Zabezpečení PC s docházkovým systémem

Hlavní PC docházky (docházkový server) by měl být zabezpečen antivirovým programem, firewallem a dalšími bezpečnostními prvky ochrany podobně jako jiné servery v počítačové síti. Otázka zabezpečení je velmi široká, zahrnuje celou řadu oblastí, existují firmy které se přímo specializují na počítačovou bezpečnost pro které pracuje celá řada vysoce specializovaných odborníků. Není absolutně možné postihnout celé toto téma v rámci jedné příručky. Otázka zabezpečení webových a databázových serverů je ještě více komplexní a specifická a vyžaduje další odborné znalosti. Výrobce docházkových systémů se soustředí primárně na funkcionalitu systému z pohledu výpočtu docházky a neklade si ambice pokrýt celou rozsáhlou oblast zabezpečení počítačů a počítačových sítí. Schopnosti docházkového programu mají z pohledu odolnosti vůči virovým a jiným útokům omezené možnosti. Přesto se vám pokusíme dát alespoň základní tipy na zabezpečení počítače s docházkou. Souhrn je na poslední straně návodu.

Základním předpokladem je pravidelná aktualizace bezpečnostních prvků vaší počítačové sítě (routery atd.), počítače s nainstalovanou docházkou (jeho operačního systému, systému BIOS, antiviru, firewallu atd.) a také samotného docházkového programu. Dále následuje několik tipů na zvýšení zabezpečení samotného docházkového programu. V první řadě se jedná o seznam příruček, které jsou na instalačním či aktualizačním disku docházkového systému a věnují se zcela nebo částečně otázkám zabezpečení docházky. Níže je jejich seznam dle abecedního řazení:

Databáze_v_NAS.pdf ... Příručka popisuje možnost přesunout databázi docházky na síťové úložiště, které má například mirorované disky, takže pokud jeden z pole disků selže, data by při správném nastavení měla být nadále dostupná.

GDPR.pdf ... Návod se týká zabezpečení osobních a citlivých dat uživatelů z pohledu ochrany osobních údajů.

Napojeni_na_domenu_active_directory_ldap.pdf ... Příručka popisuje možnost ověřování uživatelů při přihlašování do docházky vůči doménovému serveru. Takže hesla (tedy jejich heše) pak nejsou uložena v databázi docházky a ověření uživatele má na starosti doménový server.

Nastavení_práv.pdf ... Návod popisující možnosti nastavení práv uživatelů a některé další oblasti zabezpečení uživatelských účtů. Aby měli uživatelé jen ta práva do programu, která mít mají a byly jim poskytovány jen ty funkce, které odpovídají jejich roli ve firmě.

NIS2.pdf ... Příručka popisuje celou řadu oblastí kybernetické bezpečnosti v souvislosti s docházkovým systémem, včetně postupu aktualizace komponent jako je webový server či databázový server, sledování přístupů do programu, kontrolu zabezpečení uživatelských účtů, omezení přístupových IP adres atd.

Pristup_z_jinych_pc.pdf ... Návod pro zpřístupnění docházky z ostatních počítačů v síti, použitelný v případě, kdy potřebujete aby s programem pracovalo více zaměstnanců ze svých PC.

Replikace_DB.pdf ... Postup pro on-line „kopírování“ databáze na další počítač. Ten může sloužit jednak jako záloha pro případ poškození disku v hlavním PC docházky (nikoli jako ochrana před nechtěným výmazem dat) a zároveň jako rozložení zátěže na více databázových serverů. Pokud tuto replikaci nasadíte, je důležité myslet na to, že i tento další počítač je nutné chránit proti únikům a zneužití dat.

Reseni_problemu_SW.pdf ... Tato příručka se sice primárně nevěnuje zabezpečení, ale obsahuje informace vedoucí ke znovuzprovoznení systému po nějaké závadě.

Šifrované_spojení_HTTPS.pdf ... Důležitá příručka pro zabezpečení dat přenášených přes počítačovou síť. Pokud s docházkou pracujete z více PC než jen z toho hlavního na kterém je nainstalovaná, věnujte této příručce velkou pozornost.

Šifrování_databáze.pdf ... Obsahuje postup, pomocí kterého můžete pro databázi docházky použít šifrované úložiště. Pokud máte v malé firmě docházku nainstalovanou třeba na notebooku mzdové účetní a ta jej nosí sebou, měl by být počítač nejen chráněný hesly do windows, ale i úložiště by mělo být náležitě zabezpečeno, aby útočník nemohl pevný disk přenést do jiného PC a tam vidět jeho obsah.

WebAPI.pdf ... Docházka obsahuje programátorské API, pomocí kterého lze načítat data z jiných systémů nebo je do docházky zapisovat. Toto API by mělo být rovněž chráněno proti zneužití a v této příručce jsou uvedeny základní postupy takové ochrany.

Zabezpeceni_TLS.pdf ... Jedná se o starší příručku pro TLS 1.2 ale aktuálnější informace i třeba pro TLS 1.3 jsou uvedeny v dříve zmíněné příručce *Šifrované_spojení_HTTPS.pdf*

Zalohovani_databaze.pdf ... Základní kámen zabezpečení proti ztrátě dat například při poškození pevného disku nebo zcizení PC s docházkou. Nejedná se sice o informace z pohledu zabránění zneužití dat, ale o rovněž důležité informace proti jejich ztráte.

Zmena_portu_apache.pdf ... Tato příručka sice není ze své povahy zaměřena na zabezpečení, ale pojednává o řešení případů, kdy je port 80 nebo 443 pro apache server docházky obsazený jinou aplikací. Ovšem pokud změníte port na kterém webový server apache pro docházku běží, může se na to také částečně nahlížet jako na snahu o vyšší zabezpečení, protože ne všechny hackerské programy zkoumají všechny porty síťového rozhraní, ale zaměřují se na ty nejpoužívanější. Změnou portu tedy můžete částečně zvýšit úroveň zabezpečení (tzv. *security by obscurity*).

Zmena_portu_mysql.pdf ... Podobně jako předchozí příručka ani tato primárně neřeší zabezpečení, ale pomocí ní můžete změnit TCP port databáze MySQL na nějaký nestandardní a mírně tím jakoby zvýšit zabezpečení databáze.

Změna_webserveru...pdf ... Příručka obsahuje postupy pro případ, kdy z nějakého důvodu nechcete nebo nemůžete použít webový server Apache dodávaný s docházkou. Pokud se z prohledu bezpečnosti specializujete spíše na IIS či jiný webový server a rozumíte mu lépe než Apache, můžete pomocí postupů v této příručce webový server docházky změnit.
Také databázový server je možné použít jiný než standardně dodávaný MySQL či MariaDB. Docházka může fungovat například s MS SQL serverem nebo s PostgreSQL serverem. Postupy jsou na instalačním disku ve složce *Ostatní* a jejich podsložkách pro MSSQL nebo Postgres.

Výše uvedené příručky ale samozřejmě neřeší zdaleka vše, co je možné pro zabezpečení docházky udělat. Například zaměstnanci, pokud nemají k čipování pořízený terminál ale používají PC nebo mobil či tablet a podobně, nemusí mít přístup do běžného uživatelského rozhraní, ale mohou používat buď *Virtuální terminál* (viz stejnojmenná příručka) a to buď lokální nebo zcela oddělený cloudový, nebo se mohou do programu přihlašovat přes speciální hešové odkazy či QR kódy - viz příručka *Integrace docházky*.

Další rozsáhlou oblastí je zaheslování PC uživatelů přes chráněný přístup do Windows (pomocí hesel či biometricky nebo vícefaktorově), tak také zaheslování třeba spořiče obrazovky atd. Tato témata jsou ale mimo rozsah dokumentace docházkového systému a patří do obecných zásad zabezpečení počítačů a sítí.

Součástí zabezpečení je i průběžná aktualizace docházkového systému, protože aktualizace rovněž přináší další prvky ochrany a postupy pro zamezení útoků. Ve většině firem je docházka nainstalovaná v rámci interní lokální sítě LAN a je chráněná proti přístupu z veřejného internetu. Ale pokud jste třeba kvůli umožnění přístupu ze vzdálených poboček nepoužili VPN, ale server docházky má pevnou veřejnou IP adresu a je plně dostupný z internetu, věnujte zvýšenou pozornost zabezpečení sítě a počítače s nainstalovanou docházkou. Některé informace o důležitějších změnách v jednotlivých verzích programu budou uvedeny dále.

Doporučené základní úpravy konfigurace Apache a PHP:

Upravte soubor *c:\apache\apache\conf\httpd.conf* tak, že najdete řádek s položkou
`ServerSignature On`
a nastavení položky vypnete přepsáním na *Off*. Dále doplníte řádky pro vypnutí *TraceEnable* a *ServerTokens* nastaví na *Prod*, takže po úpravě bude sekce vypadat takto:

```
ServerSignature Off
ServerTokens Prod
TraceEnable Off
```

Upravte soubor *c:\apache\php\php.ini* tak, že najde řádek s položkou
`expose_php = On`
a nastavení položky vypnete přepsáním na *Off*, takže upravený záznam bude obsahovat:
`expose_php = Off`

Nyní restartujte apache web server, aby se nová konfigurace načetla. Spustíte program *c:\apache\xampp-control.exe* a v řádku *Apache* kliknete na *Stop*. Počkáte až zmizí zeleně podsvícený nápis *Running*, dále počkáte asi 5 vteřin a opět u *Apache* kliknete na *Start*. Jakmile se zeleně podsvícený nápis *Running* opět objeví, ukončíte program tlačítkem *Exit* vpravo dole.

Spusťte aplikaci *Poznámkový blok* a otevřete v ní soubor *c:\apache\htdocs\dochazka2001\phpinfo.php* Vymažte celý obsah tohoto souboru (tak aby byl zcela prázdný), napište text *Disabled* a soubor uložte.

Úpravy zabezpečení prováděné v jednotlivých verzích programu
(doporučujeme tedy pravidelně aktualizovat)

Verze 8.29 - Ochrana před poškozením databáze v případě zaplnění disku serveru
Program od této verze hlídá stav volného místa na disku hlavního PC docházky (docházkovém serveru). Tedy chrání před zaplněním disku počítače, na kterém je docházkový systém nainstalovaný. Pokud by na disku C: hlavního PC docházky došlo k úplnému zaplnění jeho kapacity a nebylo by žádné volné místo pro zápis databázových souborů, hrozila by ztráta dat či poškození DB. Proto program vždy před přihlášením uživatele zkontroluje, zda je na serveru na disku volno alespoň 10 MB kapacity či více. První drobné hlášení na úvodní obrazovce zobrazuje již při poklesu volného místa pod 100 MB. Pokud volná kapacita klesne pod hranici 10 MB, píše program na úvodní obrazovce výrazné výstražné hlášení, aby uživatel neprodleně kontaktoval správce IT, který problém vyřeší. Jestli-že volné místo klesne po 1 MB a situace s obsazením disku tedy začne být vysoce kritická, program úplně znemožní přihlášení a zastaví databázový server. Tím ještě před přihlášením uživatele předejde tomu, že by se místo na disku serveru vyčerpalo zcela a ochrání tím databázi a docházkový systém před ztrátou dat či poškozením DB. Zaměstnanci pochopitelně mohou na terminálech čipovat docházku po celou dobu naprosto bez omezení, toto nové opatření se týká jen práce s programem v počítači.

Od verze 9.43 je zapnuta *Ochrana proti útoku hrubou silou* jak pro příhlášení heslem, QR kódem a i pro přihlášení hešema a tyto pokusy se navíc logují. Čímž zajistíte, že pokud by se někdo snažil přihlašování napadnout tak, že by rychle po sobě zkoušel různé heše v parametru *login*, nebo přihlašovací hesla, docházka toto detekuje a útok v podstatě znemožní. Každé neplatné přihlášení se loguje do historie přihlašování a pokud při pokusu o přihlašení program zjistí, že v tuto vteřinu již nějaké neplatné přihlášení našel, nové přihlášení ani nevyhodnocuje a uživateli zobrazí výstrahu s informací, že se aktivovala ochrana proti útoku hrubou silou. Takže pokud je tato ochrana aktivní, může útočník zkoušet jen jeden pokus za vteřinu, což i při základním algoritmu MD5 znamená zamezení prolomení ochrany (statisticky by bylo potřeba útok provádět 3.6^30 let).

Verze 9.59 - Zlepšeno zabezpečení webového rozhraní stravovacího systému
Systém nyní používá výrazně vylepšené zabezpečení při práci strávníků s webovým rozhraním modulu objednávek obědů. Při každé akci se kontrolují silnější heše hesla strávníka, čímž je lépe zamezeno možnému podstrčení falešných údajů do přenášených dat v komunikaci se serverem docházky a tím i riziku změny objednávek jiného uživatele.
Všechny 3 typy přihlašování se logují do databáze, takže je lze dohledat v menu *"Firma / Historie logování"*. Navíc je v systému zapnuta ochrana proti útoku hrubou silou, takže pokud by se útočník snažil ze svého PC v rychlém sledu automatizovaně posílat pokusy o přihlášení s různými ID strávníka a hesly nebo heši, systém toto detekuje a umožní vyhodnotit jen jedno přihlášení ze stejné IP adresy za vteřinu, takže útok hrubou silou je bezpředmětný, protože je časově neefektivní.

Verze 9.63 - Doplněna ochrana proti útoku Slowloris
Do docházkového systému a jeho webového serveru byla doplněna ochrana proti útoku známému pod označením *Slowloris*, která brání možnému vyčerpání systémových prostředků webového serveru. Pokud tedy máte docházku přístupnou z internetu nebo chcete zamezit možnosti využití tohoto útoku uživatelům ve vaší vlastní síti a systém již máte nainstalovaný, stačí na hlavním PC docházky (docházkovém serveru) do souboru *c:/apache/apache/conf/httpd.conf* pomocí poznámkového bloku doplnit na konec souboru nové řádky s tímto obsahem:
LoadModule reqtimeout_module modules/mod_reqtimeout.so
RequestReadTimeout header=20-40,MinRate=500 body=20-40,MinRate=500
a nastavení uložit. Dále je nutné soubor *mod_reqtimeout.so* stáhnout pomocí tohoto odkazu:
https://www.dochazka.eu/dochazka3000/download/mod_reqtimeout.so
a uložit jej na disk C:\ do složky *c:/apache/apache/modules/*
Nakonec je ještě potřeba službu webového serveru restartovat. To provedete tak, že spustíte program *c:/apache/xampp-control.exe* a v řádku pro službu *Apache* kliknete nejprve na tlačítko *Stop*, vyčkáte několik vteřin až zmizí nápis *Running* a poté kliknete na tlačítko *Start*. Jakmile se opět objeví zelený nápis *Running*, ukončíte program *Xampp-control* tlačítkem *Exit* vpravo dole. Tím je ochrana proti tomuto typu útoku aktivovaná.

Verze 10.24 - Zaznamenali jsme útok využívající vzdálené spuštění kódu přes MySQL server. Pokud tedy docházku používáte s MySQL databází a je přístupná z internetu, doporučujeme upravit konfiguraci MySQL tak, že do souboru *c:/apache/mysql/bin/my.ini* do sekce *[mysqld]* doplníte řádek:
secure_file_priv="c:/apache/tmp/"
Poté upravený soubor uložíte a restartujete PC s docházkou nebo restartujete službu MySQL v programu c:/apache/xampp-control.exe a pokud by se pak služba nespustila, ověřte že existuje složka c:/apache/tmp/ a pokud by neexistovala, tak jí vytvořte a znovu spusťte službu MySQL.

Verze 10.27 - Ochrana proti útoku typu SQL injection, důležitá zejména pokud máte docházku na svém serveru přístupnou z internetu. Tento typ útoku využívá vzdálené spuštění kódu přes databázový server. Pokud tedy docházku používáte s MySQL databází a je přístupná z internetu nebo ze sítě LAN, doporučujeme upravit konfiguraci PHP tak, že v souboru *c:\apache\php\php.ini* v sekce *Data Handling* upravíte položku *auto_prepend_file* takto:
auto_prepend_file="c:\apache\htdocs\dochazka2001\prepend_sqlinj.php"
Poté upravený soubor uložíte a otestujete fukčnost docházky. Pokud by poté přestala fungovat, ověřte že máte skutečně nainstalovanou verzi docházky 10.27 nebo novější a tudíž že na hlavním PC docházky existuje ve složce *c:\apache\htdocs\dochazka2001* soubor *prepend_sqlinj.php*

Ve verzích 10.30 až 10.32 byla ochrana proti útoku typu SQL injection popisovaná v předchozím odstavci ještě dále výrazně vylepšena a zpřísněna. Zablokované přístupy se logují do error.log souboru webového serveru (zpravidla c:\apache\apache\logs\error.log) a v textu záznamu je vždy uvedeno slovo *BLOCK* s dalšími podrobnostmi jako je důvod blokování a celá *URI* adresa. Pro správce serveru může být důležité vědět, že systém si nyní ukládá do log souborů všechny IP adresy, ze kterých přišly pokusy o napadení. Jedna z částí ochrany funguje tak, že když během stejného dne zaznamená ze stejné IP adresy 3 nebo více přístupů vyhodnocených jako pokus o napadení, zablokuje na zbytek dne této IP adrese php

přístup. Ve webové složce (kterou je většinou c:\apache\htdocs\dochazka2001\) se vytváří blacklist IP adres v souboru *blacklist_ip_rrrrmmdd.log* (kde rrrr je rok, mm je měsíc a dd je den, takže třeba log pro den 3.8.2026 je v *blacklist_ip_20260803.log*) a na každém řádku je IP adresa z pokusu o napadení. Jakmile je stejná IP adresa v tomto souboru potřetí, přestanou se zde logovat její další pokusy a veškeré další přístupy přes http nebo https protokoly ke všem php souborům na celém serveru jsou pro ní na zbytek dne blokovány. Pokud ale na svém serveru provozujete ještě další php aplikace a docházelo by k falešně pozitivním logováním a blokacím třeba proto, že vaše další aplikace mohou mít dlouhé parametry v get nebo post proměnných předávaných přes http a nebo dokonce mohou obsahovat například slova shodná s příkazy sql (které docházka blokuje jako pokus o sql injection a sama je v parametrech nikdy nepoužívá), musíte použít nějaký jiný typ ochrany než tento velmi přísný který je součástí docházky a úpravu souboru php.ini popsanou v předchozím odstavci pro verzi 10.27 nepoužívejte. Pokud ale na serveru provozujete jen docházku, doporučujeme tuto ochranu nasadit a klidně jí doplnit třeba ještě i o další typy jiných dodavatelů. V poslední době totiž zaznamenáváme obrovský nárůst velmi sofistikovaných automatických útoků a jakákoli další ochrana může ještě lépe pomoci chránit vaši IT infrastrukturu. Dnešní útočníci používají celé farmy počítačů se škodlivým softwarem a často ovládaných umělou inteligencí, takže je dobrý jakýkoli typ ochrany proti těmto útokům, které dokáží generovat tisíce pokusů o napadení za hodinu.
Od verze 10.32 umí program při přihlášení zobrazit seznam podezřelých přístupů a blokovaných IP adres zaznamenaných v aktuálním měsíci, takže se administrátor hned po přihlášení do programu dozví kdy probíhaly pokusy o útok a z jakých IP adres a že byly zablokovány.

Souhrn nastavení zabezpečení u lokální instalace SW na vašem PC či serveru (netýká se cloudu)

Tyto kroky jsou souhrnem předchozích 3 stran a určitě je proveďte, zejména pokud je server docházky přístupný z internetu. Podrobnější vysvětlení je na předchozích stranách.

1) Nejprve je potřeba program aktualizovat alespoň na verzi 10.31, což provedete přímo v programu v admin. menu vlevo ve žlutém rámu přes volbu menu *E-shop* objednávkou první položky *Aktualizace SW Docházka 3000*. Jakmile vám aktualizace dorazí, nahrajte jí a až poté proveďte následující body.

2) Stáhněte soubor *mod_reqtimeout.so* pomocí tohoto odkazu:
https://www.dochazka.eu/dochazka3000/download/mod_reqtimeout.so
a uložit jej na disk C:\ do složky *c:/apache/apache/modules/*

3) Upravte soubor *c:\apache\apache\conf\httpd.conf* pomocí poznámkového bloku tak, že najdete řádek s položkou `ServerSignature On` a nastavení položky vypnete přepsáním na *Off*. Dále doplníte řádky pro vypnutí *TraceEnable* a *ServerTokens* nastaví na *Prod*, takže upravená sekce bude vypadat takto:
```
ServerSignature Off
ServerTokens Prod
TraceEnable Off
```

4) Na konec tohoto souboru *c:/apache/apache/conf/httpd.conf* doplňte nové řádky s tímto obsahem:
```
LoadModule reqtimeout_module modules/mod_reqtimeout.so
RequestReadTimeout header=20-40,MinRate=500 body=20-40,MinRate=500
```
a nastavení uložte.

5) Do souboru *c:/apache/mysql/bin/my.ini* do sekce *[mysqld]* doplníte řádek:
secure_file_priv="c:/apache/tmp/"
Poté upravený soubor uložte. Následně ověřte že existuje složka *c:/apache/tmp/* a pokud by neexistovala, tak jí vytvořte.

6) Nyní restartujte služby apache a mysql, aby se nová konfigurace načetla. Restart provedete tak, že spustíte program *c:\apache\xampp-control.exe* a v řádcích pro *Apache* i *MySQL* kliknete na tlačítka *Stop*. Počkáte až zmizí zeleně podsvícené nápisy *Running*, dále počkáte asi 5 vteřin a opět služby *Apache* i *MySQL* spustíte kliknutím na tlačítka *Start*. Jakmile se zeleně podsvícené nápisy *Running* u obou služeb opět objeví, ukončíte program tlačítkem *Exit* vpravo dole. Pokud by se některá služba nespustila, udělali jste v některém z předchozích kroků chybu a zkontrolujte je.

7) Upravte soubor *c:\apache\php\php.ini* tak, že najde řádek s položkou
`expose_php = On`
a nastavení položky vypnete přepsáním na *Off*, takže upravený záznam bude obsahovat:
`expose_php = Off`

8) Dále v tomto souboru *c:\apache\php\php.ini* najděte sekci *Data Handling* upravíte položku *auto_prepend_file* takto:
`auto_prepend_file="c:\apache\htdocs\dochazka2001\prepend_sqlinj.php"`
Poté upravený soubor uložíte a otestujete funkčnost docházky. Pokud by poté přestala fungovat, ověřte že máte skutečně nainstalovanou verzi docházky 10.31 nebo novější a tudíž že na hlavním PC docházky existuje ve složce *c:\apache\htdocs\dochazka2001* soubor *prepend_sqlinj.php*

9) Spusťte aplikaci *Poznámkový blok* a otevřete v ní soubor *c:\apache\htdocs\dochazka2001\phpinfo.php*
Vymažte celý obsah tohoto souboru (tak aby byl zcela prázdný), napište text *Disabled* a soubor uložte.

10) Nasaďte šifrovanou komunikaci dle návodu v menu *Firma / Návody PDF / Nastavení HTTPS* a pravidelně zálohujte databázi na off-line úložiště dle příručky *Záloha databáze* ve stejném menu.