GDPR vyžaduje komplexní přístup aneb jak se zorientovat v nabízených technologiích

Marian Němec I IT Security Consultant, AEC a.s.

Obecné nařízení pro ochranu osobních údajů – již téměř kultovní zkratka GDPR. Jeho schválení v dubnu 2016 proběhlo velmi tiše, o to víc se z něj však na začátku roku 2017 stala mantra pro všechny výrobce a obchodníky s bezpečnostními technologiemi. Velká část z nich slibuje, že právě jejich řešení na 100 % vyřeší požadavky GDPR. A to přesto, že stále existuje až příliš mnoho neznámých. Jak tedy poznat, který dodavatel slibuje nesplnitelné a který dané problematice skutečně rozumí? Jak vybrat vhodná opatření, aby byla zajištěna shoda s GDPR? Základem je uvědomit si, že ochrana osobních údajů vyžaduje komplexní přístup. Automobil taky neochrání posádku lépe jen tím, že mu dáte lepší brzdy.

GDPR je všude

Poslední týdny a měsíce hýbe světem informačních technologií jediné téma. Tím je nařízení Evropského parlamentu definující pravidla a podmínky zpracování a ochrany osobních údajů známé jako General Data Protection Regulation – tedy GDPR. To se na nás řítí ze všech stran a v každém okamžiku. Není jediného dne, abych neobdržel nějakou pozvánku na seminář, konferenci, webinář či minimálně informaci o tom, že nějaký produkt či služba plně vyřeší požadavky evropských zákonodárců. GDPR se stalo doslova bezpečnostní modlou a svým způsobem také prodejním hitem.

V naší praxi jsme se u zákazníků setkali s nemálo případy, kdy dodavatelé svá řešení představovali jako všelék na tuto problematiku. Přestože je většina osobních údajů zpracovávána elektronickou cestou, ochrana osobních údajů se dotýká i fyzických dokumentů (listiny, formuláře apod.) Tam žádná technologie na ochranu dat v síti či počítačích sama o sobě nepomůže. GDPR je komplexní problematika, která nemá jednostranná řešení. Vždy se musí jednat o soubory různých technik a postupů. Cílem mého článku je přinést čtenářům alespoň základní přehled dostupných nástrojů na správné pokrytí GDPR a pomoci zorientovat se v nabízených technologiích.

Bát se, či nebát GDPR

Když si Hamlet pokládal obdobnou otázku, zabýval se smyslem svého života. V otázce ochrany osobních údajů podle GDPR může být řešen smysl podnikání, zda má se všemi těmi požadavky vůbec smyl. Odpověď na otázku, zda se obávat GDPR, je v mnohém jednoduchá, ale současně velmi složitá. Základním předpokladem, jak k této otázce přistoupit, je pochopení faktu, že GDPR je závazné pro všechny subjekty, které zpracovávají „nějaké“ osobní údaje. Je úplně jedno, jestli se jedná pouze o data zaměstnanců, nebo informace o klientech. Fatálním pak může být nepochopení, co vše může být osobním údajem.

Osobním údajem se v GDPR rozumí *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby; …“*

To ve své podstatě znamená, že za osobní údaj lze považovat cokoliv, co umožní člověka přímo i nepřímo identifikovat, nebo ho učiní identifikovatelným. Podle toho je pak třeba posuzovat, zda data, která používám, jsou osobním údajem, či nikoli. Záleží současně na kontextu, kdy, jak a kde je takový údaj využíván. Musíme umět posoudit, zda v případě, že taková data uniknou mimo skupinu zaměstnanců, kteří mají právo je znát,

nebo mimo prostředí firmy, mohou být zneužita, a tak může být ovlivněn život osob, kterých se tyto údaje týkají.

Jak moc se obávat případných požadavků GDPR pak záleží hlavně na tom, s jakými daty a v jakém množství pracujeme. Větší organizace s velkým množstvím zákazníků a zaměstnanců nebo například velké nemocnice jsou logicky mnohem více ohroženy velikostí sankce než menší firmy. To ale v žádném případě neznamená, že bychom se neměli sankcí bát. Jedním z hlavních cílů GDPR je sjednocení podmínek zpracování osobních údajů v celé Evropské unii. A to včetně sankčního režimu. Jako o jednom z nástrojů pro prosazování sankcí se hovoří o principu jednotnosti. Pokud by tento princip měl platit ve své extrémní podobě, je velmi pravděpodobné, že bude jednotné i sankční schéma bez ohledu na stát, kde se bude pokuta udělovat. To by s sebou přineslo velmi extrémní pokuty, zejména ve srovnání se současným stavem.

Z tohoto důvodu by se nemělo GDPR brát na lehkou váhu. Na druhou stranu není na místě ani zbytečný strach a zbrklost při rozhodování.

Dvakrát měř a jednou řež

Tohle staré české přísloví má v sobě ve vztahu ke GDPR více pravdy, než by se mohlo na první pohled zdát. Podle mého názoru se však jedná o správný postoj, který k GDPR zaujmout. Používat něco, čemu říkáme „selský rozum". Tedy rozhodovat se rozvážně, vybírat s rozmyslem a důkladně plánovat.

Jak tedy přistoupit k naplnění požadavků GDPR? Jak bylo řečeno, ochrana osobních údajů se netýká jen dat, serverů či sítí. Kromě elektronického světa se osobní údaje vyskytují i ve fyzickém světě. A i v případě, že máme chránit primárně elektronicky zpracovávaná data, musíme řešit ochranu zařízení, které k tomu využíváme. Zabezpečení serveroven, kanceláří atd. Z toho všeho plyne jediné, ochrana osobních údajů se musí řešit komplexně ve všech oblastech. Neexistuje kouzelný software, který by vše vyřešil.

Abychom mohli vybrat vhodné řešení pro naplnění souladu s GDPR, měli bychom postupovat v logických krocích. Našim klientům doporučuji na počátku celého procesu provést analýzu zpracování osobních údajů. Tedy analýzu všech činností, které provádíme, abychom v nich identifikovali, jaké osobní údaje používáme a proč. Slovy zákona, abychom určili účel zpracování. Současně nám tato analýza přinese přehled o tom, kde získáváme osobní údaje, co s nimi děláme, kde je máme uložené, a další informace, které jsou zásadní pro správné rozhodování. Jak to myslím? Abychom mohli správně vybrat opatření na ochranu osobních údajů, tak musíme vědět, co a kde chránit. Pak je teprve na místě otázka, jakým způsobem vše řešit. Uvedu příklad: internetový obchod s 10 tisíci klienty bude muset přijmout jiná opatření než lékařka, která si drží celou evidenci pacientů v klasických fyzických chorobopisech, počítač používá pouze jako sekundární nástroj. V případě lékařky pak mezi hlavní opatření na ochranu osobních údajů patří kvalitní zámek a dveře, uzamykatelná registratura, případně mříže na oknech, elektronický zabezpečovací systém a možná i například nějaký nástroj na šifrování dat na pevném disku. Ten pro případ, že by její ordinace byla vykradena. Tato lékařka nepotřebuje sofistikované síťové monitoringy, identity managementy atd. Vždy je třeba vybírat taková řešení a postupy, které korespondují s reálnými potřebami, jež plynou právě ze znalosti zpracování osobních údajů.

Analýza zpracování je však teprve prvním krokem k tomu, abychom dosáhli svého cíle – souladu s požadavky GDPR. Dále musíme zvolit vhodný postup, jak zjištěné informace promítnout do realizace dalších opatření. Abychom pokryli celou oblast ochrany osobních údajů, musíme řešit každé jednotlivé části bezpečnosti. Když víme co a proč, musíme definovat také postupy ochrany. Sestavit bezpečnostní plán, bezpečnostní politiku, vytvořit směrnice, metodiky, začít podle těchto pravidel pracovat. Pravidla musejí rovněž být zdokumentována, musejí s nimi být prokazatelně seznámeni zaměstnanci. Řešit musíme organizační, administrativní, personální, fyzickou i technickou bezpečnost. Potřebujeme mít řešení na ochranu, postupy na kontroly, definovat co zaznamenávat, jak zálohovat, plány obnovy, jak hlásit incidenty a mnoho dalších dílčích věcí, které dohromady tvoří ucelený systém ochrany osobních údajů. Nejjednodušším a zároveň nejlepším možným řešení, je využít nějaké metodiky na ochranu informací. Za nejlepší považuji standard ISO 27001. Tento standard je již praxí prověřený, řeší bezpečnost informací jako celek a z komplexního pohledu. GDPR na něj nepřímo odkazuje, když v článku 32 uvádí, že je třeba přijmout opatření přiměřená riziku a zejména pak: *„zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování."* Systém řízení bezpečnosti informací podle uvedeného standardu je nejlepší možnou volbou. Už jen třeba z důvodu, že je v podstatě použit v rámci zákona o kybernetické bezpečnosti (což by mělo mít určitou váhu), ale i z reálné praxe máme potvrzené kladné hodnocení použití standardu pro potřebu ochrany osobních údajů regulátorem. Analýza zpracování osobních údajů tak poskytne potřebné informace pro definování hranic systému řízení bezpečnosti informací a podklady pro vypracování analýzy rizik. Analýza rizik ukáže slabá a silná místa systému a na jejím základě jsme schopni určit vhodná opatření a priority implementace. Až na základě těchto informací bychom měli začít řešit, jakou bezpečnostní technologii použít a k čemu.

Pokud bychom seřadili dílčí kroky do logické posloupnosti, vypadal by seznam činností asi takto:

- Analýza zpracování osobních údajů – zjištění co a proč nastaví parametry pro určení, jak chránit.
- Analýza současného stavu – GAP analýza souladu – zjištění reálné situace.
- Analýza rizik – zdokumentování souvisejících hrozeb a rizik.
- Výběr vhodných technicko-organizačních opatření.
- Implementace vybraných technicko-organizačních opatření.
- Aktualizace interních nařízení.
- Proškolení zaměstnanců.

Z výše uvedeného plyne jediné. Výběr technických prostředků rozhodně není dobré dělat na začátku, na základě nějakých marketingových hesel, ale až po důkladné úvaze.

Technologie mýtů zbavená

Při výběru řešení, která bychom měli použít, je třeba se rozhlížet opět s rozumem v hrsti. Osobní údaje musejí být chráněny po celou dobu zpracování. Je třeba je ochránit před přístupem osob, které nejsou oprávněny je využívat, ale i před neoprávněnými činnostmi osob, které mají právo s nimi nakládat. Nemůžeme se tedy zastavit pouze u ochrany sítě proti napadení z internetu, ale stejně tak nemůžeme řešit jen nastavení uživatelských oprávnění, a tak považovat svůj úkol za splněný. Přesto všechno by výběr produktů a služeb měl stále odpovídat reálným potřebám a požadavkům na bezpečnost.

Antivirová řešení, firewally a další obvyklé bezpečnostní prvky již nejsou dostatečné. Rozvoj technologií vytváří nové bezpečnostní výzvy, nová riziková místa, nové problémy k řešení. Celkový koncept výběru technologií by měl být postaven na třech základních cílech, kterých potřebujeme dosáhnout.

Identifikace dat

Musíme vědět, kde máme jaká data a jakou mají hodnotu/důvěrnost – to nám pomůže určit, jakým způsobem je chránit. Musíme mít data označena, abychom je dokázali rozpoznat při vytváření, používání, přenosu i likvidaci. Samotná identifikace osobních dat není jednoduchá, zejména pro automatizované algoritmy technologií. Vyhledání již existujících údajů je možné jen částečně a závisí na schopnosti rozpoznat, že jde o osobní údaj.

V případě identifikace osobních údajů při jejich vytváření pomůže klasifikace dat. Je však potřeba dát si pozor na typy dat, které je možné klasifikovat (zda jde o dokumenty, aplikační data, databáze apod.). Ne všechna data je možné označit klasifikačním stupněm a spolehat se na jejich následnou dohledatelnost. Existují i nástroje, které se snaží analýzou obsahu identifikovat citlivé informace (zejména je pak možné je nakonfigurovat pro vyhledávání osobních údajů), jejich limity tkví v již uvedené slabé schopnosti tyto informace rozpoznat. Obdobnou funkcionalitu obsahují i technologie DLP, je ale třeba si uvědomit, že DLP se zaměřuje zejména na kontrolu činností, a ne na podstatu obsahu dat, a možnosti definicí vyhledávaných informací často končí u regulárních výrazů, které nejsou dostačující. Zde právě klasifikace dat napomáhá DLP při jejich ochraně.

Při určení, kde se nacházejí osobní údaje, kdo k nim má přístup a jakými prostředky jsou chráněny, je potřebná hloubková analýza, kterou nenahradí žádný nástroj nebo technologie. Ta ale z dlouhodobého pohledu může výrazně pomoci (**tab. 1**).

Ochrana dat

V případě, že víme, kde se osobní údaje nacházejí a jakou mají podobu, je nutné zamyslet se zejména nad otázkami řízení přístupu k těmto datům, ochrany úložišť dat, zabezpečení přenosu a celého životního cyklu při práci s těmito daty. Ochranu osobních údajů můžeme z pohledu bezpečnostních cílů rozdělit zejména na důvěrnost (krádež nebo ztráta dat a jejich zneužití), integritu (změnění dat) a dostupnost dat pro oprávněné použití.

V případě úložišť dat by měla být identifikována všechna úložiště včetně koncových stanic, aplikací a nástrojů (paradoxně i těch bezpečnostních) a tato úložiště

Tabulka 1: Xxxxxxxxxx

Opatření	Může pomoct?
Klasifikační nástroj (pro dokumenty)	**Ano**, klasifikací získáme identifikaci citlivých dat při jejich vytváření.
Data Loss Prevention	**Ano**, DLP může pomoci při identifikaci dat, zejména technologie s tzv. „discovery“ funkcí.
Monitorování sítě	**Ne**, tyto nástroje nejsou schopny identifikovat osobní údaje v obsahu síťového toku.
SIEM technologie	**Ne**, funkcionalita SIEM technologií se obecně odvíjí od událostí, ne obsahu dat a rozlišovací schopnost SIEM je pod možností identifikace osobních údajů.
Monitorování uživatelů a stanic	**Ne**, tyto technologie se zaměřují na činnost uživatele a nedokážou identifikovat, zda pracuje s osobními údaji.

by měla být adekvátně zabezpečena. Je přitom potřeba myslet na dostatečné šifrování úložišť, řízení přístupů včetně monitorování, zálohování, archivace, redundance systémů atd. Na tyto bezpečnostní mechanizmy je samozřejmě možné použít standardní technické nebo procesní opatření. Obdobně musejí být osobní údaje chráněny při přenosu (např. sítí nebo přenosnými médii).

Životní cyklus osobních údajů je obecně hůře definovatelný a závisí na konkrétní společnosti nebo situaci. Obecně je možné říci, že i řadový zaměstnanec by měl dodržovat zásady ochrany osobních údajů, měl by mít zabezpečeny všechny technické prostředky, které při práci využívá, a činnosti s těmito údaji by měly být monitorovány. Monitorování samotné ale neochrání údaje před únikem (krádeží nebo ztrátou), je to jen mechanizmus, kterým se můžeme o úniku dozvědět, monitorováním nemůžeme splnit podmínku opatření proti úniku dat (**tab. 2**).

Monitoring a hlášení

Monitorování je důležité pro GDPR, protože pro naplnění požadavků GDPR je důležité vědět, že dochází k úniku. Jednou z hlavních povinností je totiž hlášení tzv. data breach. Pokud ovšem nedetekujeme, že se něco děje s daty, nemůžeme nic hlásit. Délka doby neidentifikovaného úniku osobních údajů může zásadně ovlivnit výši případné sankce za porušení nařízení.

Oznámení, že došlo k úniku dat, je však až druhým krokem vyřešení požadavků GDPR. Primárně bychom se měli zabývat zejména ochranou osobních údajů. Až po vyřešení (i když jen zdánlivém) základních předpokladů ochrany dat je potřebné řešit oznamování, že došlo k jejich úniku. Pro detekci je pak možné buď využít různé monitorovací technologie, nebo se o úniku dozvíme náhodou od samotného zaměstnance.

Na jaké technologie se tedy zaměřit?

Opět se dostáváme k tomu, že na začátku musíme vědět, co a kde chránit. To je relativně jednoduché, pokud máme data uložená v nějaké aplikaci, kde si jasně nastavíme, s jakou kategorií informací pracujeme, a podle toho přijmeme opatření. Pokud však máme osobní údaje distribuované nejen v aplikacích, ale i na stanicích a síťových složkách, je jejich dohledání extrémně náročné, možná bych si dovolil tvrdit, že v podstatě nerealizovatelné. Jedním z nejslabších bezpečnostních oblastí je neřízené a nekontrolované používání dat uživateli, jejich ukládání na lokální či síťové disky, externí pevné disky, USB paměti a současně jejich přenos s využitím moderních komunikačních nástrojů, to je jedno z nejslabších míst v téměř jakémkoli bezpečnostním konceptu. GDPR s sebou v tomto ohledu přináší renesanci produktů z kategorie DLP. Tato technologie dokáže monitorovat data na koncových stanicích a rovněž na serverech, a to i při jejich přenosu po síti. Díky jejímu nasazení lze efektivně zabránit úniku či ztrátě dat, ať již například přes externí média, jakými jsou flashdisky, USB, externí disky atp., nebo při odeslání dat elektronickou poštou, jejich sdílením do webové sítě či vytisknutím. Z pohledu GDPR se dle mého názoru bude jednat o jedno z nejlepších řešení, které umožní úspěšně chránit osobní údaje. DLP však nikdy nebude mít

Tabulka 2: Xxxxxxxxxx

Opatření	Může pomoct?
Šifrování dat	**Ano**, důsledné šifrování všech úložišť chrání důvěrnost chráněných dat.
Šifrování provozu	**Ano**, v případě přenosu osobních údajů by měla být všechna média šifrována včetně interní sítě, emailové komunikace nebo použití privátních sítí (VPN).
Řízení přístupů	**Ano**, systémy pro řízení přístupů jsou velice důležité pro vymezení oprávnění pro autorizované uživatele.
Data Loss Prevention	**Ano**, v preventivním režimu může zabránit krádeži nebo ztrátě dat v případě, že citlivá data identifikuje.
Monitorování uživatelů a systémů	**Ne**, monitorovací nástroje nedokážou ochránit data, dokážou jen zjistit, že k úniku došlo.
Monitorování sítě	**Ne**, stejně jako v případě monitorování uživatelů nedokáže zjistit, zda se jedná o osobní údaje.
SIEM	**Ne**, SIEM nástroje se zaměřují na vyhodnocování událostí tzv. „post mortem“ a nedokážou data chránit, můžou ale pomoct v detekci úniků dat.
Zabezpečení stanic (např. AV)	**Částečně**, zabezpečení koncových stanic chrání data vůči útokům na systémy, i když se nezaměřují přímo na ochranu osobních údajů, patří mezi základní vrstvu ochrany.
Síťové bezpečnostní technologie (např. FW, IDPS, NBA, WAF)	**Ne**, tyto technologie sice přispívají k celkové bezpečnosti společnosti, ale nemají přímý vliv na ochranu dat.

maximální přínos, pokud nebudete mít správně klasifikovaná a kategorizovaná data.

Zvýšení efektivity DLP může přinést používání klasifikačních nástrojů. Klasifikace informací je jedním z důležitých opatření ze standardu ISO 27001. Klasifikační stupně definují postupy distribuce, skartace, uložení, zabezpečení apod. Klasifikační nástroje velmi zefektivňují klasifikaci právě u elektronicky zpracovávaných dat. Kromě toho, že při integraci s DLP logicky pomáhají ke snazšímu vyhledávání a ochraně dat. Řešení zajišťuje kontrolu nad tím, kdo, kdy a jaký dokument klasifikoval. To postupně vede u zaměstnanců k růstu zodpovědnosti při nakládání s dokumenty s vyšším stupněm důvěrnosti. Integrace s DLP pak vede i k automatizované kontrole a ochraně při nakládání s osobními údaji.

Přes všechny přínosy DLP je třeba si uvědomit, že se nejedná o nástroj, který by zajistil plný soulad s GDPR. Argumentace některých producentů SW to nezmění. Přestože je DLP velmi silným nástrojem pro ochranu osobních údajů, jeho možnosti jsou limitované. Nedokáže zabránit únikům, pokud se jedná o oprávněné přístupy uživatele nebo data uložená a přenášená na mobilních zařízeních (data na notebooku). DLP data z ukradeného notebooku neochrání. Musíme tak uvažovat o dalších opatřeních.

Od toho nejjednoduššího, tedy rozhodnutí, že osobní údaje se nebudou ukládat na přenosná zařízení (bez DLP téměř nemožné zajistit) až pro šifrování. Kryptografie je jedním z nejúčinnějších nástrojů na ochranu dat. Šifrování samozřejmě má své uplatnění nejen při ukládání dat na stanicích a datových nosičích. Využívá se i pro ochranu dat v databázích, při zálohování, ale současně i při komunikaci. VPN (Virtual Private Network) využívá šifrování pro zabezpečení komunikačního kanálu. Šifrovaná emailová komunikace je pak již ověřeným způsobem, jak chránit data při přenosu.

Standardním a ověřeným řešením pro ochranu informací před neoprávněným přístupem je řízení přístupu. I když by se chtělo říci, že už neexistuje snad nikdo, kdo by to takto neřešil, není tomu tak. Bohužel. Standardní řízení přístupu však řeší pouze nastavení oprávnění přístupu k datům, ale už nevyřeší, zda někdo, kdo práva k osobním údajům má (vedoucí pracovník, administrátor a další privilegovaní uživatelé) tato svá práva nezneužívají. V této oblasti jsou v podstatě dvě možnosti. Buď víra ve své zaměstnance a ve vlastní úsudek při jejich výběru, nebo využití systémů, které dokážou monitorovat chování privilegovaných uživatelů. Jejich hlavní přínos však spočívá v tom, že dokážou zajistit dostatek důkazů proti uživateli, který zneužil svá práva.

Podobné je to s řešením pro analýzu a zpracování auditních logů jako SIEM. Ten zajišťuje primárně logické oddělení bezpečnosti a provozu informačních technologií. Monitorují definované události na zařízeních a jsou schopny interpretovat potenciální i reálné bezpečnostní incidenty a také aktivitu administrátorů a uživatelů. Nástroje monitoringu se stávají nepostradatelnou součástí systému řízení bezpečnosti, stejně tak pomohou i při ochraně osobních údajů. SIEM je bezpochyby silný nástroj, který ale pro svou funkci potřebuje jednak zdroje informací, se kterými pracuje, a pak také zkušeného odborníka, který při implementaci navrhne správné „use case“ a korelační pravidla. V takovém případě jsme schopni detekovat podezřelé aktivity ještě v jejich průběhu. Velmi jemným a složitým nastavením lze dokonce SIEM využít k detekci některých osobních údajů. Přesto považuji za vhodnější využívat k těmto účelům jiné nástroje.

Uvedené (a samozřejmě další) technologie přímo neadresují GDPR a ochranu osobních údajů, ale jejich správné nasazení, integrace do procesů organizace a použití má vliv na celkovou bezpečnost a tím i na ochranu osobních údajů. Každá organizace by měla pravidelně vykonávat a vyhodnocovat řadu aktivit pro vlastní ochranu, jako např. zaznamenávání autorizačních a autentizačních akcí, monitoring operací s daty, monitoring síťového provozu, monitoring přenosu dat, analýzu záznamů a jejich korelace, zaznamenávání dalších souvisejících bezpečnostních událostí atd. Tyto aktivity (řadu z nich zde kvůli rozsahu nemůžeme uvést) dále zlepšují úroveň bezpečnosti, včetně bezpečnostních technologií, ale je potřeba si uvědomit, že GDPR regulativa není jejich stěžejním záměrem a nevyřeší její popisované cíle.

Štěstí přeje připraveným

Co říct závěrem. Podle mého názoru je GDPR jen dalším legislativním opatřením, regulací, se kterou se musíme vypořádat. A podle toho k tomu musíme přistoupit. Tedy brát to se vší vážností, s přiměřeným strachem. Ale paranoia na místě rozhodně není. Abychom dosáhli souladu s požadavky normy, musíme nejprve důkladně naplánovat aktivity a kroky, které k němu směřují. Rozhodně nečekejte, že na GDPR existují jednoduchá řešení. Budete muset investovat čas, práci a také finanční prostředky. Ačkoliv bezpečnost osobních údajů nelze zajistit jen technickými prostředky, bez nich to zpravidla taky nepůjde. Hlavní je nebýt zbrklý a důkladně promyslet, co jednotlivé nástroje řeší a zda je tento přínos relevantní vůči hrozbám a nákladům.

Závěrem můžeme poradit několik jednoduchých otázek, na které se ptát před tím, než vyberete konkrétní bezpečnostní řešení:

- Jak mi uvažovaná technologie pomůže identifikovat, nalézt a označit osobní údaje?
- Jak spolehlivě dokáže identifikovat konkrétní osobní údaje (např. kombinaci jméno a IP adresa)?

- Je ochrana komplexní, nebo řeší jen dílčí oblasti?
- Zabrání technologie úniku dat, nebo jen zjistí, že k úniku dochází či došlo?
- Vytváří technologie detailní auditní záznamy o činnostech spojených s osobními údaji?

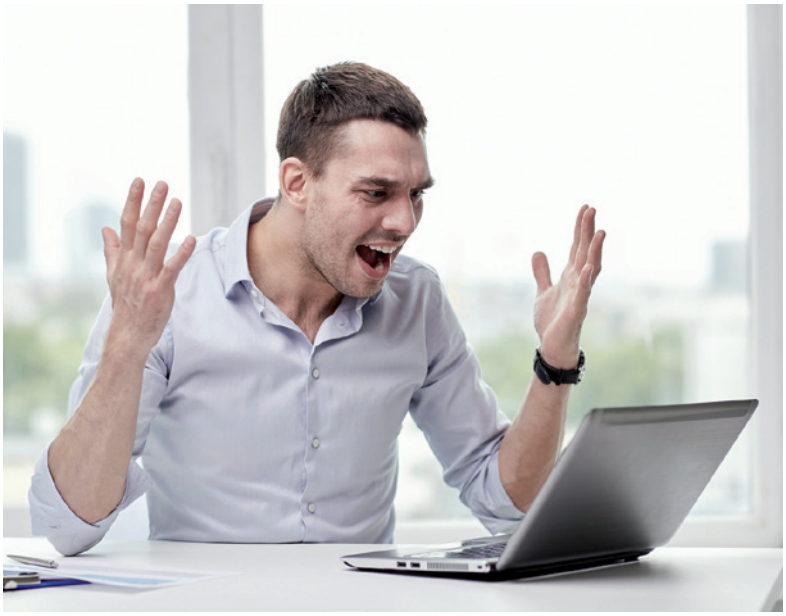
I když se zdá, že do května příštího roku je dostatek času, osobně bych tomuto klamu nepodléhal. Rozhodně je na čase začít s identifikací osobních údajů a účelů. Až poté budete schopni říci, jak moc náročné bude uvedení do souladu s GDPR. Vyberte si partnera s historií, dobrým jménem a zkušenostmi z oblasti komplexní informační bezpečnosti. Jen takový partner doporučí a naimplementuje potřebná řešení. Vyhýbejte se hlavně nereálným slibům a jednostranným řešením. Pak se nemusíte bát, že na GDPR nebudete připraveni. Současně můžete GDPR využít jako příležitost pro výrazné zlepší bezpečnosti ICT, protože přijatá opatření se promítnou v celém firemním prostředí.

Marian Němec, BA (Hons)

V oblasti informačních technologií se pohybuje celý svůj profesní život. Problematiku bezpečnosti IT začal řešit již v 90. letech minulého století z pozice informatika na městském úřadu. Později se podílel na vzniku Certifikační autority Czechia, aby se následně přes PKI systémy dostal k dalším bezpečnostním technologiím. Procesní bezpečnosti se pak věnuje od roku 2008. Podílel na mnoha projektech v oblasti implementace ISO27001 a systému ochrany osobních údajů, zejména ve veřejném sektoru. Ve volném čase se věnuje hlavně tréninku a výuce sebeobrany.

Výkyvy v rychlosti připojení stresují uživatele

Ve výzkumném projektu z konce února společnosti Ericsson a Vodafone Německo použily neurovědu k zjištění, co si uživatelé mobilního širokopásmového připojení skutečně myslí o slabém výkonu sítě. Elektroencefalogramové zařízení (zkráceně EEG) se použilo ke sledování mozkové aktivity 150 účastníků, kteří se dobrovolně přihlásili do projektu v německém Düsseldorfu. Výsledek ukázal, že i malá zpoždění a rušení zvyšují úroveň napětí a stresu a mají negativní dopad na loajalitu účastníka vzhledem ke značce operátora. Účastníci studie museli absolvovat třináct konkrétních úkolů během deseti minutového užívání smartphonu, kdy byla degradace kvality poskytované služby simulována. Úkoly zahrnovaly jednotlivé aktivity, jako prohlížení webových stránek, streamování videí, či nahrávání fotografií a selfies. Kromě EEG zařízení bylo ke sledování pozornosti a srdeční frekvence odběratelů použito i vybavení na sledování pohybu očí a měření pulsu. Vodafone je první společnost na trhu a ve světě, která ve spolupráci s Ericssonem využívá nové způsoby studia spotřebitelských emocí. Guido Weißbrich, ředitel výkonu sítě v německém Vodafone, k studii říká: "Tato studie dokazuje, jak rychle se uživatelé chytrých telefonů stali nespokojenými, když širokopásmová síť nefungovala v celé své kráse. Pouhá sekunda zpoždění při stahování či nahrávání obsahu má výrazně negativní dopad na uživatelskou zkušenost, takže musíme učinit vše, aby se při sledování videí zabránilo zdlouhavému ukládání nebo zmrazení obsahu." Vzhledem k tomu, jak byla ovlivněna loajalita předplatitelů a vnímání značky, byla studie doplněna o dotazník, který účastníci vyplnili před a po plnění jednotlivých úkolů.



Poznatky z výzkumného projektu vedly společnost Ericsson ke spuštění "Ericsson Neurometric Analysis", a k dodání poznatků ke zkušenostem do svého portfolia. Tato nová nabídka bude k dispozici operátorům po celém světě.

(Ericsson)