N°02 - 2022

# manažerská příloha

K-net Technical International Group

Vaše téma

## JAK SI SKVĚLÝ MANAŽER PORADÍ VE SVÉ FIRMĚ S OCHRANOU DAT POMOCÍ AUTENTIZACE

*Ochrana identity a zabezpečení firemních dat a systémů je v dnešní době již zavedenou realitou a v podstatě již povinnou výbavou většiny firem, které potřebují ochránit svá důležitá data.*

*Během práce se přihlašujeme běžně do svého osobního počítače nebo různých systémů a je to v podstatě rutinní činnost. Stejné je to např. s přístupem do budov, popř. povolení či zamezení přístupu různých lidí na různá místa na pracovišti.*

*Pokud ale tuto rutinu musíme provádět několikrát denně, chceme mít zajištěnu vyšší bezpečnost při přihlašování a musíme si pamatovat více složitých hesel, tak se s tímto postupem již tak snadno nespokojíme. Navíc se nepřihlašujeme jenom my, ale i kolegové, a to ještě na různých úrovních přístupů a zabezpečení.*

*V tom případě již potřebujeme sofistikovanější řešení. Přinášíme vám tedy na toto téma přehled nejrůznějších technologií a zejména pohled na problematiku očima IT manažerů či majitelů firem, kteří bezesporu řeší zabezpečení svých dat dennodenně.*

**Ing. Petr Nepustil**
vedoucí divize Produkce

**Samotné téma autentizace je velmi rozsáhlé a široké. V tomto čísle Manažerské přílohy si tedy představíme 1. část, kde se na problematiku podíváme očima manažera. V online vydání této přílohy pak téma dále rozvedeme z jiných úhlů pohledu.**

### OBSAH MANAŽERSKÉ PŘÍLOHY:




## Autentizace – co to je a k čemu slouží

Autentizace není nic jiného než postup, jak uživatel přesvědčí počítač (IT systém), že je to on a ne někdo, kdo se za něj vydává. Dobrý manažer, na rozdíl od lidí z IT oddělení ví, že autentizace ve firmě je něco diametrálně odlišného než autentizace k aplikacím, jako je např. Facebook. Nemluvě o cloudových službách, jako je např. Google Drive či Dropbox.

Majitel firmy Oracle Larry Ellison správně říká, že neexistuje žádný cloud – je to jen počítač, který patří někomu jinému. V tom samozřejmě tkví potenciální nebezpečí – k datům může mít přístup více lidí. Co s tím? Pokud používáte ve firmě cloud, máte možnost si jej nechat zkonfigurovat tak, aby autentizace uživatelů probíhala přímo u vás. Díky tomu pak máte autentizaci pod kontrolou a když někoho např. propustíte, je možné mu zablokovat přístup úplně všude a v podstatě dříve, než opustí personální oddělení. A to je důležité!

## Co chtít po IT oddělení a jak kontrolovat splnění cíle?

Dobrý manažer by neměl z principu nechat samotnou autentizaci pouze na lidech z IT oddělení. Je to vždy spolupráce obou entit. Manažer sám by totiž měl řídit rozdělení práv a IT oddělení vykonat práci samotnou. Pokud se celá věc nechá jen na IT oddělení, hrozí nebezpečí přístupu k citlivým datům pro nesprávné osoby a např. i potencionální demonstrace síly ze strany IT oddělení vůči zaměstnancům, kteří jsou z jejich pohledu problémoví apod.

## Autorizace

Proč je autentizace důležitá, je nasnadě – firemní data je potřeba chránit před neautorizovaným přístupem. Autorizace je sestřenicí samotné autentizace. Autorizace je přidělení přístupu k datům (např. ke složce na serveru, kde je soubor mzdy.xls) nebo oprávnění k nějaké akci (např. poskytnutí slevy zákazníkovi). Uživatel je reprezentován svým účtem. Například p. Petr Novák má účet firma/pnovak a tomuto účtu jsou přidělena určitá oprávnění – autorizace.
Důležité tedy je, jak spolehlivě autentizace dokáže ověřit, zda se skutečně jedná o p. Petra Nováka, než jej systém pustí „dovnitř", aby mohl dělat svoji práci.

## Opakovaná přihlášení

Správný manažer také ví, že p. Novák je najat na práci pro zákazníky, ve výrobě či v účtárně. Avšak ne na to, aby se přihlašoval (autentizoval) do svého počítače/systému. To mu v podstatě zabírá jen čas, který by měl využít jinak. Důležitá otázka tedy zní, jak to dlouho mu samotná autentizace trvá a jak často ji (jako průměrný zaměstnanec) vlastně během dne dělá.
Chcete-li mít bezpečné pracovní prostředí z pohledu ochrany dat, musí být každé zařízení bezpečně uzamčené. Běžní uživatelé se do pokušení mohou dostat velmi snadno – např. když kolega opustí svůj počítač, aby si uvařil kávu. A nechá přitom neuzamčený počítač s otevřenou tabulkou mzdy.xls. Řešením je vydání celofiremního pokynu, aby při nepřítomnosti zaměstnance byl vždy počítač uzamčený. Tím se samozřejmě zvýší bezpečnost, ale nastane menší problém – uživatel se po návratu z kávy musí přihlásit. Docílíme tím tedy toho, že se počet přihlášení k zařízení během jednoho dne neuskuteční pouze jednou, ale třeba i desetkrát. Pokud čtete tento článek a pracujete v nemocnici, tak se usmíváte správně – je to třeba čtyřicetkrát.
Prostě potřebujeme autentizaci, která je svižná a neobtěžující a může ji bez problémů provádět i v IT průměrně vzdělaný člověk. Rychlost a přiměřená jednoduchost je klíčem k pravděpodobnosti, že se zaměstnanci budou přihlašovat řádně a nebudou mít snahu „obcházet systém".

## Reálné problémy s jednoduchou autentizací

Nejčastější autentizační metodou je vložení jména a hesla. Je rozumně „levná", všichni ji znají a v mnoha situacích nejde ani nic jiného použít. A určitě jste se setkali s tím, že vás IT oddělení, auditor nebo dokonce zákon nutili k tomu, abyste si jako heslo nastavili řetězec dlouhý 17 a více znaků s vysokou složitostí. Tím se dostáváme k další manažerské a zcela legitimní otázce – k čemu je to třeba, když např. PIN vaší kreditní karty má jen 4 číslice?
Mohou za to vaše Windows. Bohužel. Pokud máte Windows např. na svém pracovním notebooku a přihlašujete se do nich stejným jménem a heslem jako do sítě (tedy reálně stejně přes den v práci a doma večer), tak máte potenciální problém. Vaše heslo je na vašem notebooku uloženo v modifikované formě, které se říká „hash". Servery, ke kterým se autentizujete do sítě v práci, jsou uložené v serverovně s omezeným přístupem a nikdo se k nim jen tak nedostane. K vašemu počítači už ale ano. Útočník si z něj může nahrát soubor, který hash vašeho hesla obsahuje a pokusit se z něj heslo zjistit. A když heslo není dostatečně bezpečné (délkou a složitostí), tak se mu to pravděpodobně podaří.
Dalším problémem navíc je, že ani dostatečně „bezpečné" heslo není řešením. Vy jako manažer i vaši podřízení jste nakonec také jen lidé a váš dokonalý mozek příroda nestvořila proto, aby si generoval a pamatoval správná a bezpečná hesla. Případnému útočníkovi, který chce zjistit vaše heslo a má v rukách soubor z vašeho počítače s hashem, stačí pouze použít slovník. Což je jednoduše velká databáze všech hesel. A v těch nejlepších databázích je, i když je to k nevíře, třeba 96 % všech hesel, která kdy na celém světě byla použita.

## Vícefaktorová autentizace

Proto používáme ve světě IT vícefaktorové autentizační systémy. Tedy systémy, které podporují různé způsoby prokázání totožnosti uživatele a které vám umožní použít dva najednou.

Možná jste už slyšeli, že vícefaktorová autentizace znamená, že se uživatel přihlásí pomocí chytré karty. Tady vás musíme zklamat – není. Je to jiná metoda, než je jméno/heslo, ale je to opět jen jedna metoda autentizace. Vícefaktorové přihlašování skutečně znamená, že se uživatel přihlásí dvakrát různým způsobem.
Vraťme se nyní k manažerskému pohledu na věc – ve firmě je spousta systémů, které si nezaslouží přehnaně bezpečnou autentizaci. Ostatně taková karta, která vás pustí do budovy, na parkoviště nebo s ní můžete je v hromadné dopravě, nevyžaduje vlastně nic navíc. Ani PIN. Prostě stačí, že ji máte a že ji přiložíte k nějaké čtečce. Když kartu ztratíte, tak to nahlásíte na příslušném oddělení. Tam ztracenou kartu zablokují a vy dostanete novou. A uživatel to zpravidla udělá hned, protože do budovy či na parkoviště prostě potřebuje vstoupit. Stejně použitelné je to i např. pro záznam docházky.
Pro klíčový informační systém a ochranu důležitých dokumentů apod. je to ale nedostačující. Zde je vhodné a někdy i povinné použít některý druhý faktor – druhé přihlášení. Jako např. přihlásit se jménem a heslem a při tom použít kartu. Důležité je také si uvědomit, že není nutné a často ani možné, aby způsob přihlášení dvěma faktory na výkonném počítači s Windows byl stejný jako na telefonu nebo tabletu. Ty jsou třeba také výkonné, ale nelze k nim připojit stejná zařízení jako k počítači. Třeba čtečku pro kartu. Tím pádem musí být druhým faktorem pro přihlášení jiný způsob.


## Náklady spojené s autentizací

Pro vícefaktorovou autentizaci tedy existuje vcelku široká nabídka specializovaných technologií. A doména Microsoft, kterou možná provozujete ve vaší firmě, mezi ně nepatří. To ale nemusí vadit – antivirus asi také máte od jiného výrobce, než je Microsoft. A zde je důležité poznamenat jednu důležitou věc – než pověříte IT oddělení, aby nějaký vhodný systém navrhlo, soustřeďte se na náklady. Nejlevněji vyjde téměř vždy to, co již ve firmě máte a provozujete. Ideálním kandidátem je právě onen čip. Buď v klasické plastové kartě (nebo jiné libovolné podobě) a který slouží k otevírání dveří, vjezdu na parkoviště, zadávání docházky, použití kopírky apod. Téměř všichni zaměstnanci ve firmě ho mají, všichni s ním umí zacházet a náklady na jeho pořízení jsou vlastně (téměř) nulové – protože jste jej už do firmy pořídili dříve a dáte mu jen nové využití.

?

## Jaký je rozdíl mezi autentizací, autorizací a autentifikací?

**Autentizace** je proces, kterým ověříme identitu uživatele. Může jít o řetězec více autentizací po sobě, který pak označujeme dvoufaktorová nebo vícefaktorová autentizace. Autentizace osobním certifikátem, byť je tento uložen na čipové kartě, je stále jedna a tudíž jednofaktorová autentizace. Více faktorů/přihlášení v rámci procesu autentizace činí autentizaci důvěryhodnější, ověřili jsme identitu uživatele s větší jistotou.

**Autorizace** je určení oprávnění uživatele v daném kontextu. Autentizace nám řekne, kdo je uživatel a autorizace pomocí tzv. ACL pak souborovému systému řekne, co uživatel může dělat se souborem, složkou atd. Autorizace je často implementována pomocí techniky rolí – role administrátora autorizuje uživatele ke správě systému, role fakturanta autorizuje pro vydání faktur, role pokladní autorizuje pro přijetí nebo vydání hotovosti. Autorizací jsou i v tisku propírané bezpečnostní prověrky. Autorizace Důvěrné, tajné, přísně tajné opravňuje k přístupu k informacím s danou nebo slabší klasifikací. A to platí pro technické i společenské systémy.

**Autentifikace** je již jen zkomolenina slova autentizace a má stejný význam.

## Čipy a jejich čtečky

Abyste takový čip mohli použít k autentizaci na počítačích (mimochodem, na mobilech to určitě nepůjde), budete potřebovat použít čtečky čipů. Na ty se nyní v článku zaměříme více, protože čtečky mohou různí dodavatelé (namlsaní z dotovaných projektů) prodávat opravdu draho.
Technicky je totiž velký rozdíl, zda potřebujete čtečku použít jen k prokázání totožnosti uživatele anebo zda s ní chcete počítač i ovládat. Tzn. karta je u zaměstnance přítomna = počítač je odemčený a zaměstnanec pracuje anebo karta přítomna není a počítač je uzamčený. Možná jste už někdy dříve souhlasili s nákupem drahé čtečky, protože byla potřeba jen v jednom provedení – a to pro účely personálního oddělení pro vydávání karet zaměstnancům. V případě druhého faktoru ve formě čipu se ale autentizace samotná týká VŠECH pracovišť. Čtečku čipů tedy nepotřebujete pouze jednu, ale desítky, stovky nebo tisíce. A roli v nákladech tak hraje každá koruna.
A tady je důležité upozornit na další věc – bezkontaktní čtečky a karty jsou v podstatě nesmrtelné. Pokud se ale rozhodnete pro karty kontaktní (nebo třeba USB tokeny apod.), pak musíte počítat s každým vsunutím a vysunutím. Klidně se totiž může stát, že po roce používání budete čtečku či kartu měnit. Proto vždy po dodavateli požadujte záruku, než podepíšete finální objednávku.

## Přihlášení certifikátem

Dalším z faktorů (způsobů) autentizace, které lze využít, je přihlášení certifikátem. Ten je často uložen na kartě společně s tzv. klíči a karta může být chráněna PINem.
To je právě ta metoda, o které vám např. vypočítavý dodavatel může tvrdit, že je to dvoufaktorová autentizace. Protože uživatel přece „vlastní" kartu a může ji použít jen když zná její PIN. Není tomu ale tak. Systém, ke kterému se uživatel totiž přihlašuje, nemá žádnou možnost zjistit, zda má uživatel správně nastavený PIN (popř. je nastaven základní 1111), popř. jestli má vůbec certifikát na kartě. Existuje mnoho systémů, ve kterých server jednoduše akceptuje, pokud je k počítači připojena čtečka s vloženou kartou, která je tzv. „smart". To je dobrá metoda a klidně ji pro autentizaci použijte. Ale pouze jako jeden faktor!

Musíme zmínit ještě další dvě záludnosti. Chytré karty s uloženými certifikáty nelze (až na úplné výjimky) znovu použít. Když váš zaměstnanec odejde, tak kartu skartujete a pro nového pracovníka použijete novou. Otázka tedy zní, kolik stojí jedna karta a jakou máte fluktuaci? Druhou záludností je vydání nového certifikátu a jeho cena. Pokud nejste velká firma, obvykle se vám nevyplatí vybudovat si certifikační systém sami. Necháte si certifikáty vydat na klíč od třetí strany. Pak tu tedy stojí další otázka nad novými náklady.

Když se na výše řečené podíváme jako manažeři zodpovědní za hospodářský výsledek (a ne jako „hračičkové" z IT), tak je jasné, že si pro zodpovědné rozhodnutí potřebujeme srovnat nabídky od více dodavatelů. Zvláště ve větších instalacích se stává cena jedné licence nebo čtečky karet značným nákladem. Také nás bude určitě zajímat, zda čtečka umí použít karty, které už ve firmě či organizaci jsou, a jak obtížná bude vlastní instalace, konfigurace a správa celé technologie.

## Řešte technické detaily

Poslední věcí, o kterou by se mohl a měl správný manažer zajímat, jsou technické detaily celého řešení autentizace. V našem článku se o nich vůbec nezmiňujeme (připravujeme si je na další číslo, pozn. redakce). Abychom vás ale neochudili a nepřipravili o důležité informace, máme pro vás radu – vyžádejte si od potencionálních dodavatelů reference. Pokud systém dodavatele ideálně používají ve více zemích světa, tam si ho pochvalují a zároveň např. pomocí Google recenzí nenajdete žádné stížnosti nebo popisy průšvihů, vše bude pravděpodobně v pořádku. Pokud byste ale zvolili použití řešení, které je nové a vypadá na první pohled skvěle, soustřeďte se na autory. Pokud se k nim dostanete a zafunguje mezi vámi chemie, jejich řešení použijte. Jen si tohoto dodavatele dopředu zavažte, ať vás v případě problémů „nenechá ve štychu". Tak se to totiž v oblasti bezpečnosti běžně dělá.
A poslední rada – pokud plánujete nechat si vypracovat a zaplatit profesionální analýzu určitého řešení, nedělejte to – je to ekonomický nesmysl (pokud nejste z armády nebo výzvědné služby).

## Další doporučení k bezpečnosti

V článku jsme zmínili nebezpečí spojené s tím, kdy se uživatelé přihlašují na počítače, který funguje s Windows registrovaným v doméně. To je vůbec nejčastější způsob, se kterým se v ČR můžete setkat. Dodatečně ochránit notebook, který zaměstnanec ztratí či mu byl ukraden, lze jen kryptováním disku. Uvnitř firmy zase počítače nejlépe ochráníte, když tam nenecháte potulovat nikoho cizího a když donutíte IT oddělení, aby neměli všude stejné heslo účtu Administrator. To se musí stále měnit a musí být na každém přístroji unikátní. A je v podstatě jedno, zda se jedná o Windows, Linux, MacOS nebo jiný OS. Když chcete, aby se uživatelé bezpečně autentizovali, musíte také chránit počítače, na kterých pracují.

**Autorem článku je Ing. Václav Šamša z partnerské společnosti TDP a my mu děkujeme za svolení s jeho otisknutím v Manažerské příloze.**

## Závěr

Věříme, že vás tento článek obohatil, popř. vám pomůže nejen ke správnému pohledu a zamyšlení ohledně zabezpečení vašich zařízení a dat, ale dále i k výběru správného a vhodného řešení.
My vám k tomu samozřejmě můžeme dopomoci a jako důvěryhodný systémový integrátor výrazně zkrátit cestu a ušetřit spoustu důležitých nákladů. Nebojte se nás tedy oslovit!
**A nezapomeňte - tento článek najdete také online, ve kterém na něj navíc naváže Petr Nepustil (vedoucí divize Produkce) a podíváme se na autentizaci více z technické stránky.**



**ZAUJALO VÁS TÉMA MANAŽERSKÉ PŘÍLOHY?**

*Přečtěte si její nezkrácenou verzi na našem webu s doplňujícími informacemi*

**k.k-net.cz/L22-2-autentizace**

**K-net Technical International Group, s.r.o.**
Olomoucká 170
627 00 Brno – Černovice
tel.: 548 220 150
GSM: 734 686 001
**Pobočka:** Rovečínská 16
679 74 Olešnice
tel.: 511 447 055

**K-net Team Praha, s.r.o.**
Sazečská 560/8
108 00 Praha 10 – Malešice
tel.: 734 686 014

**K-net Team Ostrava, s.r.o.**
Smetanovo náměstí 328/1
702 00 Ostrava
tel.: 734 686 012

facebook.k-net.cz
linkedin.k-net.cz
youtube.k-net.cz
info@k-net.cz

www.k-net.cz

Vysvětlení podtržených výrazů z Loginu a Manažerské přílohy najdete v glosáři IT pojmů na **k.k-net.cz/glosar**

**Technická příloha časopisu LOGIN 2/2022, ročník č. 17** | *Marie Hamerská, Jana Hejtmánková, Václav Šamša, Jan Crlík, Tomáš Knettig, Petr Nepustil*
*Vydala společnost K-net | Neprodejné | Uzávěrka čísla: 10. 10. 2022*