Bezpečnostná infraštruktúra novej generácie

Bezpečnostná infraštruktúra tvorí nosnú kostru základných služieb rozsiahlych informačných systémov. Správa používateľov, riadenie prístupu, kontrola využívania zdrojov a autentifikácia sú len niektoré z funkcií bezpečnostnej infraštruktúry. Je zrejmé, že vhodne navrhnutá infraštruktúra dokáže významne zlepšiť funkciu informačného systému, a to nielen v bezpečnostných parametroch, ale aj v uľahčení správy systému a zvýšení produktivity používateľov.

Podnikové prostredie sa tradične vyznačovalo najmä mohutnými, uzatvorenými informačnými systémami. Každý z týchto informačných systémov plnil presne stanovenú úlohu a komunikácia medzi nimi bola minimálna. Tento pohľad na podnikové informačné systémy je však už dávno prekonaný. Dnešný podnikový informačný systém sa už neskladá z uzatvorených subsystémov, ale tvoria ho navzájom spolupracujúce komponenty, ktoré medzi sebou intenzívne komunikujú. Takýto model jednoznačne kladne prispieva k flexibilite a použiteľnosti podnikových informačných systémov. Na vytvorenie vhodného prostredia na efektívnu komunikáciu medzi jednotlivými komponentmi informačného systému však treba splniť niekoľko predpokladov.

V prvom rade musia jednotlivé komponenty zdieľať **spoločný jazyk** – musia navzájom komunikovať rovnakým spôsobom. Spôsob komunikácie jednotlivých komponentov rieši niekoľko rôznych systémov, vhodných pre rôzne prostredia a spôsoby nasadenia. Aplikácie môžu komunikovať pomocou posielania správ (*messaging*), pomocou vzdialených volaní, využívaním Web Services alebo kombináciou týchto prístupov.

Druhým predpokladom je, že aplikácie musia mať **spoločný slovník** – musia vedieť rovnako pomenovať objekty, s ktorými pracujú. Musí existovať spôsob, ako jednotlivé komponenty budú odkazovať na objekty v systéme, či už pôjde o súbor na serveri, stránku HTML na firemnom intranete, vnútorného zamestnanca alebo obchodného partnera.

Tretím predpokladom je **bezpečnosť komunikácie**. Takmer každý informačný systém obsahuje *chránené zdroje* – informácie alebo služby, ku ktorým majú prístup len niektorí používatelia. Takéto zdroje je potrebné chrániť aplikovaním bezpečnostnej politiky platnej v organizácii, ktorá systém prevádzkuje. Bezpečnostnú politiku však treba aplikovať konzistentne a riadiť ju centralizovane, aby sa znížila možnosť chýb a nedorozumení, ktoré môžu mať v oblasti bezpečnosti deštruktívny dosah.

Časť bezpečnostnej infraštruktúry, ktorej sa venuje tento článok, sa bude zaoberať najmä splnením predpokladov zdieľania bezpečnostne relevantných objektov (predpoklad 2), zabezpečením ich konzistencie a autenticity a riadením prístupu k službám a zdrojom informačných systémov (predpoklad 3). V ďalších odsekoch prejdeme jednotlivé kroky potrebné na vybudovanie efektívnej a bezpečnej infraštruktúry, ktorá bude poskytovať základ pre spoľahlivú prevádzku moderného informačného systému.

1. FÁZA – TRADIČNÝ PRÍSTUP

Už od prvopočiatku informačných systémov sa na autentifikáciu používateľov využívalo jednoduché heslo. Autentifikácia heslom je ešte aj dnes najrozšírenejším spôsobom overovania identity používateľov.

Používateľ na takúto autentifikáciu nepotrebuje dodatočný hardvér, heslo je ľahko zapamätateľné alebo si ho možno niekde poznamenať. Systém, ktorý overuje heslá, je veľmi jednoduchý a dá sa ľahko implementovať.

Statické heslá

Heslá však majú niekoľko podstatných nevýhod, ktoré výrazne znižujú ich bezpečnosť. Útočník môže ľahko odcudziť heslo legitímneho používateľa a potom zneužiť jeho používateľské práva. Heslá sú v starších systémoch počas prenosu väčšinou nechránené alebo chránené len slabo. No hoci sú heslá chránené silnou kryptografickou metódou, stále ho môže útočník odhaliť takzvaným slovníkovým útokom. Tento útok je neefektívny len na náhodne vygenerované heslá, ktoré sú však ťažko zapamätateľné, a preto si ich používatelia často musia niekam poznačiť. Takto uložené heslo však zase môže ľahko zneužiť akákoľvek osoba pohybujúca sa v blízkosti používateľa.

Jadnorazové heslá

Dočasnou náhradou za statické heslá sú systémy s jednorazovým heslom (*One-Time-Password* systémy, napr. SecureID, SafeWord, S/Key atď.). Tie si však vyžadujú dodatočné náklady jednak na vybavenie používateľov príslušným hardvérom alebo softvérom, jednak je nevyhnutné modifikovať server, ktorý heslá overuje. Zmena v existujúcich systémoch je však minimálna.

Bezpečnosť systému sa nasadením jednorazového hesla zvýši hlavne vďaka psychologickému faktoru. Zariadenie generujúce heslá je podobné platobnej karte alebo kľúču a používatelia sú zvyknutí tieto predmety chrániť. Reálna bezpečnosť systému však stúpne len mierne. Systémy s jednorazovým heslom v žiadnom prípade nepredstavujú konečné riešenie problému, sú však vhodným medzikrokom pri vybudovaní bezpečnej infraštruktúry.

Prvý krok k infraštruktúre

Porozmýšľajte nad vaším autentifikačným systémom a zhodnoťte jeho bezpečnosť: Je dostatočne bezpečný? Aké riziká hrozia jeho zneužitím? Ako dlho ho ešte budete môcť používať? Pokúste sa dodatočne zabezpečiť váš autentifikačný systém alebo nahradiť ho dočasným riešením s jednorazovými heslami.

2. FÁZA – CENTRALIZÁCIA

Nech už vo vašom systéme používate akýkoľvek autentifikačný systém, je nesmierne dôležité, akým spôsobom sú používatelia identifikovaní a kde sú uložené ich údaje. Predpokladajme, že váš informačný systém má niekoľko vstupných bodov: prihlásenie sa do siete z PC, vstup na firemný intranet, vzdialený prístup zamestnanca z domu atď. Pri tradičnom spôsobe nasadenia týchto subsystémov má každý z týchto vstupných bodov vlastnú databázu oprávnených používateľov. Takýto spôsob nasadenia však skôr či neskôr môže priniesť vážne problémy. Predstavte si, že niektorý zo zamest-

nancov podniku bude prepustený pre nedostatočné pracovné výkony. Jeho záznam je vymazaný z databázy personálneho oddelenia, ktoré pošle správu o jeho prepustení správcovi systému zabezpečujúceho vzdialený prístup. Tento správca je však práve na dovolenke a správa skončí v jeho priečinku. Prepustený zamestnanec sa medzitým rozhodne predať databázu zákazníkov podniku konkurencii. Keďže jeho vzdialený prístup z domu ešte nebol zrušený, nič mu nebráni zoznam zákazníkov „legálne“ získať a predať.

Adresárové služby

Toto je len jeden z možných prípadov, keď nekonzistencia bezpečnostne dôležitej databázy môže spôsobiť vážne problémy. Preto je nesmierne dôležité centralizovať všetky údaje, ktoré majú dosah na celkovú bezpečnosť informačného systému. V praxi ide najmä o údaje o používateľoch systému a ich prístupových právach.

Ideálnym miestom na uloženie takýchto informácií je adresárová služba (*directory service*). V princípe ide o systém podobný telefónnemu zoznamu, kde sú uvedení všetci používatelia systému, ich osobné údaje, pracovné zaradenie, autentifikačné údaje atď. Jednotlivé komponenty systému majú právo k týmto údajom pristupovať na úrovni, ktorú potrebujú na svoju činnosť. Napríklad aplikácia personálneho oddelenia má prístup k osobným údajom, server vzdialeného prístupu však môže overiť len heslo používateľa a jeho oprávnenie k vzdialenému prístupu do siete.

Adresárová služba však nemusí obsahovať len údaje o používateľoch. Rovnako vhodná je aj na údaje o používateľských skupinách, sieťových zariadeniach, softvérových aplikáciách, konfiguráciách atď. Väčšina globálnych údajov v informačnom systéme, ktorých charakter je viac-menej statický, sa môžu s výhodou uložiť na adresárových serveroch.

LDAP

De facto štandardom pre adresárové služby je server LDAP. Skratka LDAP zmanemá *Lightweight Directory Access Protocol* a je definovaný ako internetový štandard v RFC 2830. LDAP pôvodne vznikol ako odľahčená verzia protokolu DAP, ktorý je súčasťou mohutnej rodiny odporúčaní ITU-T X.500 pre adresárové služby. Odľahčený charakter protokolu LDAP sa prejavuje v nižších nárokoch na zdroje pri dostatočnom zachovaní funkčnosti protokolu. Obsah LDAP servera je uložený v malej, jednoúčelovej databáze, optimalizovanej na čítanie. Výkon LDAP servera pri čítaní je väčšinou porovnateľný s relačnými databázami SQL s tým rozdielom, že LDAP servery sú asi 10-krát menej náročné na hardvérové zdroje. LDAP server je možné distribuovať a replikovať, čo pri správnej architektúre môže podstatne zvýšiť výkon a dostupnosť celého systému.

Druhý krok k infraštruktúre

Centralizujte vaše údaje o používateľoch pomocou LDAP serverov. Snažte sa čo najviac aplikácií modifikovať na využívanie adresárových služieb. Pri starých aplikáciách, kde nie je možné modifikovať ich funkčnosť, snažte sa zabezpečiť automatickú replikáciu údajov v adresároch do proprietárnych databáz starých aplikácií. Snažte sa bezpečnostnú infraštruktúru automatizovať a centralizovať. Zníženie počtu ľudských zásahov znižuje pravdepodobnosť chyby a šetrí náklady na prevádzku systému.

3. FÁZA 3 – VNÚTORNÁ BEZPEČNOSTNÁ INFRAŠTRUKTÚRA

V tejto fáze sú údaje o bezpečnostne zaujímavých objektoch v systéme uložené centrálne, pomocou systému adresárových serverov. Autentifikácia používateľov však stále nie je dokonalá. Použitie statických hesiel alebo niektorého z náhradných riešení začína predstavovať isté bezpečnostné riziko. Takisto na funkciu informačného systému ako celku pribudli ďalšie požiadavky. Požaduje sa dlhodobá bezpečnosť dokumentov, neodmietnuteľnosť a spolupráca s informačnými systémami mimo prostredia jedného podniku. Z bezpečnostného hľadiska je väčšina týchto požiadaviek spojená s elektronickým podpisom a asymetrickou kryptografiou.

PKI a PMI

Infraštruktúra **verejných kľúčov** (*Public Key Infrastructure, PKI*) prichádza ako veľmi vhodné riešenie týchto problémov. Pomocou systému **certifikačných autorít** (*CA*) dokáže overovať identitu kľúčov, ktoré sa môžu používateľom distribuovať na smart kartách. Kľúče a X.509 certifikáty uložené na týchto kartách spolu s LDAP servermi slúžia na vybudovanie bezpečnostnej infraštruktúry, vhodnej na použitie v moderných distribuovaných informačných systémoch.

Infraštruktúra PKI môže výborne slúžiť na autentifikáciu a overenie identity používateľa. Hľadanie práv používateľa v jeho osobnom certifikáte je však mierne nevýhodné. Preto funkciu spravovania práv jednotlivých používateľov preberá na seba **infraštruktúra správy privilégií** (*Privilege Management Infrastructure, PMI*). PMI využíva služby **atribútových autorít** (*AA*) na prideľovanie rôznych atribútov jednotlivým entitám v PKI. Tieto atribúty môžu znamenať isté pracovné zaradenie, oprávnenia k prístupom atď. Nezávislosť PKI a PMI zaručuje vysokú flexibilitu takejto spojenej infraštruktúry.

Smart karty

Kryptograficky bezpečné smart karty predstavujú flexibilný nástroj pre rôzne aplikácie od kryptograficky silnej autentifikácie cez elektronický podpis až po rôzne vernostné a mikroplatbové systémy. Smart karta je vlastne malý počítač, uložený v tenkej plastikovej karte. Smart kartu je možné programovať a vytvárať na nej malé aplikácie, ktoré dokážu komunikovať s externými systémami. Bežne sa smart karty používajú na ukladanie kľúčového materiálu a autentifikačných údajov, ktoré sa spracúvajú priamo na karte a kartu nikdy neopustia. Tak sa zabráni ich prípadnému zneužitiu.

Kryptografické smart karty je možné kombinovať aj s bezkontaktným čipom umožňujúcim vstup do budovy. Povrch kariet je možné personalizovať,

napríklad menom a fotografiou zamestnanca. V tomto prípade je možné používať kartu ako univerzálny zamestnanecký preukaz.

Tretí krok k infraštruktúre

Vymeňte svoj zastaraný autentifikačný systém za PKI. Vytvorte procesy a nasaďte technológie PKI vhodné pre vaše konkrétne prostredie. Implementujte systém smart kariet, ktoré umožňujú používateľom využívať rôzne aplikácie pomocou jednej smart karty. Upravte staršie aplikácie na spoluprácu s PKI a vytvárajte nové aplikácie, ktoré plne využijú možnosti PKI a PMI.

4. FÁZA – FEDERATED COMMERCE

Nasadenie PKI a centralizovanej správy bezpečnostných údajov predstavuje základ pre kvalitnú bezpečnostnú infraštruktúru v rámci hraníc organizácie. Informačný systém organizácie však nikdy nie je úplne izolovaný od okolitého prostredia. S nástupom B2B e-commerce a s rastom využívania Web Services sa informačný systém podniku čoraz viac integruje s externými systémami. Informačný systém musí vedieť dobre komunikovať so systémami zákazníkov, dodávateľov, odberateľov, partnerov, poskytovateľov služieb atď. Takýto rozsiahle komunikujúci informačný systém môže poskytnúť služby na vysokej úrovni, ktoré si dnes len ťažko dokážeme predstaviť. Takáto flexibilita však má aj svoju cenu. Jedným z hlavných predpokladov na vybudovanie takéhoto distribuovaného informačného systému je kvalitná bezpečnostná infraštruktúra, ktorá však nie je len uzatvoreným systémom v rámci podniku, ale siaha až za hranice podnikového systému. Bezpečnostná infraštruktúra musí byť schopná rozrásť sa do rozsiahleho priestoru extranetu a internetu. Na dosiahnutie tohto cieľa je možné výhodne využiť technológie, ktoré sa zrodili v globálnom informačnom priestore: internetové technológie.

Web Services a XML

V dnešnej dobe je už každému jasné, že hlavnou logickou štruktúrou internetu je web. Sieť WWW založená na protokole HTTP a formáte HTML bola pôvodne určená len na prezentáciu statických vedeckých hypertextových stránok, jej dnešnú podobu však asi málokto z pôvodných autorov predpokladal. Profesionálne WWW prezentácie sú tvorené z navzájom prepletených dynamických častí, ktoré vytvárajú graficky príťažlivý, zaujímavý obsah. Ukazuje sa však, že tieto aplikácie sú len akýmsi vrcholom ľadovca. Web dokáže poskytovať služby, ktoré prekračujú organizačné hranice a technologické platformy a využívajú univerzálny jazyk XML. Tieto služby v pozadí webu, nazývané Web Services, predstavujú základ pre moderné distribuované informačné systémy. Pomocou Web Services bude možné len pomocou niekoľkých kliknutí vo vývojovom nástroji pridať do aplikácie čerstvé burzové správy, aktuálne kurzy zahraničných bánk, nové produkty a akcie u dodávateľov alebo aktuálny priebeh WWW ankety pre zákazníkov. A to zďaleka nie je všetko, čo Web Services dokážu ponúknuť. V kombinácii s vhodnou bezpečnostnou infraštruktúrou vedia vykonávať bezpečné obchodné transakcie cez internet alebo včas automaticky objednať náhradné súčiastky na sklad tak, aby boli dodané práve v čase, keď technikom začnú chýbať.

Internet Identity

Na plnohodnotné využívanie internetových aplikácií a na úplné využitie Web Services je však nevyhnutné preniesť vnútornú bezpečnostnú infraštruktúru aj na vonkajšiu stranu podnikového systému. Informácie o niektorých používateľoch bude treba sprístupniť partnerským systémom. Niektoré informácie o koncových zákazníkoch budete chcieť zdieľať s externými obchodníkmi. Vaši zamestnanci musia mať pohodlný prístup k niektorým informačným systémom vašich dodávateľov atď.

Všetky tieto požiadavky sa dajú zhrnúť do jednej: každý používateľ potrebuje (aspoň) jednu identitu, ktorá by ho reprezentovala v globálnom priestore. Navyše každý používateľ musí byť schopný rozhodovať, aké údaje z jeho identity budú sprístupnené. Tomuto princípu sa hovorí global identity alebo *Internet identity* a predstavuje jeden z hlavných cieľov pre dnešné internetové aplikácie. Hlavnou otázkou v tomto smere je miesto uloženia informácií o používateľovej identite. Niektoré systémy sa snažia presadiť centralizovaný prístup (napr. Microsoft Passport), ktorý je však v tomto prípade úplne nevhodný. Sľubnou cestou sa zdá takzvaná *Federated Identity*, kde údaje o používateľoch sú uložené na rôznych serveroch, každý pod kontrolou vlastnej používateľskej skupiny. Použitie údajov je potom riadené vzťahmi dôvery medzi jednotlivými skupinami, podobne ako je to v prípade PKI. Touto cestou sa uberá Libery Alliance, čo je združenie priemyselných organizácií, vedené spoločnosťou Sun Microsystems. Podobnou cestou sa uberá aj niekoľko nezávislých projektov.

Pre podnikové prostredie je však dôležité, aby bezpečnostná infraštruktúra bola integrovaná so systémom internetovej identity a aby používatelia podnikového systému vedeli využiť výhody internetovej identity počas svojej práce. Takéto riešenie prináša značný nárast produktivity práce hlavne vysokokvalifikovaných pracovníkov a umožňuje spoľahlivo chrániť manipuláciu s osobnými údajmi o zamestnancoch vlastnými prostriedkami.

Štvrtý krok k infraštruktúre

Prepojte vlastný informačný systém s externými systémami pomocou Web Services. Infraštruktúra vybudovaná pomocou LDAP serverov a PKI poskytne silný základ pre tento krok. Zvýšte efektivitu vašich aplikácií a produktivitu práce vašich zamestnancov implementáciou systému internetovej identity. Uistite sa, že využijete systém vhodný pre váš konkrétny prípad a že ste schopní spoľahlivo chrániť osobné údaje vašich zamestnancov.

ZÁVER

Dnes je už jasné, že stojíme na začiatku novej éry vo vývoji informačných systémov. Uzatvorené systémy sa začínajú spájať, navzájom využívajú svoje služby a vznikajú globálne informačné systémy. Je známe, že hodnota siete stúpa kvadraticky s počtom používateľov, preto aj možnosti globálnych informačných systémov sú oveľa väčšie ako prostý súčet možností ich častí. So zložitosťou siete však značne stúpajú aj nároky na infraštruktúrne subsystémy a celkovú bezpečnosť komunikácie. Cesta od tradičných a málo účinných metód zabezpečenia až po modernú infraštruktúru, založenú na internetových technológiách, sa môže zdať dlhá a náročná, jej absolvovanie je však vstupenkou do sveta nových možností – vstupenkou do budúcnosti.

Ing. Radovan Semančík, Business Global Systems, a. s.