ISACA JOURNAL VOLUME 3 | 2022
DAVID PODESWIK | CRISC

Úskalia dodávateľského reťazca - Riadenie rizík

Mnohé organizácie postupne zvýšili svoju závislosť na rastúcom počte svojich dodávateľov. Ako dokazujú početné útoky na dodávateľské reťazce za posledné desaťročie , aktéri hrozieb kybernetickej bezpečnosti sa často zameriavajú na dodávateľov, pretože sú menej bezpeční ako väčšie organizácie, ktoré sú vyššie v rámci dodávateľského reťazca. Príkladom je porušenie cieľových údajov v roku 2013 a útok na dodávateľský reťazec SolarWinds v roku 2020. Tieto útoky kompromitujú softvér alebo produkty dodávateľských organizácií, ktoré sú nižšie v dodávateľskom reťazci, čo umožňuje napadnutému softvéru alebo produktom uľahčiť infiltráciu väčších organizácií.

Zvýšená závislosť spoločností od veľkých dodávateľských reťazcov a zvýšenie hrozieb, ktoré s nimi súvisia, posunuli do popredia riadenie rizík dodávateľského reťazca na základe osvedčených postupov riadenia rizík v oblasti kybernetickej bezpečnosti. Potreba riadenia rizík dodávateľského reťazca nie je v tomto desaťročí o nič dôležitejšia ako v minulom – jednoducho sa stala viac uznávanou. V máji 2021 prezident Spojených štátov amerických vydal exekutívne nariadenie, ktorým sa riadia Federálne zdroje USA na financovanie usmernení pre bezpečnosť dodávateľských reťazcov. Okrem toho v roku 2021 britský National Cyber Security Center vykonal prieskum o riadení rizík v dodávateľskom reťazci. Pri tvorbe programu riadenia rizika dodávateľského reťazca väčšina respondentov prieskumu identifikovala pre svoje organizácie prekážky, medzi ktoré patrila slabá transparentnosť dodávateľských reťazcov, nedostatok odborných znalostí v oblasti rizika kybernetickej bezpečnosti a nedostatočných nástrojov, resp. bezpečnostných mechanizmov na vyhodnotenie kybernetického rizika dodávateľov.

Programy riadenia rizík dodávateľského reťazca môžu byť pre každú organizáciu prospešné, ale bez náležitého usmernenia môžu spôsobiť zvýšenie rizika. Pomýlené postupy riadenia rizík dodávateľského reťazca, ako napr. zlučovanie viacerých súvisiacich objektov auditu alebo hodnotenia artefaktov (ďalej „podkladov“), znižuje ich účinnosť. Okrem toho tvorba unikátnych dotazníkov kybernetickej bezpečnosti prispieva k rastúcej záťaži dodávateľov, ktorá im zaberá čas na zabezpečenie chodu svojich organizácií. Riziká, vyplývajúce z týchto pomýlených praktík riadenia rizík dodávateľského reťazca, môžu byť riadené dodávateľskou organizáciou, ktorá má k dispozícii podklady bez toho, aby ich musela zhromažďovať, uchovávať, prispôsobiť pravidlám pre hodnotenie rizika , ktoré predajca predstavuje

pre organizáciu nadobúdateľa a dokážu posúdiť riziko vlastným bežne používaným systémom riadenia rizík.

Prijímanie opatrení

Proti kybernetickým rizikám dodávateľských reťazcov mnohé organizácie podnikajú kroky vytvorením zlepšených programov a procesov riadenia rizík na zmiernenie rizika. Tri spoločné mechanizmy záruk používaných na overenie zabezpečenia dodávateľského reťazca sú podobné mechanizmom používanými posudzovateľmi a audítormi na overenie kontrol podľa amerického Národného inštitútu kontroly noriem a technológie (NIST). Tieto metódy sú preskúšané, otestované a opísané v špeciálnej publikácii NIST (SP) - SP 800-171A Posudzovanie bezpečnostných požiadaviek pre Kontrolované neutajované informácie a NIST SP 800-53A Rev - Hodnotenie bezpečnosti a súkromia kontroly v informačných systémoch a organizáciách. Pri aplikovaní na dodávateľské reťazce by organizácie mali:

1. Preskúmať dôkazovú dokumentáciu.
2. Viesť pohovory s jednotlivcami alebo skupinami v rámci dodávateľského reťazca.
3. Otestovať kontroly zamerané na zistenia, či správanie dodávateľov zodpovedá očakávaniam.

Tieto metódy sú často využívané poverenými osobami alebo tímom organizácie alebo zmluvnou treťou stranou.

Ďalšou možnosťou pre zlepšenie postupov organizácie na riadenie rizík dodávateľských reťazcov je hodnotenie ochrany osobných údajov. V závislosti od vonkajších regulačných požiadaviek a politiky organizácie, podklady vybrané za účelom hodnotenia dodávateľa by mohli vyžadovať dodatočné hodnotenie osobných údajov. Príkladom všeobecného hodnotenia ochrany údajov požadovaných organizáciami je EÚ General Data Protection Regulation (GDPR) Data Protection Impact Assessment (DPIA) - (Všeobecné nariadenie o ochrane údajov - Hodnotenie vplyvu na ochranu (DPIA). Hoci toto nariadenie sa vzťahuje len na časť ochrany pri prenosoch osobných údajov, tieto isté koncepty sa objavujú v rámci mnohých podobných nariadení na celom svete. V závislosti od vymieňaných informácií a druhoch dát podliehajúcim spracovaniu, môžu byť tieto údaje vyžadované pre posúdenie ochrany súkromia alebo jednoducho ako súčasť ochrany dobrého mena organizácie.

Zabezpečené dobrými predpokladmi

Aj keď organizácie vyberajú najlepšie metódy na zvládanie nových hrozieb a hoci zámer môže byť dobrý, stále je tu pre nich a pre dodávateľské reťazce potenciál dodatočného rizika. Existuje päť zavádzajúcich praktík, ktoré často ohrozujú úsilie o riadenie dodávateľského reťazca:

1. Sústredenie dôkazov od viacerých dodávateľov na jedno miesto v rámci organizácie, čo zvyšuje riziko v dodávateľskom reťazci.
2. Minimálna znalosť dodávateľov o bezpečnosti chránených dôkazov objednávajúcej organizácie (samotná dohoda o mlčanlivosti [NDA]), nezaručuje ich bezpečnosť a vytvára riziko.
3. Zdieľané dôkazy často pre dodávateľov aj objednávateľov až exponenciálne zvyšujú rozsah rizika - miesta ohrozenia dobrého mena organizácie, jej aktív, právnych záväzkov, súladu s predpismi alebo schopnosťou fungovať s rizikom:

- Každá nová organizácia, ktorá sa oboznámi s uvedenými dôkazmi,a tak zvyšuje rozsah rizika pre každého z účastníkov.
- Keďže objednávajúce organizácie u seba zhromažďujú dokumentáciu, vytvárajú väčšie a väčšie úložiská cenných bezpečnostných informácií.

4. Tým, že poskytovatelia služieb tretích strán uvedené dôkazy ukladajú a s týmito informáciami pracujú, sa riziko ešte viac zvyšuje.
5. Objednávajúce organizácie majú často všeobecné dotazníky a požiadavky na dôkazy, čo kladie zvýšené zaťaženie pre dodávateľov, ktorí tieto informácie poskytujú a uberajú im čas, aby venovali úsilie na zlepšenie vlastnej bezpečnosti.

Zhromažďovanie a zabezpečenie podkladov

Pre organizácie sa stalo zvykom vyžiadať si od dodávateľských reťazcov dokumentáciu a dôkazy, ktoré by v prípade ich odhalenia konkurenciou mohli obe strany ohroziť. Obrázok 1 ukazuje príklady často požadovaných firemných podkladov.

Obrázok 1

Príklady často požadovaných podkladov/informácií od dodávateľov

Sieťové diagramy	Základné línie systému a bezpečnostné konfigurácie	Metódy správy kryptografických kľúčov
Plány reakcie na incidenty	Miesto nasadenia viacfaktorovej autentifikácie (MFA) [1].	Správa opráv (Patch Management) a Správa o výsledkoch vykonaných opráv
Plány kontinuity podnikania	Informácie o poskytovateľovi e-mailu	Názvy zabezpečenia koncového bodu, verzie a schopnosti
Havarijné plány	- Autentifikačný protokol, na špecifikáciu mailových serverov (SPF) [2] Sender Policy Framework, Domain Keys - Ochrana e-mailov pred spamom, spoofingom a phishingom. (DKIM) [3], - Hlásenie overenia správ a nastavenia zhody (DMARC) [4].	Verzie správy mobilných zariadení (MDM) [6]
Výsledky analýzy zraniteľností	Nástroje a pravidlá na prevenciu straty údajov (DLP) [5]	Miesta a počty bezpečnostných pracovníkov
Informácie o bezpečnosti, správa protokolov, správa udalostí (SIEM) [7].	Inventár majetku	-

[1] MFA - Multifactor Authentication.
[2] SPF - Sender Policy Framework
[3] DKIM - Domain Keys Identified Mails -
[4] DMARC - Domain Based Message Authentication Reporting
[5] DLP - Data Loss prevention
[6] MDM - Mobile Device Management
[7] SIEM - Security information and event management

Na základe rizika pre produkty a dodávateľov je vhodné uvedené položky overiť a určiť, či sú v súlade s priemyselnými normami. Ich zhromažďovanie bez konkrétneho postupu je zbytočným rizikom. Ak aktér hrozby tieto informácie získa, vytvára si tým cestu, ako môže poškodiť dodávateľa.

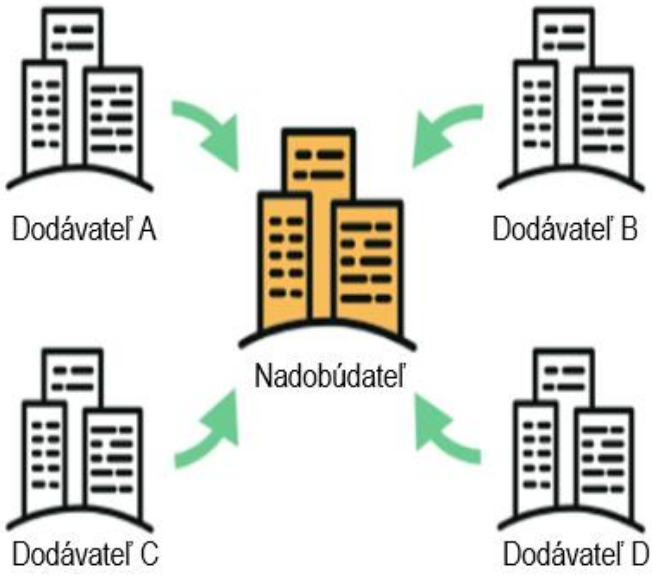
Obrázok 2 znázorňuje zhromažďovanie údajov od viacerých dodávateľov pre jedného nadobúdateľa. Hoci na tomto obrázku sú iba štyria dodávatelia, môžu tu byť stovky alebo tisíce dodávateľov, ktorí poskytujú podklady pre jedného nadobúdateľa.

Zhromažďovanie podkladov dodávateľa funguje za predpokladu, že nadobúdajúce organizácie majú potrebnú bezpečnosť, avšak žiadna organizácia úplné zabezpečenie nemá . Zakaždým, keď dodávatelia poskytujú podklady pre nadobúdacie organizácie, riskujú, že tým umožnia únik súkromných informácií, ktoré môžu byť narušené. Okrem toho , dodávatelia majú často minimálne znalosti o úrovni bezpečnosti nadobúdajúcej organizácie, ktorá umožňuje tieto informácie uložiť na neznámom mieste s neznámym zabezpečením.

Zvýšenie rozsahu rizika

Každá nadobúdajúca organizácia, ktorá získa informácie od dodávateľskej organizácie, takto zvyšuje rozsah rizika každej ďalšej organizácie, ktorá s dodávateľskou organizáciou spolupracuje.
Nadobúdacie organizácie majú často úzkoprsé myslenie, že dodávateľský vzťah je 1:1, čo je však zriedkavý prípad. Jeden dodávateľ môže zásobovať stovky, resp. tisícky ďalších organizácií.

Obrázok 2
Zhromažďovanie podkladov



Ako nadobúdajúce organizácie pokračujú v zhromažďovaní podkladov od dodávateľov, vytvárajú neustále sa rozširujúcu zásobáreň kritických bezpečnostných informácií, ktoré sú pre útočníkov zaujímavé. Ak je jedna organizácia s týmto zdrojom údajov narušená,

bezpečnosť dodávateľov je ohrozená a útočníci budú mať výhodu oproti všetkým ostatným organizáciám, ktoré s týmito dodávateľmi spolupracujú.

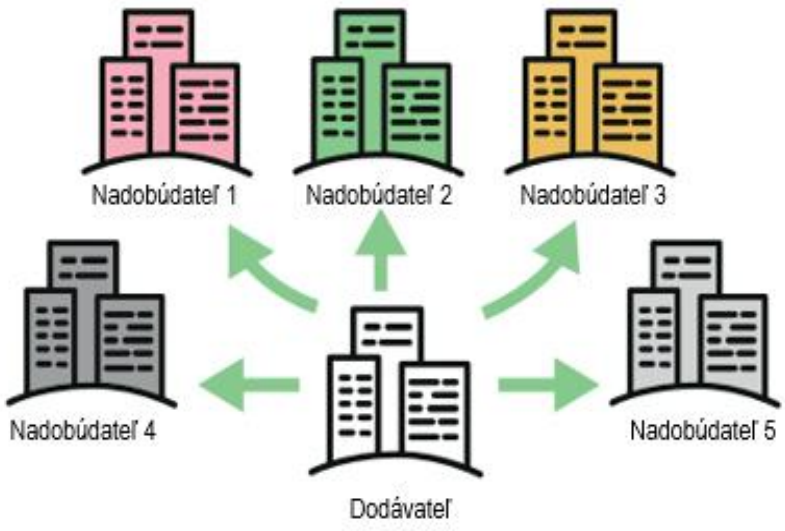
„Množstvo dotazníkov a rôznych systémov na zhromaždenie podkladov a informácií značne zaťažilo dodávateľov.“

Obrázok 3 znázorňuje vzťahy, ktoré sa vyskytujú, keď dodávateľ začne distribuovať svoje informácie viacerým nadobúdateľom. Ak každý nadobúdateľ zbiera tieto podklady, všetci zúčastnení si to musia uvedomovať. Nadobúdateľ 1 je teraz odkázaný od nadobúdateľoch 2, 3, 4 a 5, ako budú chrániť údaje pre ich dodávateľa. Toto isté vzájomné spoliehanie platí pre ostatných nadobúdateľov. Ak nadobúdatelia 1, 2, 3 a 4 chránia tieto údaje bezpečne, ale nadobúdateľ 5 už nie, informácie už nie sú v bezpečí. Všetci účastníci dodávateľského reťazca sú teraz vystavení vyššiemu riziku.

Služby dodávateľov tretích strán

Kybernetická bezpečnosť je drahá a pre nedostatok zručností pre riadne vyškolený personál sa nedá tak rýchlo dosiahnuť. To tlačí nadobúdateľské organizácie k tomu, aby tento proces riadili dodávatelia služieb tretích strán. Títo dodávatelia môžu pomôcť s preskúmaním a popisom rizík dodávateľov.
Ak však oni zbierajú podklady rovnakým spôsobom ako nadobúdatelia, problém sa tak môže ešte zhoršiť. Dodávatelia tretích strán môžu mať horšie zabezpečenie na uchovávanie kópií podkladov a postúpiť ich nadobúdateľovi. Tento príklad uvádza uloženie podkladov na troch rôznych miestach dodávateľa, nadobúdateľom a dodávateľa tretej strany, ktorý ponúka viac príležitosť pre útočníkov.

Obrázok 3
Distribúcia podkladov



Bremeno

Proces riadenia rizík dodávateľského reťazca je potrebný, ale ak sa vykoná nesprávne, môže byť záťažou. Nadobúdateľské organizácie majú často pozitívne úmysly pri zlepšovaní ich bezpečnostnej pozície, ale nemusia chápať najlepšiu cestu na jej zlepšenie. Určenie správnej hĺbky a rozsahu posúdenia rizika sa môže pre každú organizáciu líšiť.

Vyplnenie početných dotazníkov, podkladov, požiadaviek a rôzne systémy znamenajú záťaž pre dodávateľov. Mnoho dodávateľov venuje značné bezpečnostné zdroje na odpovede k dotazníkom a poskytovanie podkladov pre nadobúdateľov, a tým odklonenie personálu od úloh, ktoré môžu priniesť pozitívne zmeny na zlepšenie bezpečnosti dodávateľa.

Organizácie musia zvážiť primeranú úroveň hĺbky a krytia pre prezentované riziko. Dodávatelia, ktorí znamenajú vyššiu úroveň rizika, by mali byť dôkladnejšie preskúmaní, zatiaľ čo tí, ktorí majú nižšie úrovne rizika, by mali byť preverovaní s menšou prísnosťou. Organizácie musia zvážiť primeranú úroveň hĺbky a zabezpečenia pre prezentované riziko. Dodávatelia, ktorí poskytujú vyššie úrovne rizika, by sa mali dôkladnejšie kontrolovať, zatiaľ čo dodávatelia s nižšou úrovňou rizika by mali byť posudzovaní menej prísne.

Riešenie: Znížte rozsah rizika

Namiesto oslovovania každého dodávateľa rovnakým spôsobom by organizácie nadobúdateľa mali zvážiť kategorizáciu svojich dodávateľov na základe ich potenciálneho vplyvu a riešiť proces riadenia rizík stupňovitým spôsobom. Obrázok 4 ukazuje príklad hierarchie spôsobov merania rizika dodávateľského reťazca bez zhromažďovania podkladov . V rámci každej akcie na preskúmanie rizika posudzovateľ alebo audítor preskúma predložené osvedčenia alebo podklady a zdokumentuje ich zistenia podľa určeného systému hodnotenia rizík. Napríklad pri vyšších stupňoch rizika môže posudzovateľ alebo audítor skontrolovať podklady počas nezaznamenanej videokonferencie alebo pri osobnej návšteve. Výsledky preskúmania možno zdokumentovať v minimálnom popisnom súhrne. Okrem toho je potrebné poznamenať, či kontroly dodávateľa v konečnom dôsledku spĺňajú všetky požiadavky alebo nie. Pretože podklady zostanú v úschove dodávateľa, možno použiť ich hašovanie , aby sa zabezpečilo, že tieto preskúmané bude možné neskôr znova skontrolovať. Príklad tejto metódy je opísaný ďalej v používateľskej príručke CMMC Artifact Hash Tool. Tieto metódy zabezpečujú, že podklady nie je potrebné presúvať mimo prevádzkových priestorov a ukladať ich do veľkého úložiska. Organizácie musia určiť svoju vlastnú ochotu riskovať pre každú úroveň potenciálneho vplyvu a prispôsobiť tomu svoju stratégiu riadenia rizík.

„Namiesto rovnakého oslovovania všetkých dodávateľov organizácie nadobúdateľa by mali zvážiť kategorizáciu svojich dodávateľov na základe ich potenciálneho vplyvu a riešiť proces riadenia rizík stupňovitým spôsobom.“

Alternatívnou metódou, ktorá môže pomôcť znížiť zaťaženie dodávateľov a zmenšiť rozsah rizika pre zber podkladov, je použitie zdieľanej hodnotiacej platformy, ako je napr. Exostar.

Exostar začal spolupracovať so spoločnosťami BAE Systems, The Boeing Company, Lockheed Martin, Raytheon a Rolls Royce.“ Tieto spoločnosti majú veľmi dôverné vzťahy s dodávateľmi a v roku 2000 prezieravo vytvorili platformu, ktorá umožnila priemyslu pre letectvo a obranu správne riadiť svoje vzťahy s dodávateľmi bez toho, aby ich zaťažovali rôznymi dotazníkmi alebo zhromažďovaním nepotrebných podkladov. Používanie riadených metód, ako sú tieto, umožňuje nadobúdateľským organizáciám znížiť mieru rizika a zamerať svoje programy riadenia rizík tak, aby boli úspešné.

Obrázok 4

Príklady viacúrovňových riešení založených na potenciálnych dopadoch

Potenciál dopadov na dodávateľa	Opatrenia na zistené riziká
Kritický	Osobná návšteva, hash podkladov
Vysoký	Nezaznamenávaná videokonferencia
Stredný	Vlastné osvedčenie dodávateľa v súlade s bežne používaným štandardom kybernetickej bezpečnosti (napr. US National Institute of Technology [NIST] Special Publications [SP] 800-171A, NIST SP 800-53, Medzinárodná Organizácia pre normalizáciu [ISO]/Medzinárodná elektrotechnická komisia [IEC] 27001, Cybersecurity Maturity Model Certification [CMMC])
Nízky	Základné osvedčenie dodávateľa v súlade s bežne používaným rámcom kybernetickej bezpečnosti (napr. Federal Information Processing Standards [FIPS] Publication 200, NIST SP 800-171 Základné bezpečnostné požiadavky, CMMC úroveň 1)

Riešenie: Chráňte získané údaje

Ak nadobúdateľské organizácie získajú podklady od dodávateľov, mali by ich chrániť v súlade s priemyselnými štandardmi pre kybernetickú bezpečnosť. Medzi najdôležitejšie a ľahko prehliadnuteľné ochrany patrí šifrovanie, kontrola prístupu, stanovenie a dodržiavanie intervalu pre uchovávanie a vymazanie údajov. Podklady by sa nemali uchovávať na neurčitú dobu. K týmto údajom by mala byť priradená informácia o dobe ich uchovávania. Použiteľnosť údajov sa časom zhoršuje a akonáhle sa zistí, že už nie sú užitočné, mali by sa vymazať podľa bežne uznávaných sanitačných metód, ako je napríklad NIST SP 800-88 Guidelines for Media Sanitization.

Záver

Riadenie rizík kybernetického dodávateľského reťazca je činnosť, ktorú by mali vykonávať všetky organizácie, pričom ich strategické riadenie je nevyhnutné. Ak sú dodávatelia zaťažení neobmedzenými požiadavkami a sú nútení vzdať sa podkladov vrátane vlastnej dokumentácie, nadobúdatelia môžu tak bez toho, aby si to uvedomovali, neúmyselne ohroziť ich vlastnú bezpečnosť. Pre zníženie rizika by mali nadobúdajúce organizácie zvážiť možnosť osobných návštev, nenahrávanie videokonferencií alebo vlastné osvedčenia od dodávateľov. Okrem toho by sa hĺbka a rozsah hodnotení podkladov mali prispôsobiť úrovni rizika. Programy riadenia rizík dodávateľského reťazca môžu byť prospešné pre všetky organizácie, ale bez náležitého usmernenia môžu zvýšiť riziko pre organizácie na celom svete.

Autor článku DAVID PODESWIK | CRISC Je analytikom rizika kybernetickej bezpečnosti a dodržiavania predpisov pre spoločnosť z rebríčka Fortune 1000. Vedie tím pre riziká a súlad s kybernetickou bezpečnosťou a zameriava sa na riadenie rizík tretích strán a súlad s predpismi a politiku kybernetickej bezpečnosti.

Preklad: Ing. Dušan Makoš, CISA