ZAJÍMAVOSTI ZE SVĚTA GDPR A KYBERNETICKÉ BEZPEČNOSTI ZA ROK 2019

Česká zemědělská univerzita v Praze
Odbor bezpečnosti

Vlachynský Petr

ČZU V PRAZE

OBRANA PROTI NEVYŽÁDANÝM MARKETINGOVÝM HOVORŮM

Úřad pro ochranu osobních údajů se věnoval nevyžádaným marketingovým hovorům, které nenavazují na předchozí nákup zboží či využití služeb volajících subjektů. Primární obranou je přitom vznesení tzv. námitky proti zpracování osobních údajů vůči volajícímu subjektu.

Úřad v této souvislosti subjektům radí:

- Je dobré vědět, že pokud není Vaše číslo ve veřejném seznamu označeno zákazem marketingového volání, může být kontaktováno.
- Chytré telefony nabízejí aplikace sloužící k blokování nevyžádaných marketingových hovorů. Mezi takové patří například Nevolejte.cz – Stop Otravům!, ale i další podobné.
- Pokud už k hovoru došlo, doporučuje se, abyste volajícímu nesdělovali své osobní údaje. Volající často zná pouze Vaše jméno a příjmení a pod různými záminkami požaduje sdělení Vašich dalších osobních údajů.
- Také abyste volající subjekt identifikovali (optáním se ho přímo či využitím Vašeho práva na identifikaci účastnického čísla prostřednictvím žádosti adresované Vašemu operátorovi (§67 odst. 1 zákona o elektronických komunikacích)
- Dále Úřad jako postup uvádí vznést námitku proti zpracování osobních údajů adresovanou příslušnému volajícímu, pokud dochází z jeho strany k opakovanému kontaktování
- Případně podat stížnost Úřadu

ZVEŘEJNĚNÍ SHRNUTÍ POZNATKŮ Z DEVÍTI VZDĚLÁVACÍCH AKCÍ PRO POVĚŘENCE

Z šetření Úřadu mj. vyplývá, že účastníci lednového a únorového semináře působí současně ve funkci pověřence pro ochranu osobních údajů u 1–203 správců;

- 43,6 % z nich u správce jediného.
- 12,9 % působí u více správců a nejméně u jednoho z nich interně a
- 43,6 % působí v této roli výhradně externě.

Z odpovědí pověřenců dále vyplývá, že externí působení má vliv na přímý kontakt pověřence pro ochranu osobních údajů se subjekty údajů: ani jednou dosud nebylo kontaktováno 42,1 procenta pouze externě působících ve srovnání s 33,3 procent interně působícími pověřenci. Interně působící pověřenci jsou kontaktováni častěji a zejména se na ně častěji obracejí zaměstnanci správce (dvaapůlkrát častěji).

V BELGII PADLA PRVNÍ POKUTA

Pokuta byla vyměřena na 2.000 EUR za zneužití osobních údajů pro účely voleb. Evropský sbor přitom zdůrazňuje, že i když je pokuta nízká, je tím vyslána jasná zpráva o tom, že OÚ není radno zneužívat a správci musí přijmout svoji zodpovědnost.

MĚSTSKÝ SOUD V PRAZE VYDAL ROZHODNUTÍ OHLEDNĚ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ V OBCI

Městský soud v Praze řešil případ, ve kterém starosta obce Moravský Beroun ukázal jejím zastupitelům posudek, jehož předmětem byla šikana na obcí zřízené základní škole. V tomto posudku byli plně identifikováni jak útočníci, tak i šikanovaná oběť.

V obou případech se jednalo o nezletilé osoby, děti. ÚOOÚ však v tomto jednání spatřoval nedostatečné zabezpečení osobních údajů a v návaznosti na to uložil obci pokutu ve výši 8000Kč. Obec však podala odvolání k soudu.

Městský soud v Praze ale odvolání obce proti ÚOOÚ zamítl s tím, že v tomto případě se jednalo o systematické zpracování OÚ, navíc seznámení členů zastupitelstva obce s neanonymizovanými OÚ bylo nedůvodné a nepřiměřené, a tento postup navíc ignoroval právo na ochranu soukromí dotčených nezletilých osob. Soud dále poukázal na zásadní skutečnost, kdy bylo v posudku uvedeno i jméno šikanované oběti, která by měla být chráněna v maximální možné míře.

Narušení ochrany osobních údajů by šlo předejít v případě, že by úřad důsledně anonymizoval osobní údaje před jejich zveřejněním a měl pro tyto případy zažitý užívaný postup.

VZNIKLA NOVÁ INSTITUCE ZASTŘEŠUJÍCÍ DPO V EU

Celkově osm organizací zastřešující pověřence pro ochranu osobních údajů, včetně domácího Spolku pro ochranu osobních údajů, iniciovalo 7. června 2019 v Berlíně vznik nové instituce s názvem **Evropská federace pověřenců pro ochranu osobních údajů**, která by měla zastřešovat tyto organizace na úrovni Evropské unie. Zakládajícími státy dále jsou Německo, Rakousko, Portugalsko, Francie, Slovensko, Lichtenštejnsko a Řecko. Hlavní sídlo této instituce se pak bude nacházet v Bruselu.

Hlavním cílem nové instituce bude vytvoření profesionální sítě pověřenců ochrany osobních údajů ve výše zmíněných státech Evropské unie, rozvoj a zlepšování společných standardů a získání silnější vyjednávací pozice při jednání s institucemi Evropské unie.

„Ochrana osobních údajů posiluje důvěru klientů a v důsledku tedy i ty společnosti, které pravidla pro zpracování údajů dodržují. Řada států po celém světě nyní přibližuje své právní úpravy principům obsaženým v GDPR nebo se jimi nechá inspirovat při přípravě zcela nových předpisů. Rádi bychom této příležitosti využili a přispěli k tomu, aby ochrana osobních údajů byla vnímána jako ochranná známka ‘celé evropské ekonomiky“, uvedl Thomas Spaeing, zastupitel německého Profesního spolku pověřenců pro ochranu osobních údajů Německa.

Význam tohoto kroku je především v možné koordinaci problematiky výkonu činností DPO na evropské úrovni a vzniku podpůrných materiálů pro činnost pověřence.

ICO POKUTUJE TELEKOMUNIKAČNÍ SPOLEČNOST EE LIMITED ZA ZASÍLÁNÍ NEZÁKONNÝCH TEXTOVÝCH ZPRÁV

ICO (kancelář komisaře pro informace) pokutovala telekomunikační společnost EE Limited £ 100 000 za zaslání více než 2,5 milionu přímých marketingových zpráv svým zákazníkům bez souhlasu.

Zprávy, které byly odeslány počátkem roku 2018, vyzývaly zákazníky k aktivování přístupu a používání aplikace „Moje EE“ ke správě účtu a také k aktualizaci telefonu.

Při šetření EE uvedla, že texty jsou zasílány jako servisní zprávy, a proto se na ně nevztahují pravidla pro elektronický marketing. ICO však zjistila, že zprávy obsahovaly přímý marketing a že je společnost poslala záměrně, i když uznává, že společnost EE Limited se úmyslně nedopustila porušování zákonů o elektronickém marketingu.

CÍLENÝM ÚTOKEM UKRADLI HACKEŘI V BULHARSKU FINANČNÍ DATA MILIONŮ LIDÍ

Bulharsko se setkalo s doposud největším kybernetickým útokem ve své historii, během kterého se útočníkům podařilo dostat prostřednictvím cíleného hackerského útoku do databází bulharské národní finanční správy (NRA). Podle bulharského ministra financí Vladislava Goranova útok postihl přibližně tři procenta databází bulharské finanční správy. Odcizená data však podle něj nejsou tajná a neměla by následně ohrozit finanční stabilitu země.

Ukradená data daňových poplatníků zahrnovala jména, příjmení, adresy, názvy bulharských společností, emaily, PIN kódy a registrační čísla vozidel. Odkaz ke stažení části těchto údajů byl následně přiložen do emailové zprávy, která byla skupinou útočníků zaslána vybraným bulharským mediím. Ministr vnitra Mladen Marinov následně potvrdil, že se tato zaslaná data shodují s daty v databázích NRA.

Podle dostupných informací je hlavním podezřelým dvacetiletý mladík, který prováděl testy zranitelností počítačů a sítí pro nejmenovanou bulharskou firmu zabývající se zabezpečením počítačových systémů.

ÚOOÚ NAVRHL PŘESNĚJŠÍ ÚPRAVU ZMĚNY V OBLASTI ZPRACOVÁNÍ BIOMETRICKÝCH ÚDAJŮ ZAMĚSTNANCŮ

Úřad pro ochranu osobních údajů podal návrh Ministerstvu práce a sociálních věcí ohledně novelizace zákoníku práce. Tato novelizace by se měla týkat upřesnění využití biometrických údajů zaměstnanců na pracovišti dle zásad GDPR. Nutno podotknout, že popularita technologií založených na biometrické autentizaci v posledních letech značně roste, používají se nejčastěji při kontrole vstupu či kontrole docházky.

Při využívání takovýchto systémů však dochází ke zpracování zvláštní kategorie osobních údajů na základě souhlasu mezi zaměstnancem a zaměstnavatelem (čl.9GDPR), což bývá vhodné pouze pro minoritní aktivity. Úřad pro ochranu osobních údajů proto navrhuje umožnění zaměstnavatelům využívání biometrických údajů svých zaměstnanců v omezeném rozsahu, zejména k ochraně svých výrobních a pracovních prostředků.

NEMOCNICE V NIZOZEMÍ DOSTALA POKUTU ZA NEDOSTATEČNÉ ZABEZPEČENÍ OÚ SVÝCH PACIENTŮ

Haagské nemocnici byla nizozemským úřadem pro ochranu osobních údajů (AP) udělena pokuta ve výši 460000€. Jedná se o první udělenou pokutu za porušení GDPR v Nizozemí. Důvodem pokuty bylo nedostatečné zabezpečení osobních údajů pacientů, kdy ke zdravotní dokumentaci pacientů měla přístup nadbytečně velká část nemocničního personálu.

Hlavním důvodem pro kontrolu nemocnice byl případ holandské televizní celebrity Samanthy de Jorg, známé v Nizozemí pod přezdívkou Barbie, která se pokusila v roce 2018 o sebevraždu a byla následně v této nemocnici hospitalizována. Podle dostupných informací pak do jejího lékařského záznamu nahlédlo přibližně 200 zaměstnanců.

Haagská nemocnice porušila čl.32 GDPR, kdy nezajistila úroveň zabezpečení osobních údajů danému riziku.

ÚTOKY NEOPRÁVNĚNĚ POUŽÍVAJÍCÍ LOGO ČESKÉ POŠTY

Česká pošta dne 12.8.2019 vyvěsila na své webové stránky varování před staronovým útokem, kdy útočníci rozesílají e-maily používajíce logo České pošty, které upozorňují, že „mají balík“. Česká pošta vyzývá uživatele, aby neklikali na odkazy v e-mailu ani na něj neodpovídali. Umožnili by tak škodlivému softwaru, aby napadl jejich zařízení. E-maily odesílané opravdu Českou poštou jsou odesílány ze schránky: ceskaposta@cpost.cz.

Kromě těchto podvodných e-mailů je třeba dávat si pozor i na soutěže o mobilní telefony, které se vyskytují buď formou reklamy na sociálních sítích a v chatovacích aplikacích v barvách České pošty nebo formou zpoplatněných SMS (50Kč).

ÚŘAD UPOZORŇUJE NA NADUŽÍVÁNÍ SOUHLASŮ VE ŠKOLSTVÍ

Úřad pro ochranu osobních údajů (dále jen Úřad) na své webové stránky umístil článek upozorňující na to, že školská zařízení s příchodem nového školního roku valí na rodiče souhlasy se zpracováním osobních údajů (dále jen souhlas) v nadměrné míře. Nadužívání tohoto právního titulu je obecně správci nesprávně využíván i tam, kde jde ve skutečnosti o zpracování osobních údajů na základě jiného právního důvodu.

Ve školství se tento jev vyskytuje ve velké míře pro rutinní činnosti, které spadají nebo jsou úzce spojeny s povinnými činnostmi školy/školky podle zákona nebo ve veřejném zájmu.

UŽIVATEL VYSOUDIL NA MALL.CZ ODŠKODNĚNÍ ZA ÚNIK HESLA

Mall.cz za masivní únik osobních údajů hrozí nejenom pokuta od Úřadu, ale musí také zaplatit odškodnění konkrétnímu poškozenému.

V roce 2017 vyšel najevo masivní únik osobních údajů zákazníků využívajících služby internetového obchodu Mall.cz. Šlo o jména, příjmení, e-mailové adresy, hesla a telefonní čísla v plně čitelné podobě. Tyto údaje pak byly více jak měsíc k dispozici na serveru Ulož.to, odkud si je mohl kdokoli stáhnout. Úřad pro ochranu osobních údajů udělil Mall.cz pokutu ve výši 1,5 milionů Kč, proti které se internetový obchod odvolal u správního soudu. Toto řízení doposud probíhá.

Vzhledem k tomu, že uniklo bez mála 736 tisíc e-mailových adres a více než 766 tisíc hesel, mohlo by pro Mall.cz další odškodňování znamenat vážné finanční problémy.

Masivnímu úniku dat v České republice nedokázal zabránit ani T-mobile, kterému byla v roce 2016 ukradena data více než milionu zákazníků.

ZNEUŽITÉ BEZPEČNOSTNÍ ÚDAJE

Twitter použil osobní údaje pro lepší cílení reklamy.

V žádném případě by nemělo dojít k tomu, že svěříte-li jakékoliv společnosti osobní údaje, jako je telefonní číslo či e-mailová adresa za účelem zvýšení bezpečnosti, použije je firma pro lepší zacílení reklamy.

Twitter, poskytovatel sociální sítě a mikroblogu, oznámil, že údaje uživatelů z dvou-faktorové autorizace (2FA) přihlašování byly v některých případech použity pro lepší cílení reklamy. Společnost nicméně okamžitě ujistila všechny uživatele, že jsou všechny uživatele, že jsou jejich osobní data v bezpečí a neunikla.

Toto ale není ojedinělý případ zneužití telefonních čísel poskytnutých za účelem dvoufázové autorizace. Minulý rok se se stejným problémem potýkala i společnost Facebook, kterou Federal Trade Commission(FTC) obvinila z úmyslného používání zmíněných dat pro účely reklamy. V druhé půlce letošního roku dokonce udělila FTC Facebooku pokutu.

SLOVENSKÁ SOCIÁLNA POISŤOVŇA DOSTALA POKUTU 50.000 EURO, PORUŠILA GDPR

Sociálná poisťovňa čelí pokutě ve výši 50 tisíc euro kvůli porušení GDPR. Jedná se přitom o nejvyšší pokutu, která byla na území Slovenské republiky, kdy udělena.

Státní úřad, v jehož vedení stojí Ľubomír Vážny, pochybil v otázce zasílání citlivých informací do zahraničí běžnou poštou. Její služby využívá tisíce lidí, a to nejen na Slovensku, ale i v ostatních zemích EU.

Slováci, kteří pracují v zemích EU, platí běžně sociální pojištění a po splnění podmínek mají nárok na sociální dávky dané země. Jejich žádosti zpracovává právě Sociálná poisťovňa a vše ověřuje s úřady v zahraničí. Jedna z poštovních zásilek, ve které žádala Sociálná poisťovňa o informace zahraniční instituce, se ztratila a nikdo nedokázal říct, co se s balíčkem stalo.

Sociálná poisťovňa si verdikt v podobě pokuty ve výši 50.000 euro poslechla, samotné porušení předpisů ale odmítá a soudní verdikt napadla.

NÁVRH E-PRIVACY NEBYL SCHVÁLEN RADOU EU DO TRIALOGU

V pátek večer 22.11.2019 se v Bruselu na jednání COREPER v rámci finského předsednictví Radě EU hlasovalo o klíčovém legislativním návrhu nařízení k ochraně soukromí e-Privacy.

Návrh nebyl přijat a bude tudíž předmětem dalšího projednávání, v pořadí již sedmého předsednictví, které se jím bude nucené zabývat. Od ledna 2020 tentokrát pod vedením Chorvatů. Stávající znění e-Privacy nezískalo v hlasování potřebný většinový souhlas členských států, aby mohl být zahájen trialog (General Approach).

Výsledek hlasování byl tento:

PRO: Nizozemsko, Dánsko, Bulharsko, Irsko, Řecko, Španělsko, Kypr;

BEZ VYJÁDŘENÍ NÁZORU: (prakticky počítán jako hlas PRO): Litva, Chorvatsko, Lotyšsko

PROTI: Rakousko, Česká republika, Estonsko, Finsko, Francie, Německo, Maďarsko; Itálie; Malta; Polsko; Portugalsko, Rumunsko, Slovensko, Švédsko a Velká Británie

ZDRŽEL SE: (což se prakticky počítá také jako hlas PROTI): Belgie

SPOLEČNOSTI UNICREDIT SE SÍDLEM V ITÁLII UNIKLY ZÁZNAMY MINIMÁLNĚ 3 MILIONŮ ITALSKÝCH KLIENTŮ

Společnost Unicredit se sídlem v Itálii, která poskytuje bankovní a finanční služby, se potýká s únikem dat minimálně 3 milionů domácích zákazníků.

Italští zákazníci se přitom o svá data neobávají poprvé. Obětí útoku, který ovlivnil 400 000 klientů, byla společnost Unicredit i v letech 2016 a 2017.

Unicredit s bohatou historií sahající až do roku 1870 je největší bankovní a finanční institucí v Itálii, v Evropě patří mezi jednu z předních komerčních bank. S působností v 17 zemích s více než 8 500 pobočkami se není čemu divit.

Nejen klienti Unicredit čekají na zveřejnění dalších podrobností, banka totiž pouze potvrdila, že doposud neznámý útočník kompromitoval soubor z roku 2015, který obsahoval více než 3 miliony záznamů italských klientů. Tyto záznamy obsahovaly jména, telefonní čísla a e-mailové adresy zákazníků, včetně bydliště.

Unicredit ujistil své klienty, že se útočníci nedostali k žádným bankovním údajům, a tudíž nemůže dojít k žádným nepovoleným transakcím. Zároveň okamžitě zahájila vyšetřování. V současnosti ověřuje rozsah útoku a kontaktuje všechny klienty, kterých

PŘIŠLA VÁM NA WHATSAPP ZPRÁVA, ŽE JSTE VYHRÁLI POUKÁZKY DO TESCA? JEDNÁ SE O PODVODNOU KAMPAŇ.

Napříč Českou republikou dostávají lidé zprávu skrze komunikátor WhatsApp slibující hodnotné ceny, které mohou příjemci získat v obchodním řetězci Tesco.

Poukázku ve výši dvou tisíc korun potenciální výherci údajně obdrží na adrese www.tesco.com-entradas.com, pokud zprávu přepošle dalším dvaceti lidem. Na samotném webu je zveřejněná klamavá soutěž o iPhone, ve které je nutné odeslat zpoplatněnou SMS.

Přes Facebook se naopak šíří podvodné stránky na Penny a Lidl, které slibují výhru v podobě iPhonu a získání poukázek v hodnotě dvou až dvaceti tisíc korun.

Na podvodnou kampaň, která se dotýká obchodních domů Lidl, Tesco a Penny a ve které se snaží šejdíři získat od českých uživatelů peníze a bankovní či osobní údaje, poukázali analytici české kybernetické společnosti Avast.

30 TISÍC ZAMĚSTNANCŮ FACEBOOKU BYLO OKRADENO

Zloděj totiž ukradl ze zaparkovaného auta jednoho ze zaměstnanců kromě jiných věcí i přenosný pevný disk s nešifrovanými údaji zhruba 30 tisíc zaměstnanců.

Na disku mohl zloděj najít jména, čísla bankovních účtů, platy zaměstnanců, ale také bonusy a poslední čtyři číslice čísla sociálního pojištění. I přesto, že se tiskové oddělení snažilo zaměstnance uklidnit prohlášením, že nezaznamenali jakékoliv zneužití dat, celá událost byla samozřejmě nahlášena policii.

ÚŘEDNÍK CHYBOVAL KVŮLI POUHÉ SHODĚ JMÉNA S JINOU OSOBOU

Muž z Moravy, který se díky úředníkovi ocitl v situaci, kdy musel neustále vysvětlovat, že není hledanou osobou, tedy Čechem se stejným jménem a datem narození.

I úředníci mohou udělat chybu. V poslední době jich není málo. Ombudsmanka měla co dočinění s úředníky, kteří nedostatečně ověřili údaje a zaměnili na základě shody jmen různé osoby.

Jedním z posledních případů byl muž z Moravy, který se díky úředníkovi ocitl v situaci, kdy musel neustále vysvětlovat, že není hledanou osobou, tedy Čechem se stejným jménem a datem narození. Kvůli údajnému dluhu ho navštívili exekutoři, a i přesto, že jim vše vysvětlil, ho navíc po letech zadržela na hraničním přechodu policie, neboť po druhé osobě s totožným jménem bylo vyhlášeno celostátní pátrání. Tím ale jeho trápení neskončilo. Později mu přišlo předvolání z městského úřadu v Čechách. Údajně spáchal přestupek, když se dopustil rvačky v hospodě. O svém jmenovci ví mnohé, například jeho rodné číslo nebo informace o rozvodu.

To ovšem není ojedinělý případ. Ombudsmanka řešila také případ stěžovatele, který byl vyzván k odevzdání řidičského průkazu v důsledku zákazu řízení na 12 měsíců. Ani on nebyl tím pravým viníkem a úředníci ho zaměnili za jinou osobu stejného jména a příjmení. Jindy zase úřad doručoval písemnost osobě, která nemá datovou schránku, a to do datové schránky jmenovce.

BENEŠOVSKÁ NEMOCNICE

Kryptovirus zcela ochromil nemocnici ve středu 11. prosince a k útoku se nikdo nepřihlásil. Provoz v nemocnici se podařilo během pár dní obnovit, nicméně tým IT se situací dále zabývá a pracuje na nápravě.

JAKÁ JSOU NEJHORŠÍ HESLA ROKU 2019?

Čím dál častěji se společnost potýká s nedostatečným zabezpečením a případným porušením dat. Podobné případy ovlivnily během letošního roku miliardy uživatelů internetu.

Není se čemu divit, že se čím dál intenzivněji mluví o nedostatečné kybernetické bezpečnosti jednotlivců i firem. S koncem roku 2019 byla zveřejněna nejhorší letošní hesla.

Nezávislí anonymní vědci společně s firmou NordPasssestavili seznam dvě stě nejoblíbenějších hesel, která unikla v průběhu roku 2019. Společnosti se podařilo shromáždit 500 milionů hesel a výsledky studie byly více než jen znepokojující. Lidé mají špatné návyky, hesla nevolí podle toho, jestli jsou bezpečná, ale aby byla snadněji zapamatovatelná. A sdílejí je napříč internetovými službami.

Velmi populární jsou kombinace čísel, která se snadno zapamatují. Tedy zpravidla 12345 či 111111 nebo 123321. Uživatelé také rádi používají řetězce písmen, které tvoří svislou či vodorovnou linii na klávesnici, tj. asdfghjkl, qazwsxnebo 1qaz2wsx. Heslo “password” je také velmi populární a mezi respondenty ho používalo 830 846 lidí.

Jakých pět nejoblíbenějších hesel se objevilo v žebříčku na předních příčkách?

- 1.12345
- 2.123456
- 3.123456789
- 4.test1
- 5.password

Nejvíce znepokojivý je fakt, že společnost SplashDatastudie zveřejňuje několik posledních let a výsledky zůstávají totožné.