24. 4. 2007

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Nepřítel firemních informačních systémů se skrývá ve vlastních řadách

SPRÁVA IDENTITY A PŘÍSTUPU: JAK ZALEPIT PODNIKOVÝ DATOVÝ CEDNÍK

Skóre:	0.72
Název zdroje:	Hospodářské noviny
Datum vydání:	24.04.2007
Nadpis:	Nepřítel firemních informačních systémů se skrývá ve vlastních řadách
Strana:	14
Mutace:	komerční příloha
Rubrika:	ICT revue
Autor:	(bks)
Oblast:	Celostátní deníky
Zpracováno:	24.04.2007 04:54
Identifikace:	DCHN20070424040007 cz
Klíčová slova:	správy (8x), správou (6x), SPRÁVA (4x), práva (3x), správu, porušení zákonných, správě, legislativy, legislativě, zákonných, legislativou, zákonnými

NADTITULEK: SPRÁVA IDENTITY A PŘÍSTUPU: JAK ZALEPIT PODNIKOVÝ DATOVÝ CEDNÍK

Když si ovšem i po implementaci systému IAM lidé stále píší hesla na papírky nalepené na monitor, protože se bezpečností systému odmítají zabývat, hodnota celého projektu klesne na nulu.

Ačkoliv se média v otázce bezpečnosti informačních systémů zabývají hlavně vnějšími riziky, jako jsou hackeři, viry, spyware apod., není žádnou novinkou, že reálné nebezpečí ve firmách způsobují většinou ti "uvnitř", ať už záměrně či neúmyslnou chybou. Lidé, kteří pracují v organizaci, totiž dobře znají její systémy i jejich případné slabiny. Mají k systémům navíc i možnost fyzického přístupu, který nebývá dobře ošetřen. Podle loňského průzkumu společnosti CA, jehož se zúčastnilo 715 odborníků v IT z Evropy a Blízkého východu, zhruba osmdesát procent organizací hodnotí riziko útoku zevnitř firmy jako významné a zhruba čtyřicet procent respondentů neočekává v této oblasti žádné zlepšení. Stejný průzkum však ukázal, že ačkoliv firmy obecně považují správu identity a řízení přístupu za důležitou součást řešení problému, pouze šestnáct procent respondentů v tuto chvíli vlastní nebo plánuje její zavedení do svého systému zabezpečení.

Příliš mnoho pijavic

Co to vlastně správa identity a řízení přístupu je a proč by jim měly organizace věnovat větší pozornost? Co je to vlastně "identita", proč vyžaduje správu a proč se používá při řízení přístupu?

"V současném globálním podnikatelském prostředí musí být organizace rychlejší než jejich konkurence a dokázat více s menším množstvím zdrojů. I ty největší podniky se usilovně snaží o

dynamiku začínajících podnikatelů. Pro využití příležitostí a překonání hrozeb je proto pro firmy nezbytně nutné zvyšovat i efektivitu a bezpečnost IT. Ovšem díky rostoucímu počtu interních a externích informačních systémů, které firmy využívají, dochází k nárůstu složitosti celého prostředí," říká Marcel den Hartog, Security Solutions Marketing Director ve společnosti CA a dodává: "Typická velká organizace používá stovky aplikací, spolupracuje s tisíci partnery, má desítky tisíc zaměstnanců a statisíce zákazníků. Všechny uvedené subjekty potřebují přístup k aplikacím a datům a ten musí být pak zabezpečen a odpovídat pravidlům organizace, platné legislativě nebo alespoň všeobecně uznávaným postupům. V současné době se jedná o velmi složitý a přitom pro fungování organizací klíčový úkol."

Cílem efektivní správy identity a řízení přístupu (IAM - Identity and Access Management) je automatizovat řízení cyklu souvisejícího se správou uživatelů a jejich oprávnění v systémech - tzn. od vytvoření přístupu přes všechny změny až po případné zrušení uživatele (zaměstnanec, zákazník, obchodní partner nebo dodavatel) v systémech organizace a zamezení jeho přístupu k poskytovaným aplikacím a případně dalšímu nepočítačovému vybavení, jako jsou telefony, kancelářské prostory a další. Když se tedy jedná o tak důležitý systém, který šetří náklady, proč podniky nevyužívají výhody IAM při provozování informačních systémů? Jaké další problémy, kromě výše zmíněných provozních rizik, může nedostatečné řešení správy identity podnikům způsobit?

Nepružná infrastruktura hrozbou

Organizace mají často prostředí, které vznikalo v průběhu delší doby a překotným vývojem, a jež proto může skrývat celou řadu bezpečnostních problémů. Funkce zabezpečení jsou implementovány do jednotlivých platforem nebo dílčích aplikací, což s sebou přináší vysoké náklady na údržbu a silně omezuje flexibilitu. Každá taková platforma a aplikace mívá často své vlastní úložiště identit a oprávnění, které vyžaduje samostatnou správu a aktualizaci. Takový model neumožňuje dosažení dnes požadované flexibility. Nutnost reakce na měnící se požadavky v oblasti zabezpečení a nadnárodních regulací, jako je Sarbanes-Oxley nebo Basel, vynucuje rovněž komplexnější přístup k problematice, což pak zvyšuje náklady na údržbu IT infrastruktury, omezuje flexibilitu a odčerpává prostředky na strategické investice.

Kýžené zlepšení služeb

Častý telefonát "zase jsem zapomněl své heslo" je stále hlavním problémem administrátorů v IT. V typické firmě představují problémy s hesly a nedostupnosti uživatelských účtů významnou část práce technické podpory (v průměru 40 %). Manuální správa přístupových práv uživatelů v různých odděleních je značně nákladná a zvyšuje rizika pracovních prostojů, kdy zaměstnanec čeká na poskytnutí odpovídajících přístupových práv k systému.

Další dimenze problém podle Marcela den Hartoga z CA nabývá, když je nutné poskytnout některou z forem vzdáleného přístupu k zabezpečenému prostředí i externím subjektům. Při obchodování s partnery není příliš praktické spravovat všechny účty koncových uživatelů uvnitř firmy. Procesy a technologie si většinou žádají, aby měla možnost administrace i partnerská organizace. Vzhledem k tomu, že přístupová práva často vychází i ze smlouvy s konkrétním partnerem, jsou potřeba natolik flexibilní postupy, aby umožnily zohlednění těchto jednotlivých dohod.

Při manuální správě je rovněž poměrně běžné, že nastavení všech potřebných přístupových práv pro nové nebo pracovní náplň měnící zaměstnance trvá i několik dní. V řadě situací to je dlouhodobě nepřijatelně nízká úroveň služeb a někdy se může jednat i o porušení zákonných požadavků.

Kdo zajistí soulad se zákonnými předpisy

"Během posledních let jsme zažili rostoucí počet finančních skandálů renomovaných firem, vzestup informačních hrozeb a rostoucí obavy o bezpečnost osobních dat. Tyto trendy vedly k zavedení nové legislativy v oblasti finančního výkaznictví, zabezpečení a ochrany osobních údajů. Z toho vyplývá, že pro úspěšné splnění zákonných požadavků je stále důležitější kontrola přístupu oprávněných osob ke správným informacím. Lepší postupy správy identity mohou snížit náklady a zvýšit efektivitu, ale ještě důležitější je, že správně implementovaný systém IAM, založený na jasně definovaných rolích, poskytuje během provádění auditu přesné informace o tom, kdo, kdy a proč měl přístup ke kterým datům," varuje Marcel den Hartog. Systém IAM podle něj rovněž umožňuje precizní oddělení jednotlivých odpovědností, takže například uživatel, který zakládá novou fakturu, nemůže současně získat oprávnění k jejímu odsouhlasení.

Takový systém navíc eliminuje riziko spojené s tím, že administrátoři běžně vytvářejí uživatelské účty s oprávněními, která jsou vyššího řádu, než mají oni sami. Kromě jiného se ve skutečně velké společnosti může běžně stát, že IT manažeři nebudou schopni zjistit, kdo má k čemu vlastně přístup a kde jsou klíčová podniková data uložena. Efektivní IAM systém vzniku takové situace zabrání.

Implementace - možný kámen úrazu

Jste již přesvědčeni o přínosech kvalitní IAM strategie. "V tuto chvíli však stojíte před hlavním problémem a tím je úspěšná implementace systému. Zmiňovaný výzkum provedený naší společností ukazuje, jak náročný úkol to může být, protože 68 procent dotázaných podniků řadí na první příčku mezi překážky pro zavádění nových technologií problémy s existujícími firemními postupy a procesy. Kvalitní IAM řešení mohou být skutečně efektivní pouze v případě, že jsou nasazena ve správně nastaveném prostředí," varuje Marcel den Hartog a dodává: "Pokud je zaveden systém IAM a lidé si stále píší hesla na papírky nalepené na monitor, protože se bezpečností systému odmítají zabývat, hodnota projektu se bude blížit nule." Je naprosto nezbytné, aby každý podnik v rámci zavedení systému IAM komunikoval a prosazoval konzistentní pravidla bezpečnosti IT.

Postup pro úspěšné nasazení systému IAM lze stručně shrnout do následujících čtyř kroků.

- Určení rolí

Jedná se o klíčovou část pro nastavení rozsahu dat, ke kterým má mít každý jednotlivec přístup. Role je základní prvek, údaj, na němž je postavena celá řada funkcí IAM systému. Role by měly účinně mapovat podnikovou strukturu provozních úkonů a zodpovědností a promítnout ji do systému oprávnění tak, aby měli správní lidé ve správnou chvíli přístup ke správným zdrojům. Propojení oprávnění a odpovědností uživatelů organizaci zajistí maximální flexibilitu při zakládání nebo změně přístupových práv pro zaměstnance, obchodní partnery či zákazníky.

- Integrace do podnikových procesů

Každý IT administrátor má své vlastní metody práce. IAM systém nutně nevnucuje změny zavedených postupů, ale umožňuje je automatizovat, což přináší bezpečnější a jednodušší správu jak pro administrátora, tak i pro organizaci. Integrované řízení pracovních postupů řeší většinu složitých úkolů a zároveň zajistí dodržování podnikových pravidel a postupů. Organizace vybavená systémem správy identity a přístupu založeného na rolích může rovněž mnohem snadněji realizovat jakékoliv restrukturalizace a reorganizace.

- Integrace technologie poskytování a odebírání přístupu do různých aplikací

Klíčovým faktorem, který ovlivňuje náročnost zavedení systému správy identity, je to, jak snadno jej

lze propojit se stávajícím IT prostředím.

- Implementace automatizované správy životního cyklu identity zaměstnanců zajišťující změny a odebírání oprávnění dle změn rolí

Akumulace přístupových práv v průběhu životního cyklu dané identity a černé uživatelské účty lidí, kteří firmu nebo danou pozici již opustili, jsou dvě největší rizika současného pracovního prostředí v IT. Automatické zajištění přístupových práv potřebných k efektivní práci zaměstnance je nezbytné, ale stejně důležité je jejich okamžité odebrání při změně jeho role.

Důležité je rovněž to, že zaměstnavatel definuje počátek a konec každého IAM procesu - začátek se rovná přijetí nového zaměstnance a konec se shoduje s okamžikem ukončení pracovního poměru. Ačkoliv je to na první pohled zřejmá záležitost, dá se najít mnoho pravidelně se opakujících příkladů, kdy firma při odchodu zaměstnance nezrušila přístupová práva k citlivým systémům. Jedno významné evropské letiště při bezpečnostním auditu zjistilo, že stovky bývalých zaměstnanců, kteří ve společnosti pracovali v posledních deseti letech, mají stále přístup do zabezpečených oblastí systému. Aby k takovým situacím nedocházelo, je třeba tento proces automatizovat, a omezit tak rizika plynoucí z lidských chyb. Ušetří se tím rovněž čas strávený prováděním změn.

Ideální postup by byl přijmout zaměstnance, přidat jej do IAM systému, přidělit mu role odpovídající jeho pracovní náplni a nechat systém automaticky přidělit přístupová práva a rovněž další záležitosti, jako je přidělení počítače, identifikační karty, podnikového auta atd. Pokud poté dojde k jakékoliv změně pracovní náplně zaměstnance ve firmě, systém IAM příslušnou změnu automaticky zapracuje a následně poskytne a odebere odpovídající přístupová práva. Tímto způsobem se předejde "černým pasažérům" - osobám, které po několika změnách pracovních pozic nasbírají přístupová práva téměř ke všem systémům a zdrojům.

Sdružování identit mimo zabezpečenou doménu

Vzhledem k rostoucímu množství firem, které poskytují své služby přes internet, je důležité zmínit se ještě o tzv. identity federation (sdružování identit).

"Co se stane, když budete chtít poskytnout přístupová práva pro aplikaci nebo služby mimo vaši zabezpečenou doménu?" ptá se Marcel den Hartog z CA a odpovídá: "V rámci sloučené struktury správy identit se bezpečnost řeší integrací zabezpečovacích systémů partnerských organizací, takže se informace o uživatelích, zabezpečení a oprávnění sdílejí mezi obchodními partnery podle předem daných a kontrolovaných pravidel jakoby v jedné bezpečnostní doméně."

Protože vnější hrozby se budou i nadále rozvíjet, je nanejvýš důležité věnovat adekvátní pozornost činnosti interních pracovníků - ať se jedná o zaměstnance, partnery nebo dodavatele. Nemá to nic společného se změnami kompetencí nebo důvěryhodností lidí, jde o jednoduchý požadavek plynoucí ze stále se zvyšující složitosti a změn pracovního prostředí, což vytváří rostoucí počet příležitostí k nechtěnému i záměrnému narušení bezpečnosti. Nelze se prostě spolehnout na to, že uživatelé budou jednat zodpovědně. "Odpovědností organizací je vytvořit prostředí, v němž je bezpečnost vnímána jako přirozená součást kultury a cesta k efektivnímu a produktivnímu způsobu práce. Úspěšně zavedený systém správy identity a přístupu organizacím umožní automatizovat značnou část procesů souvisejících se zabezpečením informačních systémů a zároveň i dosáhnout maximálně efektivního provozu a přehledu o dění, což pozitivně ovlivní spokojenost uživatelů a je i v souladu s nejnovější legislativou," uzavírá Marcel den Hartog, Security Solutions Marketing Director ve společnosti CA.

Zpracovatel: Anopress IT a.s.

© EPRAVO.CZ – Sbírka zákonů, judikatura, právo | www.epravo.cz