ZAJÍMAVOSTI ZE SVĚTA GDPR A INFORMAČNÍ BEZPEČNOSTI LEDEN 2021

Česká zemědělská univerzita v Praze
Odbor bezpečnosti

Vlachynský Petr
ČZU V PRAZE

Odpovědnost správce za OÚ z externího informačního systému

Podle GDPR odpovídá za zpracování osobních údajů vždy správce osobních údajů. Současně má povinnost zajistit, a i doložit jejich řádné zpracování. Vše se začalo řešit zejména kvůli nedávno provedené kontrole veřejné vysoké školy. Přijímací řízení, ve kterém osoba podala přihlášku ke studiu, je vedeno elektronicky prostřednictvím informačního systému. Kontrolovaný subjekt se bránil tím, že příslušný informační systém je dodáván externím dodavatelem a některé funkcionality plynou z nastavení tohoto systému.

Ředitel odboru dozoru Jiří Žůrek na stránkách Úřadu pro ochranu osobních údajů dodává: „Jednalo se například o překlápění osobního údaje z modulu „uchazeč“ do modulu „student“, a to s ohledem na rozsah shromažďovaných osobních údajů. Zejména pak šlo o způsob přihlášení do informačního systému pomocí rodného čísla. Tady Úřad v rámci provedené kontroly konstatoval, že je nepřípustné, aby rodné číslo uchazeče o studium bylo využíváno za účelem přihlašování do příslušného informačního systému, je-li přihláška ke studiu podávána elektronicky.“

Je třeba se zabývat tím, zda je zpracování legitimní, zda byla porušena zásada účelového omezení a zda není přítomné riziko pro zabezpečení zpracování. To se v tomto případě však nestalo. Pokud si objekt vybere informační systém, musí současně posoudit možnost všech funkcionalit a nastavení a respektovat znění čl. 25 GDPR v oblasti záměrné a standardní ochrany osobních údajů a článku 5 odst. 1 obecného nařízení (např. minimalizace údajů).

Každý subjekt by navíc měl mít na paměti, že nelze automaticky považovat splnění všech povinností GDPR jen na základě toho, že jiní správci tento informační systém využívají.

Pozor na častý phishing!

21. 1. 2021 varoval NÚKIB před vlnou phishingových e-mailů šířících se na českém internetu. Útočníci chtějí získat přihlašovací údaje k e-mailovým schránkám. Postup je zpravidla následující.

Uživatel nejdříve obdrží zprávu, že byl nalezen problém s jeho e-mailovým účtem. Typově se jedná například o zprávy "Dokončete prosím proces aktualizace, aby váš e-mail zůstal aktivní", nebo "Prostor vaší poštovní schránky je plný", ke kterým je připojen podvodný odkaz a vyplnění přihlašovacích údajů. I přesto, že e-mail a odkaz působí amatérsky, útočníci zneužívají schránky uživatelů k rozesílání phishingů dále, tudíž zprávy mohou chodit z legitimních adres, což přispívá k rychlejšímu šíření.

V druhé fázi jsou pak z napadeného účtu rozesílány další zprávy, nejčastěji s konspiračními teoriemi či žádostmi o peníze. I přesto, že tyto zprávy neobsahují odkazy ani přílohy, NÚKIB důrazně doporučuje zprávy neotvírat a smazat je.

Své přihlašovací údaje si hlídejte, případně si s danou osobou telefonicky ověřte, že se opravdu jedná o její žádost.

Pozor na falešné SMS zprávy o výsledcích vašich testů na COVID-19

NÚKIB upozorňuje na falešné SMS a e-maily s výsledkem testu na COVID-19. Jde o klasický phishing–tedy pokus přimět uživatele pod falešnou záminkou kliknout ve-mailu na odkaz, který může vést například na stránku s malwarem.

E-maily přicházejí jak lidem, kteří byli na testech na covid-19, tak i lidem, kteří na testech nebyli. V případě, že podobný e-mail dostanete, důrazně doporučujeme neotvírat odkazy ani přílohy, pokud si nejste zcela jisti, že je zpráva legitimní. To lze ověřit například kontrolou adresy odesílatele, která by měla odpovídat e-mailové zdravotnického zařízení, které vás testovalo.

Podobu takového podvodného emailu vidíte na obrázku.

-------- Forwarded Message --------
Subject:Výsledky testů č. 2910-211
Date: Sun, 25 Oct 2020 22:59:05 +0000
From:VFN <support@landmarkswimmingpools.com>
Reply-To:lab@vfn.cz
To:[redacted]

Dobrý den,

v odkazu níže naleznete výsledky svých testů na CoVid-19 z naší laboratoře.

Výsledky: https://vfn.cz/laborator/vysledky-online/e939rd12313

Tento email byl vygenerován automatickým systémem, neodpovídejte na něj prosím.

Vojenská fakultní nemocnice Praha.

Určeno pro:[redacted] Datum odeslání: 10/25/2020 10:59:05 pm

Konec běhání po úřadech. Přichází bankovní identita

Obíhat úřady kvůli každé maličkosti a pamatovat si přihlašovací údaje pro nejrůznější portály nebaví nikoho. Obojí by se letos mělo stát minulostí díky takzvané bankovní identitě. Jednoduchý nástroj umožní ověřit totožnost digitálně pomocí přihlašovacích údajů do internetového bankovnictví.

Online tak snadno podáte daňové přiznání nebo podepíšete smlouvy s telefonními operátory či dodavateli energií. Novinku umožnila novela zákona o bankách, která začala platit od 1. ledna 2021.

„Jde o jeden z největších digitalizačních projektů českého bankovního sektoru, který občanům výrazně zjednoduší život," říká Monika Zahálková, výkonná ředitelka České bankovní asociace, která projekt iniciovala.

Bankovní identitu může využít až 5,5 milionu obyvatel Česka, kteří mají internetové bankovnictví. Jako první mají možnost tímto způsobem komunikovat s veřejnou správou.

„První banky, které již prošly náročným akreditačním procesem u ministerstva vnitra, jsou v tuto chvíli v závěrečné fázi příprav a testování svých technických řešení a třeba do Portálu občana se již mohou přes svou bankovní identitu v rámci zkušebního provozu přihlásit první náhodně vybraní klienti," uvádí Zahálková.

V tuto chvíli mohou například zažádat o výpis z bodového hodnocení řidiče nebo o výpis z rejstříku trestů. Ještě letos získají také možnost podat elektronickou žádost o nový řidičský průkaz.

Do budoucna by se tímto způsobem mohli přihlašovat i na portál Moje daně. Bankovní identita by měla umožnit rovněž žádat online o sociální dávky nebo získat e-recept či potvrzení od lékaře.

Zdroj: Forbes.cz

WhatsApp na tenkém ledě

Irský úřad pro ochranu dat dokončil kontrolu zpracování osobních údajů společnostní WhatsApp, která se týkala především informování uživatelů o zpracování jejich dat a získávání souhlasu. Irský úřad dle neoficiálních informací předložil úřadům z dalších členských států EU před Vánoci návrh rozhodnutí k připomínkám. Irský úřad navrhuje konstatovat porušení GDPR a uložení pokuty v rozmezí 30-50 milionů euro.

Uživatelé této aplikace v posledních týdnech reagovali hromadnými přesuny na více zabezpečené aplikace pro komunikaci.

NÚKIB a SÚJB na společné cestě za bezpečností

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) a Státní úřad pro jadernou bezpečnost (SÚJB) chtějí nadále spolupracovat. Budou společně kontrolovat subjekty, které podléhají jejich regulaci, s cílem hlubší expertízy, zefektivnění kontroly, úspory času a snížení zátěže pro kontrolované subjekty.

Nadále totiž bude sjednocená předpisová základna i pohled na infrastrukturu. Obě strany chtějí zefektivnit předávání informací a spolupracovat na přípravě podkladů pro školení či cvičení v rámci prevence.

Předsedkyně SÚJB Dana Drábová se na stránkách NÚKIB vyjádřila následovně: „význam kybernetické bezpečnosti roste ve všech oblastech, je tedy stále důležitější také pro zajištění jaderné bezpečnosti našich jaderných zařízení, zejména jaderných elektráren. Jsem ráda, že se nám podpisem memoranda podařilo formalizovat rámec spolupráce mezi NÚKIB a SÚJB, která výborně funguje na pracovní úrovni a již přinesla důležité výsledky, například přesnější vymezení IT systémů jaderných elektráren spadajících do kritické informační infrastruktury."

Ředitel NÚKIB Karel Řehka při podpisu memoranda uvedl, že „pod regulaci NÚKIB i SÚJB spadají subjekty a systémy, bez kterých se stát a jeho občané nemohou obejít. Proto jsme se shodli, že je třeba spojit naši expertízu a nejen postupovat jednotně při kontrolách, ale také si vyměňovat informace, které jsou pro naši práci nezbytné."

Kybernetická bezpečnost v ČR se musí vypořádat s řadou výzev

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) na svých stránkách zveřejnil tiskovou zprávu Nejvyššího kontrolního úřadu. NKÚ v letech 2015 až 2019 prověřoval zajištění kybernetické bezpečnosti.

Součástí NÚKIB je vládní CERT (Computer Emergency Response Team), který zaznamenal v období od roku 2017 do poloviny roku 2020 celkem 916 hlášení kybernetických incidentů, přičemž na první polovinu roku 2020 připadá 31 % z nich. Kybernetická bezpečnost v ČR vyžaduje investice a resorty bohužel nemají ani zdaleka přehled o tom, kolik peněz na ni doopravdy vynakládají. Dle šetření je to zhruba 2,8 miliardy korun, což není dostačující. ČR nedokáže monitorovat či vyhodnocovat finance směřující právě do kybernetické bezpečnosti.

Inspirací by nám mohla být Velká Británie, kde jsou výdaje na kybernetickou bezpečnost zvláštní položkou rozpočtu.

Jakým výzvám se musí ČR postavit? Měl by vzniknout podrobný model nebo schéma fungování spolupráce nejen mezi NÚKIB a MV. Je třeba dokončit automatizovanou platformu napomáhající ke sdílení informací o kybernetických bezpečnostních hrozbách a incidentech. NÚKIB a MV nemají dostatek odborníků, mají problém s jejich získáváním a případně také udržením těchto pracovníků.

Uniklá data ze slovenské aplikace Moje eZdravie

V rámci aplikace Moje eZdravie byla ohrožena data 390 tisíc pacientů. Na chybu umožňující přístup k datům bez jakéhokoliv ověření či šifrování upozornila slovenská IT firma Nethemba nejdříve úřady, které chybu opravily, a až poté veřejnost. Odborníci si současně stěžovali na absenci ochrany dat a mechanismu bránícímu hromadnému stahování údajů. Únik osobních údajů, tedy například jména, příjmení, rodného čísla, data narození, pohlaví, čísla mobilního telefonu, místa pobytu či e-mailu, útočníci zneužívají k phishingů či vishingu.

Bezpečnostní standard pro videokonference

Karanténa i čím dál tím oblíbenější práce z domova donutila Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) a Národní agenturu pro komunikační a informační technologie (NAKIT) vytvořit Bezpečnostní standard pro videokonference. Díky této spolupráci vznikl dokument nabitý radami, doporučeními a příklady.

Není se čemu divit, závislost na komunikačních technologiích v průběhu času roste. Mnoho zaměstnanců nebylo připraveno pracovat z domova, nemluvě o zajištění bezpečné komunikace. Čerpat z něj mohou doslova všichni, od institucí státní správy a samosprávy po soukromé firmy či neziskové organizace. Cílem je zejména nastavit bezpečné prostředí pro komunikaci se svými zaměstnanci, spolupracovníky či partnery.

Ředitel NAKIT a vládní zmocněnec pro ICT Vladimír Dzurillase přitom na stránkách NÚKIB nechal slyšet: „Digitalizace státní správy se týká i problematiky lepšího a efektivnějšího fungování úřadů a organizací. Videokonference se díky opatřením nouzového stavu staly ze dne na den standardem i nutností pro každodenní práci. I tyto technologie je třeba do informačních systémů zakomponovat bezpečným způsobem, aby jejich instalací a používáním nevznikla bezpečnostní hrozba. Spolu s NÚKIB, a za přispění státních i komerčních partnerů, jsme připravili tento dokument, který by měl všem organizacím pomoci s definicí požadavků na videokonferenční systém, jeho implementaci a bezpečný provoz.“

Minimální bezpečnostní standard

Experti z Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), Národní agentury pro komunikační a informační technologie (NAKIT) a Ministerstva vnitra vytvořili, s cílem pomoci společnostem s kybernetickou bezpečnostní, padesátistránkový dokument Minimální bezpečnostní standard. Konkrétně se jedná o organizace jako jsou obecní úřady, zdravotnická zařízení, školy nebo i soukromé firmy, které nejsou zahrnuty v zákonu o kybernetické bezpečnosti, ale měly by respektovat a dodržovat základní pravidla.

V jedné části se dokument věnuje managementu organizací a ve druhé IT specialistům. Blíže vše na stránkách NÚKIB popisuje ředitel odboru regulace NÚKIB Adam Kučínský:„Pro manažery popisujeme zejména nastavení řídících a kontrolních procesů, které je v organizaci nezbytné zavést a dodržovat. Zároveň zdůrazňujeme jejich důležitost, neboť podle našich zkušeností je základním předpokladem systematického přístupu ke kybernetické bezpečnosti právě podpora ze strany vrcholového vedení při jejím prosazování.“

Koncepce rozvoje a Národní strategie kybernetické bezpečnosti ČR

NÚKIB zveřejňuje svou Národní strategii kybernetické bezpečnosti České republiky na období let 2021 -2025 a Koncepci rozvoje.

První dokument čítá 24 stran a je rozdělen do 3 částí: SEBEVĚDOMĚ V KYBERPROSTORU, SILNÁ A SPOLEHLIVÁ SPOJENECTVÍ, ODOLNÁ SPOLEČNOST 4.0. V úvodním slovu v dokumentu Národní strategii kybernetické bezpečnosti České republiky na období let 2021 -2025 se ředitel NÚKIB Karel Řehka vyjadřuje ke kyberprostoru a moderním technologiím jako k nedílné součásti našich životů, současně zmiňuje, že v minulém roce byly na zabezpečeném kyberprostoru životně závislé zájmy ČR.

Dokument Koncepce rozvoje má 54 stran a je rozdělen do osmi kapitol, důraz je kladen na současnost, výzvy, vize NÚKIB, rozvoj kapacit do roku 2027, směr dalšího rozvoje a vyplývající požadavky.

Dokumenty najdete pod odkazem zde: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/

Základní bezpečnostní opatření od NÚKIBU

ZÁKLADNÍ BEZPEČNOSTNÍ OPATŘENÍ PRO VRCHOLOVÉ VEDENÍ ORGANIZACE

Tento dokument je určen vrcholovému vedení organizací a čelným představitelům institucí – osobám, které mají největší vliv na směřování dané organizace a mají významné rozhodovací pravomoci. Důležitost těchto osob je však zároveň staví do pozice, kdy jsou lákavým cílem pro útočníky snažící se narušit kybernetickou bezpečnost organizace. Z tohoto důvodu je pro tyto osoby doporučeno dodržovat níže uvedená opatření ke snížení rizika ohrožení fungování organizace a naplňování povinnosti péče řádného hospodáře. Zároveň je potřeba mít vždy na paměti, že chování vrcholového vedení má odraz v chování běžných zaměstnanců – pokud vrcholové vedení pravidla nerespektuje, lze těžko vyžadovat plnění pravidel i po řadových zaměstnancích.

Tento dokument je doporučením a nenahrazuje žádné právní předpisy, tedy zejm. právní úpravu kybernetické bezpečnosti. Tento dokument nemůže nikdy pokrýt veškerá opatření, která lze aplikovat. Další opatření nad rámec tohoto dokumentu, vhodná pro danou organizaci, mohou navrhnout bezpečnostní specialisté v dané organizaci.

HLAVNÍ BEZPEČNOSTNÍ PRAVIDLO

RESPEKTOVAT BEZPEČNOSTNÍ POKYNY SPECIALISTŮ V DANÉ ORGANIZACI.
Každá organizace by se měla snažit dosahovat bezpečného prostředí a nakládání s daty. Za tímto účelem organizace také obvykle zaměstnává specialisty, kteří mají zabezpečení organizace na starosti. Jejich doporučeními, pokyny a návrhy je nutné se řídit a dodržovat je, jinak nemůže být bezpečnost nikdy na přijatelné úrovni. Neváhejte se na ně obrátit v případě dotazů nebo potřeby upřesnění těchto základních opatření.

PRÁCE S FIREMNÍM POČÍTAČEM NEBO SMARTPHONEM

NEPOUŽÍVAT SOUKROMÁ ZAŘÍZENÍ PRO PRACOVNÍ ÚČELY.
Soukromá zařízení nejsou pod správou organizace. S používáním soukromých zařízení je obvykle spojeno jejich neustálé přenášení, snížený dohled či sdílení se členy rodiny. Dále obsahují aplikace, které nejsou nutné k pracovním účelům. To vše přináší zvýšené riziko pro bezpečnost uživatele i celé organizace. Pokud jsou v organizaci soukromá zařízení přesto používána, obraťte se na bezpečnostní specialisty v organizaci a řiďte se jejich pokyny.

OMEZIT PŘÍSTUP K PRACOVNÍM ZAŘÍZENÍM A UZAMKNOUT JE POKAŽDÉ, KDYŽ JE POTŘEBA SE OD NICH VZDÁLIT.
Nehlídané zařízení dává prostor útočníkovi. Odemknuté zařízení bez dozoru dává komukoliv prostor k manipulaci s ním i jeho obsahem. To je potřeba mít na paměti nejen v kanceláři, ale především na veřejných místech (např. na konferenci, ve vlaku, apod.).

U počítače s Windows je nejjednodušší způsob rychlého zamknutí klávesová zkratka WIN + L.

U MAC počítače je nejjednodušší způsob rychlého zamknutí klávesová zkratka COMMAND + CONTROL + Q.

U mobilního zařízení stisknutí zamykacího tlačítka.

NEPŘIPOJOVAT NEZNÁMÉ USB FLASH DISKY, EXTERNÍ DISKY A JINÁ PAMĚŤOVÁ ZAŘÍZENÍ.
Neznámá zařízení mohou obsahovat škodlivý kód, který se ihned po připojení dostane do zařízení. V případě nevyhnutelné nutnosti připojit neznámé médium je potřeba provést alespoň antivirovou kontrolu tohoto zařízení.

POUŽÍVAT HESLA, ČÍSELNÉ KÓDY NEBO JINÉ ZPŮSOBY ZABEZPEČENÍ TAK, JAK JE MÁ ORGANIZACE ZAVEDENÉ.
V případě ztráty nebo odcizení je zařízení podstatně lépe chráněno.

VOLIT DLOUHÉ, ZAPAMATOVATELNÉ FRÁZE PRO HESLA, PŘÍPADNĚ POUŽÍVAT SPRÁVCE HESEL.
Šifrovaný správce hesel umožňuje jednoduchou a bezpečnou správu všech potřebných přihlašovacích údajů a hesel na jednom místě.

PŘI ZADÁVÁNÍ PŘIHLAŠOVACÍCH ÚDAJŮ A HESEL SE UJISTIT, ŽE JE NIKDO CIZÍ NEVIDÍ, NAPŘÍKLAD POHLEDEM PŘES RAMENO.
Především v případě pohybu na veřejném místě s větším počtem lidí, kamer nebo fotoaparátů (např. na konferenci, ve vlaku apod.), je zvýšené riziko, že útočník jednoduše zjistí a následně použije tyto údaje. V případě mobilních telefonů preferovat odemykání zařízení pomocí otisku prstu nebo skenu obličeje.

PROVÁDĚT AKTUALIZACI ZAŘÍZENÍ A NEVYPÍNAT PRAVIDELNÉ AUTOMATICKÉ AKTUALIZACE SYSTÉMU A PROGRAMŮ.
Aktualizace zařízení je způsob, jakým výrobce zařízení opravuje nově známé zranitelnosti, které by mohly toto zařízení ohrozit. Pokud má být aktualizace provedena, je potřeba jí nebránit a neodsouvat termín jejího provedení. Termín pravidelných automatických aktualizací je obvykle možno v zařízení nastavit. Stejně jako je tomu v případě aktualizací systému, také programy je potřeba aktualizovat. Program, který doposud fungoval bez problému, může být bez aktualizace téměř nepoužitelný a nebezpečný.

VYUŽÍVAT MOŽNOSTI ŠIFROVÁNÍ DAT NA INTERNÍCH I EXTERNÍCH ZAŘÍZENÍCH.
Šifrování zabezpečí data především při ztrátě nebo odcizení zařízení. Data na pracovním počítači by měla být šifrována, ale je nutno mít na paměti také ostatní zařízení, na kterých se tato data vyskytují.

PRAVIDELNĚ ZÁLOHOVAT DATA.
Vždy existuje riziko ztráty dat. Může se jednat o poruchu zařízení, jejich ztrátu nebo cílený útok, který data nenávratně zašifruje. Je proto vhodné myslet na zálohu důležitých dat a tuto zálohu uchovávat na jiném místě než v zařízení samotném, šifrovat a připojovat ji k zařízení pouze v okamžiku zálohování. Nezálohujte pracovní data na jiná než organizací určená zařízení.

VYVAROVAT SE POUŽITÍ VEŘEJNÉ WI-FI A DALŠÍCH VEŘEJNĚ NEBO ZDARMA POSKYTOVANÝCH SLUŽEB.
Veřejně poskytovaná Wi-Fi a další služby jsou jednoduchým způsobem, jak může útočník proniknout do zařízení a mít přehled o všech činnostech, především o použití přihlašovacích údajů a hesel. Problémem jsou zejména veřejné a nezabezpečené Wi-Fi (např. bez hesla, ale také s veřejně dostupným heslem – např. restaurace, konference apod.), a pokud to není nutné, je vhodné se k nim vůbec nepřipojovat. Tento problém je možné snížit použitím zabezpečeného spojení (tzv. VPN), nejvhodnější je pak používat VPN v kombinaci s mobilním internetem.

VĚNOVAT ZVÝŠENOU POZORNOST BEZDRÁTOVÝM TECHNOLOGIÍM, JAKO JE WI-FI, BLUETOOTH, NFC A DALŠÍ.
Bezdrátové technologie v zařízení je vhodné zapnout jen tehdy, pokud jsou využívány – představují potenciální cestu, jak proniknout do zařízení.

NESDÍLET INFORMACE, KTERÉ JDOU NAD RÁMEC POTŘEBY AKTUÁLNÍ SITUACE.
Vše, co je obsahem komunikace, může být v budoucnu zneužito.

MÍT NA PAMĚTI, ŽE NIC NENÍ ZADARMO.
Nabídky a on-line služby zdarma, které jsou jindy placené, je potřeba důkladně zvažovat.

POKUD PROBÍHÁ KOMUNIKACE V ČASOVÉ TÍSNI, JE POTŘEBA O TO VÍCE UVAŽOVAT O JEJÍM OBSAHU A SDĚLOVÁNÍ POŽADOVANÝCH INFORMACÍ.
Útočníci rádi pracují s časovou tísní – teď je třeba něco vykonat, napravit, sdělit. Je potřeba to mít na paměti. Škoda z prodlení bývá menší než důsledky neuvážených činů.

ZABEZPEČENÍ ON-LINE ÚČTŮ

NEPOUŽÍVAT SOUKROMÉ ÚČTY PRO PRACOVNÍ ÚČELY A OBRÁCENĚ.
Soukromé účty (e-mailové schránky, cloudové služby, apod.) uživatele nejsou pod dohledem organizace a jsou tak pro organizaci zvýšeným rizikem např. z důvodu zvýšeného rizika infikování firemní sítě škodlivým kódem. Platí to i obráceně; pracovní účty není žádoucí používat pro soukromé účely.

PŘÍSTUPY K PRACOVNÍM ÚČTŮM CHRÁNIT HESLY. PRO KAŽDOU SLUŽBU POUŽÍVAT JINÉ UNIKÁTNÍ HESLO.
V případě používání slabého hesla je jeho prolomení útočníkem otázkou okamžiku. Pokud dojde k vyzrazení hesla k jednomu účtu, má útočník možnost použít stejné heslo i u jiných účtů.

NESDĚLOVAT JINÝM OSOBÁM PŘIHLAŠOVACÍ ÚDAJE A HESLA K VLASTNÍM ÚČTŮM A SLUŽBÁM.
V případě pracovního e-mailu, pracovního intranetu nebo hesla do počítače může mít takové jednání závažné následky.

V PŘÍPADĚ, ŽE JE TO MOŽNÉ, VYUŽÍVAT VÍCEFAKTOROVOU AUTENTIZACI, A TO PŘEDEVŠÍM U SLUŽEB JAKO ELEKTRONICKÉ BANKOVNICTVÍ, PRACOVNÍ NEBO SOUKROMÝ E-MAIL A DALŠÍ.
Běžným způsobem realizace vícefaktorové autentizace je obdržení kontrolní SMS po zadání přístupových údajů. V organizaci však mohou existovat i jiné způsoby vícefaktorové autentizace uživatelů.

PRO BĚŽNOU ČINNOST VYUŽÍVAT BĚŽNÝ UŽIVATELSKÝ ÚČET. ADMINISTRÁTORSKÝ ÚČET JE URČEN PRO TY, KDO VYKONÁVAJÍ SPRÁVU SYSTÉMŮ A ZAŘÍZENÍ V ORGANIZACI.
Administrátorský účet s vyššími oprávněními je určen výhradně pro správu systému, typicky prostřednictvím IT oddělení.

NEPOUŽÍVAT KONTROLNÍ OTÁZKY PRO OBNOVENÍ HESLA.
Nikdy není vhodnou alternativou k obnovení hesla zadávat kontrolní otázky typu „nejmenší planeta sluneční soustavy" či „rodné jméno manželky". Podobné informace jsou či mohou být dohledatelné z veřejných zdrojů. Je-li taková kontrolní otázka povinná, je potřeba k ní přistupovat jako k heslu a volit ji tak, aby nebyla dohledatelná.

Další doporučení a vzdělávací kurzy:
https://www.nukib.cz/cs/infoservis/doporuceni/

www.nukib.cz

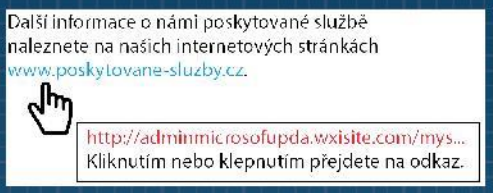
Národní úřad pro kybernetickou a informační bezpečnost

KONTROLOVAT, ZDA WEBOVÉ STRÁNKY PODPORUJÍ PROTOKOL HTTPS.
V případě internetových stránek, které vyžadují přihlášení (zejm. internetové bankovnictví, e-mail apod.), je potřeba věnovat pozornost, zda je taková stránka zabezpečena HTTPS protokolem. Pokud tomu tak není, nejsou zadané údaje vhodně zabezpečeny a jsou jednoduše zneužitelné.

Zobrazení HTTPS protokolu v internetovém prohlížeči

Zobrazení v internetovém prohlížeči bez protokolu HTTPS (přes tyto stránky nezadávat hesla)

NA INTERNETOVÉ ODKAZY KLIKAT OBEZŘETNĚ.
Je-li to možné, zkontrolovat, že odkaz nevede na podezřelou URL adresu. Skutečná URL adresa se po umístění kurzoru myši na odkaz bez rozkliknutí zobrazí vedle kurzoru (viz ilustrační obrázek), případně v okénku v levém dolním rohu stránky. Pokud nelze ověřit, kam odkaz vede, neklikat na něj.



SPRÁVNÁ A BEZPEČNÁ KOMUNIKACE

PŘISTUPOVAT K INFORMACÍM NA INTERNETU KRITICKY, NEMUSÍ BÝT PRAVDIVÉ.
Je potřeba ověřovat, zda jsou informace skutečně pravdivé a zda jsou uvedeny v patřičném kontextu.

NEZVEŘEJŇOVAT OSOBNÍ ANI JINÉ CITLIVÉ INFORMACE.
Je potřeba zvážit, zda je skutečně nutné určité informace zveřejňovat. Data narození, náboženské vyznání nebo například fotografie mohou být následně zneužity, a to ať už proti konkrétním osobám, tak i proti organizaci, kterou tyto osoby zastupují.

OVĚŘIT IDENTITU PROTISTRANY PŘI KOMUNIKACI.
Je potřeba mít na paměti, že osoba, se kterou je komunikováno, se může vydávat za někoho jiného, což je zvláště důležité při prvotní komunikaci. Pokud existuje podezření, že osoba není tou, za kterou se vydává, je možné např. zavěsit a zavolat zpátky na telefonní číslo z oficiálního seznamu.

VĚNOVAT OBSAHU E-MAILŮ ZVÝŠENOU POZORNOST A V PŘÍPADĚ PODEZŘELÉHO E-MAILU NEBO PŘÍLOHY INFORMOVAT IT/BEZPEČNOSTNÍ ODDĚLENÍ ORGANIZACE.
Prostřednictvím příloh e-mailové zprávy se může jednoduše šířit škodlivý kód, který se po otevření přílohy aktivuje. Z tohoto důvodu je potřeba otevírat jen takové e-maily a jejich přílohy, které jsou důvěryhodné, a o těch podezřelých informovat IT oddělení.

CO JE TO PHISHING?
Phishing je podvodná technika, prostřednictvím které se útočníci snaží například získat osobní nebo citlivé informace (přihlašovací údaje, datum narození, číslo platební karty atd.), nasměrovat uživatele na podvodnou stránku, nebo zaslat závadnou přílohu. Phishing se nejčastěji šíří formou e-mailových zpráv, které vypadají jako odeslané z důvěryhodných institucí. Neváhejte se obrátit na bezpečnostní specialisty v organizaci s dotazy, jak phishing poznat, případně využijte doporučení zveřejněná na stránkách NÚKIB, v sekci Infoservis – Doporučení – Spear-phishing a jak se před ním chránit.