

Redakční otázky k tématu

**ŘÍZENÍ PŘÍSTUPU, AUTENTIZACE A IDENTITY MANAGEMENT**  
odborného on-line magazínu ICT SECURITY – [www.ictsecurity.cz](http://www.ictsecurity.cz)

**Nadpis článku:**

*Jaké jsou možnosti řízení identity a přístupu uživatelů ve Vaší společnosti?*

**Autor odpovědí:**

Mgr. Marian Lysák, Senior Security Consultant, COMGUARD a.s.

**1) Proč se organizace má zabývat řízením přístupu a řešit identity management? Pro které oblasti podnikání zejména je řízení přístupu a identity management nezbytně nutné?**

Identity management má širší význam pro identifikace osob vůči síti, informačním systémům, organizaci apod. Kromě identifikace také hraje důležitou roli autorizace přístupu k určitým datům. V oblasti IT má běžná organizace zpravidla několik informačních systémů, velice často bez centrální správy uživatelské databáze. Identity management systémy mají právě zajišťovat globální struktury uživatelů, které slouží pro jednotný přístup k systémům a aplikacím. Zaměstnanec se má zařadit do této struktury hned po přijetí do zaměstnání. V rámci této struktury se definují cílové objekty přístupu včetně podrobných práv pro přístup k daným systémům. Meziprvkem pak distribuuje nebo dále zpřístupňuje tyto identifikační funkce a autorizační informace do systémů. Elegantním doplňkem může být komponenta SSO (např. software **SSO od firmy ActivIdentity**), která úzce spolupracuje se strukturami identity managementu. Uživatel se přihlásí jednou a další přihlášení do různých systémů jsou již automatická.

**2) Jaké jsou největší výzvy, slabiny a rizika v oblasti řízení přístupu?**

Obecným problémem v oblasti řízení přístupu bývá integrace centrálního identifikačního mechanismu do všech aplikací a síťových prvků v síti organizace. Málokdy se povede řešení, ve kterém do centrálního managementu uživatelů jsou začleněny všechny prvky, ke kterým je potřeba se autentizovat a dále přistupovat. Mechanismy autentizace pomocí certifikátů a jednorázových hesel jsou dobrým řešením pro autentizaci uživatelů (např. software od firmy **ActivIdentity**). Biometricky teprve čekají na svoje uplatnění. Potýkají se s problémy spolehlivosti. Zaměstnanec, který se řízne do prstu a tím pozmění strukturu otisku prstu nebo se přes noc nevyspí a jeho sítnice bude druhý den ráno poznamenaná nevyspáním, se může potkat s problémem, že se nedostane do firemních systémů a nebude moci vykonat svoji práci. Biometrické autentifikátory se budou muset lépe přizpůsobit těmto změnám.

### **3) Jak nejlépe vyřešit otázku autentizace u sdílených zdrojů (počítače, tiskárny...)?**

V dnešní době je autentizace ke sdíleným zdrojům běžnou záležitostí. K autentizaci ke sdíleným zdrojům se používají běžná fixní hesla, která odpovídají určitým parametrům (délka, složení znaků, obměna v čase). Na trhu jsou již bezpečnější řešení, např. přístup pomocí jednorázových hesel (např. software **4TRESS Authentication Server od ActivIdentity**) nebo přístup pomocí certifikátů (např. software **ActivClient a CMS od ActivIdentity**).

### **4) Co je lepší: softwarové nebo hardwarové prostředky řízení přístupu? Jaký typ autentizace považujete za nejbezpečnější?**

Rozdíl mezi softwarovým a hardwarovým autentifikátory nejsou v celkovém pohledu dramatické. Např. hardwarový generátor jednorázového hesla a softwarový generátor jednorázového hesla obsahuje stejné softwarové rutiny pro generování hesla. Otázkou je spíše dostupnost tohoto prvku pro třetí stranu, která by toho chtěla zneužít a získat identitu daného uživatele a potažmo autorizaci pro přístup k systémům. K dalšímu dotazu, myslím, že biometricky mohou směřovat k největší bezpečnosti. Zejména pak jedinečné identifikátory daného jedince (DNA, sítnice, otisk prstu ...).

### **5) Jedním z nejčastějších prohřešků je přístup zaměstnance do systému (resp. do jeho částí) i po ukončení pracovního poměru. Jak jej nejlépe řešit?**

Otázka nahrává právě Identity managementu, který tento problém spolehlivě odstraní. Zaměstnanec, který je první den v práci, získá omezený přístup z Identity Managementu do systémů ve zkušební lhůtě. Pak se jeho působnost rozšíří postupně, jak získává zkušenosti a zapojí se do různých činností nebo při jeho kariérním růstu. Vše jednou končí a zaměstnanec odchází od společnosti. Zodpovědný pracovník označí tuhle situaci v Identity Managementu, který toto rozdistribuuje do všech systémů tak, aby již pracovník neměl k systémům přístup. Bez Identity Managementu by musel zodpovědný pracovník smazat postupně všechny účty, kam měl zaměstnanec přístup. Rizikem je, že na něco se zapomene a zaměstnanec, kterému skončil pracovní poměr, má stále přístup k firemním informacím.