Správa informační bezpečnosti

Využití internetu v podnikání patří dnes k běžné praxi. Stále více míst, včetně malých odlehlých pracovišť, je připojeno do komunikační infrastruktury podniku, aby bylo možné využívat centralizovaná datová úložiště a jednoduché sdílení aplikací. Pro uživatele to znamená ulehčení jejich práce a pro podniky zvýšení efektivity. Ovšem správcům sítí a pracovníkům odpovědným za bezpečnost informací tento trend přináší obtížně řešitelné úkoly, protože v zákulisí informačních systémů dochází doslova k explozi počtu programů potřebných k podpoře běhu různých aplikací.

Podniky i dodavatelé bezpečnostních systémů akceptují jako nevyhnutelnou skutečnost, že nárůst počtu připojených míst, popř. zákazníků, znamená také nárůst počtu bezpečnostních komunikačních bran. Instalace, konfigurace a provoz nesčetných systémů s komplikovanými vzájemnými vazbami ovšem vedou k enormnímu nárůstu požadavků na správu informačních systémů. Důsledky jsou za prvé růst nákladů a za druhé pokles spolehlivosti a funkčnosti – protože kde je vyžadováno hodně zásahů správců systémů, tam je také hodně prostoru pro jejich chyby. Situace se vyostřuje s růstem počtu systémů pro optimalizaci konektivity a provozu informačních sítí, jež jsou často součástí bezpečnostních komunikačních bran. Všechny plní speciální úkoly a nepatří v užším smyslu k bezpečnostním systémům, ale přesto musí být zahrnuty do celkového konceptu.

Redukovat složitost

Složitost bezpečnostní infrastruktury nesmírně vzrostla. Správu systému ulehčuje jednoduché uživatelské rozhraní a snadná obsluha bezpečnostních komunikačních bran, ale to nestačí. Značné problémy činí čistě jen enormní množství systémů.

Je nutné radikální řešení, které umožní nejen nyní, ale i v budoucnu vykonávat efektivní správu komunikační infrastruktury. Nabízejí se různé přístupy, jak složitost systémů dlouhodobě účinně zredukovat a tím zajistit jejich hospodárnost a funkčnost. Na prvním místě stojí inteligentní správa bezpečnostních bran, která využívá podobnosti zabezpečovaných systémů. Stejně důležitá je konvergence dosud oddělených systémů do několika málo systémů centrálně spravovaných. K tomu musí být zabezpečena spolehlivá dokumentace všech změn komunikační infrastruktury, protože nedostatečný přehled o nich patří k častým zdrojům chyb a růstu nákladů.

Využití podobností

Jednoduchý příklad objasňuje základní problém správy systému informační bezpečnosti: když se lidé nastěhují do bytového domu, mají nejprve všechny byty v podstatě identické technické vybavení. V tomto prostředí je velmi jednoduché starat se o údržbu. Ale nájemníci si své byty začnou dříve nebo později sami měnit a přizpůsobovat svým požadavkům. Společná opatření, která se mají týkat celého domu, se stávají stále náročnějšími. Přesto se byty od sebe neliší úplně, stále v nich lze nalézt mnoho podobných rysů. Při nerespektování těchto podobností by bylo nutné na jednotlivé byty pohlížet jako na zcela samostatné jednotky a spravovat je nezávisle.

Proč představuje uplatnění podobného přístupu pro mnoho dodavatelů bezpečnostních řešení zásadní problém, ačkoliv v něm spočívá potenciál využitelný k optimalizaci správy? Odpověď je možné nalézt v základní koncepci správy: obvykle se používá koncepce založená buď na profilech, nebo na zařízeních. Správa založená na profilech je skvělá pro případ, kdy je třeba spravovat velké množství identických komunikačních bran. Individuální atributy jednotlivých zařízení ale přinášejí růst nákladů. Naproti tomu stojí koncept správy založené na zařízeních, která plně respektuje vlastnosti jednotlivých přístrojů, ale není možné ji efektivně použít pro správu velkého množství zařízení.

Řešení spočívá jedině v kombinaci obou přístupů, jak to prosazuje např. společnost Phion. Jako relativně mladá společnost není tento rakouský dodavatel bezpečnostních systémů zatížen minulostí a mohl si dovolit jít od začátku vlastní cestou a vyvinout takovou koncepci správy bezpečnosti komunikační infrastruktury, která se od dosavadních radikálně liší. Na jedné straně umožňuje respektovat individuální vlastnosti jednotlivých komunikačních bran a na druhé straně umožňuje efektivně spravovat to, co mají společné. Kombinuje výhody přístupů založených na profilech i zařízeních a omezuje jejich nevýhody. Příkladem úspěšné realizace může být společné výpočetní centrum v Insbrucku s 650 komunikačními branami s firewally. I přes rozdílnou konfiguraci jednotlivých bran lze systém spravovat s rozumnými náklady a úsilím.

Konvergence

Efektivní správa komunikačních bezpečnostních bran využívající jejich podobnost je nezbytný krok – ale jen první. V komunikačních sítích je umístěno mnoho dalších zařízení, jako jsou směrovače (*routery*) nebo přepínače (*switche*), a také systémy pro optimalizaci provozu sítí. Všechny mají svůj význam, ale složitost jejich vzájemných interakcí znemožňuje uplatnit efektivní pracovní postupy při správě systémů a zabírá velkou kapacitu oddělení údržby informačních systémů.

Jednoznačným trendem je proto konvergence bezpečnostních metod a techniky: do jednotného konceptu správy jsou integrována dílčí, vzájemně se doplňující řešení. Patří sem nejprve nástroje pro zajištění bezpečnosti a vysoké dostupnosti, ale při propojení závodů včetně odlehlých filiálek prostřednictvím WAN nemohou zůstat stranou ani systém inteligentního řízení provozu na síti (*traffic intelligence*) a systém optimalizace komunikace prostřednictvím WAN. Systém *traffic intelligence* se stará o to, aby poruchy a rušení na síti měly na komunikaci co nejmenší vliv a aby kritická data vždy došla jejich adresátovi. Optimalizace komunikace prostřednictvím WAN zabezpečuje, aby objem přenášených dat byl co nejmenší, a dosáhlo se tak rychlé odezvy.

Pod heslem *Branch Office Box* (BOB) se v současné době ostře diskutuje o tom, jak daleko má či může integrace těchto systémů jít. Někteří dodavatelé považují BOB za zařízení pro optimalizaci provozu na WAN s několika málo přídavnými funkcemi. Filiálky ale potřebují i řešení pro zabezpečení a inteligentní správu provozu na síti a nezbývá jim, než použít pro tyto účely speciální systémy, což je spojeno s náklady na jejich instalaci a údržbu. Naproti tomu stojí výrobci jako Phion: na základě zkušeností se složitými komunikačními sítěmi prosazují strategii konvergence. Například bezpečnostní komunikační brány Netfence od společnosti Phion zahrnují funkce zajištění bezpečnosti, dostupnosti a inteligentní správy provozu na síti. Dodatečně do nich lze integrovat i funkci optimalizace komunikace prostřednictvím WAN, a podniky tak mají možnost pomocí jednoho zařízení zaručit bezpečnou a spolehlivou komunikaci se vzdálenými filiálkami s jednotnou, centralizovanou a efektivní správou.

Závěr

Více než o efektivitě správy by se dnes mělo hovořit o efektivitě celé bezpečnostní infrastruktury, ať už z funkčního nebo nákladového hlediska. Doba, kdy byl podnik s vnějším prostředím spojen jednou nebo dvěma komunikačními branami, je dávno pryč. Složitá komunikační infrastruktura vyžaduje nové přístupy ke správě sítí a bezpečnosti, které poskytují na jedné straně potenciál ke zvyšování efektivity a na druhé straně jsou dostatečně flexibilní, aby vyhověly individuálním požadavkům uživatelů kdekoliv na světě. To ale samo o sobě nestačí: jen tehdy, pokud jednotlivé důležité systémy konvergují do jednotného bezpečnostního řešení, může být celá struktura hospodárně a technicky rozumně spravována.

Dr. Klaus Gheri, CTO phion AG