Soulad Docházky 3000 se směrnicí NIS2 o kyberbezpečnosti

pokyny k aktualizaci komponent a nastavení konfigurace docházkového systému

Tato příručka popisuje postup při zapracování funkcí pro podporu kyberbezpečnosti v IT a slouží jako podpora pro dosažení souladu docházkového systému se směrnicí NIS2. Vyžaduje SW Docházka 3000 ve verzi 9.50 nebo vyšší. Pokud máte starší verzi, najdete aktualizaci přímo v programu v levém admin. menu *E-Shop*.

Směrnice NIS2 (Network and Information Security) je nová směrnice EU (2016/1148) o kybernetické bezpečnosti, která má za cíl vytvořit jednotnou úroveň ochrany v oblasti kybernetické bezpečnosti v celé EU prostřednictvím zavedení požadavků a opatření ve všech členských státech. Národní legislativa adoptuje směrnici prostřednictvím nového zákona o kybernetické bezpečnosti s vykonávacími vyhláškami, který vejde v platnost nejpozději 17. října 2024.

V návaznosti na tuto legislativu obsahuje již SW Docházka 3000 od verze 9.50 v menu *"Zaměstnanci / Nařízení GDPR / Směrnice NIS2"* funkce související s kybernetickou bezpečností a jedná se například o následující funkce:

- zjištění verzí programových komponent, doporučení a postupy jejich aktualizace na nejnovější bezpečné verze (přechod na aktuální apache 2.4.63 a MariaDB 11.3)

- šifrování dat (úložiště) včetně záloh databáze a síťových přenosů (HTTPS s TLS 1.3)

- identifikace serveru či hlavního PC docházky v počítačové síti

- logování přístupu uživatelů, verzí jejich OS, prohlížeče, vynucení šifrování https atd.

- možnost omezit přístup do SW jen z povolených IP adres či počítačů

- vyhodnocení bezpečnosti uživatelských hesel a možnost vynucení jejich složitosti a stáří

- identifikace docházkových terminálů v počítačové síti

- podpůrné funkce a protokoly pro zavedení NIS2 (např. velikost podniku dle počtu zaměstnanců...)

- ochrana přihlašování do programu proti útoku hrubou silou s pokusy o uhodnutí hesla

Účelem těchto a dalších návazných funkcí v docházkovém systém je podpora pro zapracování požadavků NIS2 do vašich IT systémů a firemních procesů týkajících se bezpečnosti dat atd. Podrobné pokyny naleznete přímo v programu Docházka 3000 v nápovědě dostupné přes ikonu modrého otazníku dole přímo v modulu *"Zaměstnanci / Nařízení GDPR / Směrnice NIS2"*.

Implementace směrnice NIS2 ve vaší organizaci by měla obsahovat zejména tyto kroky:

1) Ověření zda vůbec pod NIS2 spadáte, tedy zda poskytujete regulovanou službu, naplňujete finanční nebo zaměstnanecký ukazatel, nebo jste součástí dodavatelského řetězce některého vašeho odběratele který pod NIS2 spadá. Docházka vám i pomůže např. s vyhodnocením zaměstnaneckého ukazatele.

2) Vypracovat plán opatření, ve kterém si vyhodnotíte jaká opatření je třeba pro splnění požadavků směrnice NIS2 zavést. Zde vám docházka pomůže s ověřením aktuálnosti jí používaných programových komponent, zabezpečení datových přenosů a úložiště databáze, identifikací serveru a čipovacích terminálů, stavu zabezpečení uživatelských účtů a přístupů do programu (identifikace počítačů ze kterých se přihlašují zaměstnanci do programu a jaký používají typ OS počítače a webového prohlížeče), ze kterých adres se loguje administrátor, zda se používá šifrované spojení a z jakých veřejný adres přichází podezřelý datový provoz (například časté nezdařené pokusy o přihlášení do programu).

3) Realizace opatření je dalším krokem k naplnění požadavků směrnice NIS2 a zde vám docházka pomůže tím, že přehledně v tabulce vidíte které problémové položky například v aktuálnosti programových komponent či oblasti zabezpečení dat a přenosů či přihlašování uživatelů jsou již splněny a které je ještě potřeba realizovat.

4) Prokázání shody s NIS2 by mělo být finálním krokem. Ovšem ve skutečnosti je třeba zdůraznit, že v oblasti bezpečnosti dat se vše stále rychle vyvíjí a tak se vlastně jedná o kontinuální proces, který nelze nikdy považovat za finálně dokončený.

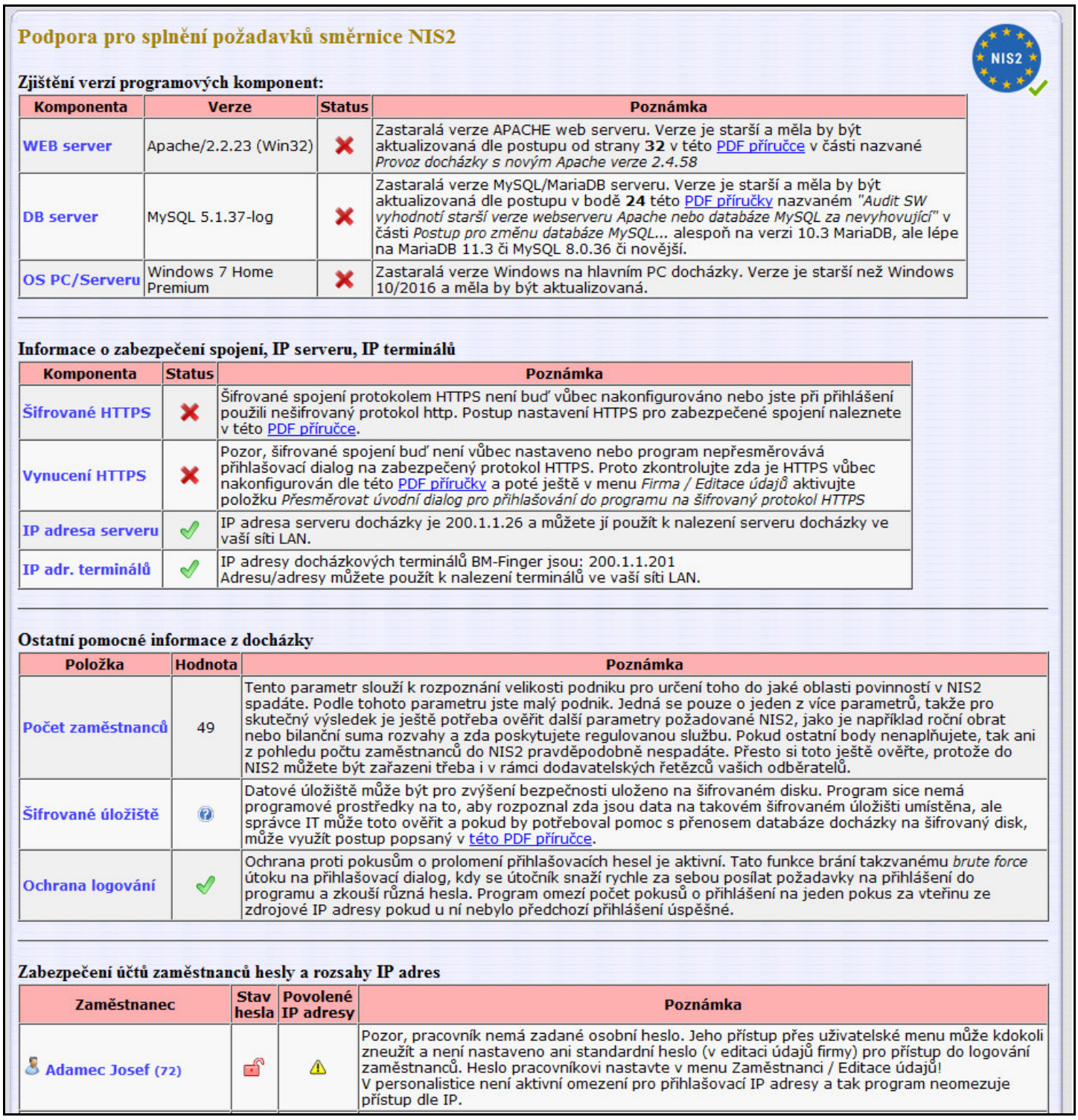
Tato příručka se zabývá postupem aktualizace programových komponent a nastavení programu tak, aby vám splnění požadavků NIS2 co nejvíce usnadnila. Cílem této příručky není najít nějaké snadné a rychlé řešení zajištění bezpečnosti IT systémů ve vaší firmě jako celku, soustředí se jen na oblast docházkového systému v případě, kdy audit SW vyžaduje splnění kritérií i v docházkovém systému, který ale za běžných okolností nelze u drtivé většiny firem považovat za kriticky důležitou součást infrastruktury pro směrnicí regulované služby.

Zjištění současného stavu komponent a konfigurace docházky:

Ve výchozí instalaci prostředí docházky se u starších verzí používaly varianty služeb a konfigurace systému tak, aby vše fungovalo i na velmi starých počítačích vyrobených i třeba kolem roku 2000 a to včetně podpory starých 32 bitových operačních systémů jako byly Windows 98, 2000, XP a servery Windows NT, 2000, 2003 a podobně. Výchozí instalace docházky stále i na těchto starých počítačích a operačních systémech funguje a aby to bylo možné, používá verze webového serveru Apache a databáze MySQL které na těchto systémech fungují. Od roku 2008 sice vypadla podpora starých Windows NT a 98 a tak tenkrát byly verze programových komponent aktualizovány, ale stále byla zajištěna podpora i pro Windows 2000, aby se u zákazníků mohly tyto starší počítače pro docházku stále používat, protože byly součástí například telefonních ústředen a tak zákazníci dali přednost instalace docházky na tento počítač když jiný stále běžící ve firmě třeba ani nebyl.

Proto výchozí instalace programu dlouhou dobu používala dnes již velmi zastaralé komponenty jako je webový server Apache verze 2.2.23 a MySQL databáze verze 5.1.37, které fungovaly univerzálně na všech operačních systémech od Windows 2000 po Windows 11 a to jak ve 32 bitové tak 64 bitové edici systému a na Windows serveru od verze 2000 až po verzi 2022, opět 32 i 64 bitových.

Bylo tedy zajištěno, že když si zákazník pořídil systém Docházka 3000, bude mu fungovat v podstatě na úplně libovolném PC s Windows a nebylo nutné kvůli docházce měnit počítač, server nebo operační systém. Bohužel pro splnění moderních IT bezpečnostních kritérií vyžadovaných směrnicí NIS2 již není možné tyto univerzální komponenty používat. Pokud docházku necháte běžet na staré verzi prostředí, tak po spuštění kontroly v menu *„Zaměstnanci / Nařízení GDPR / Směrnice NIS2“* zobrazí program řadu problémů označených červenými či žlutými varovnými ikonami. Viz následující obrázek.



Podpora pro splnění požadavků směrnice NIS2

Zjištění verzí programových komponent:

Komponenta	Verze	Status	Poznámka
WEB server	Apache/2.2.23 (Win32)	✖	Zastaralá verze APACHE web serveru. Verze je starší a měla by být aktualizovaná dle postupu od strany **32** v této PDF příručce v části nazvané *Provoz docházky s novým Apache verze 2.4.58*
DB server	MySQL 5.1.37-log	✖	Zastaralá verze MySQL/MariaDB serveru. Verze je starší a měla by být aktualizovaná dle postupu v bodě **24** této PDF příručky nazvaném *"Audit SW vyhodnotí starší verze webserveru Apache nebo databáze MySQL za nevyhovující"* v části *Postup pro změnu databáze MySQL...* alespoň na verzi 10.3 MariaDB, ale lépe na MariaDB 11.3 či MySQL 8.0.36 či novější.
OS PC/Serveru	Windows 7 Home Premium	✖	Zastaralá verze Windows na hlavním PC docházky. Verze je starší než Windows 10/2016 a měla by být aktualizovaná.

Informace o zabezpečení spojení, IP serveru, IP terminálů

Komponenta	Status	Poznámka
Šifrované HTTPS	✖	Šifrované spojení protokolem HTTPS není buď vůbec nakonfigurováno nebo jste při přihlášení použili nešifrovaný protokol http. Postup nastavení HTTPS pro zabezpečené spojení naleznete v této PDF příručce.
Vynucení HTTPS	✖	Pozor, šifrované spojení buď není vůbec nastaveno nebo program nepřesměrovává přihlašovací dialog na zabezpečený protokol HTTPS. Proto zkontrolujte zda je HTTPS vůbec nakonfigurován dle této PDF příručky a poté ještě v menu *Firma / Editace údajů* aktivujte položku *Přesměrovat úvodní dialog pro přihlašování do programu na šifrovaný protokol HTTPS*
IP adresa serveru	✓	IP adresa serveru docházky je 200.1.1.26 a můžete jí použít k nalezení serveru docházky ve vaší síti LAN.
IP adr. terminálů	✓	IP adresy docházkových terminálů BM-Finger jsou: 200.1.1.201 Adresu/adresy můžete použít k nalezení terminálů ve vaší síti LAN.

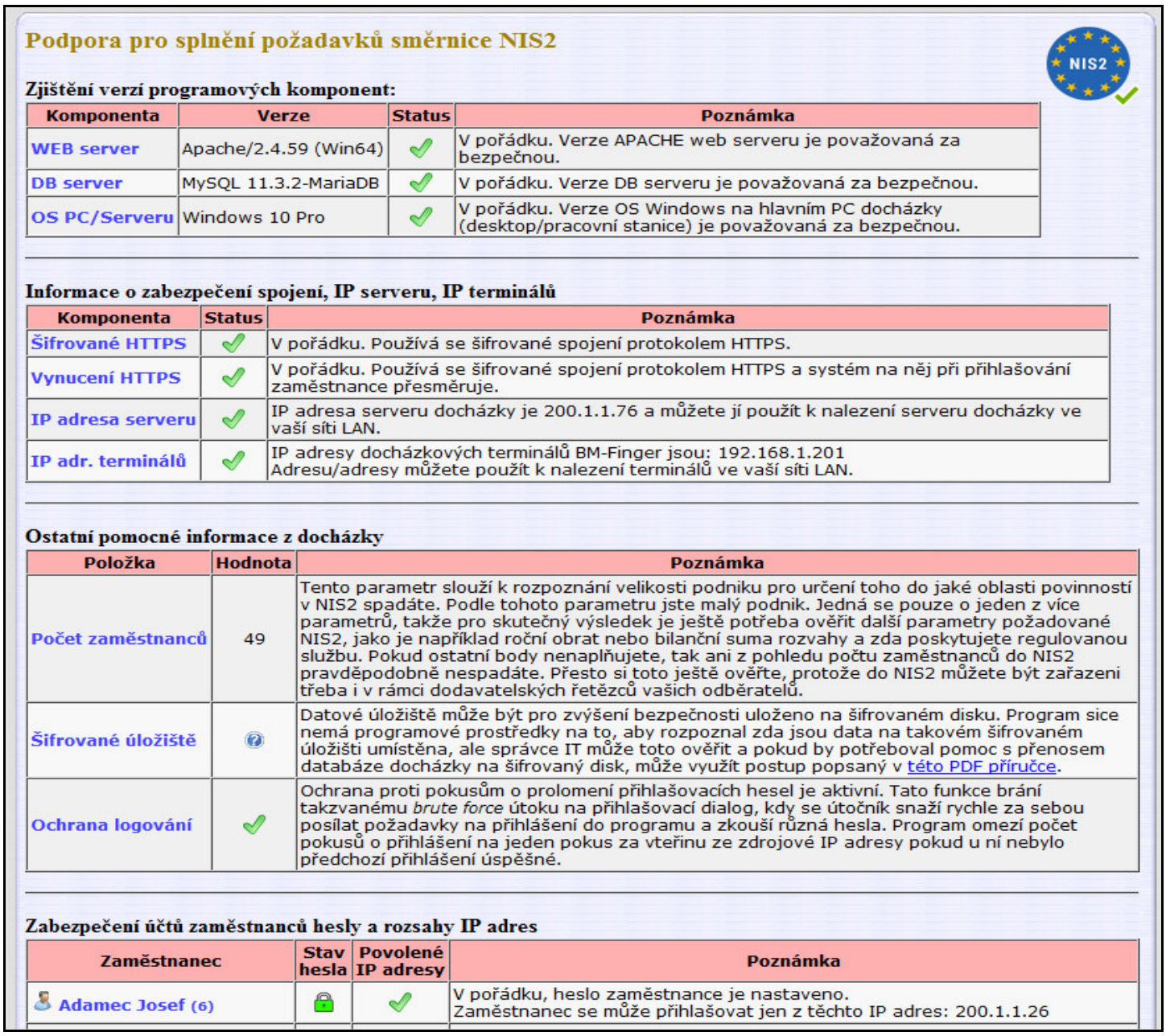
Ostatní pomocné informace z docházky

Položka	Hodnota	Poznámka
Počet zaměstnanců	49	Tento parametr slouží k rozpoznání velikosti podniku pro určení toho do jaké oblasti povinností v NIS2 spadáte. Podle tohoto parametru jste malý podnik. Jedná se pouze o jeden z více parametrů, takže pro skutečný výsledek je ještě potřeba ověřit další parametry požadované NIS2, jako je například roční obrat nebo bilanční suma rozvahy a zda poskytujete regulovanou službu. Pokud ostatní body nenaplňujete, tak ani z pohledu počtu zaměstnanců do NIS2 pravděpodobně nespadáte. Přesto si toto ještě ověřte, protože do NIS2 můžete být zařazeni třeba i v rámci dodavatelských řetězců vašich odběratelů.
Šifrované úložiště	?	Datové úložiště může být pro zvýšení bezpečnosti uloženo na šifrovaném disku. Program sice nemá programové prostředky na to, aby rozpoznal zda jsou data na takovém šifrovaném úložišti umístěna, ale správce IT může toto ověřit a pokud by potřeboval pomoc s přenosem databáze docházky na šifrovaný disk, může využít postup popsaný v této PDF příručce.
Ochrana logování	✓	Ochrana proti pokusům o prolomení přihlašovacích hesel je aktivní. Tato funkce brání takzvanému *brute force* útoku na přihlašovací dialog, kdy se útočník snaží rychle za sebou posílat požadavky na přihlášení do programu a zkouší různá hesla. Program omezí počet pokusů o přihlášení na jeden pokus za vteřinu ze zdrojové IP adresy pokud u ní nebylo předchozí přihlášení úspěšné.

Zabezpečení účtů zaměstnanců hesly a rozsahy IP adres

Zaměstnanec	Stav hesla	Povolené IP adresy	Poznámka
Adamec Josef (72)	🔓	⚠	Pozor, pracovník nemá zadané osobní heslo. Jeho přístup přes uživatelské menu může kdokoli zneužít a není nastaveno ani standardní heslo (v editaci údajů firmy) pro přístup do logování zaměstnanců. Heslo pracovníkovi nastavte v menu Zaměstnanci / Editace údajů! V personalistice není aktivní omezení pro přihlašovací IP adresy a tak program neomezuje přístup dle IP.

Cílem této dokumentace je aktualizace komponent docházky a nastavení systému tak, aby se žádný problém dále nevyskytoval a vše bylo pokud možno co nejblíže ke shodě s požadavky na zabezpečení IT systémů dle směrnice NIS2. Tedy aby výsledek testu vypadal jako na obrázku z následující strany.



Podpora pro splnění požadavků směrnice NIS2

Zjištění verzí programových komponent:

Komponenta	Verze	Status	Poznámka
WEB server	Apache/2.4.59 (Win64)	✓	V pořádku. Verze APACHE web serveru je považovaná za bezpečnou.
DB server	MySQL 11.3.2-MariaDB	✓	V pořádku. Verze DB serveru je považovaná za bezpečnou.
OS PC/Serveru	Windows 10 Pro	✓	V pořádku. Verze OS Windows na hlavním PC docházky (desktop/pracovní stanice) je považovaná za bezpečnou.

Informace o zabezpečení spojení, IP serveru, IP terminálů

Komponenta	Status	Poznámka
Šifrované HTTPS	✓	V pořádku. Používá se šifrované spojení protokolem HTTPS.
Vynucení HTTPS	✓	V pořádku. Používá se šifrované spojení protokolem HTTPS a systém na něj při přihlašování zaměstnance přesměruje.
IP adresa serveru	✓	IP adresa serveru docházky je 200.1.1.76 a můžete jí použít k nalezení serveru docházky ve vaší síti LAN.
IP adr. terminálů	✓	IP adresy docházkových terminálů BM-Finger jsou: 192.168.1.201 Adresu/adresy můžete použít k nalezení terminálů ve vaší síti LAN.

Ostatní pomocné informace z docházky

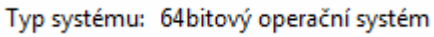
Položka	Hodnota	Poznámka
Počet zaměstnanců	49	Tento parametr slouží k rozpoznání velikosti podniku pro určení toho do jaké oblasti povinností v NIS2 spadáte. Podle tohoto parametru jste malý podnik. Jedná se pouze o jeden z více parametrů, takže pro skutečný výsledek je ještě potřeba ověřit další parametry požadované NIS2, jako je například roční obrat nebo bilanční suma rozvahy a zda poskytujete regulovanou službu. Pokud ostatní body nenaplňujete, tak ani z pohledu počtu zaměstnanců do NIS2 pravděpodobně nespadáte. Přesto si toto ještě ověřte, protože do NIS2 můžete být zařazeni třeba i v rámci dodavatelských řetězců vašich odběratelů.
Šifrované úložiště	?	Datové úložiště může být pro zvýšení bezpečnosti uloženo na šifrovaném disku. Program sice nemá programové prostředky na to, aby rozpoznal zda jsou data na takovém šifrovaném úložišti umístěna, ale správce IT může toto ověřit a pokud by potřeboval pomoc s přenosem databáze docházky na šifrovaný disk, může využít postup popsaný v této PDF příručce.
Ochrana logování	✓	Ochrana proti pokusům o prolomení přihlašovacích hesel je aktivní. Tato funkce brání takzvanému *brute force* útoku na přihlašovací dialog, kdy se útočník snaží rychle za sebou posílat požadavky na přihlášení do programu a zkouší různá hesla. Program omezí počet pokusů o přihlášení na jeden pokus za vteřinu ze zdrojové IP adresy pokud u ní nebylo předchozí přihlášení úspěšné.

Zabezpečení účtů zaměstnanců hesly a rozsahy IP adres

Zaměstnanec	Stav hesla	Povolené IP adresy	Poznámka
Adamec Josef (6)	🔒	✓	V pořádku, heslo zaměstnance je nastaveno. Zaměstnanec se může přihlašovat jen z těchto IP adres: 200.1.1.26

Bohužel pro splnění požadavků se již nepodařilo najít verze služeb fungujících na starších operačních systémech a tak nebude možné s dále uvedenými úpravami podporovat starší 32 bitové procesory a operační systémy, ale bude třeba docházku provozovat na 64 bitových systémech Windows 10 a novější nebo Windows server 2016 a novější.

Před provedením dalších kroků tedy ověřte, zda skutečně používáte 64 bitovou verzi operačního systému Windows. Například tak, že ve správci souborů kliknete pravým tlačítkem myši na ikonu *Tento počítač* a dáte volbu *Vlastnosti*. Musí se zobrazit 64 bitový typ systému



Níže uvedené postupy vyžadují docházku verze 9.50 nebo vyšší. Pokud máte nižší číslo verze, což zjistíte na úvodní obrazovce, kde je uvedeno zelenou barvou písma vedle barevného loga, nepokračujte a nejprve objednejte aktualizační CD.

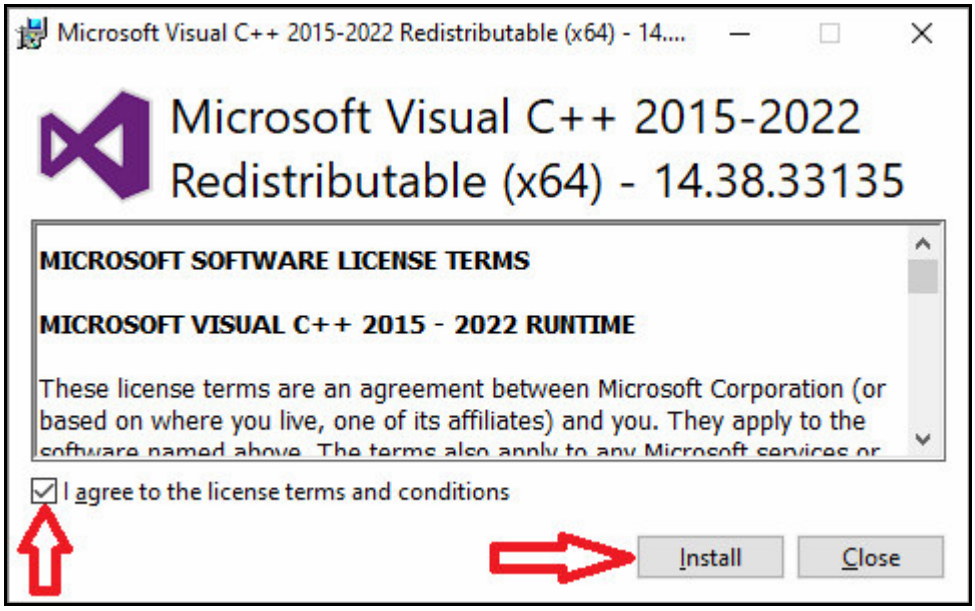
Aktualizaci Docházky 3000 na verzi 9.50 nebo vyšší, která nový Apache a TLS 1.3 podporuje, objednáte přímo v programu přes administrátorské menu *E-shop / Aktualizace SW Docházka 3000 / Koupit*

Instalace podpůrných knihoven pro nový Apache a MySQL.

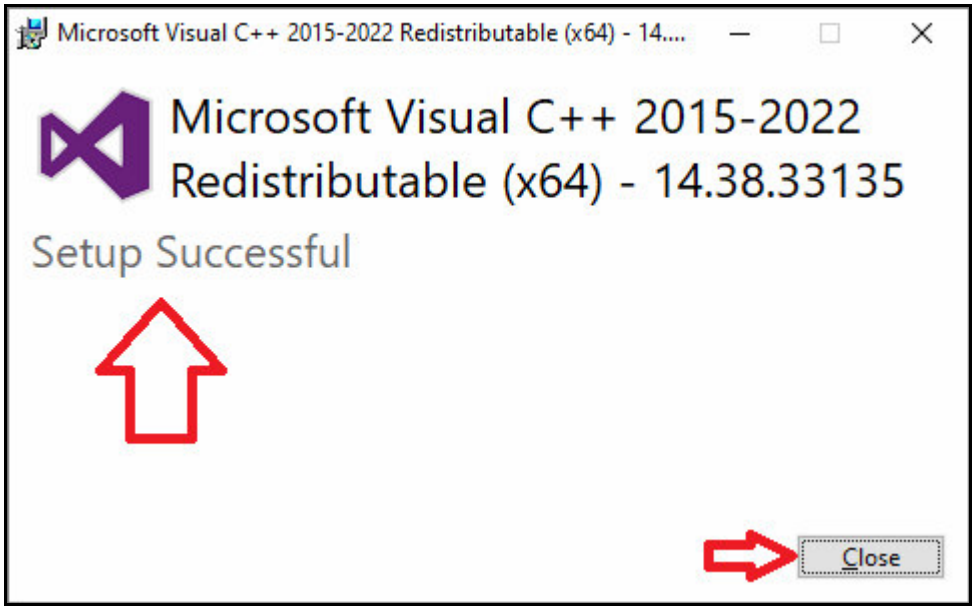
Nejprve ověřte, zda již v systému máte komponentu *Microsoft Visual C++ 2015 to 2022 Redistributable (64-bit)* verze *14.38.33135* a pokud ne, stáhnete jí pomocí tohoto odkazu:
https://www.dochazka.eu/dochazka3000/download/vc_redist_x64_2015_2022.exe

Program *vc_redist_x64_2015_2022.exe* se vám uloží pravděpodobně do složky *Stažené soubory* a odtud jej spustíte.

Po přečtení licenčních podmínek je pro instalaci nutné zatrnout volbu „*I agree to the licence terms ...*“ a poté kliknout na tlačítko *Install*



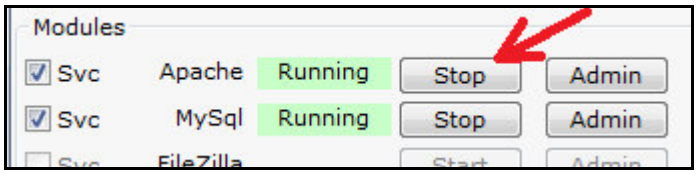
Provede se instalace a mělo být zobrazeno že proběhla úspěšně.
Poté tlačítkem *Close* instalační program ukončíte.



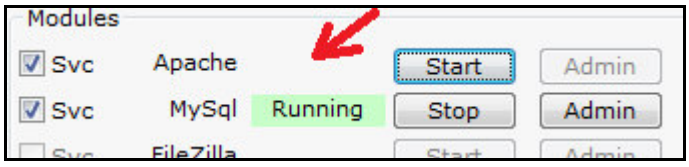
Bez instalace této komponenty by nešla spustit služba Apache v bodě D následujícího kroku a ani instalace nové verze databázového serveru MariaDB popisovaná v další části příručky by nefungovala.

Instalace nové verze Apache web serveru verze 2.4.63

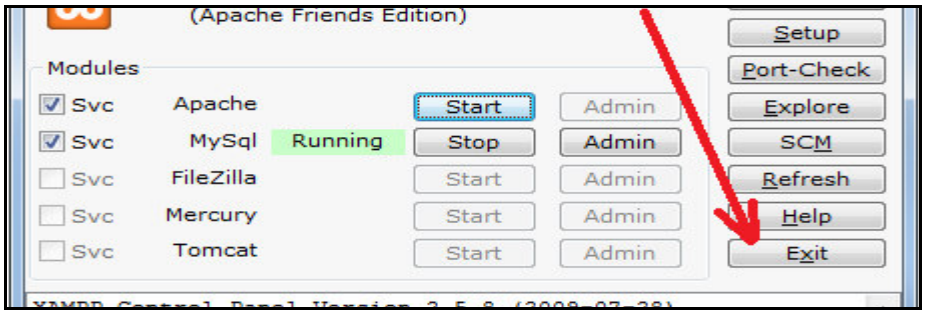
A) zastavte webový server Apache tak, že spustíte program *c:\apache\xampp-control.exe* a kliknete v něm na tlačítko *Stop* pro server Apache:



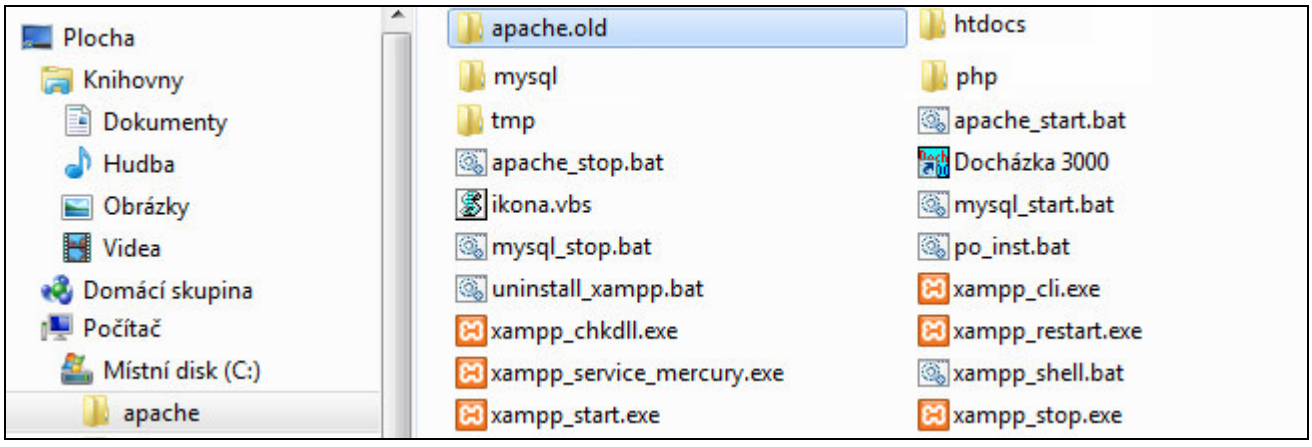
Vyčkáte, až se apache zastaví, což se pozná tak, že v jeho řádku zmizí zelený nápis *Running*



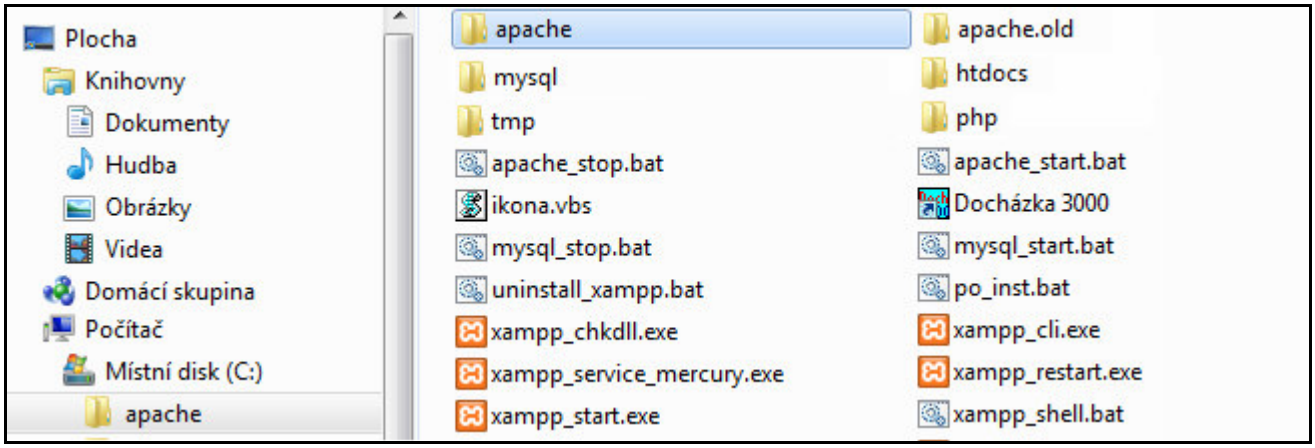
Nakonec program *Xampp-Control* ukončíte tlačítkem *Exit*



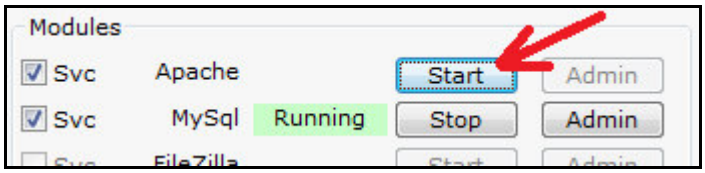
B) na disku *C:* ve složce *c:\apache* přejmenujte podsložku *c:\apache**apache*\ na *apache.old*



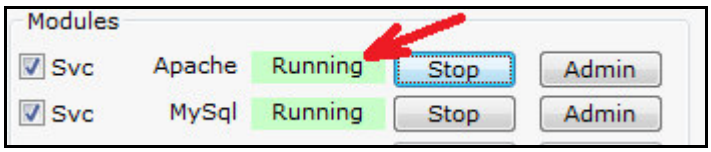
C) Stáhněte zip soubor s novou verzí Apache z webu výrobce pomocí tohoto odkazu:
https://www.dochazka.eu/dochazka3000/download/apache_2_4_63.zip
Stažený soubor rozzipujte na disk *C:* do složky *c:\apache* čímž zde vznikne nová podsložka *apache*, takže obsah *c:\apache* pak bude tento:



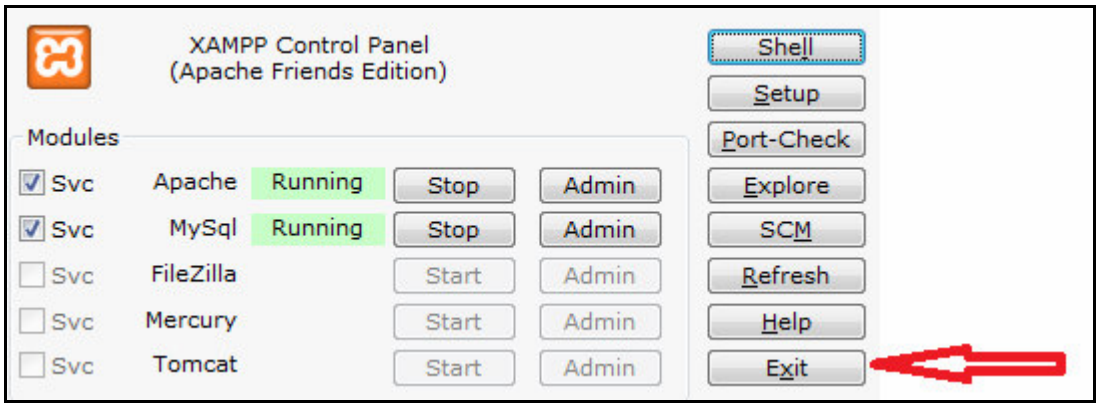
D) Opět nastartujete webový server Apache tak, že spustíte program *c:\apache\xampp-control.exe* a kliknete v něm na tlačítko *Start* pro server Apache:



Vyčkáte, až se Apache spustí, což se pozná tak, že se v jeho řádku znovu objeví zelený nápis *Running*

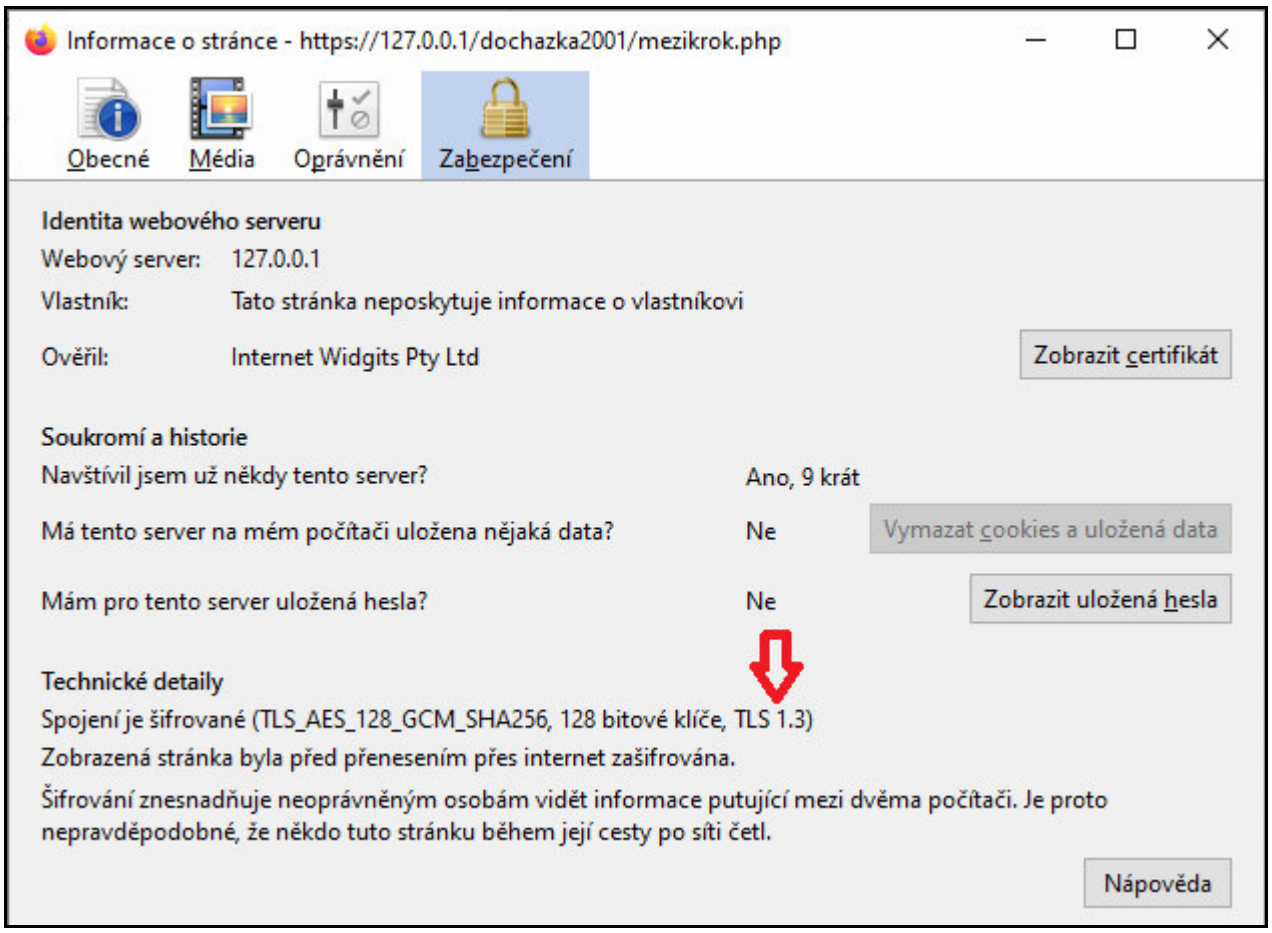


Nakonec program *Xampp-Control* opět ukončíte tlačítkem *Exit*



Pokud by se Apache nespustil, tak buď jste v předchozích krocích udělali chybu, nebo nemáte 64 bitovou verzi Windows (pak vraťte původní apache smazáním nové složky a přejmenováním původní apache.old na apache), nebo není ve windows přítomna podpora pro *Microsoft Visual C++ Redistributable Visual Studio 2015-2022* a tu stáhnete a nainstalujete z tohoto odkazu: *https://aka.ms/vs/17/release/VC_redist.x64.exe* nebo dle postupu z úvodu této příručky.

E) Pokud se apache správně spustil, měla by být docházka opět funkční, lze použít i šifrovaný https protokol a prohlížeč by měl při přístupu přes https (po odsouhlasení použití přístupu přes self-signed certifikát) podporovat spojení přes TLS verze 1.3 Viz obrázek na další straně. Samozřejmě jen v případě, že jste výše uvedený postup provedli správně



Pokud byste si chtěli vygenerovat nový self-signed certifikát, spusťte soubor *c:\apache\apache\makecert.bat*

Pro přístup z ostatních počítačů po síti LAN do docházky je ještě třeba povolit ve firewallu windows přístup na port 80 a pro přístup přes šifrovaný protokol *https* je třeba povolit port 443. Příručka je v programu Docházka 3000 v menu *Firma / Návody PDF / Přístup po síti*. U šifrovaného https protokolu vám vzhledem k self-signed certifikátu prohlížeč napíše varování, že nelze ověřit web přes důvěryhodnou autoritu. Je třeba prohlížeči i přesto přístup povolit (například schválením vyjímky v možnostech) nebo by jinak bylo nutné zajistit si certifikát od ověřovací autority (např. *Let's encrypt*). Viz dále pokyny přímo v programu v menu *Firma / Návody PDF / Nastavení HTTPS*.

Kontrola v menu *„Zaměstnanci / Nařízení GDPR / Směrnice NIS2“* již pak bude u apache psát že je vše v pořádku

Komponenta	Verze	Status	Poznámka
WEB server	Apache/2.4.63 (Win64)	✓	V pořádku. Verze APACHE web serveru je považovaná za bezpečnou.

Pokud budete přistupovat přes https, tak bude v pořádku i chráněný přístup přes šifrovaný protokol.

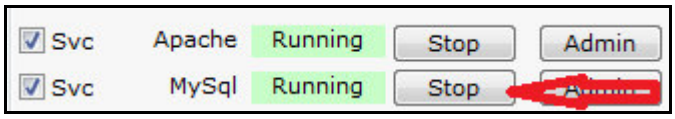
Komponenta	Status	Poznámka
Šifrované HTTPS	✓	V pořádku. Používá se šifrované spojení protokolem HTTPS.
Vynucení HTTPS	✓	V pořádku. Používá se šifrované spojení protokolem HTTPS a systém na něj při přihlašování zaměstnance přesměruje.

A když v menu *Firma / Editace údajů* zapnete položku *„Přesměrovat úvodní dialog pro přihlašování do programu na šifrovaný protokol HTTPS“* bude v pořádku i vynucení přesměrování na https z nešifrovaného http při přihlašování uživatelů.

U verzí docházky 9.75 až 9.82 lze použít stejný postup pro starší apache verze 2.4.59 který byste pro tyto starší verze stáhli zde: https://www.dochazka.eu/dochazka3000/download/apache_2_4_59.zip

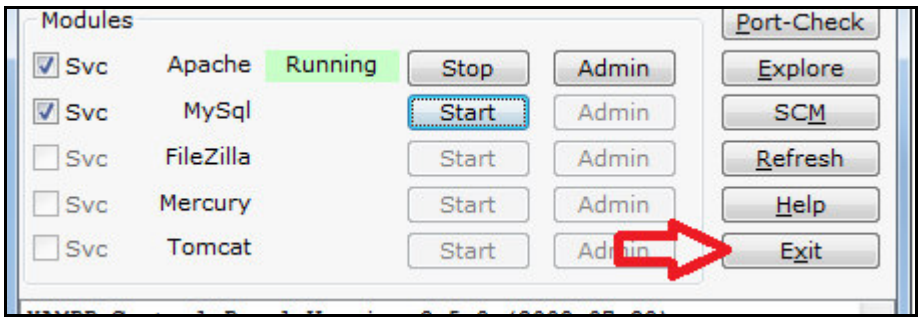
Instalace nové verze SQL databáze MariaDB verze 11.3.2

A) zastavte databázový server MySQL tak, že spustíte program *c:\apache\xampp-control.exe* a kliknete v něm na tlačítko *Stop* pro server MySQL:

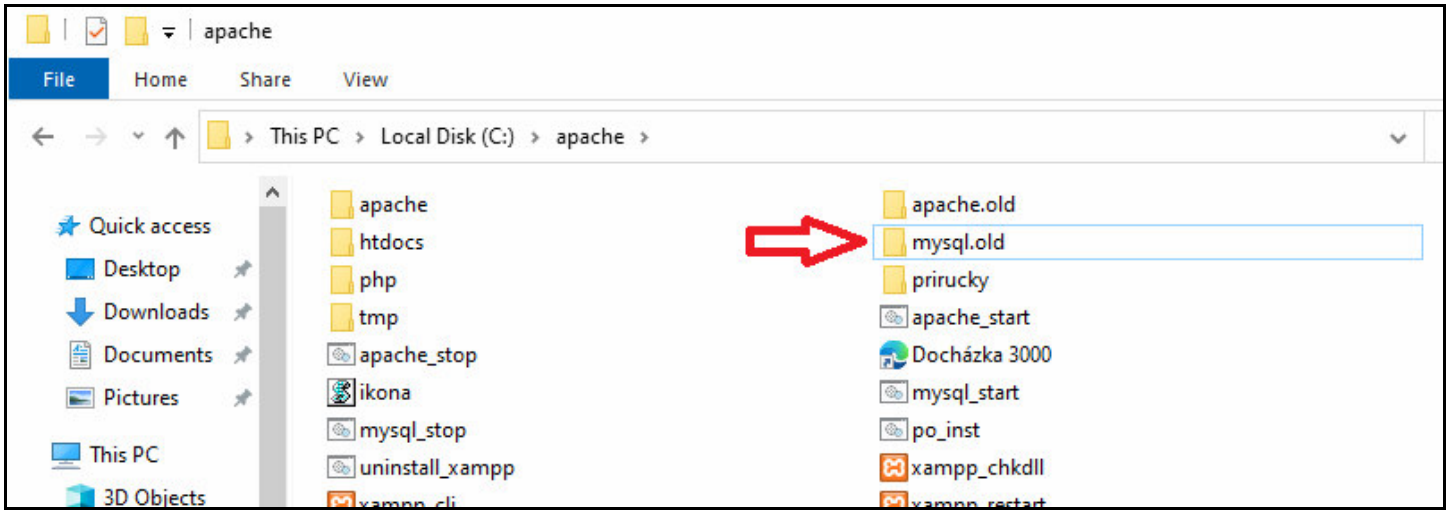


Vyčkáte, až se MySQL zastaví, což se pozná tak, že v jejím řádku zmizí zelený nápis *Running*

Nakonec program *Xampp-Control* ukončíte tlačítkem *Exit*

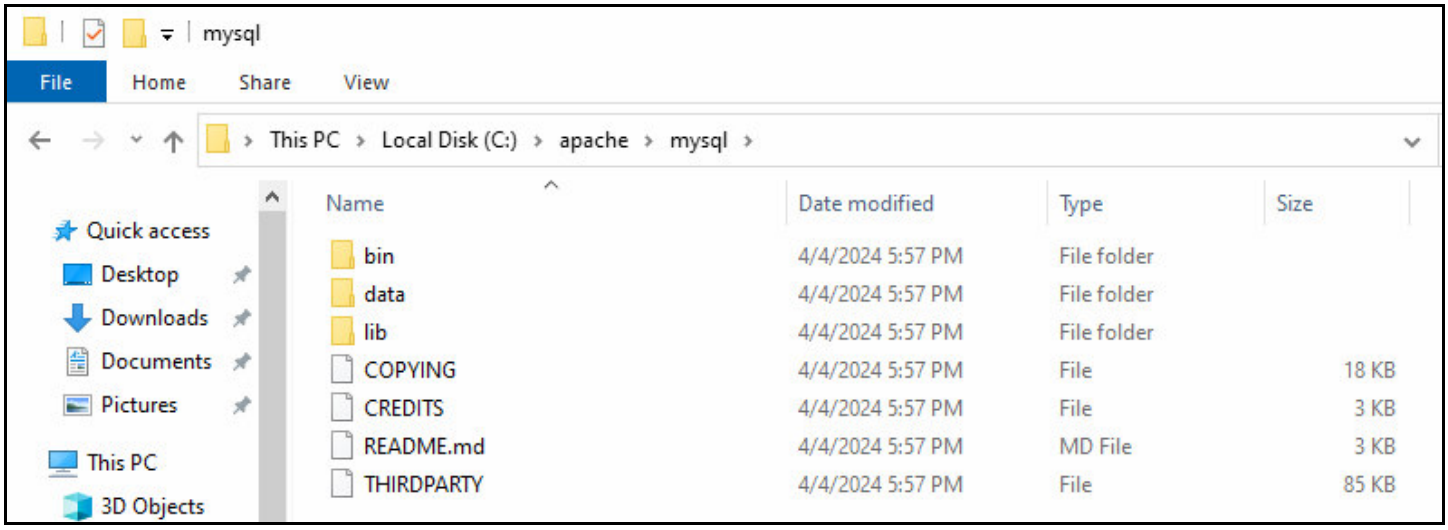


B) na disku *C:* ve složce *c:\apache* přejmenujte podsložku *c:\apache**mysql** na mysql.*old*

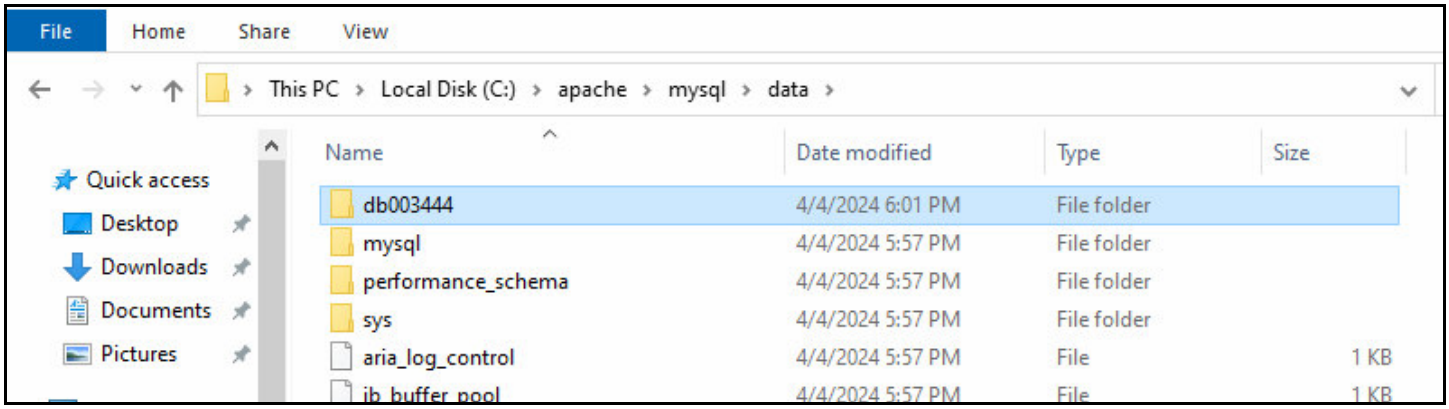


A vytvořte novou prázdnou složku *mysql*

C) Stáhněte zip soubor s novou verzí databáze MariaDB z webu výrobce pomocí tohoto odkazu:
https://www.dochazka.eu/dochazka3000/download/mariadb_11_3_2.zip
Stažený soubor rozzipujte na disk *C:* do složky *c:\apache\mysql* vytvořené nově v předchozím bodě, takže obsah *c:\apache\mysql* pak bude tento:

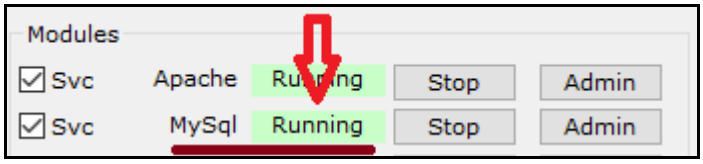


D) Do nové podsložky *c:\apache\mysql\data* nakopírujte z původní složky databáze *c:\apache\mysql.**old**\data* složku *db003444* s databází docházky. Tím se data docházky přenesou z původní staré verze MySQL do nové databáze MariaDB.

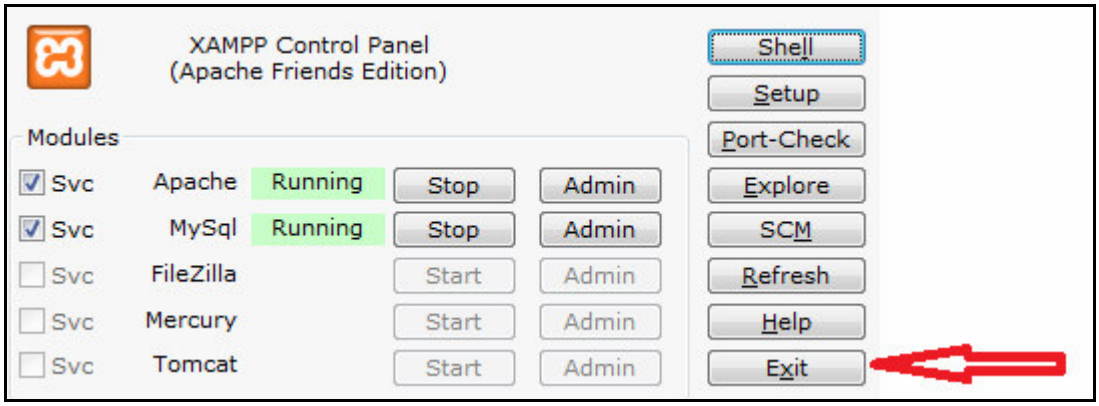


E) Opět nastartujete databázi MariaDB tak, že spustíte program *c:\apache\xampp-control.exe* a kliknete v něm na tlačítko *Start* pro službu MySQL:

Start nové služby může chvilku trvat, ale během půl minuty by měla být spuštěná. Vyčkáte tedy, až se MariaDB spustí, což se pozná tak, že se v řádku MySQL objeví zelený nápis *Running*



Nakonec program *Xampp-Control* opět ukončíte tlačítkem *Exit*



Pokud by se databáze nespustila, tak buď jste v předchozích krocích udělali chybu, nebo nemáte 64 bitovou verzi Windows (pak vraťte původní mysql smazáním nové složky a přejmenováním původní mysql.old na mysql), nebo není ve windows přítomna podpora pro *Microsoft Visual C++ Redistributable Visual Studio 2015-2022* a tu stáhnete a nainstalujete z tohoto odkazu: *https://aka.ms/vs/17/release/VC_redist.x64.exe*

F) Pokud se databáze MySQL / MariaDB správně spustila, měla by být docházka opět funkční, takže se zkuste do programu přihlásit.

Vše by mělo normálně fungovat a všechna data budou v programu dostupná. Kontrola v menu *„Zaměstnanci / Nařízení GDPR / Směrnice NIS2“* již pak bude u DB serveru psát že je vše v pořádku.

Zjištění verzí programových komponent:

Komponenta	Verze	Status	Poznámka
WEB server	Apache/2.4.59 (Win64)	✓	V pořádku. Verze APACHE web serveru je považovaná za bezpečnou.
DB server	MySQL 11.3.2-MariaDB	✓	V pořádku. Verze DB serveru je považovaná za bezpečnou.
OS PC/Serveru	Windows 10 Pro	✓	V pořádku. Verze OS Windows na hlavním PC docházky (desktop/pracovní stanice) je považovaná za bezpečnou.

Volitelná možnost nastavit heslo pro spojení D3000 do MariaDB/MySQL:

Docházka si standardně instaluje databázi tak, že přímo do databáze se nedá připojit z počítačové sítě. Funguje jen lokální spojení z aplikace docházky do databáze, ale databáze není ze sítě LAN dostupná. Pro práci s docházkou po síti není potřeba aby byla po síti dostupná přímo i samotná databáze, stačí že je dostupný Apache web server a ten už si požadavky na databázi řeší v rámci serveru, tedy jako lokální spojení. Proto u výchozích instalací je lokální přístup do databáze bez hesla a síťový přístup není do DB povolený. Pokud byste ale chtěli mít samotnou databázi přístupnou ze sítě, tedy používat jí i mimo aplikaci docházky, je z bezpečnostních důvodů bezpodmínečně nutné databázový účet *root* chránit heslem a případně použít i další nástroje DB pro síťový přístup, jako povolené IP adresy, práva k tabulkám atd. Podrobný popis tohoto nastavení je nad rámec této příručky a je k dispozici na webu *mysql.com* nebo *mariadb.org* v dokumentaci. Zde jen uvádíme, že pokud budete databázový účet *root* chránit heslem, je třeba toto heslo nastavit v Docházce 3000, aby se aplikace dokázala do databáze *db003444* lokálně připojit a měla k ní veškerá práva.

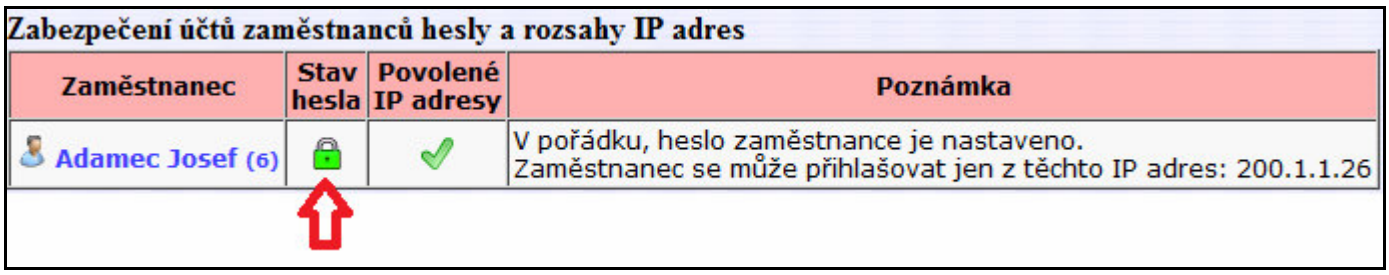
Heslo se nastaví v souboru *c:\apache\htdocs\dochazka2001\access.php* tak, že jej zapíšete do prázdného pátého řádku. Nic jiného v souboru neměňte, jinak přestane docházka fungovat i kdyby bylo heslo správně. Heslo samozřejmě nestačí nastavit jen v tomto souboru docházce, musí se nastavit i uživateli *root* v samotném databázovém serveru. Viz dokumentace k databázi na webu výrobce DB.

```
<?
/*
localhost
root
heslo
db003444
local
xg57c64c83a0b103g6
*/
?>
```

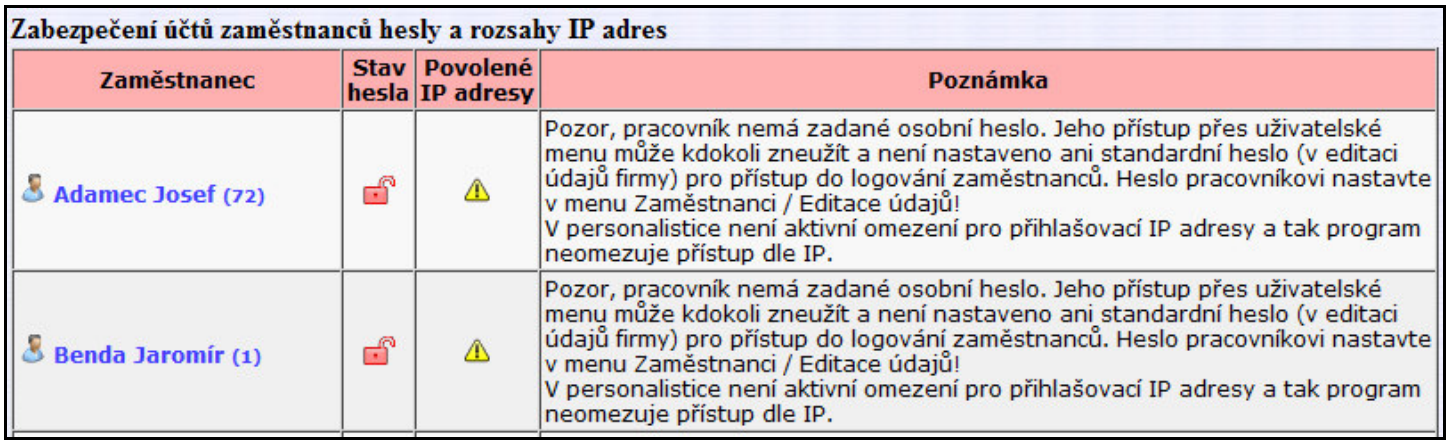
Kontrola zabezpečení uživatelských účtů

V tomto kroku zkontrolujete zda mají všichni uživatelé nastavena hesla pro přihlašování do programu a případně lze zajistit povolení přihlašování každého zaměstnance jen z jeho PC nebo ze seznamu jemu povolených počítačů k přihlášení, pokud chcete mít i tuto položku pod kontrolou.

Nejprve tedy v menu *„Zaměstnanci / Nařízení GDPR / Směrnice NIS2“* v tabulce *„Zabezpečení účtů zaměstnanců hesly a rozsahy IP adres*“ prohlédněte zda jsou u všech zaměstnanců v kolonce *Stav hesla* zobrazeny ikony zeleného zamčeného zámečku.

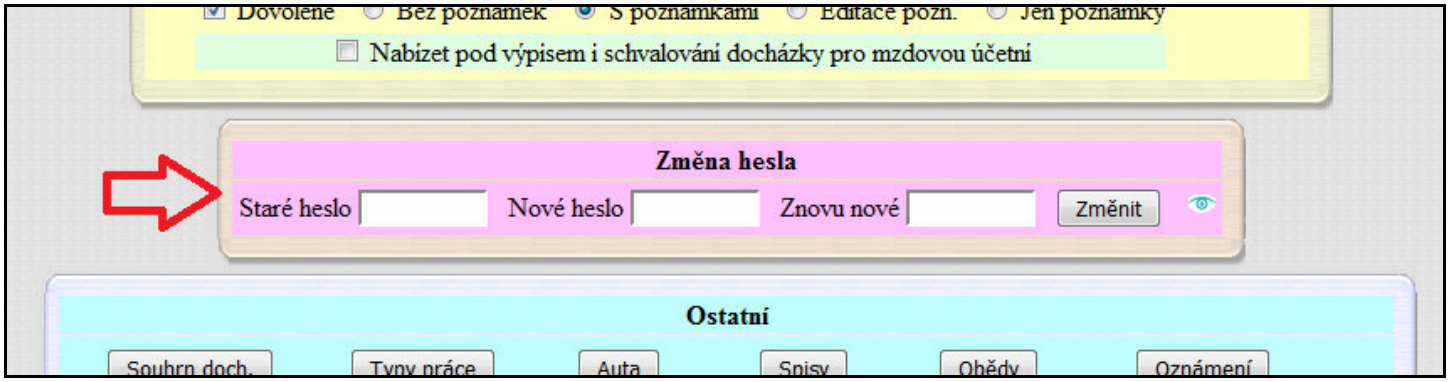


Pokud ano, hesla mají zaměstnanci nastavena. V opačném případě uvidíte ikonu červeného odemčeného zámečku:



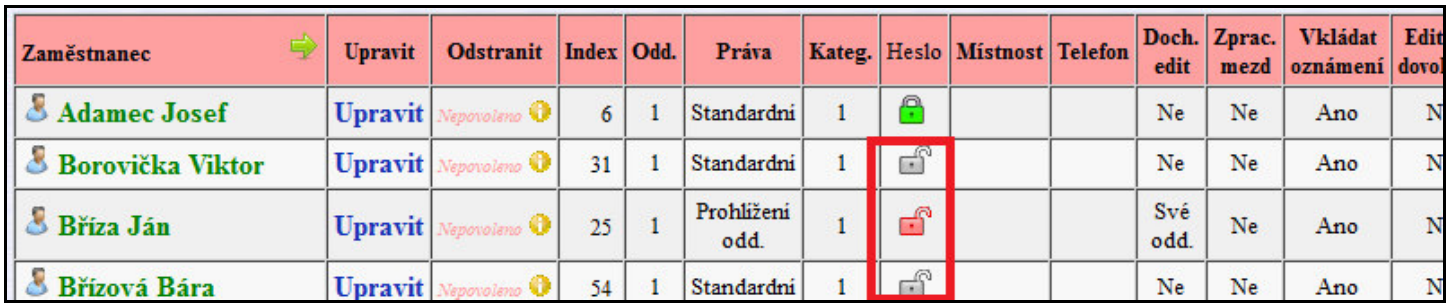
Jestli zaměstnanci s programem sami pracují, mohou si hesla nastavit sami ze svého uživatelského menu kde v modré části *Ostatní* kliknou na tlačítko *Heslo*

Zobrazí se nový rám ve kterém si pracovník může sám heslo změnit (staré heslo má prázdné)



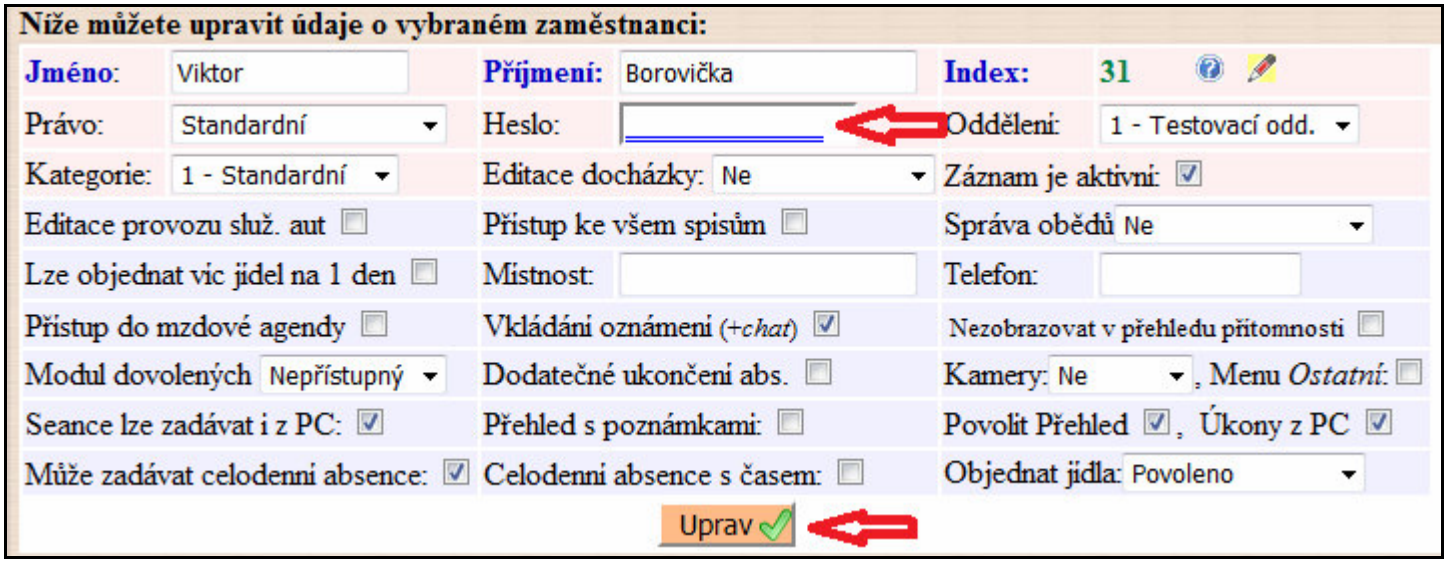
Nebo pokud nechcete čekat až si pracovníci zadají hesla dobrovolně sami, nebo když s programem ani nepracují a přesto chcete jejich účty v docházce chránit (což by bylo vhodné) můžete jako administrátor zadat hesla zaměstnancům sami nebo je nechat vygenerovat náhodně jedním kliknutím.

V menu *„Zaměstnanci / Editace údajů“* uvidíte tabulku zaměstnanců a u těch, kteří nemají heslo nastaveno, bude zobrazen buď odemčený šedivý zámeček (pracovník má jen omezené právo přístupu jen na svou docházku) nebo dokonce červený odemčený zámeček (např. vedoucí pracovník který má nějaká editační práva nebo práva prohlížení docházky ostatních).



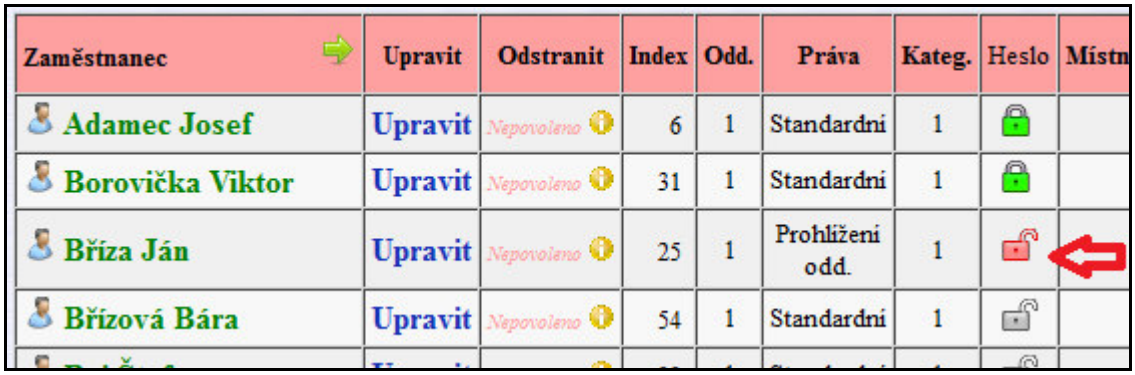
Zaměstnanec	Upravit	Odstranit	Index	Odd.	Práva	Kateg.	Heslo	Místnost	Telefon	Doch. edit	Zprac. mezd	Vkládat oznámení	Edit dovol
Adamec Josef	Upravit	Nepovoleno	6	1	Standardni	1				Ne	Ne	Ano	N
Borovička Viktor	Upravit	Nepovoleno	31	1	Standardni	1				Ne	Ne	Ano	N
Bříza Ján	Upravit	Nepovoleno	25	1	Prohlíženi odd.	1				Své odd.	Ne	Ano	N
Březová Bára	Upravit	Nepovoleno	54	1	Standardni	1				Ne	Ne	Ano	N

Pokud chcete hesla zadat pracovníkům ručně, kliknete u zaměstnance vždy na odkaz ***Upravit*** vpravo od jména a v dolním editačním formuláři heslo prostě ručně zapíšete a změnu uložíte.

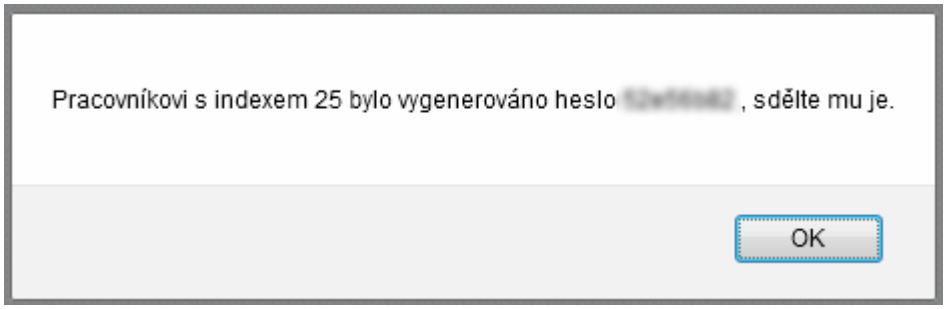


Hesla pak musíte pracovníkům sdělit, aby se měli jak do programu přihlásit. Druhou samozřejmě lepší možností je zaměstnance si zavolat a nechat jej ať heslo do kolonky napíše sám, abyste jej ani vy neznali.

V případě, kdy zaměstnanci s programem ani nepracují a jen jim chcete prostě nechat nějaká hesla vygenerovat aby účty nebyly nechráněné, stačí prostě kliknout na ikonu šedého nebo červeného odemčeného zámečku a program heslo vygeneruje sám.



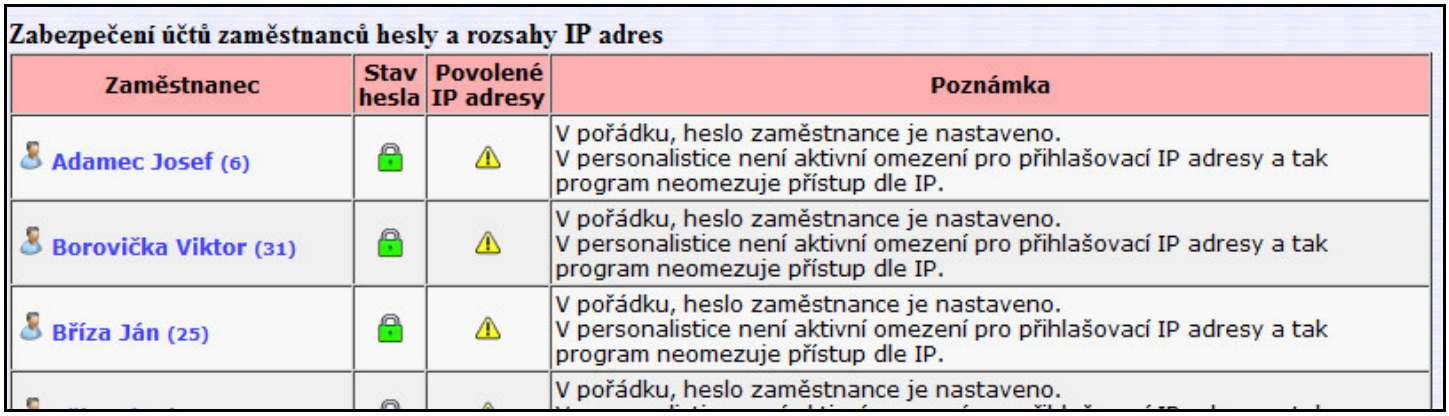
Zaměstnanec	Upravit	Odstranit	Index	Odd.	Práva	Kateg.	Heslo	Místn
Adamec Josef	Upravit	Nepovoleno	6	1	Standardni	1		
Borovička Viktor	Upravit	Nepovoleno	31	1	Standardni	1		
Bříza Ján	Upravit	Nepovoleno	25	1	Prohlíženi odd.	1		
Březová Bára	Upravit	Nepovoleno	54	1	Standardni	1		



Pokud chcete zamezit přístupu do menu přihlašování zaměstnanců, stačí v menu „*Firma / Editace údajů*“ zadat nějaké heslo do položky „*Standardní heslo*“ (a stejné do *Znovu standardní* pro kontrolu), čímž se zablokuje přístup do přihlášení do uživatelské části a pak se do programu k přihlášení dostanou jen ti vedoucí a zaměstnanci, kteří budou toto standardní heslo znát a zadají je do prvního dialogu při výběru firmy. Tímto lze bezpečnost dále posílit.

Politika hesel dle NIS2: Hesla musí být dlouhá 12 a více znaků pro uživatele, 17 pro administrátory a 22 pro technické účty. Heslo se musí měnit nejpozději po 18 měsících a znovu ho nelze použít při 12 po sobě jdoucích obměnách. Dále je povinností zamezit zadávání jednoduchých a často používaných hesel, hesel s mnohonásobně se opakujícími znaky, hesel ve kterých se používá přihlašovací jméno, e-mail, název systému a podobně.

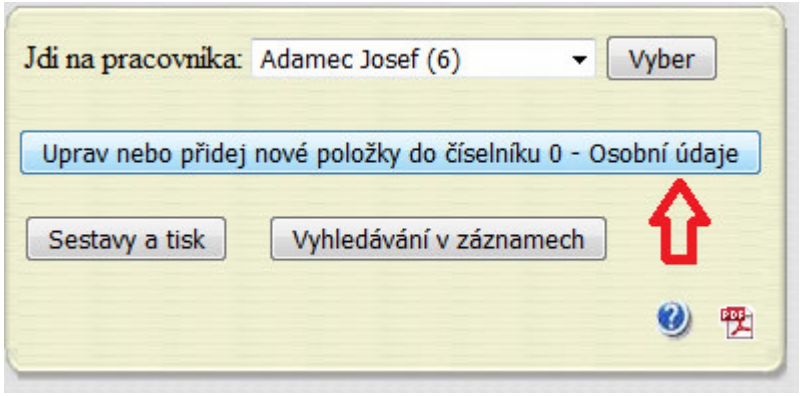
Po nastavení hesel postupně všem uživatelům již tedy můžete v menu „*Zaměstnanci / Nařízení GDPR / Směrnice NIS2*“ v tabulce „*Zabezpečení účtů zaměstnanců hesly a rozsahy IP adres*“ zkontrolovat, že všechny účty jsou chráněné heslem – je zobrazený zelený zamčený zámeček.



Zabezpečení účtů zaměstnanců hesly a rozsahy IP adres

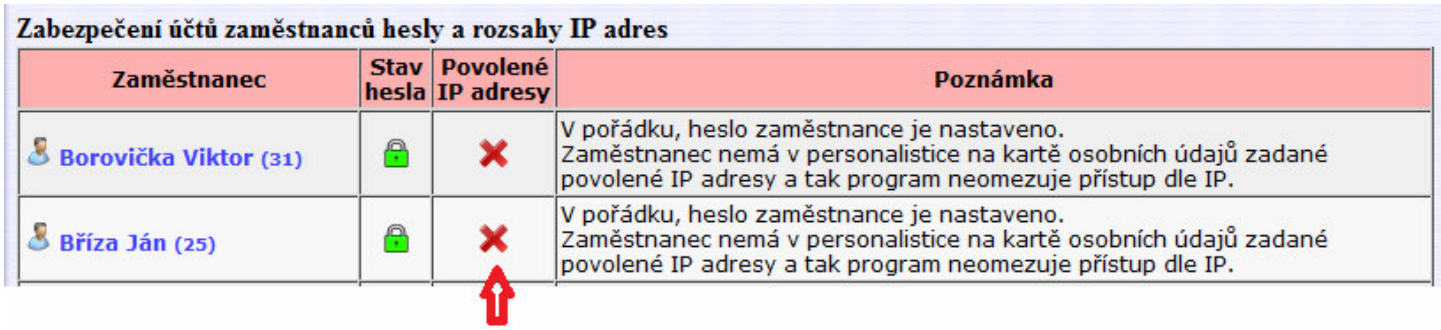
Zaměstnanec	Stav hesla	Povolené IP adresy	Poznámka
Adamec Josef (6)			V pořádku, heslo zaměstnance je nastaveno. V personalistice není aktivní omezení pro přihlašovací IP adresy a tak program neomezuje přístup dle IP.
Borovička Viktor (31)			V pořádku, heslo zaměstnance je nastaveno. V personalistice není aktivní omezení pro přihlašovací IP adresy a tak program neomezuje přístup dle IP.
Bříza Ján (25)			V pořádku, heslo zaměstnance je nastaveno. V personalistice není aktivní omezení pro přihlašovací IP adresy a tak program neomezuje přístup dle IP.
			V pořádku, heslo zaměstnance je nastaveno.

Zbývá ještě další možnost posílení zabezpečení a to ta, že můžete konkrétní pracovníky nechat přihlašovat do uživatelského menu docházky jen z povolených počítačů. Na výše uvedeném obrázku je v položce *Povolené IP adresy* zobrazený žlutý vykřičník. Nejprve je tedy potřeba nastavit číselník v personalistice na kartě osobních údajů tak, aby vůbec bylo možné IP adresy zadávat. Provedete to v menu *Zaměstnanci / Personalistka* kliknutím na tlačítko „*Uprav nebo přidej nové položky do číselníku 0-Osobní údaje*“ v dolním žlutém rámu.



Otevře se nastavení číselníku a v něm u položky 21 *IP adresa* aktivujete zatržítko *Platný* a nastavení uložíte tlačítkem *Uprav* v tomto řádku 21 vpravo.

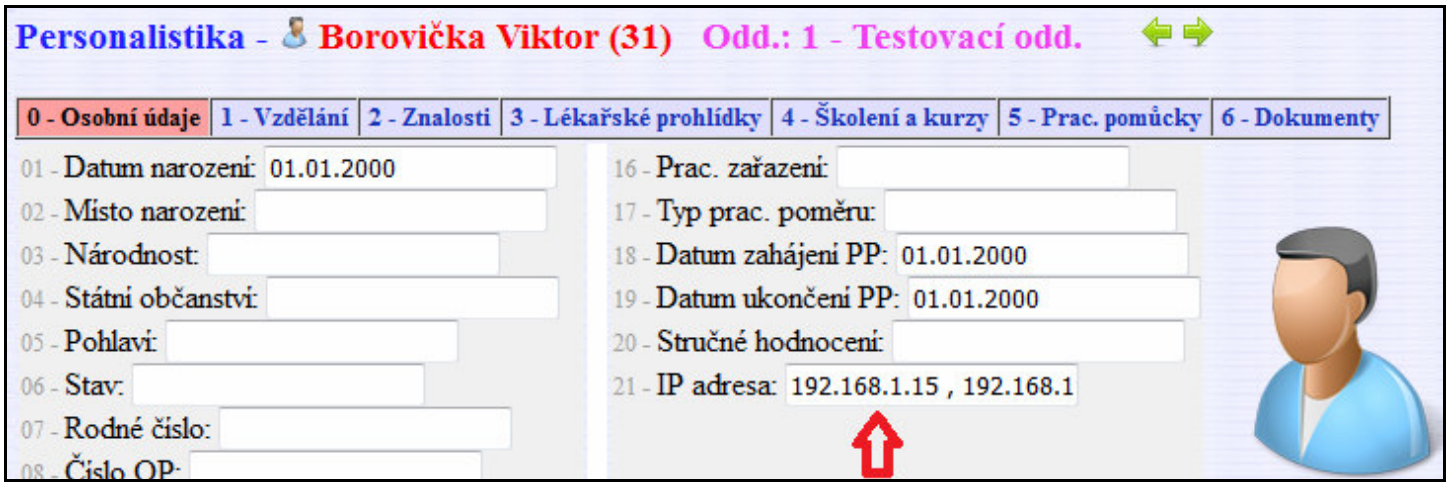
V menu „*Zaměstnanci / Nařízení GDPR / Směrnice NIS2*“ v tabulce „*Zabezpečení účtů zaměstnanců hesly a rozsahy IP adres*“ se nyní místo žlutých vykřičníků ve sloupečku pro povolené IP adresy zobrazí ikony červených křížků, což znamená že omezení na IP adresy je již povoleno ale pracovníci ještě nemají adresy nastaveny.



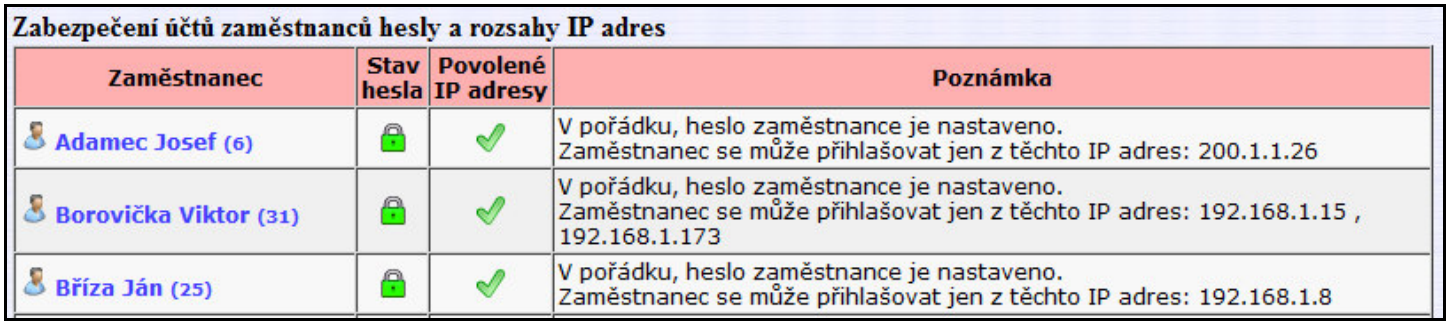
Zabezpečení účtů zaměstnanců hesly a rozsahy IP adres

Zaměstnanec	Stav hesla	Povolené IP adresy	Poznámka
Borovička Viktor (31)			V pořádku, heslo zaměstnance je nastaveno. Zaměstnanec nemá v personalistice na kartě osobních údajů zadané povolené IP adresy a tak program neomezuje přístup dle IP.
Bříza Ján (25)			V pořádku, heslo zaměstnance je nastaveno. Zaměstnanec nemá v personalistice na kartě osobních údajů zadané povolené IP adresy a tak program neomezuje přístup dle IP.

Nyní se tedy vrátíte do menu *Zaměstnanci / Personalistka* a postupně na kartách *0-Osobní údaje* jednotlivých pracovníků nastavíte IP adresy povolených počítačů. Adres lze zadat více, oddělují se čárkou. Každému zadáte ty IP adresy, které patří jeho počítači / počítačům. Předpokladem samozřejmě je, že IP adresy počítačů se nemění (jsou přiděleny staticky) a jedná se IPv4 adresy.



Jakmile budete mít povolené počítače u zaměstnanců nastaveny, bude již v menu „*Zaměstnanci / Nařízení GDPR / Směrnice NIS2*“ v tabulce „*Zabezpečení účtů zaměstnanců hesly a rozsahy IP adres*“ ve sloupečku pro povolené IP adresy místo červených křížků zobrazena zelená fajka, což znamená že povolené IP adresy počítačů pro přihlašování jsou nastaveny a v řádku pro poznámku jsou i vypsané.



Zabezpečení účtů zaměstnanců hesly a rozsahy IP adres

Zaměstnanec	Stav hesla	Povolené IP adresy	Poznámka
Adamec Josef (6)			V pořádku, heslo zaměstnance je nastaveno. Zaměstnanec se může přihlašovat jen z těchto IP adres: 200.1.1.26
Borovička Viktor (31)			V pořádku, heslo zaměstnance je nastaveno. Zaměstnanec se může přihlašovat jen z těchto IP adres: 192.168.1.15 , 192.168.1.173
Bříza Ján (25)			V pořádku, heslo zaměstnance je nastaveno. Zaměstnanec se může přihlašovat jen z těchto IP adres: 192.168.1.8

Obecně lepším postupem pro řízení povolených počítačů je ale správná konfigurace firewallu.

Tímto je základní konfigurace programu pro směrnici NIS2 dokončena.

Ostatní informace k zabezpečení

Program ale umožňuje i další kroky zabezpečení, jako například uložení dat databáze na šifrovaném úložišti (disku). Odkaz na příručku najdete v části *Ostatní pomocné informace z docházky* v řádku *Šifrované úložiště*

Ostatní pomocné informace z docházky

Položka	Hodnota	Poznámka
Počet zaměstnanců	49	Tento parametr slouží k rozpoznání velikosti podniku pro určení toho do jaké oblasti povinností v NIS2 spadáte. Podle tohoto parametru jste malý podnik. Jedná se pouze o jeden z více parametrů, takže pro skutečný výsledek je ještě potřeba ověřit další parametry požadované NIS2, jako je například roční obrat nebo bilanční suma rozvahy a zda poskytujete regulovanou službu. Pokud ostatní body nenaplňujete, tak ani z pohledu počtu zaměstnanců do NIS2 pravděpodobně nespadáte. Přesto si toto ještě ověřte, protože do NIS2 můžete být zařazeni třeba i v rámci dodavatelských řetězců vašich odběratelů.
Šifrované úložiště		Datové úložiště může být pro zvýšení bezpečnosti uloženo na šifrovaném disku. Program sice nemá programové prostředky na to, aby rozpoznal zda jsou data na takovém šifrovaném úložišti umístěna, ale správce IT může toto ověřit a pokud by potřeboval pomoc s přenosem databáze docházky na šifrovaný disk, může využít postup popsaný v této PDF příručce.
Ochrana logování		Ochrana proti pokusům o prolomení přihlašovacích hesel je aktivní. Tato funkce brání takzvanému *brute force* útoku na přihlašovací dialog, kdy se útočník snaží rychle za sebou posílat požadavky na přihlášení do programu a zkouší různá hesla. Program omezí počet pokusů o přihlášení na jeden pokus za vteřinu ze zdrojové IP adresy pokud u ní nebylo předchozí přihlášení úspěšné.

Dále je k dispozici celá řada statistik a logovacích informací o používání programu. Některé najdete v ostatních modulech menu *„Zaměstnanci / Nařízení GDPR“* . Ale základní přehled o logování je v odděleném samostatném zeleně podbarveném rámu v menu *„Zaměstnanci / Nařízení GDPR / Směrnice NIS2“* dole. Jedná se vlastně o výběr určitých okruhů z historie logování, která je s rozšířenými možnostmi dostupná v menu *„Firma / Historie logování“* kde lze dohledat úplně všechny záznamy o přihlašování do programu. Ale v menu ke směrnici pro NIS2 jsou předvybrané záznamy podle určitých kritérií tak, aby nezahltily správce zbytečným množstvím informací a vybraly jen nějakým způsobem „zajímavé“ záznamy.

V první části *Logování uživatelů do programu* je posledních 100 přihlášení. Tedy běžný klasický výpis posledních přístupů do programu

Logování uživatelů do programu (posledních 100 přihlášení)

Datum	Pracovník	IP adresa	OS info	Stav	HTTPS
04.04.2024 19:21:27	Administrátor	200.1.1.26	/	OK	
04.04.2024 19:21:24	Administrátor	200.1.1.26	/	Chyba	
04.04.2024 19:12:05	Administrátor	200.1.1.6	/	OK	
04.04.2024 18:18:27	Adamcová Jaroslava (6)	200.1.1.244	/	OK	
04.04.2024 18:18:25	Výběr zaměstnance	200.1.1.26	/	OK	
04.04.2024 11:49:01	Administrátor	200.1.1.2	/	OK	

Zde je vidět například zda byl při logování použil šifrovaný protokol (sloupeček https), jaký operační systém a typ webového prohlížeče byl použit, zda se přihlášení povedlo (uživatel zadal správné heslo) a další informace o tom kdo se kdy a z jakého PC logoval.

Zajímavější je již druhá tabulka, která se soustředí čistě na logování administrátora docházky a vypisuje všechny IP adresy počítačů které kdy byly pro přístup do administrace použity. U každé IP adresy je informace o posledním použití. Zde lze tedy dohledat i podezřelé přístupy za celou dobu používání programu.

IP adresy ze kterých se do programu logoval administrátor

IP adresa	Poslední datum	OS Info	Stav	HTTPS
127.0.0.1	11.10.2021 11:18:50	/	OK	
192.168.254.1	24.03.2021 13:21:18	/	OK	
200.1.1.1	13.01.2019 19:19:02	/	OK	
200.1.1.10	07.10.2022 10:48:21	/	OK	

Třetí tabulka zelené části zobrazuje všechny neplatné pokusy o přihlášení. Posledních 100 pokusů o logování kdy bylo použito neplatné heslo. Umožní tedy zjistit například podezřele časté nezdařené pokusy o přihlášení, takže se můžete zaměřit na sledování chování konkrétního uživatele nebo počítače ze kterého jsou tyto neplatné pokusy o přihlášení prováděny.

Posledních 100 nepovedených pokusů o přihlášení

IP adresa	Poslední datum	Poslední pracovník	OS Info	Stav	HTTPS
200.1.1.26	04.04.2024 19:27:32	Administrátor		Chyba	
200.1.1.26	04.04.2024 19:21:24	Administrátor		Chyba	
200.1.1.75	11.12.2023 17:41:03	Administrátor		Chyba	
200.1.1.75	11.12.2023 17:40:58	Administrátor		Chyba	
200.1.1.75	11.12.2023 17:40:50	Administrátor		Chyba	
200.1.1.4	14.11.2023 08:16:20	Výběr zaměstnance		Chyba Login neplatným hešem	
200.1.1.26	14.11.2023 08:16:06	Výběr zaměstnance		Chyba Login neplatným hešem	
200.1.1.4	14.11.2023 08:09:53	Výběr zaměstnance		Chyba Login neplatným hešem	
200.1.1.4	13.11.2023 18:40:20	Výběr zaměstnance		Chyba Login neplatným hešem	
200.1.1.4	13.11.2023 18:38:15	Výběr zaměstnance		Chyba Login neplatným hešem	
200.1.1.26	02.11.2023 09:34:54	Abrahám Adam (1134)		Chyba	
200.1.1.26	26.10.2023 18:53:29	Abrahám Josef (840)		Chyba	
200.1.1.4	26.10.2023 17:14:32	Komosná Oldřiška (10)		Chyba	
200.1.1.4	24.10.2023 12:17:03	Abrahám Adam (1134)		Chyba	
200.1.1.26	19.10.2023 10:57:35	Abrahám Adam (1134)		Chyba	
200.1.1.26	19.10.2023 10:57:30	Komosná Oldřiška (10)		Chyba	

Čtvrtá tabulka zase vybírá jen přihlášení provedená mimo lokální síť, pro každou externí adresu jeden záznam s posledním nejnovějším přihlášením. Jedná se tedy o seznam veřejných internetových adres ze kterých se kdy do programu přistupovalo a kdy se do programu hlásil někdo vzdáleně, nikoli z počítačů uvnitř vaší firemní sítě.

Přístupy z veřejných IP adres

IP nezačínající *192.168. , 10. , 127. , 172.*

IP adresa	Poslední datum	Poslední pracovník	OS Info	Stav	HTTPS
200.1.1.1	13.01.2019 19:19:02	Administrátor		OK	
200.1.1.10	07.10.2022 10:48:21	Administrátor		OK	
200.1.1.100	25.12.2018 13:49:31	Administrátor		OK	
200.1.1.109	01.11.2017 17:38:32	Administrátor		OK	
200.1.1.11	16.04.2021 18:06:39	Blatný Josef (853)		OK	
200.1.1.118	08.04.2017 09:37:34	Administrátor		OK	
200.1.1.129	28.11.2016 16:49:51	Administrátor		OK	
200.1.1.130	31.03.2017 11:19:38	Zich Karel (809)		OK	
200.1.1.138	02.02.2017 11:12:30	Administrátor		OK	
200.1.1.143	25.01.2018 14:32:25	Administrátor		OK	
200.1.1.146	27.12.2017 18:19:44	Administrátor		OK	
200.1.1.149	12.03.2019 17:46:57	Administrátor		OK	
200.1.1.150	03.04.2021 14:17:28	Administrátor		OK	
200.1.1.153	18.03.2019 15:00:00	Administrátor		OK	

Výše uvedené logy tedy mohou pomoci při detekování bezpečnostních incidentů a pro ujištění, zda je program opravdu používaný jen z těch počítačů které máte ve své správě. Tyto logy mohou být IT specialistům velmi nápomocné při zabezpečování počítačové sítě. Zobrazení všech logování do programu s možností vyhledávání najdete, jak již bylo uvedeno, v programu v menu „*Firma / Historie logování*“.

Samozřejmě při kontrolách a auditech nestačí jen vědět kdo se kdy do programu hlásil, ale je dobré mít i informaci o tom co v programu dělal a na jaká data se díval, případně na jaká data má právo se dívat i kdyby se zatím o toto nepokusil. Tato část souvisí do značné míry i s ochranou osobních údajů a tak je řešená v ostatních modulech v menu *Zaměstnanci / Nařízení GDPR*. Abychom zde nedublovali dokumentaci k této problematice, tak podrobný popis najdete v PDF příručce v menu *Zaměstnanci / Nařízení GDPR / Dokumentace*.

Zde tedy stručně informace o tom, že základní přehled toho kdo má právo na přístup do vybraných modulů systému ve kterých mohou být osobní údaje jiných zaměstnanců, naleznete v menu *Zaměstnanci / Nařízení GDPR / Ověření práv OÚ*

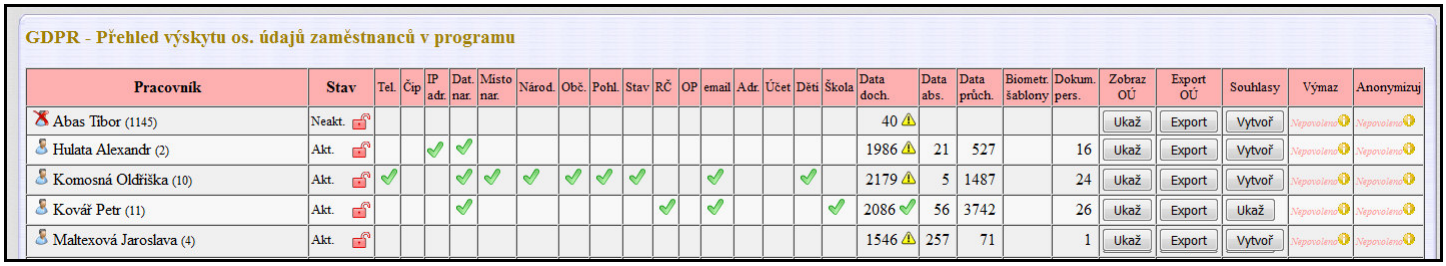
GDPR - Přehled práv umožnujících přístup k os. údajům jiných zaměstnanců

Pracovník	Stav	Editace zaměstnanců	Personalista vedoucí	Personalista administrátor	Záloha databáze	Export DB do XML	Export DB do Json	Správa term. BM-Finger	Analýza OLAP	Přidělování admin. práv	Modul GDPR	Spisy	Mzdy	Oznámení	Jiná práva administrace
Abrahám Adam (1134)	Akt.														
Abrahám Josef (840)	Akt.	✓	✓					✓	✓		✓	✓	✓		✓
Adamcová Jaroslava (6)	Akt.								✓						✓

Logy skutečně provedených přístupů do modulů s těmito daty a typy provedených akcí určitého správce na datech konkrétního zaměstnance najdete v menu *Zaměstnanci / Nařízení GDPR / Logy přístupu*

Datum	Čas	Správce	IP adresa	Pracovník	Akce	Modul
01.02.2024	04:21:31	Administrátor	200.1.1.4	Adamcová Jaroslava (6)	Editace	Admin. / Zaměstnanci / Editace údajů
01.02.2024	04:25:27	Administrátor	200.1.1.4	Adamcová Jaroslava (6)	Zobrazení	Admin. / Zaměstnanci / Personalistika
01.02.2024	04:32:15	Administrátor	200.1.1.4	Zich Karel (809)	Editace	Admin. / Zaměstnanci / Editace údajů
01.02.2024	05:20:08	Administrátor	200.1.1.4	Abas Tibor (1145)	Editace	Admin. / Zaměstnanci / Editace údajů
01.02.2024	09:40:14	Adamcová Jaroslava (6)	200.1.1.4	Adamcová Jaroslava (6)	Vložení ab.	Uživ.menu / Prohlížení docházky / Vložení absence
01.02.2024	09:40:33	Blatný Josef (853)	200.1.1.4	Blatný Josef (853)	Vložení ab.	Uživ.menu / Prohlížení docházky / Vložení absence
01.02.2024	09:45:07	Abrahám Josef (840)	200.1.1.4	Abrahám Josef (840)	Vložení ab.	Uživ.menu / Prohlížení docházky / Vložení absence
01.02.2024	09:47:08	Maltexová Jaroslava (4)	200.1.1.4	Abrahám Josef (840)	Editace	Uživ.menu / Editace docházky
01.02.2024	09:49:36	Maltexová Jaroslava (4)	200.1.1.4	Abas Tibor (1145)	Editace	Uživ.menu / Editace docházky

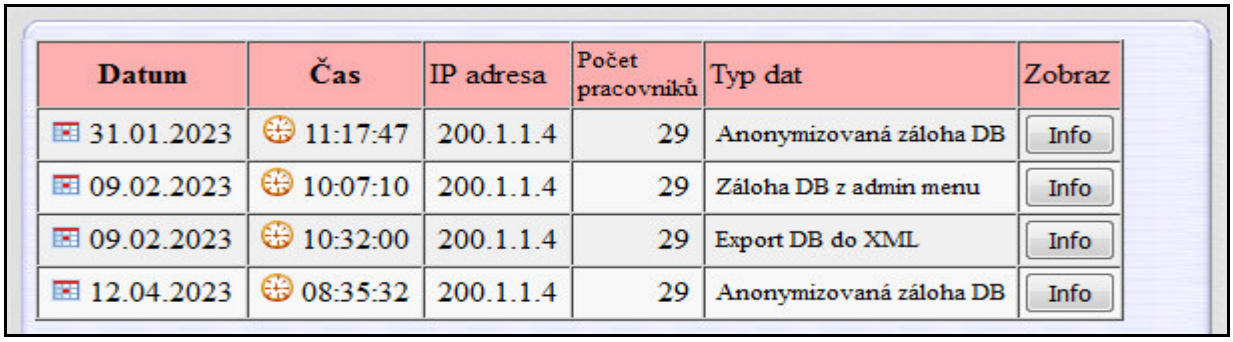
Přehled uložených osobních údajů v databázi u jednotlivých zaměstnanců je v menu *Zaměstnanci / Nařízení GDPR / Osobní údaje*



GDPR - Přehled výskytu os. údajů zaměstnanců v programu

Pracovník	Stav	Tel.	Čip	IP adr.	Dat. nar.	Místo nar.	Národ.	Obč.	Pohl.	Stav	RČ	OP	email	Adr.	Účet	Děti	Škola	Data doch.	Data abs.	Data průch.	Biometr. šablony	Dokum. pers.	Zobraz OÚ	Export OÚ	Souhlasy	Výmaz	Anonymizuj
Abas Tibor (1145)	Neakt.																	40 ⚠					Ukaž	Export	Vytvoř	Nepovoleno	Nepovoleno
Hulata Alexandr (2)	Akt.			✓	✓													1986 ⚠	21	527		16	Ukaž	Export	Vytvoř	Nepovoleno	Nepovoleno
Komosná Oldřiška (10)	Akt.	✓			✓	✓	✓	✓	✓	✓			✓			✓		2179 ⚠	5	1487		24	Ukaž	Export	Vytvoř	Nepovoleno	Nepovoleno
Kovář Petr (11)	Akt.				✓						✓		✓				✓	2086 ✓	56	3742		26	Ukaž	Export	Ukaž	Nepovoleno	Nepovoleno
Maltexová Jaroslava (4)	Akt.																	1546 ⚠	257	71		1	Ukaž	Export	Vytvoř	Nepovoleno	Nepovoleno

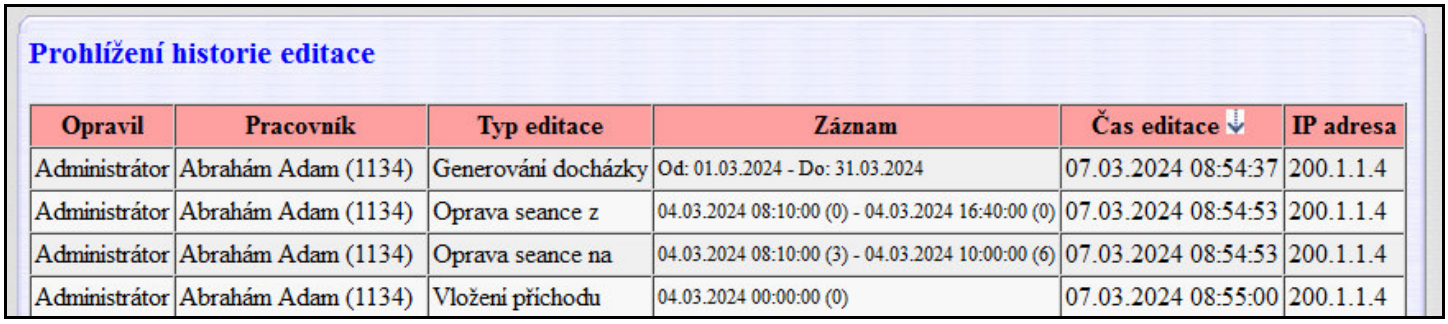
A program uchovává i informace o zálohách databáze provedených přes jeho menu, datum a typ zálohy atd., což je v menu *Zaměstnanci / Nařízení GDPR / Evidence záloh DB*



Datum	Čas	IP adresa	Počet pracovníků	Typ dat	Zobraz
31.01.2023	11:17:47	200.1.1.4	29	Anonymizovaná záloha DB	Info
09.02.2023	10:07:10	200.1.1.4	29	Záloha DB z admin menu	Info
09.02.2023	10:32:00	200.1.1.4	29	Export DB do XML	Info
12.04.2023	08:35:32	200.1.1.4	29	Anonymizovaná záloha DB	Info

Kde lze přes tlačítko *Info* zobrazit jmenný seznam zaměstnanců jejichž data jsou v té které záloze uložena.

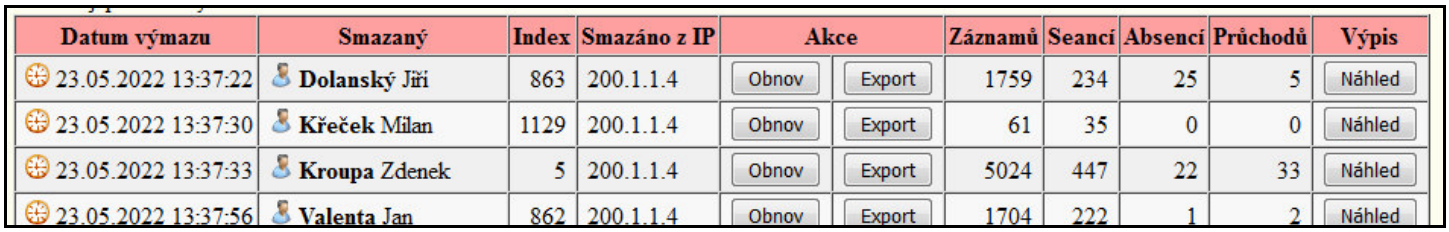
Logují se i konkrétní změny docházkových dat, tedy kdo a kdy a z jakého PC provedl vložení, výmaz či opravu jakého záznamu a u oprav i to jak vypadal záznam před opravou a na co byl opraven. Tento log se nachází v menu *Zaměstnanci / Editace docházky / Historie oprav*



Prohlížení historie editace

Opravil	Pracovník	Typ editace	Záznam	Čas editace	IP adresa
Administrátor	Abrahám Adam (1134)	Generování docházky	Od: 01.03.2024 - Do: 31.03.2024	07.03.2024 08:54:37	200.1.1.4
Administrátor	Abrahám Adam (1134)	Oprava seance z	04.03.2024 08:10:00 (0) - 04.03.2024 16:40:00 (0)	07.03.2024 08:54:53	200.1.1.4
Administrátor	Abrahám Adam (1134)	Oprava seance na	04.03.2024 08:10:00 (3) - 04.03.2024 10:00:00 (6)	07.03.2024 08:54:53	200.1.1.4
Administrátor	Abrahám Adam (1134)	Vložení příchodu	04.03.2024 00:00:00 (0)	07.03.2024 08:55:00	200.1.1.4

Pokud byste potřebovali data již smazaných zaměstnanců, najdete vše v menu *Zaměstnanci / Editace údajů / Vymazaní zaměstnanci – Archiv*. Kde lze přes *Náhled* prohlédnout docházku a přes *Obnov* přenést zaměstnance zpět do aktivní databáze k podrobnější analýze všech na něj navázaných dat. Takže ani smazáním zaměstnance se jeho data neztratí a lze je kdykoli znovu prohlédnout.



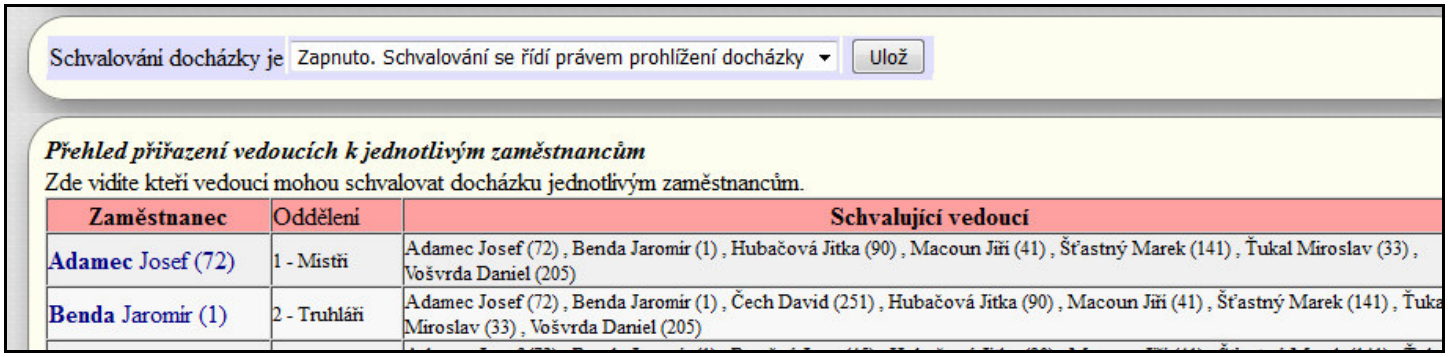
Datum výmazu	Smazaný	Index	Smazáno z IP	Akce		Záznamů	Seancí	Absencí	Průchodů	Výpis
23.05.2022 13:37:22	**Dolanský** Jiří	863	200.1.1.4	Obnov	Export	1759	234	25	5	Náhled
23.05.2022 13:37:30	**Křeček** Milan	1129	200.1.1.4	Obnov	Export	61	35	0	0	Náhled
23.05.2022 13:37:33	**Kroupa** Zdenek	5	200.1.1.4	Obnov	Export	5024	447	22	33	Náhled
23.05.2022 13:37:56	**Valenta** Jan	862	200.1.1.4	Obnov	Export	1704	222	1	2	Náhled

Co se týče logování pohybu zaměstnanců, tak v menu *Ostatní / Průchody* dohledáte nejrůznější záznamy které souvisí nejen s čipováním docházky (příchodů a odchodů), případně přerušení a absencí, ale pokud je systém napojený i na přístupové terminály pro otevírání dveří, pak je zde vidět s přesností na vteřiny kdo kdy kterými dveřmi prošel nebo kdy si čipoval docházku.

Přehled průchodů

Datum	Pracovník	Stanoviště	Akce	Kód
24.04.2020 08:06:56	Erben Karel Jaromir (2)	1 - BM-F900	Odchod	0|0
24.04.2020 08:59:01	Erben Karel Jaromir (2)	1 - BM-F900	Příchod	0|0
24.04.2020 10:50:48	Pavlik Antonin (20)	10 - Nezadané	Otevření	Otevřeno
24.04.2020 13:32:07	Císařová Karolina (10)	1 - BM-F900	Příchod	0|0
24.04.2020 13:35:14	Pavlik Antonin (20)	11 - Nezadané	Otevření	Otevřeno
24.04.2020 13:36:09	Císařová Karolina (10)	1 - BM-F900	Odchod	0|0

V programu lze i pro každého zaměstnance dohledat kdo se může dívat na jeho docházku nebo i kdo jí může editovat. Pokud v menu *Firma / Schvalování docházky* nastavíte položku *„Schvalování docházky je“* na volbu *„Zapnuto. Schvalování se řídí právem prohlížení docházky“*, zobrazí se u každého pracovníka seznam těch, kteří se dostanou na jeho docházková data.



Schvalování docházky je Zapnuto. Schvalování se řídí právem prohlížení docházky Ulož

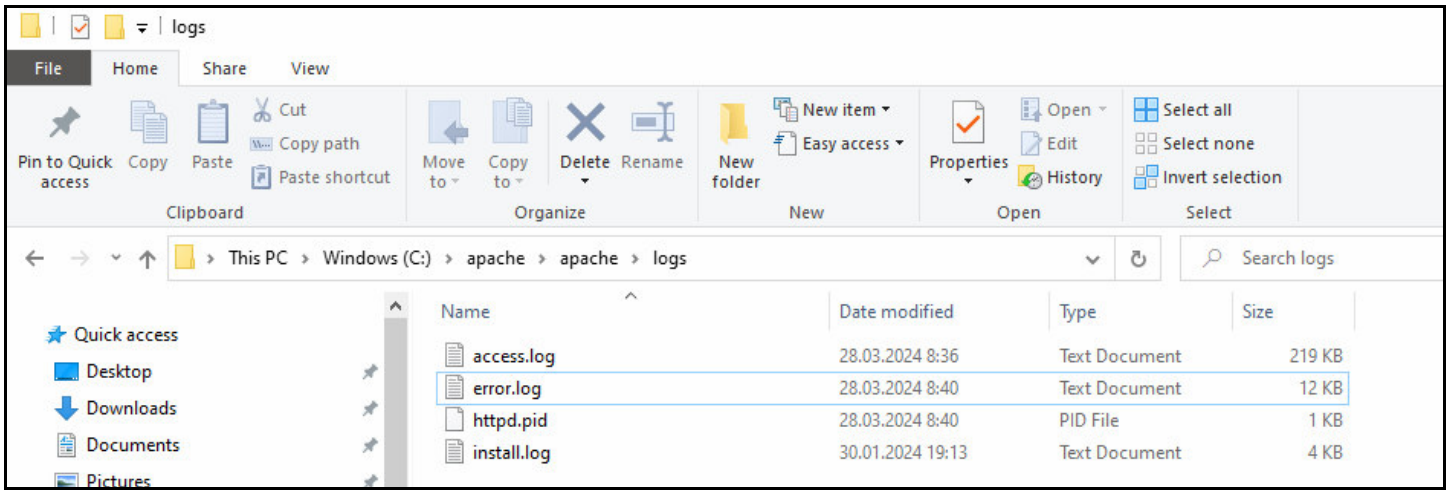
Přehled přiřazení vedoucích k jednotlivým zaměstnancům

Zde vidíte kteří vedoucí mohou schvalovat docházku jednotlivým zaměstnancům.

Zaměstnanec	Oddělení	Schvalující vedoucí
Adamec Josef (72)	1 - Mistři	Adamec Josef (72) , Benda Jaromír (1) , Hubačová Jitka (90) , Macoun Jiří (41) , Šťastný Marek (141) , Ťukal Miroslav (33) , Vošvrda Daniel (205)
Benda Jaromír (1)	2 - Truhláři	Adamec Josef (72) , Benda Jaromír (1) , Čech David (251) , Hubačová Jitka (90) , Macoun Jiří (41) , Šťastný Marek (141) , Ťuka Miroslav (33) , Vošvrda Daniel (205)

Přepnutím na volbu pro právo editace docházky pak zjistíte kdo může komu docházku editovat.

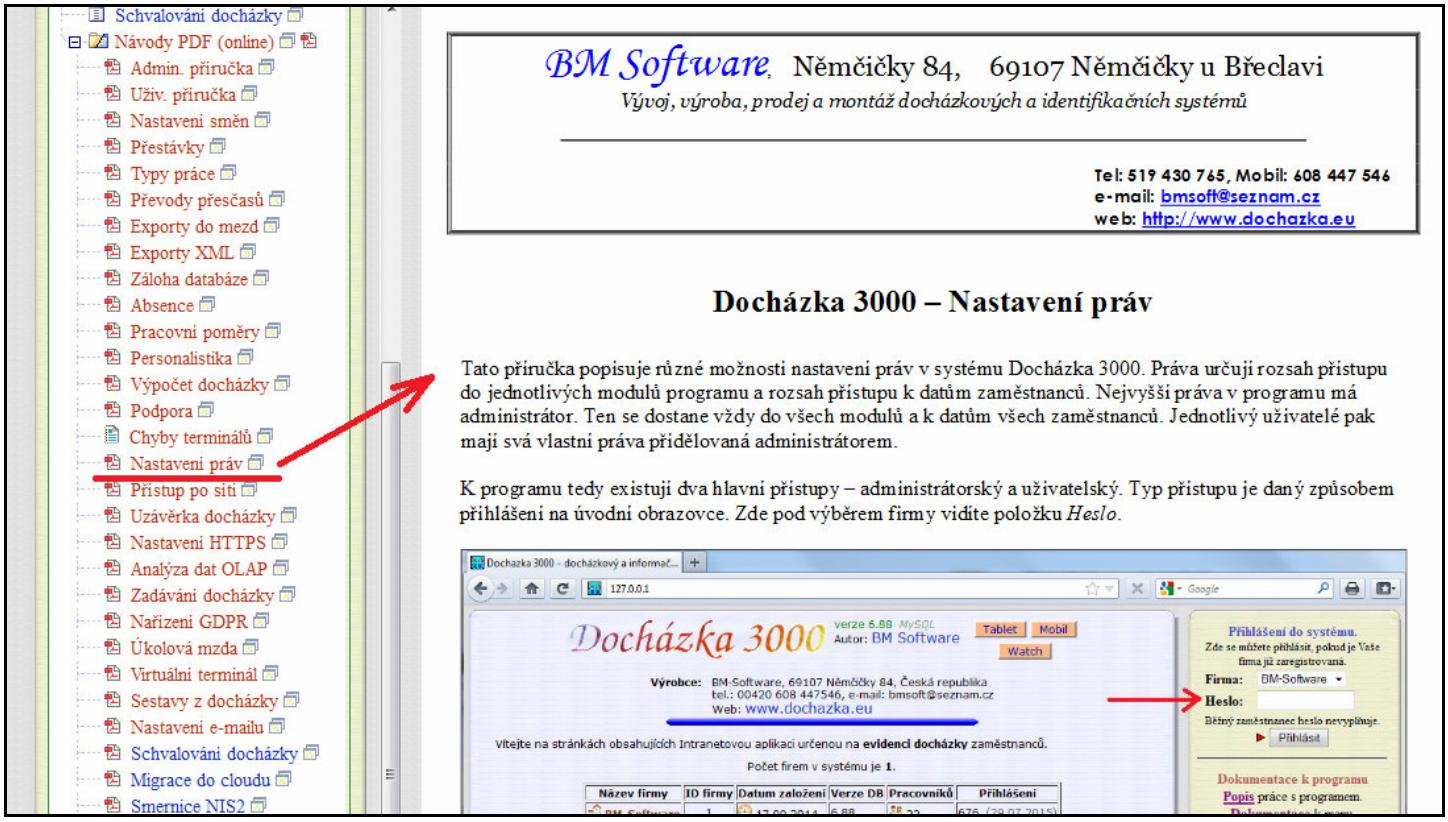
Program v těchto výše uvedených modulech eviduje většinu událostí a umožní v nich i vyhledávat a třídit záznamy. Pokud ovšem potřebujete ještě daleko podrobnější informace o přístupu na webový server docházky, tak další množství informací, tentokrát pro více technicky zdatné správce IT, naleznete přímo v logu apache web serveru. Ten se nachází na hlavním PC docházky (serveru) na disku C:\ ve složce *c:\apache\apache\logs*



Je zde několik souborů, minimálně soubor *access.log* s platnými voláními na existující adresy a soubor *error.log* s chybovými zprávami. I ten může být při zjišťování o podrobnostech o případných kybernetických útocích důležitý, protože zde se logují všechny nezdařené pokusy o načtení stránek které nejsou součástí docházky. Na serverech otevřených do internetu bez dalšího náležitého zabezpečení zde časem bývá opravdu obrovská spousta záznamů. Tyto dva log soubory mohou posloužit jako vodítko pro IT specialisty při řešení incidentů a hledání slabých míst v zabezpečení sítí.

Nastavení práv zaměstnanců pro přístup k funkcím programu:

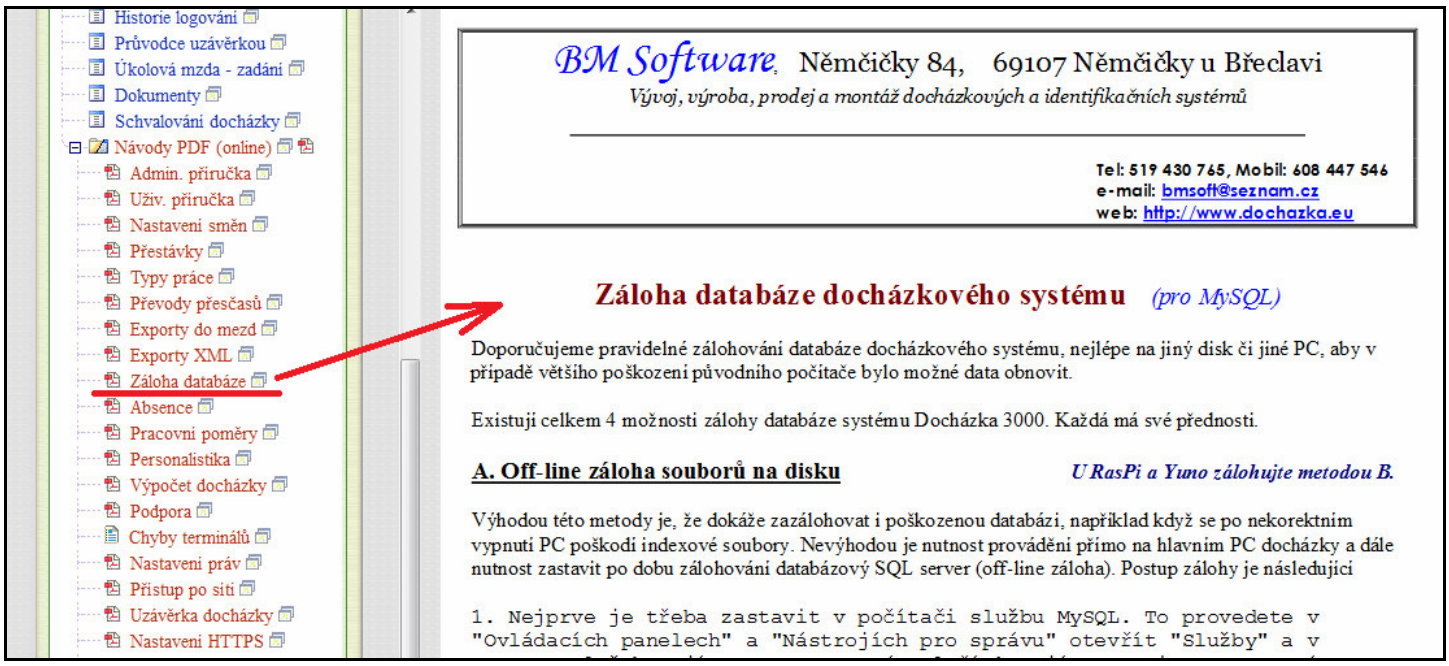
Program samozřejmě umožňuje nastavit zaměstnancům různá práva pro přístup k jednotlivým modulům a tím pádem to, jaká data kdo může prohlížet nebo editovat či mazat. Podrobná příručka k nastavení práv, která celou tuto problematiku vysvětluje, je přímo v programu v menu *„Firma / Návody PDF / Nastavení práv“*.



Od verze 9.55 je zde i přehled přístupových práv vedoucích na editaci či prohlížení docházky podřízených, takže rychle dohledáte kdo se dostane na čí docházku k prohlížení nebo i k editaci.

Zálohy databáze:

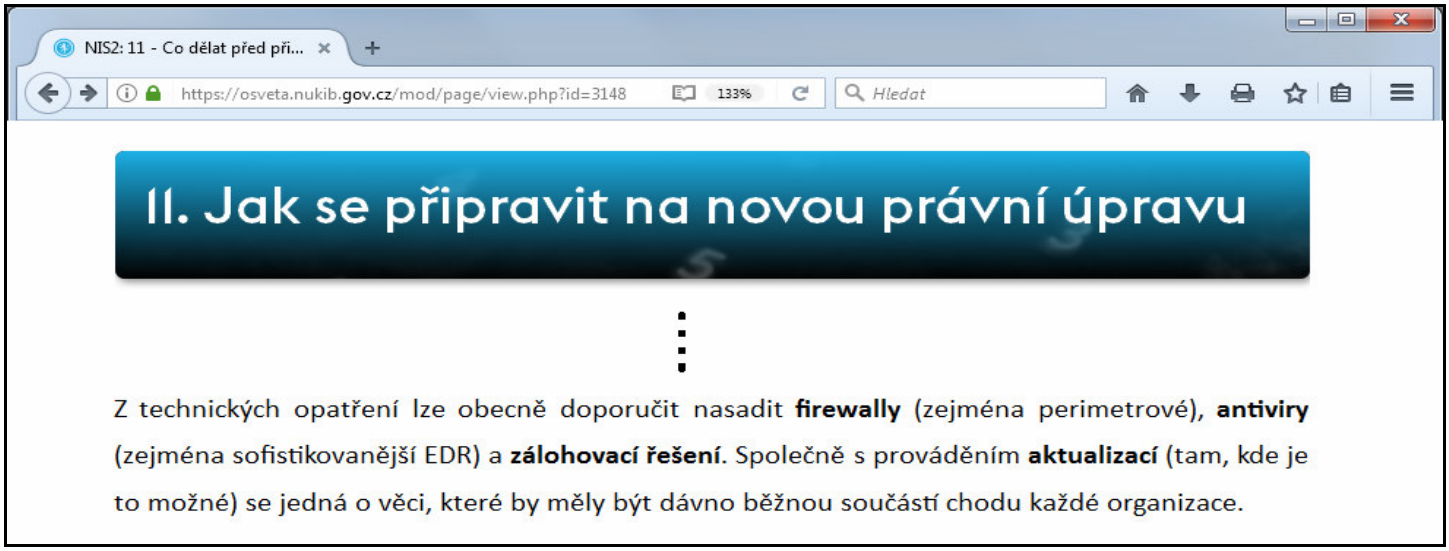
Do oblasti zabezpečení patří samozřejmě také zálohování a obnova dat programu. Podrobnou příručku, která popisuje pět možných typů záloh, od ručních po automatické, od záloh za provozu po off-line zálohy, možnost záloh do cloudu nebo na jiný síťový disk atd. atd., vše je popsáno v návodu v menu *„Firma / Návody PDF / Záloha databáze“*. Příručku také najdete na instalačním nebo aktualizačním disku ve složce */Prirucky*



Ve stejném menu *„Firma / Návody PDF“* nebo ve složce */Prirucky* na CD jsou i všechny další návody, jako *Administrátorská příručka* pro správce systému, *Uživatelská příručka* pro běžné zaměstnance, vedoucí, personalisty atd., *Přístup po síti* pro nastavení přístupu do programu z ostatních počítačů, *Nastavení HTTPS* pro aktivaci šifrovaného spojení, *Nařízení GDPR* pro celou oblast nařízení o ochraně osobních údajů a celá řada dalších návodů. Například i příručka *Podpora* pro možnost využití placené podpory ze strany výrobce nebo základní podpory dostupné zdarma na telefonu nebo e-mailem. Nebo příručka *Migrace do cloudu* pro případ, že byste neměli kapacity k tomu zabývat se správou hlavního PC docházky (serveru) včetně záloh databáze a aktualizací programu a chtěli celu tuto problematiku přenechat na výrobci programu.

Příprava technických opatření obecně:

Základní technická opatření jsou shrnuta na webu NUKIBu do 4 bodů: firewall, antivir, zálohování, aktualizace:



Zdroj výše uvedeného k 10. dubnu 2024: *https://osveta.nukib.gov.cz/mod/page/view.php?id=3148*

<u>Docházka 3000 v cloudu</u> - vyjádření provozovatele zda je poskytovatelem regulované služby:

Podle kriterií na webu NUKIB je provozovatel cloudové verze programu Docházka 3000 mikropodnikem, jelikož nenaplňuje zaměstnanecký ukazatel pro větší subjekty a ročním obratem splňuje kritéria mikropodniku.

Při počítání velikosti subjektu se postupuje v souladu s doporučením komise 2003/361/ES o definici mikropodniků, malých a středních podniků.

Pro posouzení velikosti subjektu musí být naplněn zaměstnanecký nebo finanční ukazatel.

Kategorie podniku	Počet zaměst-nanců: roční pracovní jednotka (RPJ)	Roční obrat	nebo	Bilanční suma roční rozvahy
Střední podnik	< 250	≤ 50 milionů EUR	nebo	≤ 43 milionů EUR
Malý podnik	< 50	≤ 10 milionů EUR	nebo	≤ 10 milionů EUR
Mikropodnik	< 10	≤ 2 miliony EUR	nebo	≤ 2 miliony EUR

Při posuzování naplnění finančních ukazatelů si daný podnik může vybrat takový ukazatel, který je pro něj výhodnější.

Podle přílohy k připravované vyhlášce o kritériích pro identifikaci regulované služby spadá cloudová docházka do služby 16.11 – *Poskytování řízené služby*. Ve vyhlášce je uvedeno, že režim vyšších povinností se týká velkých podniků a režimu nižších povinností se týká středních podniků. Proto není provozovatel cloudové docházky poskytovatelem regulované služby z pohledu směrnice NIS2.

16.11. Poskytování řízené služby (MSP)	Poskytovatel řízené služby, který v rámci podnikatelských vztahů poskytuje vzdáleně nebo přímo u zákazníka řízenou službu související s instalací, správou, provozem nebo údržbou technických nebo programových prostředků, je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je velkým podnikem, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.

Poskytovatelem regulované služby není ani z pohledu služby 16.6, protože cloudová docházka nenaplňuje definici poskytování služby cloud computingu a navíc NIS2 řeší tuto službu jen pro velké a střední podniky, nikoli pro mikropodniky.

16.6. Poskytování služby cloud computingu	Poskytovatel služby cloud computingu je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, b) je poskytovatelem státního cloud computingu podle zákona o informačních systémech veřejné správy[21], II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.

Ani náplni služby 16.7 cloudová docházka neodpovídá, jelikož se nejedná o přímé poskytování služby datového centra a navíc NIS2 opět řeší tuto službu jen pro velké a střední podniky, nikoli pro mikropodniky.

16.7. Poskytování služby datového centra	Poskytovatelem služby datového centra je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je velkým podnikem, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.

Provozovatel cloudové Docházky 3000 tedy z pohledu NIS2 není poskytovatelem regulované služby.