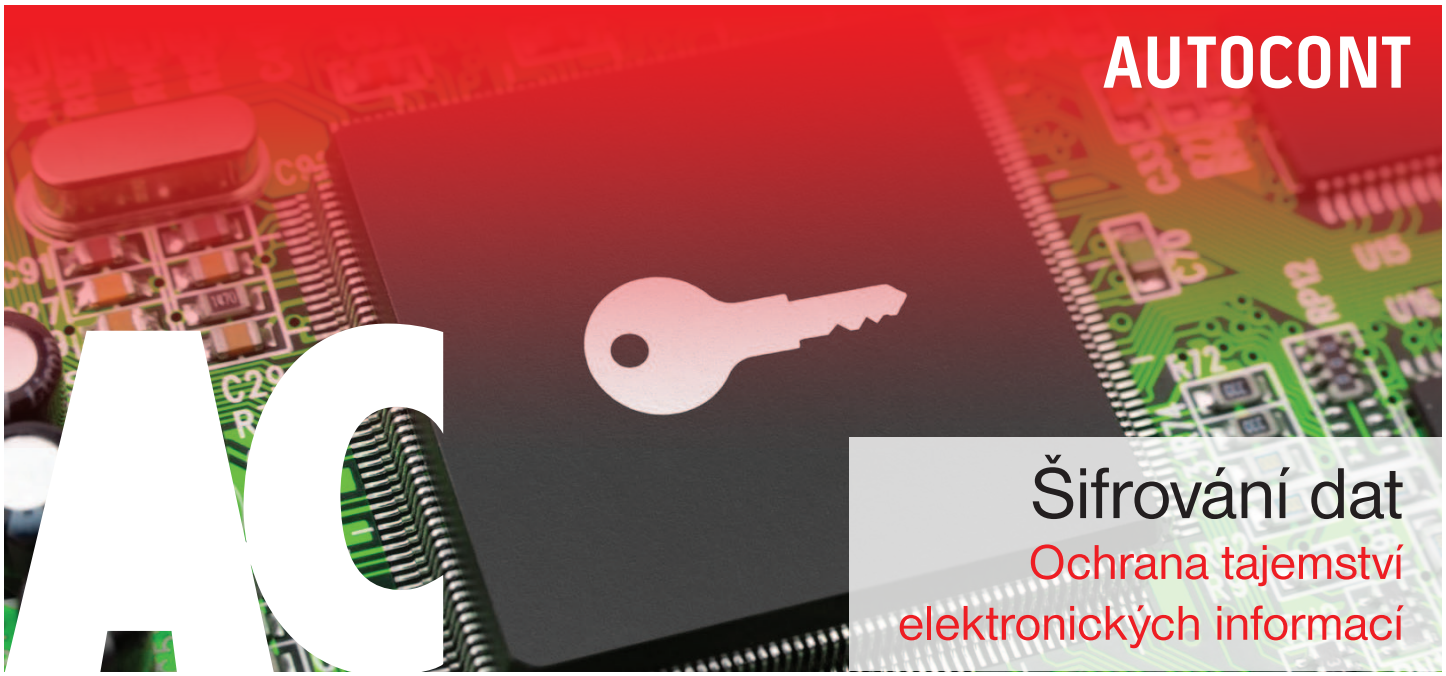

Šifrování dat

Ochrana tajemství elektronických informací

ŠIFROVÁNÍ DAT ZAJIŠTUJE PŘEDEVŠÍM JEJICH OCHRANU PROTI NEOPRÁVNĚNÉMU POUŽITÍ. ŠIFROVÁNÍM JE TEDY ZARUČENA OCHRANA TAJEMSTVÍ V DATECH A S TÍM SPOJENÉ FINANČNÍ DOPADY PŘI JEJICH ZTRÁTĚ ČI ZNEUŽITÍ.

Nasazení šifrování umožní mj. splnit některé z požadavků GDPR (nařízení EU), jako je:
- zajištění důvěrnosti osobních údajů (OÚ)
- zohlednění rizik zpracování OÚ, mezi něž patří např. ztráta, resp. únik nebo kompromitace, neoprávněný přístup k OÚ, a také neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných OÚ

Do firemního prostředí se nejčastěji aplikuje řešení, kdy je držitelem šifrovacích klíčů majitel dat a záloha klíče je chráněna na dalším místě dle typu nabízeného řešení. Technicky pak produkt určený pro šifrování nabízí záložní způsob, jak se k šifrovacímu klíči dostat v případě jeho ztráty vlastníkem, poškození hardware apod. Technologie šifrování je jedinou možností jak uchovat tajemství v datech, a přesto je mít uložená ve firemních i ve veřejných prostředcích, jako jsou servery, cloudy, externí média aj. Šifrování je možné aplikovat dle různých scénářů a požadavků bezpečnosti. Nejčastěji se rozlišuje šifrování zaměřené na šifrování složek a souborů, šifrování datových úložišť, jako jsou pevné disky, flash disky aj. a šifrování e-mail komunikace.

Pro šifrování ve firmě je třeba mít řešení, které zajistí přístup k datům jejich vlastníkům, ale v případě ztráty či zničení šifrovacích klíčů zajistit procesně náhradu klíčů. Další poptávanou potřebou je mít možnost sdílet šifrovaná data ve skupině uživatelů. V případě, že držitelem tajemství je pouze vlastník dat, má zodpovědnost spolehlivě zálohovat šifrovací klíče. V případě ztráty klíčů, či nemožnosti se ke klíčům dostat, je možné data považovat za zcela ztracená/zničená. Technologie šifrování dat je nezbytným nástrojem v každém prostředí, kde je třeba dbát na cenu dat. Příklady úniku informací a jejich dopadů je možné nalézt každý rok na stránkách novin a časopisů od osobních škod, jako je odcizení důvěrných fotografií celebrit, firemních ztrát informací klientů bank, pojišťoven, až po ztráty vojenských tajemství s dopady na dění v celém světě.

Šifrování médií - úložišť dat

Jde o šifrování pevného disku jako celku, či určeného oddílu, šifrování flash disků či jiného úložiště. Použití takového média je možné pouze za přítomnosti šifrovacích dat. Šifrovaná data jsou dostupná odemčením softwaru a zpřístupněním pro operační systém. Odemčený systém tedy taková data umožňuje uživateli plně využívat.

Produkty určené k šifrování médií

Produkty umožňují taková nastavení, aby například externí médium, než jej bude moci uživatel využívat, bylo předtím vynuceně zašifrováno.

Ochrana souborů a složek

Soubory, které uživatel využívá, jsou zranitelné pro možnost odcizení z míst, ke kterým má uživatel přístup. Soubory jako takové je tedy nutné rovněž chránit šifrováním. Aplikace určené do firemního prostředí umožňují, aby byl uživatel schopen takové šifrované soubory sdílet s dalšími uživateli používajícími šifrování.

Šifrování elektronické pošty

Elektronická pošta - email, je jeden z nejdůležitějších způsobů komunikace. Informace, které si lidé předávají elektronickou formou, jsou plně srovnatelné s poštou klasickou. Přesto velké množství takové komunikace bohužel stále není důvěrně předáno od odesílatele k určenému příjemci.

Šifrování pošty od odesílatele k příjemci je možno realizovat pomocí asymetrické kryptografie. Klienti si vzájemně předají veřejné elektronické klíče (elektronický podpis).

Dle požadované konfigurace je možné šifrování na odchozí poštu aplikovat klientem, či vynuceně politikou společnosti.

Šifrování je možné také aplikovat až na email bránu, kde dochází k vynucení šifrování dle požadavků společnosti. V možnostech produktů je například reálné zajistit, aby email obsahující důvěrné informace byl doručen jako šifrované PDF, či byl dostupný pro příjemce pouze přes webového klienta.

Microsoft PKI

Role serveru ActiveDirectory Certification Services umožňuje pracovat s asymetrickou kryptografií. Při její schopnosti napojení na MS doménu se rozšíří možnosti konfigurace. Aplikování účelů vydání certifikátů na doménové skupiny, uživatele či počítače je díky propojení možné automatizovat. S PKI lze dostáhnou funkcí pro ověření/prokázání identity, šifrování elektronické pošty, autorizaci vůči aktivním prvkům apod.

Microsoft Bitlocker

Ve vybraných edicích operačních systému Microsoft Windows Vista a novějších je možné využívat dodaný produkt Bitlocker. Tento produkt zajišťuje šifrování celých disků, diskových oddílů, externích médií.

Microsoft RMS

Technologie RMS je určená pro produkty Microsoft Office (MS Word, MS Excel, MS PowerPoint, SharePoint). Produkt umožňuje aplikovat ochranu soborů šifrováním a omezením jejich použití. Soubor pod ochranou RMS nemůže být například vytištěn či přeposlán apod. Podpora RMS v MS Asure umožňuje více možností, než umožňuje řešení služby na serveru - on premise.

CryptZone

Produkt CryptZone aplikuje podobnou ochranu jako Microsoft RMS. Není omezen pouze na soubory MS Office, ale je možné jej aplikovat na většinu formátů. Produkt také umožňuje vynucení šifrování na externí média.

Symantec PGP

Produkt PGP je dobře znám nejen ze světa Linuxu, ale hlavně pro svou technologii asymetrické kryptografie. Uživatel vlastnící veřejný a privátní klíč nedostává důvěru od certifikační autority jako je tomu u technologie PKI, ale jeho klíče jsou podepisovány od ostatních uživatelů klíčů PGP.

PGP rozšířilo své funkce tedy nejen na možnost fixovat emailovou komunikaci, ale také na šifrování souborů a složek celých disků, diskových oddílů, externích médií a souborů k jednorázovému předávání.

Totemo Encryption Gateway

Produkt je bránou pro SMTP komunikace. Pomocí široké škály pravidel je možné na e-mail dle různých parametrů aplikovat šifrování. Totemo dovede zajistit politikou předání důvěrných informací příjemci i v případě, že od příjemce nemáme veřejný klíč. Pro ochranu privátních klíčů či jejich snadnějšímu využívání je možné využít dodatečný hardware určený pro uchovávání takových klíčů autorizací uživatele.

USB klíče

USB klíče jsou malá hardware zařízení, která uchovávají privátní klíče uživatele. Ten pro přístup ke klíčům používá autorizaci ke klíči (PIN, heslo). Výhoda klíče je, že není způsob jak ze zařízení klíč vyexportovat.

Smart karty

Karty velikosti platebních karet je možno využívat pro uchovávání privátních klíčů uživatele a skloubit tuto vlastnost z čipu na elektronické zámky pro vstupy do budov/kanceláří apod. Karty mají na rozdíl od USB klíčů výhodu personifikace například potiskem fotografie nositele, loga firmy apod.