# ZAJÍMAVOSTI ZE SVĚTA GDPR A KYBERNETICKÉ BEZPEČNOSTI ČERVEN 2020

Česká zemědělská univerzita v Praze
Odbor bezpečnosti

Vlachynský Petr
ČZU V PRAZE

# Úřad pro ochranu osobních údajů

UOOU od ledna do května letošního roku obdržel více než 100 ohlášených případů porušení zabezpečení osobních údajů. Bezpečnostním incidentem postižené subjekty byly převážně z oblastí finančnictví a bankovnictví, školství, zdravotnictví a veřejné správy, z velké části obce.

Vážným a častým důvodem ohlášení byl phishingový útok do počítačového systému. Taková událost se týkala také zdravotnických zařízení.

Mezi méně závažné incidenty patřilo například hlášení o nabourání se do systému studentem střední školy, který získal a zneužil přístupové údaje svého učitele a následně si upravil některé údaje v docházce a prospěchu.

Významný počet případů porušení zabezpečení je způsoben nedostatečným poučením a proškolením jednotlivců, následkem jejichž pochybení, např. neuvážlivou manipulací s elektronickou poštou, pak dojde ke zpřístupnění údajů nebo umožnění narušení systému (phishingový útok).

# Měření teploty na pracovišti

Měřením tělesné teploty při vstupu na pracoviště, v poslední době spojované s Covidem-19, dostal od ÚOOÚ zelenou.

Zvýšená teplota je jedním z typických příznaků onemocnění COVID-19. Údaj o teplotě těla lze ale zároveň podřadit mezi tzv. **citlivé osobní údaje** vypovídající o zdravotním stavu. Jeho zpracování je tedy zásahem do soukromí a v daném případě i do dalších práv zaměstnance, například nebude-li mu následně umožněn vstup na pracoviště.

ÚOOÚ proto pro odstranění pochybností zveřejnil svůj postoj, že uvedené opatření zaměstnavatele v podobě měření teploty zaměstnanců při vstupu na pracoviště lze za současných výjimečných podmínek považovat za zpracování osobních údajů v oprávněném zájmu zaměstnavatele, který napomůže zaměstnavateli dostát jeho povinnostem v oblasti pracovního práva při předcházení ohrožení zdraví zaměstnanců. Zákoník práce totiž ukládá.

ÚOOÚ zároveň doplnil, že měření teploty zaměstnanců nemusí být vždy posuzováno jako zpracování osobních údajů. Pokud není naměřená teplota zaznamenána ve spojení se jménem nebo jinými údaji umožňujícími identifikaci konkrétní osoby, nejde o zpracování osobních údajů v působnosti nařízení GDPR. Může se jednat například o případy, kdy senzor pouze měří teplotu procházejících osob, aniž by ukládal jakékoliv údaje, a pouze upozorní na zaznamenání zvýšené teploty.

# Evropskému parlamentu unikly osobní údaje

Postiženo bylo více než tisíc zaměstnanců a členů Evropského parlamentu, konkrétně se jednalo o 1 200 účtů úředníků a zaměstnanců a dalších 15 000 účtů odborníků na záležitosti EU.

# Praha sbírá osobní údaje, ale už neříká, co s nimi dělá

Při vyřizování „Lítačky“ do pražské MHD pro své dítě přes internet, musíte nahrát fotografii své občanky a rodný list dítěte. Nebo pro výdej parkovací karty zase potřebují rodné čísla. Přitom ale není jisté, co s citlivými údaji dělá.

Operátor Pražského podniku to vysvětluje tím, že jde o ověření totožnosti, jako na fyzicky na úřadě. Co se ale s požadovanými dokumenty děje dále, to už nikdo nezjistí. Známka o rodném listu nebo třeba o rodném čísle chybí jak v sekci osobní údaje pražské služby Lítačka, tak v Záznamech o činnostech zpracování karty Lítačka. To vše i přes to, že to unijní nařízení GDPR vyžaduje. Navíc uchovávání kopie občanských průkazů zákon výslovně zakazuje.

# Vyjádření Sboru pro ochranu osobních údajů a Úřadu na ochranu osobních údajů k Chytré karanténě

Sbor připouští, že monitorování výskytu koronavirové nákazy za pomoci moderních technologií je v zájmu celého lidstva. I v této mimořádné době je však třeba dbát na adekvátní zajištění ochrany osobních dat subjektů údajů. „Stav nouze je okolnost, která může legitimizovat omezení svobod, ovšem jen za předpokladu, že tyto restrikce budou úměrné a omezené jen na dobu nouze,“ napsal ve svém stanovisku.

Blíže se pak v této souvislosti věnuje oblastem zákonnosti zpracování, klíčovým zásadám zpracování osobních údajů, užití mobilních dat o poloze a oblasti zaměstnávání.

ÚOOÚ se vyjádřil k mimořádnému opatření ministerstva zdravotnictví v souvislosti s projektem chytrá karanténe, které nařizuje provozovatelům mobilních komunikačních sítí (operátorům) a bankám zpracovávat „provozně-lokalizační“ údaje a údaje „o době a místě použití elektronického platebního prostředku“, tedy o pohybu a chování osob nakažených nemocí COVID-19.

Celý text najdete zde: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=41505

Důležité informace také zde: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=6134

# Koronavirus hraje zločincům do karet

Dle analýzy antivirové společnosti ESET vyšlo najevo, že počet podvodných stránek se oproti loňskému roku zvedl o 21%. Nejčastěji jde o phishingové weby, které se často vydávají za bankovní instituce, zpravodajské portály či servery velkých obchodních řetězců a známých značek.

Nejčastěji jim jde o důvěrné hesla, čísla kreditních karet nebo další citlivé údaje. Uživatelé tak nevědomky pomáhají počítačovým pirátům ovládnou jejich účet a možnost jim tak ukrást peníze přes internetové bankovnictví.

Pandemie koronaviru je momentálně téma, které podvodné stránky využívají nejvíce, aby vylákaly údaje od uživatelů.

# Únik dat v EasyJet

Uniklé data se týkají více než 9 milionu zákazníků.

Britská BBC se nechala slyšet, že aerolinka EasyJet informovala britský úřad pro ochranu osobních údajů (ICO) o velkém úniku dat, konkrétně se jednalo o e-mailové adresy, údaje o cestách či data z platebních karet. O části incidentu věděla aerolinka již v lednu. O úniku dat z platebních karet, který se týká 2 208 zákazníků, informoval EasyJet až začátkem dubna.

Dle EasyJetu útočníci zatím data nijak nezneužili. Doporučení ICO ovšem mluví jasně: klienty s uniklými e-mailovými adresami je nutné varovat a upozornit je na riziko phishingu.

# Vir Agent.ASH si lidé často stahují sami

Agent.ASH patří mezi nejrozšířenější viry na internetu. Soustředí se přitom výhradně na chytré telefony a počítačové tablety, které běží na platformě Android. Tento trojský kůň slouží útočníkům k tomu, aby do napadeného zařízení stáhl další nezvané návštěvníky.

Zajímavé na tom je, že si jej do svého zařízení nejčastěji nainstalují uživatelé sami. A to stažením aplikace z neoficiálního zdroje, aby se vyhli placené verzi.

Uživatelé tak zpravidla ani netuší, že si ve snaze ušetřit pár korun stáhnou do zařízení právě Agent.ASH, poté nabudou dojmu, že aplikace je nějakým způsobem poškozená, a dále se problému již nevěnují.

# V Holandsku se řeší aplikace TikTok

Poslední dobou stále více populární aplikace na videa TikTok se dostává v Nizozemsku do sporu s místním dozorovým úřadem.

Každým dnem miliony dětí a teenagerů tráví čas nad touto čínskou aplikací, ale zapomínají nad rizikem ochrany svých osobních údajů. V tom jim nejspíš pomůže nizozemský kontrolní úřad, který tuto aplikaci prověří.

# Škodlivý kód WannaCry jako nejrozšířenější vyděračský virus

Tento škodlivý kód již způsobil kolaps drah, benzínek a nemocnic všude po světě. Ani po letech se však na něj nepodařilo vyzrát, a tak je stále číslo jedna mezi nejrozšířenějšími vyděračskými viry na světě.

Společnost Kaspersky pak vyčíslila, že během jediného měsíce tento vir infikuje až 4,3 milionů počítačů.

Nejvíce postižené je v tomto směru Rusko, kde vir napadl 45% z celkového napadeného počtu. Je to dáno tím, že v chudších lokalitách je stále hojně využívaný zastaralý operační systém Windows XP, který byl škodlivým kódem WannaCrypton nejvíce zranitelný.

# Česko versus kyberútoky

Nejnovější analýza kybernetické společnosti Check Point ukaázala, že česko čelí kyberútokům častěji než ostatní státy. Týdně jsou jich stovky, konkrétně 530, kdy celosvětový průměr je 491 útoků týdně.

Celkem bylo za rok 2019 odhaleno 8417 činů. Kybernetická kriminalita tak rok od roku razantně stoupá. Celkově se kriminalita, která mimochodem v posledních 8 letech klesla o 40%, přesunula do kyberprostředí.

**Počet trestných činů z oblasti kyberkriminality v letech 2011 až 2019:**

| Rok | Počet trestných činů |
|---|---|
| **2011** | 1502 |
| **2012** | 2195 |
| **2013** | 3108 |
| **2014** | 4348 |
| **2015** | 5023 |
| **2016** | 5344 |
| **2017** | 5654 |
| **2018** | 6815 |
| **2019** | 8417 |

Zdroj: Policie ČR