SOPHOS
Security made simple.

Obecná regulace ochrany dat v Evropské unii

Výklad požadavků na ochranu dat a metod jejich uplatňování

Od roku 1995, kdy byl schválen poslední významný evropský právní předpis upravující ochranu dat (směrnice o ochraně údajů 95/46/EU), se změnilo mnohé. Například mobilní zařízení jsou všudypřítomná a není neobvyklé mít u sebe hned dvě či tři zároveň. Citlivá podniková data se pohybují mimo tradiční podnikovou linii obrany. Zaměstnanci posílají elektronickou poštou dokumenty sami sobě, přistupují k datům prostřednictvím svých vlastních chytrých telefonů a tabletů a ukládají data do cloudu. V současné době jsou běžným jevem závažné útoky na osobní údaje, které vystavují zákazníky nebezpečí zneužití identity a ztráty finančních prostředků. Podniky riskují ztrátu přízně zákazníků a investorů, jakož i hrazení pokut. Tento dokument se věnuje celkovému významu nařízení o ochraně údajů (General Data Protection Regulation - GDPR) pro organizace.

A Sophos Whitepaper July 2017

Proč je zapotřebí změna?

Podobně jako většina států USA, tak i všechny členské státy Evropské unie (EU) implementovaly zákony upravující ochranu údajů, které odrážejí novou realitu rozpuštění tradiční obranné linie komunikačních sítí. V USA i v EU existují v této věci mezi jednotlivými zeměmi určité rozdíly. Již více let nedošlo k výraznému přepracování evropských norem ochrany dat. Tyto skutečnosti v kombinaci s potřebou reagovat na významný vývoj technologií, k němuž došlo od roku 1995, oživuje snahy o modernizaci a homogenizaci zákonných norem ochrany dat v Evropské unii.*[1]

GDPR je vyvrcholením řady let práce orgánů EU na reformě norem ochrany dat. Ta si klade za cíl proměnit poněkud různorodou legislativu jednotlivých zemí na jednotnou celounijní infrastrukturu (GDPR povoluje určité derogace pro jednotlivé země, např. mezní věk osoby poskytující souhlas k zacházení s osobními údaji). GDPR má podobu nařízení, což znamená, že se uplatňuje v každém členském státu přímo v té podobě, v níž je schválena. Předchozí legislativa ochrany dat ve členských státech byla vytvořena na základě směrnice, kterou každá z členských zemích implementovala do své národní legislativy s určitým stupněm volnosti, což způsobilo rozdíly mezi jednotlivými zeměmi. Cílem nařízení je posílení práv ochrany soukromí občanů Evropské unie, obnovení důvěry v činnosti prováděné prostřednictvím komunikačních sítí a zvýšení kvality ochrany údajů o zákaznících požadováním zavedení nových procesů a řídicích mechanizmů po podnicích.

Nařízení oficiálně vstoupilo v platnost dne 24. května 2016 a od tohoto okmžiku běží dvouleté období, jež mají členské země k dispozici pro implementaci nových požadavků.*[2] Je však zapotřebí připomenout, že jde o nejzazší termín implementace změn. Členské státy mohou nové nařízení uplatnit hned, jakmile to bude možné. Například Nizozemí příslušné změny ve svých zákonech upravujících ochranu dat již provedlo.

Samotný text sestává z 99 článků*[3] a - podobně jako jakýkoli jiný zákon - může umožňovat odlišné interpretace. Cílem tohoto dokumentu není poučit čtenáře o zcela novém zákonu, ale poskytnout výklad k potřebě ochrany bezpečnosti osobních údajů, jejíž součástí je i soubor velmi závažných pokut. Další informace o směrnici získáte ze zdrojů uvedených v příloze tohoto dokumentu.

Evropská unie (EU) představuje jedinečné hospodářské a politické partnerství 28 evropských států, jejichž území pokrývá většinu kontinentu. Každá z těchto zemí má svou vlastní kulturu a legislativu, nicméně provádí rovněž politickou a legislativní integraci v řadě oblastí. Důvodem existence Evropské unie je předcházení možným konfliktům mezi členskými státy a posilování obchodu a volného pohybu zboží a osob v Unii.

Derogace je výjimka nebo částečná úleva od závazků určitého zákonného předpisu.

Hlavní prvky reformy

V této části uvádíme několik hlavních článků, které se týkají uchovávání osobních údajů v bezpečí a potenciálních důsledků porušení této povinnosti.

Článek 32*[3] se věnuje bezpečnosti zpracování dat:

1. *S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:*
   a) pseudonymizace a šifrování osobních údajů;
   b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
   c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
   d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Jednoduše řečeno, článek požaduje po organizacích implementaci vhodných bezpečnostních opatření k ochraně osobních údajů. Článek výslovně odkazuje na „šifrování osobních údajů" jako na jeden z prostředků k dosažení tohoto účelu.

Článek rovněž uvádí „schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování (osobních údajů)". V souvislosti s šifrovací technologií to znamená mít kromě šifrování údajů rovněž robustní proceduru správy klíčů. V širším důsledku to znamená mít spolehlivý plán obnovy z havárie.

Pro případ, kdy došlo k porušení zabezpečení osobních údajů, **článek 33***[3] určuje, že společnost musí tuto skutečnost ohlásit dozorovému úřadu do 72 hodin od okamžiku, kdy se o tomto porušení dozvěděla. Nicméně společnost může a nemusí být povinna oznámit tuto skutečnost jednotlivcům, jejichž údaje byly napadeny. **Článek 34** uvádí:

1. *Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu subjektu údajů.*

2. *(...)*

3. *Oznámení subjektu údajů uvedené v odstavci 1 se nevyžaduje, je-li splněna kterákoli z těchto podmínek:*

   a) správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování;
   b) správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů podle odstavce 1 se již pravděpodobně neprojeví;
   c) vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

Terminologie návrhu úpravy ochrany dat

Osobní údaje
Veškeré informace, jež přímo nebo nepřímo umožňují identifikaci určitého jednotlivce. Mohou se týkat osobního, profesního nebo veřejného života dotyčné osoby. Může jít o jméno, fotografii, e-mailovou adresu, informace o bankovním spojení, o příspěvky dotyčné osoby na sociálních sítích, o lékařské informace nebo například o adresu IP počítače této osoby.

Správci údajů
Rozhodují o podmínkách, účelech a způsobech zpracování osobních údajů. Může jít o jednotlivce, obchodní společnosti, podniky nebo o orgány veřejné moci. Jako příklad jednotlivců lze uvést lékaře, lékárníky a politiky, který uchovávají údaje o svých pacientech, klientech a voličích.

Zpracovatelé údajů
Zpracovávají osobní údaje jménem správců údajů, avšak neprovádějí rozhodnutí o podmínkách, účelech ani prostředcích zpracování (dodavatelé služeb). Společnosti např. zpracovávající mzdy a společnosti zajišťující průzkum trhu mohou zpracovávat osobní údaje pro jiné (např. jiné společnosti nebo orgány veřejné moci, které tak plní funkci správce údajů). Pokud však rozhodují o podmínkách či účelech nebo pokud jednají nad rámec pokynů správců údajů, stávají se správcem pro dotyčnou konkrétní činnost zpracování. Nové nařízení stanovuje pro zpracovatele přímé povinnosti, například splnění požadavků na zabezpečení.

Subjekt údajů
Osobní údaje se používají k identifikaci fyzické osoby. Tato osoba je "subjektem údajů".*[2]

Pokud byly v momentu ztráty osobní údaje ochraňovány takovým způsobem, že byla nesrozumitelná (a proto byla pro neoprávněnou osobu nepoužitelná, jako například při použití šifrování) - a společnost může tuto skutečnost prokázat svému dozorovému úřadu, nemá společnost povinnost oznámit takovéto narušení bezpečnosti osobám, jejichž osobní údaje se ztratily nebo byly odcizeny.

Pro případ, že společnost některou z těchto povinností nesplní - nepřijme vnitřní zásady nebo neimplementuje vhodná opatření zajišťující a dokládající splnění požadavků nebo neinformuje dozorový úřad či subjekt údajů o narušení bezpečnosti osobních údajů (v souladu s požadavky) - určuje **článek 83***[3] o administrativních pokutách potenciální maximální sankci takto:

1. *Za porušení následujících ustanovení lze v souladu s odstavcem 2 uložit správní pokuty až do výše 20 000 000 EUR, nebo jedná-li se o podnik, až do výše 4 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší:*

Shrnutí: Pokud nepoužijete správnou technologii k ochraně osobních údajů, může se stát, že budete muset za tuto skutečnost zaplatit - přímo dozorovému úřadu a nepřímo poškozením své pověsti a ztrátou přízně a důvěry svých zákazníků. Podniky, jež šifrují svá data, ochraňují své zákazníky - a samy sebe.

Vynucování regulace

GDPR výrazně posiluje vynucovací pravomoci. Nová maximální pokuta ve výši 20 miliónů EUR nebo 4% globálního ročního obratu představují významné zvýšení dosavadní maximální výše pokut. Například ve Velké Británii může úřad Information Commissioner Office udělit pokutu do výše 500 000 liber. To znamená, že důsledky porušení ochrany dat jsou mnohem více závažné.

Kdo je dotčen nařízením GDPR?

GDPR má globální dopad, neboť ovlivňuje každou společnost, která obchoduje s občany Evropské unie - bez ohledu na její sídlo. Situace je velmi podobná řadě zákonů USA, jež upravují ochranu údajů. Například určitá francouzská společnost obchodující s americkými zákazníky v Kalifornii musí plnit požadavky kalifornského zákona pro ochranu údajů. Pokud tato společnost obchoduje rovněž se zákazníky v Massachusetts, musí plnit rovněž požadavky massachusettského zákona pro ochranu údajů atd. Některé z předností nového zákona:

- Jeden trh EU, jedno právo - Evropské ani neevropské podniky již nepotřebují zkoumat a znát podrobnosti 28 různých souborů pravidel a nařízení.
- Jednotný proces - Tentýž proces bude realizován v případech poškození bezpečnosti dat a/nebo porušení povinností.
- Tatáž pravidla platí pro všechny společnosti - V rámci EU se pro podniky uplatňuje stejný soubor pravidel bez ohledu na sídlo těchto podniků.

Jak plnit požadavky GDPR

Pro řadu podniků, jež musejí plnit požadavky nových předpisů, je nejlepším způsobem přípravy implementace solidní strategie ochrany údajů, jež ochraňuje údaje před ztrátou v důsledku záměrného i neúmyslného jednání.

Třebaže nová legislativa nepožaduje konkrétní typ technického opatření, vícekrát zmiňuje šifrování jako prostředek zabezpečení osobních údajů a zamezení jejich čitelnosti ze strany neoprávněných osob. Jak tedy organizace plní požadavky jiných předpisů, které určují podmínky ochrany osobních údajů? Jako příklad zákonů, jež požadují opatření k ochraně dat, které jsou obdobou opatření vyžadovaných nařízením o ochraně údajů Evropské unie, lze uvést zákony HIPAA (Health Insurance Portability and Accountability Act), PCI DSS (Payment Card Industry Data Security Standard) a SOX (Sarbanes-Oxley). Šifrování proměňuje údaje do nečitelné podoby a je proto široce přijímaným prostředkem k realizaci těchto požadavků. Po ztrátě či odcizení jsou zašifrované údaje v podstatě bezcenné. Nikdo nemůže přistupovat k dotyčným údajům. A při kombinaci šifrovaných dat s bezpečnostními systémy, jež zabraňují v krádežích údajů, máte nejlepší šanci udržet svá data v bezpečí.

Závěr: Chcete-li se připravit na změny předepsané nařízením pro ochranu dat, musíte věnovat pozornost technologiím pro šifrování a ochraně před škodlivým kódem.

Jak vám Sophos pomáhá se zvládnutím problematiky ochrany údajů

Vytvoření strategie ochrany údajů může být velmi obtížný proces, a to zejména v případě, že se váš podnik touto problematikou dosud přímo nezabýval. Kde tedy začít? Solidní strategii ochrany dat nevytvoříte za den. Je dobré vědět, že 57 % útoků na data generují hackeři a škodlivý kód a 23 % útoků na data je způsobeno neúmyslným prozrazením (lidská chyba).*[4] Zabezpečení před těmito hrozbami je dobrý začátek. Sophos pro tento účel doporučuje tři základní kroky.

Odstraňte hlavní příčiny ztráty dat

Záměrné útoky a neúmyslné ztráty či odcizení jsou dvě hlavní příčiny porušení bezpečnosti dat. Centrální šifrování zařízení Sophos je nejsnadnější metoda centrální správy kompletního šifrování disků pro všechny vaše počítače PC a Mac. Zašifrování celého disku je nejzákladnější formou šifrování. Doporučuje se pro všechny počítače k ochraně uložených dat. Udrží vaše data v bezpečí při ztrátě a odcizení zařízení.

Služba Sophos Mobile rozšiřuje tuto ochranu na data ve vašich mobilních zařízeních a dále zajišťuje vzdálené vyhledání, vymazání a zablokování vybraných zařízení. Svá mobilní zařízení můžete spravovat a zabezpečovat při vynaložení minimálního času a úsilí.

Služba Sophos Intercept X pracuje vedle vaší stávající antivirové ochrany na zajištění pokročilé ochrany před škodlivým kódem, zneužitím slabin a vyděračskými útoky - udržuje vás v bezpečí před nejnovějšími útoky na vaše data.

Všechna tato řešení jsou součástí systému Sophos Central, který poskytuje jednoduché, snadno použitelné a kompletně vybavené obslužné rozhraní.

Nepouštějte si hrozby domů

V současném prostředí s propracovanými a agresivními malwarovými útoky je zásadní podmínkou vícevrstvé zabezpečení, které je schopno blokovat útoky na všech úrovních vaší sítě. Řešení XG Firewall ochraňuje vaše síťová zařízení zachycováním těchto útoků na vnější linii obrany dříve, než mohou proniknout k vašim zařízením.

Sophos Email Appliance automaticky blokuje nebo šifruje citlivé e-maily a přílohy (např. soubory PDF), a zajišťuje tak trvalou ochranu vašich dat. Podezřelé zprávy jsou zastaveny dříve, než se dostanou do vaší schránky.

Zabraňte lidským chybám

Většině z nás se již stalo, že jsme odeslali zprávu nesprávné osobě. Jde-li o citlivé údaje, může tato nevinná chyba vyvolat vysokou pokutu. Šifrování na úrovni jednotlivých souborů poskytované řešením Sophos SafeGuard znamená, že data jsou chráněna i po opuštění vašich zařízení nebo sítě (např. příloha zprávy elektronické pošty, uložení na cloud), takže i když dojde k porušení bezpečnosti dat, máte šanci, že případná pokuta nebude zdaleka tak vysoká.

Již řadu let se s děsivou pravidelností ve sdělovacích prostředcích objevují informace o velmi závažných porušeních bezpečnosti dat. Nařízení GDPR stanovuje pro zúčastněné osoby maximální výši pokuty 20 miliónů EUR nebo 4 % globálního ročního obratu, což je mnohem vyšší pokuta než dosud. A netýká se to pouze dobře známých značek. Požadavky nařízení musí splňovat **každá** organizace uchovávající údaje o občanech Evropské unie.

Zajištění důvěrnosti a bezpečnosti údajů o zákaznících je nutnou podmínkou. Sophos poskytuje technologie pro šifrování a ochranu dat, jež mohou vaší organizaci pomoci při plnění požadavků GDPR.

Příloha

1. Řízení kvality v rámci reformy ochrany dat v EU. Evropská komise, 21. prosince 2015
2. Řízení kvality: nová pravidla EU pro ochranu dat vracejí občanům jejich práva. Evropský parlament, 1. června 2016
3. Nařízení 2016/679/EU Evropského parlamentu a rady ze dne 27. dubna 2016
4. Porušení bezpečnosti dat 2016 - Privacy Rights Clearinghouse

Celosvětové obchodní zastoupení
Tel: +44 (0)8447 671131
E-mail: sales@sophos.com

2017-07-28 WP-CZ (NP)

SOPHOS