Agilní přístup k bezpečnosti

Jak nepodlehnout vnějšímu nátlaku při jejím budováním

Lubomír Almer

Pružný neboli agilní přístup k bezpečnosti je jedním ze základních klíčů k jejímu komplexnímu budování v organizaci. Výběru řešení by vždy měla předcházet analýza přínosů, které jeho implementací získáme, v kombinaci s porovnáním dalších obdobných řešení. Namísto toho se v dnešní době nezřídka setkáváme s rozhodováním o nákupu na základě umu obchodního zástupce prodat či schopnosti marketingového oddělení řešení zpropagovat. Je velice těžké, ne-li až nemožné, tomuto systematickému ovlivňování odolat a nezakoupit „vše řešící krabičku“, kterou stačí pouze připojit do infrastruktury a zajistit si tak „plnou bezpečnost“, bez dodatečných nákladů. Tento článek poskytuje metodický postup jak k budování bezpečnosti přistupovat agilně a vyvarovat se tak mj. nákupu technologického řešení, které nereflektuje bezpečnostní potřeby organizace.

Co je to agilní přístup k bezpečnosti?

Zjednodušeně řešeno se pod tímto pojmem skrývá aktivita realizovaná na straně organizace, kdy aktivně přistupuje k budování bezpečnosti a výběru řešení a opatření. Tento přístup spočívá zejména v posouzení, zda zvažované řešení je pro organizaci dostatečně přínosné. Nejedná se však pouze o hodnocení nákladů a přínosů. Z agilního pohledu na bezpečnost není důležitá pouze otázka, co nám implementace přinese, ale hlavně jaké hrozby tím minimalizujeme. Cílem agilní bezpečnosti je tedy pokrytí komplexního spektra hrozeb a zranitelností, kterých daná hrozba může zneužít. Pro tento přístup k bezpečnosti je nezbytné si uvědomit fakt, že ne všechny hrozby jsme schopni vyřešit implementací technologického řešení. Jinými slovy, agilní přístup slouží k minimalizaci hrozeb prostřednictvím procesních, technologických a lidských řešení či opatření, kde pouze kombinace všech tří složek vede ke komplexnímu zabezpečení. Tento přístup zohledňuje nejen implementaci výše zmíněných řešení a opatření, ale i skutečnost, kdy jsou hrozby zvládány jiným způsobem, např. akceptovány organizací, přeneseny na jiný,

zpravidla ekonomicky silnější subjekt, nebo je z důvodu jejich existence přerušena činnost. Sumárně jsou tedy zvažovány činnosti v podobě implementace, akceptace, transferu nebo přerušení.

Jak použít agilní přístup k bezpečnosti v praxi

Jak již bylo uvedeno, klíčem k agilní bezpečnosti je pružný přístup. Jedná se o aktivity realizované na straně organizace převážně v podobě různých druhů analýz. A to nejenom analýzy, co nám zvažované řešení přinese, ale hlavně analýzy současného stavu, analýzy rizik a analýzy určující soulad organizace s požadavky na ni kladených z národní a mezinárodní legislativy. Pouze kombinací těchto typů analýz získáme potřebné vstupní informace pro agilní budování bezpečnosti. Každá z těchto analýz má svá úskalí a je tedy nezbytné si stanovit provázanost a přesná kritéria, která musí daná část analýzy obsahovat, aby poskytla dostatečné informace nezbytné k budování bezpečnosti. Souhrnně můžeme jednotlivé analýzy považovat za pilíře, na kterých zmíněný přístup stojí, a které jsou pro jeho funkčnost zcela nezbytné.

Analýza určující soulad organizace s požadavky kladenými na ni z národní a mezinárodní legislativy nám stanovuje minimální bezpečnostní rámec, který musí organizace naplnit. Jako první krok je nezbytné provést identifikaci legislativy, která je přímo vztažená na danou organizaci a je tudíž pro ni povinná. Zmíněný minimální bezpečnostní rámec je základní odrazovou platformou, ze které agilní bezpečnost vychází. Následně je vhodné se zaměřit i na další legislativu, normy, standardy, rámce a další, ve kterých je možné identifikovat rozšiřující bezpečnostní opatření. Tato opatření mohou mít pozitivní vliv na budování bezpečnosti, nebo mohou sloužit jako inspirace vedoucí k jejímu zdokonalení. Slouží rovněž jako rozšíření minimálního bezpečnostního rámce na širší rámec. Ať už organizace využije minimální nebo širší rámec mělo by následovat posouzení míry souladu organizace s požadavky z ní vyplývajících. V rámci tohoto vyhodnocení musí být veškerá identifikovaná opatření podrobena vyhodnocení vhodnosti jejich implementace. Analýza současného stavu nám umožňuje přesně posoudit aktuální situaci, tj. implementované technologické řešení, procesní a personální opatření.

Z hlediska technologických opatření nás zajímá nejen to, o jaké řešení se jedná, ale i jakým způsobem bylo implementováno, zda této implementaci předcházela analýza, ale zejména rizika, jež opatření pomáhá eliminovat. Zde se dostáváme k prvnímu úskalí. To spočívá v situaci, kdy ve velmi omezeném množství případů je na pořízení technologického řešení nahlíženo prostřednictvím analýzy rizik. Ač se tato skutečnost může jevit jako logická, v praxi nebývá vždy používána. Organizacemi používané analýzy rizik slouží v některých případech pouze pro potřeby naplnění formálních požadavků, jako je např. certifikace, a organizace s nimi dále kontinuálně nepracují. Je tedy možné se setkat se statickou tabulkou obsahující výčet aktiv, hrozeb a zranitelností, které sice jsou pro organizaci relevantní, ale nejsou z hlediska agilního přístupu k budování bezpečnosti dostatečně detailní, byť jsou pro získání certifikace dostatečné. Naším doporučením v tomto je dynamická analýza rizik, kterou je vhodné provádět prostřednictvím sofistikovaných softwarových řešení typu Governance, Risk and Compliance nebo Integrated Risk Management. Tento typ řešení umožňuje práci s riziky značně zjednodušit, zautomatizovat a tudíž i zefektivnit. Díky jeho použití získáváme přesný a aktuální pohled na rizika v organizaci a máme tak přesné informace nezbytné k rozhodování. Tyto přesné informace je možné použít tvorbě plánu zvládání rizik z hlediska technologických opatření.

Procesní opatření je vhodné posuzovat kontextuálně a v ideálním případě veškeré používané, nebo nově navrhované procesy otestovat v situaci, pro kterou byly navrženy. Opatření tohoto typu by měly být posuzovány převážně z hlediska schopnosti reakce, tj. zda nám daný proces umožňuje dostatečně rychle a efektivně reagovat na aktivaci zdroje hrozby. Tyto opatření nám tudíž musí umožňovat předejít aktivaci zdroje hrozby, nebo nám musí snižovat její dopad. Pokud ne je nezbytná jeho optimalizace.

Personální opatření spočívají především ve vybudování adekvátně velkého týmu a neustálém prohlubování jeho znalostí. V rámci agilního přístupu je na lidský faktor nahlíženo jako na neustále se měnící proměnou. Do které musí být kontinuálně investováno z hlediska znalostí, a z hlediska množství zajistit vzájemnou zastupitelnost, čímž je minimalizován tzv. jediný bod selhání. Zcela nezbytné je v rámci posouzení lidského faktoru hodnotit i poměr mezi úrovní bezpečnosti a operativou, tj. zda je realizační (operativní) tým schopen naplnit požadavky bezpečnostního týmu. V rámci plnění požadavku nesmí dojít k přehlcení ani jednoho týmu, což by mělo za následek nežádoucí dopad na reakční schopnost organizace. Převážně musí být zvažována možnost, že k navýšení bezpečnosti od jistého okamžiku budeme potřebovat navýšení operativy.

Výše zmíněná opatření a řešení musí být ustanoveny ve strategii rozvoje bezpečnosti. Tato strategie jasně stanovuje, kdy která opatření implementovat a jaké hrozby jimi budou minimalizovány. Implementace opatření je následně promítnuta do analýzy rizik, kde snižuje hodnoty rizika a utváří tak trend zvládání rizik v organizaci. Strategie rozvoje bezpečnosti propojená s analýzou rizik může dále sloužit i k obhajobě nákladů vynakládaných na bezpečnost, jelikož jasně vypovídá, jak daná implementace snižuje konkrétní rizika.

Co nám agilní přístup přináší

Agilní přístup koncepčně vychází z výše uvedených analýz, které jsou pro jeho fungování nezbytné. Samotný přístup, pak spočívá především v tom, že výběr každého řešení je přímo ovlivněn výsledky analýzy rizik. A to tak, že je upřednostněno (implementováno dříve) to opatření, které nejvíce sníží hodnotu celkového rizika. Zde je nezbytné poukázat na skutečnost, že agilní přístup je orientovaný na celkovou hodnotu rizika, tj. součet všech dílčích rizik a výběr opatření je hodnocen pouze z tohoto pohledu. Implementace opatření je tedy přímo vztažena na identifikované hrozby s cílem jejich minimalizace. Důležitým přínosem je také fakt, že nám tento přístup poskytuje podklady nejen pro strategická rozhodnutí, ale i pro jejich obhajobu před managementem organizace. A díky tomuto přístupu jsme schopni identifikovat, jak nám dané opatření snižuje rizika a zvyšuje tak míru bezpečnosti. ■

Ing. Lubomír Almer

Autor článku je Security Specialist společnosti AEC a.s.