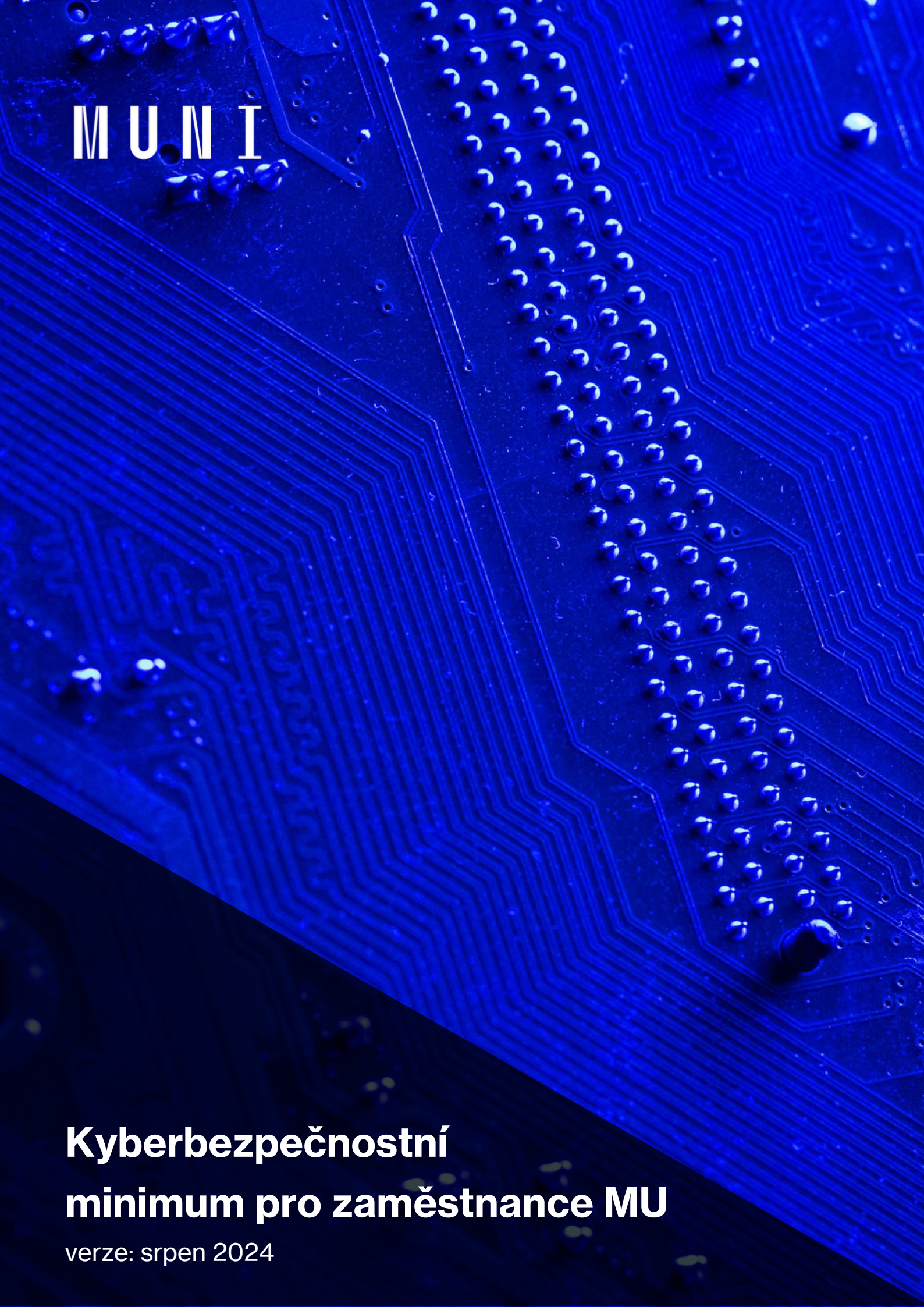

MUNI

Kyberbezpečnostní minimum pro zaměstnance MU

verze: srpen 2024

MUNI

Institucionální školení zokb

Tento dokument slouží jako textová opora pro školení **Základů kybernetické bezpečnosti pro zaměstnance MU**, jehož cílem je posilovat u zaměstnanců bezpečnostní návyky při pohybu v online prostoru. Školení představuje základní bezpečnostní doporučení a konkrétní opatření pro koncové uživatele, které je nutno zavést nejen z důvodů zákonných povinností, ale také s ohledem na zvyšující se nároky na bezpečnost uživatelů v kybernetickém prostoru. Školení vzniklo v návaznosti na povinnosti vyplývající ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a směrnici MU č. 10/2017, používání informačních technologií. Jako forma pro seznámení se s těmito povinnostmi vzniklo online školení, jehož obsah vytvořil a garantuje Kyberbezpečnostní tým MU[1].

Proč další Institucionální školení?

Zákon o kybernetické bezpečnosti č. 181/2014 Sb. (dále jen „ZoKB“) a na něj navazující předpisy ukládají institucím jako je Masarykova univerzita řadu nových povinností. Jednou z nich je i nutnost školení zaměstnanců v oblasti kybernetické a informační bezpečnosti s cílem posilovat návyky při pohybu v online prostředí. S přihlédnutím k uvedenému je rovněž nutné školit zaměstnance periodicky, analogicky ke školení *Bezpečnosti a ochrany zdraví při práci* (BOZP).

V prostředí Masarykovy univerzity mají uživatelé povinnost se seznámit primárně se Směrnicí č. 10/2017, používání informačních technologií. Tato směrnice vymezuje základní rámec týkající se práv a povinností uživatelů informačních technologií na Masarykově univerzitě. Směrnice obsahuje nejen definice základních pojmů, ale také například práva a povinnosti uživatele při práci s IT systémy, software a zařízeními na MU.

Aby se povinnost neomezila pouze na formální seznámení se s touto směrnicí, vytvořil Kyberbezpečnostní tým Masarykovy univerzity online školení a tuto textovou oporu. Tvoří jej nejen obecná doporučení a zákonem stanovený obsah, ale i specifika Masarykovy univerzity v návaznosti na interní univerzitní předpisy.

[1] https://csirt.muni.cz

MUNI

Obsah

MUNI

I. Práce s hesly

Heslo je jedním ze základních atributů kybernetické bezpečnosti. Společně s uživatelským jménem tvoří základní ochranný mechanismus sloužící k ověření a identifikaci uživatele.

Do většiny služeb na univerzitě se přihlašujeme pomocí **Jednotného přihlášení MUNI.** Jeho hlavní výhodou je, že si nemusíte vytvářet a spravovat uživatelské účty u každé služby zvlášť – stačí vám zadat **UČO** a **primární heslo**. Na MU se používá i **sekundární heslo**, které slouží pro přihlášení k méně kritickým službám, jako je Eduroam, centrálně spravované počítače v učebnách či fakultní e-learningové systémy (mimo IS MU) apod.

Rozdíly mezi hesly a návody týkající se jejich změny či nastavení naleznete na webu IT MU.

Frázová hesla

Frázové heslo se skládá z několika zapamatovatelných slov (např. trhatfialkyB34M-*dynamitem). Frázové heslo by mělo obsahovat: min. 12 znaků, číslice, velká písmena a speciální symboly (např. znaky, interpunkční znaménka). Jeho základem může být část básně, scenérie, kterou vídáte cestou do práce, anebo třeba vzpomínka z dětství.

Není doporučeno užívat hesla, která obsahují **snadno zjistitelné údaje**, jako je např. jméno vašeho dítěte nebo datum narození. Do hesel není vhodné ani umisťovat číslice či speciální symboly na předvídatelné pozice, jako je číslice na konci řádku nebo nahrazení písmene O číslicí 0.

Co když používám jednoduchá hesla?

Slovníkový útok je technika, při které útočník na přihlašovacích formulářích systematicky zkouší různá slova a fráze z předem sestaveného slovníku (seznamu). Útočník využívá používaná hesla založená na běžných slovech, jménech, číslech nebo frázích, které jsou snadno zapamatovatelné. K vytvoření kombinací hesel může využít veřejně dostupná data, a to např. údaje z prolomených hesel, které se objevily v rámci úniků dat.

Správce hesel

Některé studie ukazují, že lidé jsou schopni si zapamatovat až **10 různých hesel**. Nicméně počet účtů, pro které je nutné mít nastavené heslo, je mnohem vyšší. To může vést k používání stejného hesla nebo podobných hesel pro více účtů, což zvyšuje riziko kompromitace ostatních účtů v případě, že by jedno heslo bylo prolomeno. Existuje však řešení, jak si nastavit unikátní hesla pro jednotlivé účty a nemuset si je všechna pamatovat.

Správce hesel funguje jako databáze, kde jsou jednotlivá hesla a uživatelská jména ukládána a chráněna šifrováním. Správce hesel funguje na principu přihlašování skrze jediné heslo, tzv. master password neboli **hlavní heslo**. Toto heslo by mělo být opravdu silné, protože chrání všechny účty a přihlašovací údaje, které jsou ve správci hesel uloženy. Správce hesel taktéž umožňuje generovat hesla pro nově vzniklé či užívané online účty. Zpravidla nabízí i **rozšíření pro prohlížeče**, které po přihlášení do správce umožní automatické vyplnění přihlašovacích údajů.

> Ukládání hesel do prohlížeče (třeba do Google Chrome nebo Mozilla Firefox) **nelze ztotožňovat s používáním** správce hesel. Primární funkcí prohlížečů totiž správa hesel není! Z toho důvodu je vhodnější zvolit nástroj, který se na ukládání a správu hesel specializuje, a vy si tak můžete být jistí, že jsou hesla dostatečně zabezpečená. Stále netušíte, jakého správce hesel zvolit? Doporučujeme vám prostudovat náš shrnující web na správce hesel!

Které správce hesel doporučujeme?

Pro uživatele Apple zařízení postačí využít Apple Klíčenku, ta je součástí operačního systému. Pro uživatele zařízení s Windows, Android OS nebo pokud zařízení s různými OS kombinujete, doporučujeme Bitwarden (ideálně placenou verzi Premium, která stojí cca 250 Kč/rok).

Co naopak silně nedoporučujeme?

Byť to mnohé prohlížeče aktivně nabízí (např. Google Chrome), není to jejich hlavní účel. Lepší řešení je využít doplněk správce hesel do prohlížeče (nabízí je i námi doporučovaný Bitwarden). **Nikdy nesdílejte vaše hesla, sdílená hesla nikdy nepředávejte v otevřené podobě**! Hesla neposílejte ani přes MS Teams. Bezpečnější varianta je např. zašifrovaný e-mail.

MUNI

II. Vícefaktorové ověření

Vícefaktorové ověření[2] (Multi-factor Authentication, dále jen „MFA“) poskytuje pokročilejší úroveň ochrany, a to ve formě přidání dalšího faktoru ověření totožnosti přihlašujícího, které je doplněním obligátního hesla. Přidaný faktor může mít mnoho podob, např. kód zaslaný v SMS nebo e-mailu, jednorázový kód (tzv. TOTP) generovaný speciální aplikací či fyzický (má podobu USB klíčenky) nebo digitální (je uložen ve správci hesel) bezpečnostní klíč.

Základním pilířem tohoto ověřování je fakt, že přidaný faktor je pro útočníka velmi náročné získat nebo duplikovat, ať už kvůli limitovanému času nebo osobní vzdálenosti. Útočník se tedy nemůže dostat v přihlašovaní dál, i když by se mu podařilo zcizit, prolomit nebo uhádnout heslo.

Pozor! Použití dvou různých hesel za sebou **není vícefaktorového ověření**. Účinnost vícefáktorového ověření snižuje také například povolení náhledů zpráv na uzamčené obrazovce mobilního zařízení. Doporučujeme proto zobrazování náhledů zpráv zakázat, nebo nevyužívat formu ověření skrze SMS.

Tam, kde je to možné, doporučujeme vícefaktorové ověření využívat, a to zejména u klíčových služeb a nástrojů, kde by útočník v případě zjištění hesla mohl způsobit významné škody. Jde zejména o e-mailové schránky, elektronické bankovnictví, správce hesel či významné informační systémy univerzity IS MU a INET MU. V rámci Masarykovy univerzity je žádoucí aktivovat MFA i pro prostředí Microsoft M365.

Proč mít nastaveno vícefaktorové ověření?

Shoulder surfing je technika sociálního inženýrství, při které útočník sleduje svou oběť, když zadává své citlivé informace (hesla, PIN kódy, čísla kreditních karet) na zařízení s displejem. Podstata útoku tkví v tom, že se útočník snaží strategicky přiblížit k oběti, což mu umožní mít přímý výhled na displej a pečlivě monitorovat stisky kláves nebo znaků. Útočník pro tento útok využívá přelidněná místa, jako jsou např. veřejné dopravní prostředky, kde je snazší být v těsné blízkosti cíle.

Jak si nastavit vícefaktorové ověření?

V souladu s informacemi a návody na webu IT MU doporučujeme pro zvýšení zabezpečení vašeho účtu a identity použít jako primární možnost **bezpečnostní klíč** (WebAuthn) a jako sekundární **ověřovací kód** (TOTP). Nastavit aktivaci vícefaktorového ověření pro jednotlivé služby je možné skrze Uživatelský profil pro správu vybraných služeb.

[2] MFA = Multi-Factor Authentication. Alternativně se lze potkat i s pojmem dvoufaktorové ověřování (2FA = Two-Factor Authentication). Pojmy 2FA a MFA lze v kontextu tohoto školení tedy považovat za zaměnitelné.

a) **Bezpečnostní klíč (WebAuthn)**

Je fyzické zařízení nebo aplikace využívající asymetrickou kryptografii. Jako bezpečnostní klíč může sloužit počítač či chytrý telefon (např. Windows Hello pro Windows či Touch ID pro macOS) nebo speciální USB klíčenka (např. YubiKey). Pokud si nejste jistí, zda zařízení touto funkcí disponuje, doporučujeme jej otestovat skrze následující odkaz.

Jak to funguje? Při přihlášení server posílá výzvu, kterou bezpečnostní klíč „podepisuje“. Server poté ověří, zda tato odpověď byla podepsána soukromým klíčem, jež náleží k uloženému veřejnému klíči.

b) **Ověřovací kód (TOTP)**

Jedná se o jednorázové kódy s omezenou časovou platností, které generuje speciální (TOTP) aplikace (např. Aegis Authenticator pro Android a Raivo OTP pro iOS). Pro správné nastavení vícefaktorového ověření je potřeba přidat token pro ověřovací kódy a vše vzájemně propojit ve vícefaktorovém ověření Jednotného přihlášení MU. Posléze stačí jen kód zobrazený v aplikaci zkopírovat a vložit nebo opsat při přihlášení. K aktualizaci kódu dochází každých 30 sekund.

Doporučení: Je-li to možné, dejte přednost bezpečnostnímu klíči před jednorázovým kódem. Bezpečnostní klíč je pohodlnější na používání a odolá phishingu.

MUNI

III. Zabezpečení zařízení

Zabezpečit si svá digitální zařízení, která využíváme, jako jsou počítače, tablety a chytré telefony, je klíčové pro ochranu soukromí v dnešním digitálním světě. Nedostatečně zabezpečená zařízení jsou totiž velmi lákavým cílem pro útočníky. Ti na ně mohou například naistalovat škodlivý software, což může mít fatální následky na vaše soukromí v podobě krádeže citlivých dat anebo peněz z bankovních účtů.

Jak si zabezpečit své zařízení?

Prvním krokem pro zabezpečení vašich digitálních zařízení je **zajistit jejich fyzickou bezpečnost**. Nenechávejte proto svá zařízení odemknutá, pokud je opouštíte. Přece jen ve vašich zařízeních schraňujete spoustu cenností, které stojí za to si střežit.

Dále pak doporučujeme, abyste **měli každé zařízení uzamčené** ideálně pomocí otisku prstu, rozpoznání obličeje anebo pomocí PINu. Co naopak nedoporučujeme, je používat odemykání pomocí gesta u mobilních zařízení, které je pro útočníka velmi snadné prolomit. Dalším naším tipem pro vás je: **Nepůjčujte zařízení**, které používáte pouze vy (ať už k pracovním nebo soukromým účelům), jiným lidem! Buďte obezřetní. Snížíte tak riziko, že vám někdo ukradne například vaše přihlašovací údaje k bankovnímu účtu anebo jiné cennosti.

Pokud by se vám někdy stalo, že **naleznete USB disk**, **SD kartu** anebo jiné **paměťové médium**, rozhodně jej nezapojujte do vlastního zařízení. Nikdy totiž nevíte, co v něm může být. Přestože vás láká zjistit, co jste našli, existuje riziko, že se na daném zařízení nachází škodlivý software, který by mohl poškodit váš počítač. Proto doporučujeme přemoct vlastní zvědavost a **předat médium na kontrolu IT oddělení**, kde se o něj postarají.

Pozor na návnady!

Baiting je metoda sociálního inženýrství, při které útočník nechá infikované zařízení (např. USB disk či jiné paměťové médium) na místě, kde jej oběť může snadno nalézt (např. výtah, parkoviště, vchod do budovy). Poté využívá zvědavosti oběti, která vloží toto médium do svého zařízení. Tím se nainstaluje škodlivý kód, který umožní útočníkovi získat přístup do zařízení oběti nebo do celé sítě, ve které se zařízení nachází.

V neposlední řadě vám doporučujeme, abyste **udržovali váš operační systém** a **antivirus** (ať už na svém počítači anebo mobilu) **aktualizovaný**. To znamená neodkládat nabízené aktualizace! Každý program v sobě má chyby, které mohou útočníci zneužít ve svůj prospěch. Aktualizace jim to znemožní. Ideální řešení je **nastavit** si **automatické aktualizace**.

Dva antivirové programy = silnější zabezpečení?

Přítomnost dvou a více antivirů na zařízení způsobuje konflikty při kontrole souborů. Běžné antivirové aplikace sledují soubory v **reálném čase** – např. při spuštění webového prohlížeče bude antivir kontrolovat soubor firefox.exe, který je součástí prohlížeče. Pokud na zařízení běží několik antivirů, každý z nich se bude snažit tento soubor zkontrolovat současně. Výsledkem je, že **soubor nebude správně** zkontrolován, protože v jednom okamžiku může být přístupný pouze jedné aplikaci.
Existuje však výjimka v případě **Microsoft Defender**, který je součástí operačního systému Windows. Pokud si uživatel nainstaluje jiný antivirový program, Windows Defender se automaticky vypne, aby se předešlo konfliktům a duplicitnímu skenování.

Naší závěrečnou radou, jak zachovat vaše zařízení zabezpečené, je: **Stahujte soubory pouze z oficiálních a ověřených zdrojů**. Snížíte tak riziko, že si do počítače anebo do mobilu stáhnete škodlivý virus, který vám vaše zařízení zablokuje. Ovšem i v oficiálních obchodech, jako je App Store nebo Obchod Google Play, se mohou vyskytovat nebezpečné aplikace. Proto si vždy **pozorně přečtěte**, o jaké přístupy vás stažená aplikace žádá. Povolte pouze ty, které jsou nutné pro fungování samotné aplikace. Střežte si své soukromí a nepovolujte aplikacím nahlížet tam, kam nahlížet nepotřebují. Buďte obzvláště obezřetní v případě žádostí o přístup ke kameře, mikrofonu, kontaktům anebo ke zprávám! Vhodné je také sledovat hodnocení aplikace, které dokáže napovědět, zda bude aplikace škodlivá.

MUNI

IV. Práce s daty

Pojmem **data** lze označit veškeré informace zaznamenané v digitální podobě, které zaměstnanec v rámci výkonu své **práce obdrží, zpracovává či vytváří.** Každý zaměstnanec by měl dbát o vhodné uložení a zajištění dat způsobem, aby nedošlo k jejich ztrátě, poškození či zneužití.

Ukládání a zálohování dat

Ukládání a zálohování jsou procesy, které zajišťují ochranu a uchování důležitých dat a informací. Jejich cílem je minimalizovat riziko ztráty dat v důsledku hardwarové poruchy zařízení, počítačových virů či jejich náhodného smazání. Na univerzitě existuje široká škála možností pro **ukládání a zálohování dat**, přičemž jednotlivá úložiště poskytují různé úrovně zabezpečení.

Před tím, než se rozhodnete, kam uložit svá data – zda na USB disk, síťové úložiště nebo do cloudu, je vhodné se podívat, jaká úložiště jsou vhodná, pro jaké typy dat. Nejste-li si jisti, s jakým typem dat pracujete, neváhejte se obrátit na odborníky z ÚVT.

Proč ukládat a zálohovat?

Ransomware je **škodlivý software**, který má za cíl zašifrovat data, případně zablokovat uživateli přístup k zařízení. K dešifrování dat většinou požaduje útočník zaplacení výkupného v digitálních měnách, jako je Bitcoin. Ransomware je možné **stáhnout v nepozornosti**, např. z přílohy v e-mailu nebo při návštěvě napadeného webu či skrze jiný infikovaný stroj v síti. Jakmile uživatel přílohu spustí, tak dojde k zašifrování dat, přičemž vyskočí požadavek na výkupné. Bez dešifrovacího klíče není možné se k zašifrovaným souborům již dostat. Budete-li svá data zálohovat, výrazně snížíte riziko jejich nenávratné ztráty.

Jak ukládat a zálohovat data v prostředí MU?

Uživatelé mohou využívat pro ukládání a zálohování dat úložiště poskytované Microsoft 365, konkrétně se jedná o cloudové služby OneDrive a Sharepoint. Je nutno zdůraznit, že pracovní informace a data by měla být ukládána pouze v oficiálně doporučovaných a používaných nástrojích organizace.

a) **OneDrive** je „osobní“ úložiště, které umožňuje uživatelům ukládat, sdílet a synchronizovat své soubory a dokumenty online. Toto úložiště je vhodné pro uložení vašich souborů, které nepotřebujete sdílet. Složku OneDrive si můžete do vašich zařízení připojit dle návodů na IT MU.
b) **SharePoint** je určen především pro sdílení dokumentů a usnadnění spolupráce s nimi v rámci oddělení, týmu nebo napříč organizací.

Zálohování zajistí ochranu a uchování důležitých dat a informací v případě jejich náhodného smazání, hardwarové poruchy zařízení nebo ransomware.

Můžete kombinovat víc úložišť třeba podle účelu, např.:

- pracovní data zálohujte na **pracovní** Disk Google (přihlášení pomocí UČO@mail.muni.cz) nebo OneDrive (přihlášení pomocí UČO@muni.cz)
- soukromé fotky a videa na **osobní** Disk Google (přihlášení vaším osobním Google účtem)

Doporučení: Zaveďte „zlaté pravidlo“ zálohování 3–2–1! Tři kopie, dvě média, z toho každé na jiném místě (doma/v práci). Může to znít přehnaně, ale u opravdu důležitých dat, jejichž ztrátou byste utrpěli finančně či emočně (např. výzkumná data, rozepsaný článek, rodinné fotky), vám toto pravidlo zajistí klidný spánek.

Není povoleno využívat soukromá úložiště (např. Dropbox, **osobní** Google Disk) pro ukládání pracovních informací a dat.

Přístupová oprávnění

Při používání úložišť (SharePoint, OneDrive) je důležité monitorovat přístupová oprávnění ke sdíleným dokumentům pro minimalizaci rizika neoprávněného přístupu a sdílení. Na webu IT MU naleznete návody a postupy, jakým způsobem je možné zkontrolovat nastavení jednotlivých oprávnění či jak vhodně nasdílet dokumenty, aby nedošlo k nežádoucím únikům informací mimo definovaný okruh uživatelů. **Doporučení: Nastavujte sdílení konzervativně, tedy pouze oprávněným osobám.** Sdílejte soubory pouze s těmi, kdo k nim mají mít přístup, a nezapomeňte sdílení zrušit, pominou-li důvody. Návody, jak sdílení nastavit, naleznete na it.muni.cz. **Nesdílejte pracovní data veřejně.** Není-li k tomu důvod, nikdy nesdílejte pracovní data „všem v internetu“. Výjimkou mohou být např. volně dostupné prezentace a PR materiály, kde je to naopak žádoucí.

ŠIFROVÁNÍ DISKU

Šifrování disku zajišťuje, že i když někdo získá fyzický přístup k vašemu disku, data na něm budou nečitelná. Pokud vaše zařízení někdo ukradne, šifrování zabrání útočníkovi v přístupu k vašim citlivým informacím.

- Na Windows šifrování zajišťuje součást systému zvaná **BitLocker.**
- Na macOS šifrování aktivujete pomocí nástroje **FileVault.**
- Moderní **mobilní zařízení** jsou šifrována automaticky, je však nutné používat zámek obrazovky.

Doporučení: Aktivujte si šifrování disku na vašich počítačích! Aktivaci šifrování disku zvládne každý, je to na pár kliknutí a opět tím posílíte bezpečnost vašich dat.

V. BEZPEČNÁ KOMUNIKACE

Uživatelé MU mají k dispozici univerzitní poštovní schránky s adresami **učo@muni.cz** a **učo@mail.muni.cz**. Zaměstnanci navíc mohou požádat o vytvoření fakultní poštovní schránky prostřednictvím lokální podpory IT. K e-mailové komunikaci je možné přistupovat prostřednictvím webových rozhraní nebo skrz aplikace, tzn. poštovní klienty (např. Microsoft Outlook, Mozilla Thunderbird či iCloud).

V rámci organizace je jako hlavní prostředek komunikace preferován e-mailový systém M365 s licencí pro MS Outlook. Další možnosti e-mailového nastavení je možné provést v IS MU. Alternativou je také využití e-mailu @mail.muni.cz s přesměrováním do MU Gmail.

Návody týkající se konfigurace e-mailové schránky naleznete na webu IT MU.

Doporučené platformy pro videokonference jsou MS Teams či Google Workspace. Alternativně lze taktéž využít aplikaci Zoom. Zdůrazňujeme, že pro práci s těmito aplikacemi je nezbytné striktně dodržovat přihlášení prostřednictvím univerzitní licence.

Mějte na paměti, že pracovní témata často obsahují citlivé informace

Není proto vhodné přesměrovávat pracovní poštu do osobních e-mailových schránek. Důvod je ten, že jsou využívány servery třetích stran pro příjem a odesílání zpráv, a není tím zaručena ochrana citlivých údajů, dat a zabezpečení!

Své pracovní záležitosti komunikujte výhradně přes oficiální pracovní kanály. Nesdělujte tedy informace tohoto druhu přes osobní komunikační platformy (např. Messenger, WhatsApp apod.) či sociální sítě (Facebook, Instagram apod.).

KOMUNIKAČNÍ PLATFORMY NA MU

MS Teams je kolaborativní nástroj umožňující individuální a skupinové pracovní chaty, audio a videohovory či videokonference. Je součástí univerzitní licence Microsoft 365. Mimo to mají zaměstnanci k dispozici i Zoom či Google Meet. Je však nutné přihlašovat se prostřednictvím vašeho univerzitního účtu. Výhodou těchto nástrojů je skutečnost, že komunikace je vždy šifrována.

Tzv. **end-to-end šifrování** je základem zabezpečené elektronické komunikace. Funguje tak, že odesílající strana data před odesláním zašifruje a k jejich dešifrování dochází až na straně příjemce. Obsah zprávy tak při své cestě po síti není čitelný pro nikoho mimo příjemce.

Jak si zabezpečit poštu?

Šifrování je základem ve správně zabezpečené elektronické komunikaci. Funguje tak, že u zpráv, které jsou odesílány, dochází k jejich zašifrování pomocí veřejného klíče příjemce, který ji posléze dešifruje svým privátním klíčem. Tím se zařídí, aby zpráva nebyla při své cestě kyberprostorem kýmkoli jiným čitelná – což třeba poskytují nástroje s tzv. end-to-end šifrováním (tj. zprávu mohou dešifrovat pouze komunikující strany).

Pokud potřebujete elektronicky podepisovat dokumenty nebo zabezpečit e-mailovou komunikaci, existuje možnost využít **osobní certifikáty**. S pomocí osobního certifikátu, který je vydán důvěryhodnou certifikační autoritou přes službu Trusted Certificate Service (TCS), můžete prokázat svou identitu v e-mailové komunikaci. Kromě toho je na Masarykově univerzitě možné získat osobní kvalifikovaný certifikát, který je uznáván i orgány státní správy. Certifikáty lze využít v několika případech. Patří sem ověřování identity osoby nebo objektu, ochrana soukromí pro zajištění, že informace budou dostupné pouze pro určené osoby. Dále pak šifrování, které zabezpečuje, že informace zůstanou nečitelné pro neoprávněné osoby, a digitální podpisy, které zajišťují neodvolatelnost a integritu zprávy.

Připojení

Při prohlížení webových stránek webový prohlížeč předává informace potřebné pro správné zobrazení stránky (např. rozlišení obrazovky, nastavený jazyk). Tyto informace však mohou být využity ke snížení anonymity uživatele.

> Pro zjištění, jaké informace o vás prohlížeč prozrazuje, můžete navštívit webovou stránku https://amiunique.org.

Wi-Fi (Wireless Fidelity) je technologie, která umožňuje bezdrátové připojení k internetu prostřednictvím rádiového spektra. Wi-Fi se často používá pro připojení počítačů, chytrých telefonů, tabletů a dalších zařízení k internetu v domácnostech, kancelářích a veřejných místech, jako jsou kavárny nebo letiště. Abyste se mohli připojit k Wi-Fi síti, potřebujete zařízení, které podporuje bezdrátové připojení (jako je chytrý telefon nebo počítač), a přístup k Wi-Fi routeru nebo jinému zařízení, které poskytuje připojení k internetu.

VPN (Virtual Private Network) je síť, která umožňuje připojit se k internetu prostřednictvím bezpečného a šifrovaného připojení, které chrání vaše soukromí. Když používáte VPN, vaše skutečná IP adresa (číselná identifikace konkrétního zařízení, např. počítače) v prostředí internetu je skrytá a namísto toho se zobrazuje IP adresa VPN serveru. Při práci **mimo univerzitní síť** (mimo připojení kabelem či přes Eduroam) vždy využívejte z důvodu bezpečnosti připojení přes VPN. Masarykova univerzita poskytuje VPN zaměstnancům a studentům **bezplatně**. Návod na instalaci naleznete na stránkách IT služby MU.

MUNI

VI. PHISHING

V online prostředí komunikujeme neustále – posíláme i přijímáme velké množství e-mailů a zpráv z nejrůznějších zdrojů. Komunikace v kyberprostoru však přináší mnoho nástrah. Jak tedy zajistit adekvátní úroveň zabezpečení?

Phishing je podvodná technika, při které se útočník obvykle vydává za důvěryhodnou osobu nebo instituci a přiměje oběť za pomocí **manipulace** (urgence, časového nátlaku), aby pro něj něco vykonala, nejčastěji:

- poslala mu informace,
- nainstalovala si škodlivý software,
- klikla na odkaz v e-mailu, který vede na podvrženou webovou stránku. Na této stránce jsou většinou umístěny podvodné formuláře k **zadání přihlašovacích údajů, čísel platebních karet a dalších citlivých informací**.

Phishingové e-maily jsou mimořádně nebezpečné. Mohou se snadno zamaskovat mezi běžné pracovní e-maily, což zvyšuje riziko, že uživatelé bez povšimnutí kliknou na podvržené odkazy nebo poskytnou citlivé informace, aniž by si uvědomili, že se jedná o podvod.

Hlavičky e-mailu

Odesílatel e-mailu může být podobný jménu a adrese e-mailu legitimní organizace (například bankovní instituci), ale ve skutečnosti se liší např. mírně upraveným názvem nebo doménou (část za zavináčem: @mail.muni.cz). V případě našeho univerzitního prostředí se můžeme setkat s hlavičkami podobnými inet-mt@ics.mun**l**.cz místo oficiální inet-mt@ics.muni.cz.

Co dělat?

Je nutné kontrolovat adresu odesílatele a každou nepatrnější změnu v názvu domény (jako je použití písmena *„v“* místo *„u“* apod.).

Jak vypadá nesprávná webová adresa?

https://www.muni.cz

https://www.mvni.cz („v“ místo písmene „u“)

Tělo e-mailu

Je důležité kontrolovat **obsah phishingového e-mailu**, který může obsahovat URL odkazy vedoucí na neznámé webové stránky a požadavky na citlivé informace, jako jsou přihlašovací údaje a čísla platebních karet. Útočníci mohou v e-mailech navozovat falešné urgentní situace (například výhrůžky ztrátou dat), aby uživatele pod tlakem donutili k rychlému jednání bez dostatečného zvážení.

Co dělat?

I když se tyto e-maily mohou zdát na první pohled jako důvěryhodné, podstatné je si uvědomit, že legitimní autorita (např. banka nebo univerzita) nikdy nebude požadovat citlivé údaje, jako je např. heslo, prostřednictvím e-mailu. Kriticky zhodnoťte obsah e-mailu a webových stránek, na které je odkazováno. Hlídejte si neobvyklý text s gramatickými chybami, krkolomnými frázemi a nesmyslným oslovením. Dále se ujistěte, že odkazy vedou na legitimní webové stránky a že URL adresa je opravdu ta, kterou chcete navštívit.

Patičky e-mailu

Loga umístěna v patičkách e-mailů jsou nejčastěji zneužita, aby navodila pocit, že se jedná o oficiální e-mail. V momentě, kdy uživatel vidí logo instituce, kterou zná a důvěřuje jí, je méně opatrný a může být náchylnější k zadání citlivých informací, aniž by si uvědomil, že se jedná o útok.

Co dělat?

Při přijímání e-mailů od neznámých odesílatelů je nutné být opatrný a nenechat se uchlácholit zdánlivě věrohodně vypadajícími prvky. V případě pochybností o jejich pravosti neklikejte na odkazy. Místo toho kontaktujte přímo danou instituci či odesílatele, aby ověřili pravost e-mailu.

Přílohy e-mailu

Podezřelé přílohy mohou na první pohled působit dojmem, že se jedná o legitimní soubory nebo dokumenty (PDF, DOC, MP3). Signifikantním rysem je to, že právě název podvržené přílohy má odlišnou příponu – místo „DOC“ nebo „DOCX“ jsou užita jiná písmena, která se neshodují s ikonou. Podezřelé mohou být také komprimované přílohy (RAR, ZIP).

Co dělat?

Nutné je mít **funkční a aktualizovaný antivirový** program, přílohu neotvírat a případně využít nástroj pro kontrolu podezřelých souborů.

Útočníci dokáží být vynalézaví!

Vishing (voice-phishing) a **Smishing** (SMS phishing) jsou nové formy útoků využívající momentu překvapení a neznalosti uživatele.

a) **Vishing** funguje na principu podvodného zavolání na soukromé či pracovní číslo uživatele. Volající se představí jako pracovník banky nebo technické podpory a naléhá na uživatele k rychlé reakci v souvislosti s údajnými problémy na jejich účtech. Obvykle dojde k přesycení uživatele množstvím informací typu „účet byl napaden“ či „banka zaznamenala neautorizovanou platbu“ atd., přičemž volající naléhá, že je nutno obratem jednat.

b) **Smishing** využívá podobný způsob útoku, avšak pomocí podvodných textových zpráv. Útočníci zprávy maskují jako legitimní komunikaci od důvěryhodných subjektů (banky nebo mobilní operátoři), přičemž se pokoušejí získat citlivé informace, jako jsou přihlašovací údaje (uživatelská jména, hesla, mobilní kódy atd.) nebo údaje o platebních kartách.

Naše závěrečná rada zní: **Kriticky hodnoťte požadavky**, které jsou na vás kladeny! Důvěryhodné subjekty, jako jsou banky či jiné instituce, nikdy nebudou požadovat citlivé informace a údaje, jako je např. heslo, prostřednictvím e-mailu, hovoru nebo SMS zprávy.

VII. Hlášení incidentů

O bezpečné online prostředí na univerzitě se stará Kyberbezpečnostní tým Masarykovy univerzity (dále jen „CSIRT-MU“), který je součástí Ústavu výpočetní techniky. Mezi jeho

činnosti spadá koordinace a řešení bezpečnostních incidentů souvisejících s infrastrukturou MU.

Pokud jste se stali obětí útoku nebo máte podezření, že vám do schránky přišel například podvodný e-mail, neváhejte se obrátit na členy CSIRT-MU, a to skrze zaslání e-mailu na adresu csirt@muni.cz anebo vyplnění kontaktního formuláře.

Při nahlašování incidentů je třeba:

- **Uvést zdroj hlášení**, tedy vaše jméno, příjmení a UČO.
- **Definovat problém**, tedy vlastními slovy co nejpřesněji popsat, co za komplikaci řešíte. Každá drobnost dopomůže příslušnému pracovníku k vyřešení potíží, protože situaci lépe pochopí.
- **Předat důkazy.** Pokud vám například přišel podvodný e-mail, přepošlete ho rovnou celý, a to včetně příloh, odkazů **a hlaviček e-mailu**. V případě jiných problémů je vhodné dodat například i screenshot obrazovky.