeho zájmu o Symet kontaktujte prosím našeho specialistu pana Roberta Strakoše (rstrakos@lekis.cz, tel. 602 572 916), který pro vás připraví individuální nabídku.

LEKIS pro Windows v Nemocnici Havlíčkův Brod, p.o.

Program Lekis pro Windows máme instalován v nemocniční lékárně v Havlíčkově Brodě od roku 2009. Přechod na nový software byl tehdy nezbytný. Původní lékárenský program na platformě MS-DOS udržovaný jedním programátorem již nedokázal pružně reagovat na příliv číselníků a vládních výmyslů jako arkus tangens a zároveň měl velké problémy s připojováním na externí služby.

Po deseti letech soužití jsme se s ním rozloučili, což bylo dobře.
Dneska s úsměvem vzpomínám na silvestrovskou noc strávenou v lékárně v napětí, zda druhý den vůbec otevřeme, nebo na oněch několik hodin, kdy jsem každý leden dobýval roční údaje pro ÚZIS. Přitom část dat bylo nutné prostě odhadnout, a zároveň se strefit přibližně do loňských čísel, protože jak víme, statistiky nejvíce vzruší velké odchylky a hned volají, co se stalo.
Naše lékárna zásobuje kromě Nemocnice Havlíčkův Brod i nemocnice v Ledči nad Sázavou a v Humpolci, léky jsou deponované na pěti skladech, takže jedním z rozhodujících faktorů pro výběr SW byla možnost vedení všech skladů na jedné instanci, bez nutnosti spouštět pět programů. Převod dat ze starého SW proběhl zcela bez problémů, jediné, co jsme při přechodu na nový lékárenský program dotvářeli, bylo zasílání elektronických žádanek a jejich následné zpracování, tedy základní nemocniční logistika. Představu procesu jsme měli, elektronické žádanky jsme používali již od konce 90. let a velmi brzo jsme nalezli vhodnou podobu celého procesu v Lekisu – s automatickou změnou stavů žádanek a s možností jejich řazení do skupin dle objednaného zboží.
Od doby implementace uplynulo již devět let, v Lekisu přibylo mnoho funkcionalit, které pomáhají mně i mým kolegům. V současnosti na firmě Lekis oceňuji především progresivní přístup k novým technologiím i pružnost ve vztahu k měnící se legislativě a k našim požadavkům.
Instalace Lekisu v Nemocnici Havlíčkův Brod má jednu zvláštnost. Postaral se o ni náš nemocniční IT pracovník Tomáš, jehož zvykem je pojmenovávat servery jmény pohádkových postaviček. Takže uzávěrky běžně tisknu na některé z tiskáren, které jsou pověšené na Cipíska, protokoly k přípravě cytostatik jsou na Asterixovi, zatímco například faktury naleznu na Štaflíkovi. Je to fajn, ale s rozvojem elektronizace lékárenství jsme se dostali do jistých potíží, protože nám přidáváním či obměnou komponent postupně docházejí pohádková jména, navíc se postavičky dostávají do absurdních kolizí. Jen pro představu – ostrá verze Lekisu je instalována na serveru Arabela, testovací verze byla logicky na Rumburakovi, kterého ovšem časem nahradil Blekota. Databázový server se jmenuje Saruman. Při letošní přeinstalaci byla komunikace mezi IT pracovníky (které jinak vůbec nerozumím) asi následná: „Tak je nová verze nahraná na Xenii, Arabela nyní kouká do Blekoty a až to otestujete, Arabelu odřízneme, připojíme Xenii k Sarumanovi a bude hotovo.„

Mgr. Vít Vodrážka

První ročník veletrhu OBCHODNÍ DNY pro lékárny

Ve středu 12. září se společnost Lekis zúčastnila prvního ročníku veletrhu Obchodní dny pro lékárny. Veletrh se konal na Výstavišti Flora ve městě Olomouc. Pořádala jej společnost Health Communication, která se věnuje marketingové komunikaci v prostředí farmacie.

RÁDI BYCHOM PODĚKOVALI ORGANIZÁTORŮM, ALE TAKÉ VŠEM ZÚČASTNĚNÝM, KTEŘÍ NAVŠTÍVILI NÁŠ STÁNEK A DOZVĚDĚLI SE MNOHO NOVÝCH A ZAJÍMAVÝCH INFORMACÍ ZE SVĚTA FARMACIE.

Jelikož patří společnost Lekis na trhu informačních systémů pro lékárny mezi leadery, na akci jsme nemohli chybět. S našimi zákazníky, ale také s nově příchozími jsme mluvili hlavně o tom, čemu se v rámci našich služeb věnujeme a především o funkčnosti protipaděkové směrnice v našem systému. Zároveň jsme ukázali některé z našich novinek v hardwaru a také v nabídce dalších bezpečnostních produktů. Odhalili jsme i naše systémové novinky a další zajímavosti ze zákulisí společnosti.

VÝHERNÍ křížovka

Soutěžíme o hodnotné sety léčebné kosmetiky Avène

Správné řešení vyplňte do formuláře na https://www.lekis.cz/krizovka, nejpozději však do 31. 12. 2018. Zasláním tajenky dáváte souhlas se zpracováním svých údajů pro marketingové účely. Soutěžíme o hodnotné sety léčebné kosmetiky Avène. Výherci budou zveřejněni na stránkách společnosti Lekis a v informačních řádcích v Lekis pro Windows.

Tajenka: Nezapomeňte...

KAMERUNSKÁ ŘEKA			SPOJKA (KNIŽNĚ) / PŘEDLOŽKA				NELÁSKA						OZNAČENÍ LETADEL NORSKA / ŠVÉD. SÍDLO		
NEZNÁMÝ							GEODETICKÝ MĚŘICÍ DALEKOHLED / ZN. VOLTAMPÉRU								
	PARÁDA	LATINSKÁ SPOJKA A / DOVNITŘ (SLOVEN.)			HLASITÉ PÍSKNUTÍ / Tajenka část 1						HOVOROVÝ SOUHLAS / Tajenka část 2			SVÁŽENÍ	NÁŠ AUTOMOBILOVÝ ZÁVODNÍK F1
SPZ PRIEVIDZA			MPZ CARLOW (VELKÁ BRITÁNIE) / EIGE-NHOWEROVA PŘEZDÍVKA			OPATŘENÍ PROTI VNIKU BAKTERIÍ DO ORGANISMU / CITOSLOVCE FÍČENÍ							ČÍN. CITERA / OTEVŘENÁ KLÍČEM		
RUSKÉ SÍDLO				ZN. HAFNIA / VYSOKÉ KARTY			STŘEŠNÍ KONSTRUKCE / SPZ NUORO (ITÁLIE)					SPZ OSTRAVY			
UMĚLÉ SLADIDLO								CITOSLOVCE ZVUKU TRUBKY / LUTEINIZAČNÍ HORMON				ANGL. PES / CITOSL. ÚDIVU			
	ŽÁDNÝ ČLOVĚK	VYSOKÉ KARTY (SLOVENSKY) / MORAVSKÝ ARCHEOLOG A PALEONTOLOG (1860-1937)				RUSKÁ ŘEKA / POSTAVA OPERY: NÁPRAVNÍK - HAROLD			SÍLA MEZI KOLY AUTA A VOZOVKOU / INDICKÝ FILM						
NUKLEOVÁ KYSELINA (ZKR.)			ZESÍLENÝ ZÁPOR / STŘEDOMOŘSKÝ OSTROV				NÁZEV PÍSMENE H / NÁŠ KONSTRUKTÉR (JAN)			KANAD. ŘEKA / ANGL. TRÁPENÍ				EVROPAN	PLATIDLO AFGHÁNISTÁNU
UMÍNĚNÝ ZÁPOR				BĚLOVESKÁ KYSELKA / ANGL. ZKR. PŘETÍŽENÍ (OVERLOAD)				NAČEPOVAT / INICIÁLY TENISTY AGASSIHO							
UKAZATEL VÝBUŠNÉ HODNOTY									ZRALÁ POHLAVNÍ BUŇKA / OZNAČENÍ LETADEL KOSTARIKY						
UTKÁNÍ DVOJIC					ODE DNE VYDÁNÍ (Z LAT.) / ÉRA						BIBLICKÝ OBR / AMER. HEREC (1949-)				
ŠPANĚL. ŘEKA				ESTONSKÉ SÍDLO / MRAVNÍ ČISTOTY				AKADEMICKÁ ZKRATKA / MEZINÁRODNÍ KÓD JUGOSLÁVIE				DOMÁCKY ALENA / OLYMPIJSKÁ ZKR. (MEZINÁRODNÍ OLYMPIJSKÝ VÝBOR)			
	MPZ LEICESTER (VELKÁ BRITÁNIE)	POLOMĚR	VZÁCNĚ JEHLIČNANY / ČÁSTICE ZVOLACÍ						KÓD JEMENU / ZKRATKA KNOKAUTU				DAMENIZAČNÍ SLABIKA	OSOBNÍ ZÁJMENO	SPZ VYŠKOV
SPOJKA						INDIÁNSKÁ ZBRAŇ				VRCHOLSKÉ PAHORKATINY					
FRANCOUZSKY BRZDA						JÁ				PATŘÍCÍ EVĚ					

PŘIPRAVTE SE NA PROTIPADĚLKOVOU SMĚRNICI JIŽ DNES

Nabízíme vám snímače za speciální cenu, při objednávce uveďte kód Magazín Lekis

7.390,-
bez DPH 21%

SVOBODA POHYBU

Bezdrátový ruční snímač

Motorola Zebra DS2278

1D/2D laserová čtečka
*Technologie **Bluetooth 4.0 s dosahem až 7 m***
Scan-To-Connect pro snadné spárování
Baterie s kapacitou 2400 mAh a dobou nabití 4 hodiny

2.840,-
bez DPH 21%

Ruční snímač

Zebra DS2208

Malé rozměry, nízká váha
Direct Code Indicator
Bezproblémové skenování i kódů se špatnou kvalitou
Jednoduchý design
Stojan a USB kabel součástí balení
Odolné zpracování s ochranou IP42

4.340,-
bez DPH 21%

Ruční / stacionární snímač

Motorola Zebra DS9208

Mnohasměrné čtení kódů z libovolného média
Zaměřovací bod
Velké snímací okénko
Automatické přepínání mezi snímacími režimy
Odolnost proti pádu z výšky 1,5 m na beton

PRO RYCHLÝ PŘÍJEM

15.990,-
bez DPH 21%

Vestavný pultový snímač

Datalogic Magellan 3550HSi

Zdvojnásobená rychlost
Funkce Object Sense Illumination

Tyto námi nabízené snímače si poradí nejen s 2D kódy, umí také načíst klientské karty a elektronické recepty z displejů mobilů.

Cenu včetně zapojení a konfigurace vám ochotně sdělí Váš servisní technik.
Objednávejte na obchod@lekis.cz nebo na pobočkách Benešov 317 763 711 či Ostrava 597 575 300.
Nabídka platí do 20. 12. 2018 nebo do vyprodání zásob. Neručíme za tiskové chyby.