HORIZON3.ai

~~TRUST BUT~~ VERIFY

WHITE PAPER

Posílení celého řetězce: Ověřená strategie obrany dodavatelského řetězce

Dodavatelský řetězec

Posílení celého řetězce: Ověřená strategie obrany dodavatelského řetězce

Porozumění prostředí kybernetických hrozeb a inovacím v oblasti řízení bezpečnostní úrovně dodavatelů

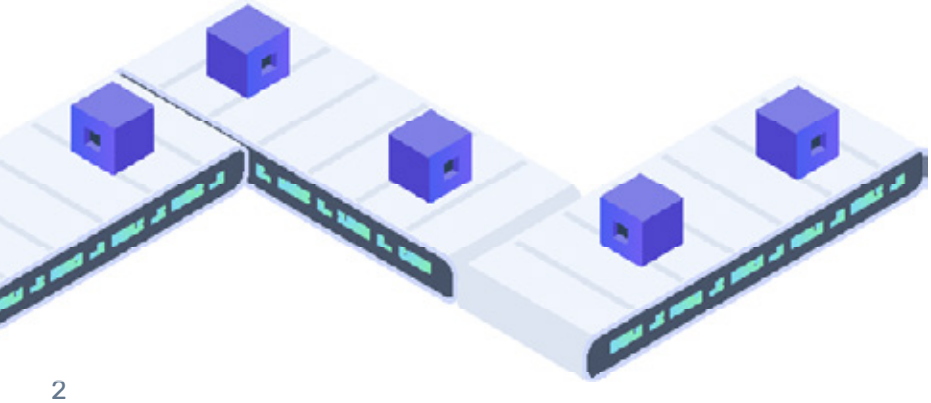
Dnešní kybernetičtí útočníci si dobře uvědomují, že útoky na menší firmy, které dodávají komponenty, díly, software a služby svým větším odběratelům „výše v řetězci", mohou způsobit výrazné narušení dodavatelského řetězce. Protože tito odběratelé na menších dodavatelích závisí kvůli včasným dodávkám, jakékoli výpadky sítě vedoucí k odstávkám výroby mohou výrazně ohrozit udržitelnost podnikání odběratelů v horní části řetězce.

Rizika dodavatelského řetězce na úrovni vedení společnosti jsou stále viditelnější, protože útočníci se čím dál více zaměřují na menší dodavatele, kteří často představují nejslabší článek. To následně představuje významnou hrozbu pro provozní integritu a kontinuitu podnikání organizací, a činí z této problematiky kritické téma, které musí CEO, COO a CISO neprodleně řešit.

V tomto white paperu se zaměřujeme na vyvíjející se prostředí kybernetických hrozeb zaměřených na dodavatelský řetězec a upozorňujeme na rostoucí zranitelnost menších dodavatelů vůči sofistikovaným kybernetickým útokům. Zkoumáme strategické postupy, které útočníci využívají, včetně práce s open-source intelligence (OSINT) k identifikaci a zneužití slabin v dodavatelském řetězci, čímž vznikají významná rizika pro provozní integritu a kontinuitu podnikání.

Ústředním bodem naší analýzy je představení **NodeZero™ pro řízení bezpečnostní úrovně dodavatelů (Supplier Security Posture Management)** - inovativního řešení navrženého ke zmírnění těchto rizik prostřednictvím autonomního penetračního testování a průběžného hodnocení. Popisujeme proces identifikace, hodnocení a prioritizace dodavatelů z hlediska zvyšování jejich bezpečnosti a doplňujeme jej o reálné případové studie, které zdůrazňují zásadní význam robustních mechanismů obrany dodavatelského řetězce.

Prostřednictvím těchto témat si tento white paper klade za cíl poskytnout generálním ředitelům (CEO), provozním ředitelům (COO) a ředitelům informační bezpečnosti (CISO) ověřenou strategii, jak posílit ochranu dodavatelských řetězců proti kybernetickým hrozbám, zajistit provozní odolnost a zachovat důvěru partnerů i zákazníků.



HORIZON3.ai
~~TRUST BUT~~ VERIFY

Obsah

Kritická závažnost problému

Provázanost dodavatelských řetězců znamená, že kyberneticky způsobený výpadek v jednom bodě může vést k významným narušením, finančním ztrátám a poškození reputace u subjektů výše v řetězci. V dnešních prostředích just-in-time (JIT) a štíhlé výroby není zajištění bezpečnosti dodavatelského řetězce pouze otázkou ochrany dat, ale také udržení kontinuity podnikání a důvěry partnerů i zákazníků.

Realita je taková, že vaše zneužitelná útočná plocha už dnes nezahrnuje pouze vlastní IT infrastrukturu, ale také IT infrastrukturu vašich dodavatelů a distributorů. Vzhledem k tomu, že je to zřejmý fakt, pojďme si vymezit kroky, které mohou útočníci podniknout při identifikaci nejzranitelnějších a nejvlivnějších cílů v rámci dodavatelského řetězce, a to s využitím OSINT a dalších strategických kritérií pro výběr cílů.

Jak útočníci využívají OSINT při identifikaci svých cílů

Open-source intelligence (OSINT) je pro útočníky klíčovým nástrojem v počátečních fázích útoku na dodavatelský řetězec. Využíváním veřejně dostupných informací mohou útočníci zmapovat dodavatelský řetězec cílové organizace, identifikovat klíčové dodavatele a získat akceschopné zpravodajské informace, aniž by vzbudili podezření. Současní útočníci k tomu využívají různé zdroje OSINT, včetně sociálních sítí, firemních webových stránek, regulatorních podání a dalších zdrojů, aby si vytvořili komplexní přehled o síti dodavatelského řetězce cílové organizace.

Techniky efektivního sběru OSINT informací

Útočníci používají pro sběr OSINT širokou škálu technik – od automatizovaného webového scrapingu až po manuální vyhledávání na oborových fórech a zpravodajských serverech. Využívají také pokročilé OSINT nástroje a vyhledávače, které jim umožňují rychle procházet a filtrovat obrovské množství dat. Účinnost OSINT průzkumu spočívá ve schopnosti útočníka syntetizovat nesourodé informace do uceleného obrazu o prostředí dodavatelského řetězce.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Jak útočníci strategicky vybírají své cíle

Strategický výběr dodavatelů jako cílů útoku na dodavatelský řetězec je sofistikovaný proces, který využívá rozsáhlé zpravodajské poznatky a detailní porozumění dynamice dodavatelského řetězce. Kromě OSINT útočníci uplatňují i další konkrétní kritéria pro výběr cíle, což jim umožňuje maximalizovat škody, které mohou organizacím způsobit.

Kritičnost pro dodavatelský řetězec

Jedním z hlavních kritérií pro výběr cíle je kritičnost dodavatele pro provoz organizací výše v dodavatelském řetězci. Útočníci upřednostňují dodavatele, jejichž narušení by mělo nejvýraznější dopad, přičemž zohledňují faktory, jako je jedinečnost dodávaného produktu či služby, obtížnost nahrazení daného dodavatele a celkový vliv na dodavatelský řetězec.

Hodnocení zranitelností

Kromě kritičnosti útočníci posuzují také zranitelnost potenciálních cílů. To zahrnuje analýzu úrovně kybernetické bezpečnosti dodavatele, včetně přítomnosti známých zranitelností a slabin, účinnosti stávajících bezpečnostních opatření a možnosti zůstat neodhaleni. Útočníci vyhledávají cíle se slabými bezpečnostními opatřeními, zastaralou infrastrukturou nebo historií bezpečnostních incidentů.

Potenciál následného dopadu

Útočníci při výběru cíle zohledňují také potenciál následného dopadu. Dodavatelé s rozsáhlými vazbami nebo ti, kteří jsou klíčovou součástí dodavatelských řetězců více organizací, jsou obzvlášť atraktivní – narušení se totiž může řetězit a kaskádovitě šířit dál, ovlivnit široké spektrum subjektů a maximalizovat způsobené škody.

Viditelnost a reputace

Viditelnost a reputace dodavatele v rámci odvětví hrají při výběru cíle také významnou roli. Útok na známého a respektovaného dodavatele může zesílit vnímaný dopad útoku, narušit důvěru napříč celým dodavatelským řetězcem a potenciálně vést k širší destabilizaci, která přesahuje samotná okamžitá provozní narušení.

Případová studie: Útok na dodavatelský řetězec Toyoty a jeho dopady

V roce 2022 kybernetický útok na společnost Kojima Industries, dodavatele dílů pro Toyotu, názorně ukázal, jak zásadní dopad mohou mít zranitelnosti v dodavatelském řetězci na globální korporace i celé ekonomiky. Útok na jediného dodavatele výrazně ovlivnil společnost Toyota a donutil ji zastavit provoz ve 14 továrnách, což vedlo k odhadované ztrátě přibližně 375 milionů dolarů. Tento incident demonstruje vzájemnou provázanost moderních průmyslových odvětví, kde kybernetický útok na jednoho dodavatele může způsobit rozsáhlé finanční ztráty a provozní narušení. Zároveň slouží jako zásadní připomínka významu kybernetické bezpečnosti na všech úrovních dodavatelského řetězce.

Další příklady incidentů v dodavatelském řetězci

- Útok na dodavatele společnosti Okta (Říjen 2023)
- Útok na dodavatele společnosti JetBrains (Září/Říjen 2023)
- Útok na dodavatele společnosti MOVEit (Červen 2023)
- Útok na dodavatele společnosti 3CX (Březen 2023)
- Útok na dodavatele firmy Applied Materials (Únor 2023)
- Útok na dodavatele firmy Fantasy Wiper (Prosinec 2022)
- Útok na dodavatele společnosti Visser (Únor 2020)

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Role autonomních pentestů při zvyšování bezpečnosti dodavatelů

V reakci na tyto sofistikované hrozby se autonomní penetrační testování ukazuje jako klíčový obranný nástroj. Tím, že simuluje taktiky, techniky a postupy (TTP) reálných útočníků, poskytují autonomní pentestingová řešení, jako je NodeZero od Horizon3.ai, organizacím i jejich dodavatelským řetězcům proaktivní způsob, jak identifikovat a zmírňovat zranitelnosti a slabiny dříve, než mohou být zneužity.

NodeZero, bezpečně spuštěný přímo v síťové infrastruktuře dodavatelů, odhaluje zneužitelné slabiny a zranitelnosti, o nichž dodavatelé často ani nevědí. Následně zjištěné problémy prioritizuje, aby dodavatelé mohli tato rizika efektivně odstranit. Poté NodeZero ověří, že byly odhalené problémy skutečně a správně napraveny ještě dříve, než se stanou kritickým rizikem pro dodavatelský řetězec – a tím pomáhá udržet provozní odolnost i kontinuitu podnikání.

Pro CEO, COO a CISO: Strategické přínosy NodeZero pro řízení bezpečnostní úrovně dodavatelů

NodeZero pro řízení bezpečnostní úrovně dodavatelů představuje osvědčený přístup ke zmírňování kybernetických rizik. Nabízí platformu pro průběžné hodnocení, která umožňuje pravidelné sebehodnocení úrovně IT bezpečnosti dodavatelů. Tato strategie podporuje procesy just-in-time (JIT) a štíhlé výroby tím, že efektivně posuzuje kybernetickou obranu dodavatelů, snižuje zátěž na straně dodavatelů a maximalizuje snížení rizik pro odběratele. Mezi přínosy patří:

- **Kontinuita podnikání:** NodeZero zajišťuje, že systémy dodavatelů jsou odolné vůči útokům, a pomáhá tak udržet nepřerušené výrobní a dodavatelské toky klíčové pro modely just-in-time (JIT) a štíhlé výroby.
- **Řízení rizik:** Díky NodeZero se robustní úroveň kybernetické bezpečnosti stává nedílnou součástí strategie řízení rizik společnosti a pomáhá předcházet neočekávaným nákladům spojeným s kybernetickými incidenty.
- **Provozní efektivita:** Autonomní penetrační testování NodeZero snižuje potřebu rozsáhlých interních bezpečnostních týmů, externích penetračních konzultantů a specializovaných dovedností, a je tak v souladu se zásadami štíhlého provozu.
- **Konkurenční výhoda:** Bezpečný dodavatelský řetězec je ten, který je spolehlivý, a tato spolehlivost se promítá do konkurenční výhody, protože zákazníci a partneři důvěřují organizacím, které kladou důraz na kybernetickou bezpečnost napříč celým řetězcem.
- **Soulad s předpisy a reputace:** Využívání pokročilých nástrojů, jako je NodeZero, prokazuje náležitou péči v oblasti kybernetické bezpečnosti, pomáhá organizacím plnit regulatorní požadavky a posiluje jejich reputaci.

Navrženo pro moderní závislost na dodavatelských řetězcích

NodeZero pro řízení bezpečnostní úrovně dodavatelů poskytuje zásadní vrstvu bezpečnostního hodnocení pro organizace, které jsou závislé na dodavatelích třetích stran zajišťujících produkty či služby, na nichž jsou odběratelé přímo závislí.

Tato závislost je obzvláště patrná v prostředí s vysokými nároky, jaké představují modely just-in-time (JIT) a štíhlé výroby. Zajištění toho, aby výrobní sektor dokázal udržet integritu a spolehlivost svých hodnotových řetězců, je proto naprosto zásadní. Integrací NodeZero do strategie zabezpečení dodavatelského řetězce mohou CEO, COO a CISO chránit svůj provoz před kybernetickými hrozbami a zachovat plynulý chod procesů, který je klíčový pro jejich úspěch. Stejný přístup lze uplatnit i v dalších odvětvích následovně:

Ukázkové scénáře:

- Finanční instituce prostřednictvím průběžného testování pomocí NodeZero sleduje zlepšování bezpečnosti u svých softwarových dodavatelů, zajišťuje soulad s předpisy a chrání zákaznická data.

- Poskytovatel zdravotní péče využívá NodeZero k průběžnému hodnocení svých farmaceutických dodavatelů a rychle identifikuje i řeší zneužitelné zranitelnosti dříve, než by útok mohl ovlivnit provoz.

- Výrobní společnost identifikuje dodavatele kritických komponent s vysokým rizikovým skóre kvůli zastaralým systémům. Po vyhodnocení a odstranění zranitelností pomocí NodeZero se dodavatelovo rizikové skóre zlepší, čímž se posílí bezpečnost dodavatelského řetězce.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Přínosy přístupu společnosti Horizon3.ai

NodeZero pro řízení bezpečnostní úrovně dodavatelů nabízí vícerozměrný přístup k identifikaci a zmírňování kybernetických rizik souvisejících s dodavateli:

Identifikace slabých článků: Využitím OSINT a externího mapování aktiv NodeZero hodnotí dodavatele a přiřazuje jim riziková skóre u těch, u nichž je pravděpodobné, že se stanou cílem útočníků.

Prioritizace pro zapojení: Organizace mohou na základě vypočtených rizikových skóre prioritizovat dodavatele pro průběžné bezpečnostní testování a zajistit tak, že se úsilí efektivně zaměří na posílení bezpečnosti dodavatelů.

Automatizace zapojení a školení: Zjednodušuje integraci vybraných dodavatelů do platformy NodeZero a doplňuje ji komplexním školením, aby bylo zajištěno efektivní využívání autonomního penetračního testování.

Průběžné reportování bezpečnostní úrovně: Poskytuje detailní a kontinuální přehled o bezpečnostní úrovni dodavatelů, umožňuje viditelnost v reálném čase a strategickou reakci na nově vznikající hrozby.

Proč by se dodavatelé měli zapojit

Dodavatelé mají pádné důvody se do tohoto přístupu zapojit:

Rozšířená odpovědnost za bezpečnost: Uvědomění si, že jejich bezpečnostní úroveň dnes přesahuje hranice jejich vlastní organizace – zapojení do tohoto přístupu tak zvyšuje nejen jejich vlastní bezpečnost, ale posiluje celý ekosystém, jehož jsou součástí.

Řízení vztahů s jasně vymezenými hranicemi: Horizon3.ai úzce spolupracuje s organizacemi i jejich dodavateli a poskytuje jim vedení, jak zajistit, aby byly sdíleny pouze relevantní bezpečnostní informace. Tím je zachována důvěrnost dat a zároveň umožněna nezbytná míra transparentnosti.

Měnící se požadavky na řízení rizik dodavatelů: S tím, jak větší společnosti přepracovávají své postupy hodnocení rizik dodavatelů tak, aby vyžadovaly důkladné bezpečnostní testování a reportování, budou dodavatelé motivováni tyto požadavky plnit, aby si udrželi klíčové obchodní vztahy.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

NodeZero pro řízení bezpečnostní úrovně dodavatelů: **Případ použití**

Je zřejmé, že tradiční bezpečnostní opatření a přístupy mohou v některých dodavatelských prostředích selhávat v tom, aby účinně identifikovaly a zmírňovaly zneužitelná rizika. V prostředí menších dodavatelů bývají bezpečnostní osvědčené postupy často odsouvány na vedlejší kolej – zejména kvůli absenci lidí, kteří by se bezpečnosti věnovali naplno, nedostatečným rozpočtům na bezpečnost a také proto, že vedení si ne vždy plně uvědomuje vlastní rizika. Často zaznívá: „Jsme jen malý dodavatel. Proč by si nás někdo vybíral jako cíl?“

Vědoma si této oprávněné obavy vyvinula jedna americká agentura Ministerstva obrany (Department of Defense), která je silně závislá na sektoru Defense Industrial Base (DIB), proaktivně program založený na NodeZero pro řízení bezpečnostní úrovně dodavatelů. Cílem této iniciativy bylo motivovat dodavatele k posouzení jejich infrastruktur, identifikaci zneužitelných rizik, nápravě těchto rizik a tím zajistit, aby se riziko nepřenášelo na agenturu DoD. Celý program byl financován agenturou DoD.

Přístup který se osvědčil

Agentura DoD nejprve identifikovala kritické malé a středně velké dodavatele, kteří představovali nejvyšší provozní rizika, a ve spolupráci s Horizon3.ai tyto dodavatele zapojila do instance platformy NodeZero spravované agenturou DoD. Tento proces zahrnoval:

Cílená identifikace: Agentura DoD vybrala dodavatele klíčové pro provozní integritu a tento seznam poskytla společnosti Horizon3.ai.

Automatizované zapojení: Společnost Horizon3.ai zajistila zapojení a integraci vybraných dodavatelů do platformy NodeZero.

Komplexní školení a podpora: Společnost Horizon3.ai poskytla agentuře DoD cílené školení a průběžnou podporu, aby umožnila efektivní využívání platformy ze strany dodavatelských týmů.

Průběžné a automatizované testování: Dodavatelé využívali schopnosti platformy NodeZero k pravidelnému, autonomnímu penetračnímu testování s cílem identifikovat a odstraňovat zneužitelné zranitelnosti.

Automatizované reportování: Agentura DoD průběžně dostávala reporty o aktuálním stavu i o zlepšeních bezpečnostní úrovně svých dodavatelů.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Významné pozitivní výsledky a snížení rizik

- Jedna firma ze sektoru Defense Industrial Base (DIB) provedla během posledních čtyř měsíců více než 70 čtrnáctidenních penetračních testů pomocí NodeZero, přičemž potřebné úsilí bylo minimální – v zásadě pouze nastavení a spuštění jednotlivých testů.
- Další DIB firma provedla svůj první externí penetrační test už dva dny po zapojení a NodeZero prokázal, že dokáže zneužít známý zranitelný softwarový produkt v její síti.
- Další DIB firma zjistila, že NodeZero dokázal získat přístup k testovacím datům, manuálům a dalším citlivým informacím uloženým v její síti.

Výsledky nasazení NodeZero v dodavatelském řetězci agentury DoD

Tato iniciativa prokázala významné zlepšení kybernetické odolnosti dodavatelského řetězce agentury DoD, zejména v těchto oblastech:

Snížení zranitelností: Měřitelný pokles kritických zranitelností u zapojených dodavatelů, který vedl ke snížení celkového rizikového profilu jak dodavatelů, tak samotné agentury DoD.

Provozní kontinuita: Posílená bezpečnostní opatření vedla k výraznému zlepšení provozní odolnosti, s menším počtem narušení, nižším rizikem a předvídatelnějšími výsledky.

Strategické poznatky: Automatizované reportování poskytlo praktické poznatky, které umožnily cílená zlepšení a efektivnější alokaci zdrojů.

Posílená spolupráce: Tento proces podpořil kulturu spolupráce v oblasti bezpečnosti, přičemž dodavatelé se více zapojili do proaktivních postupů kybernetické bezpečnosti..

Poznámka: Výše uvedená agentura DoD nadále rozšiřuje rozsah programu a každý den do něj zapojuje další dodavatele.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Více o NodeZero pro řízení bezpečnostní úrovně dodavatelů

NodeZero odhaluje útočné cesty ke každé slabině, kterou identifikuje, a detailně popisuje jednotlivé kroky, jimiž by útočník mohl proniknout obranou dodavatele. Odkrývá slepá místa v bezpečnostní úrovni dodavatelů, která přesahují rámec známých CVE a zranitelností řešitelných aktualizacemi – například snadno kompromitovatelné přihlašovací údaje, vystavená data, chybné konfigurace, nedostatečné bezpečnostní kontroly či slabé bezpečnostní politiky. Slabiny jsou prioritizovány podle jejich dopadu, což dodavatelům umožňuje jasně pochopit, co je potřeba řešit nejdříve. NodeZero zároveň poskytuje podrobné pokyny, které podporují nápravná opatření ze strany dodavatelů. Zde je několik dalších přínosů, které NodeZero nabízí:

- **Hodnocení širokého spektra oblastí:** NodeZero posuzuje on-premises infrastruktury, externí útočné plochy, cloudové služby, systémy pro správu identit a přístupů (IAM), datovou infrastrukturu a další.
- **Autonomní řetězení útočných vektorů:** NodeZero se laterálně pohybuje sítí, propojuje slabiny stejně jako útočník a následně je bezpečně zneužívá – čímž poskytuje důkaz zneužitelnost.
- **Prioritizace hrozeb:** NodeZero určuje, které slabiny jsou skutečně zneužitelné a mají kritický dopad, a pomáhá tak dodavatelům seřadit nápravná opatření podle priority. Zároveň upozorňuje na systémové problémy, díky čemuž lze jedním opatřením odstranit více slabin najednou – například úpravou bezpečnostních politik.
- **Provoz bez agentů a speciálního hardwaru:** NodeZero je samoobslužná SaaS platforma, která bezpečně funguje i v produkčních prostředích. Nevyžaduje žádnou údržbu hardwaru ani softwaru a nepotřebuje perzistentní ani přístupové agenty.
- **Umožnění kontinuálního, neomezeného a koordinovaného nasazení:** NodeZero umožňuje dodavatelům zvýšit efektivitu zabezpečení tím, že mohou plánovat a spouštět velké množství penetračních testů na svých nejrozsáhlejších sítích a dokonce provádět více penetračních testů současně.
- **Provádění autonomních operací:** Platforma NodeZero průběžně rozšiřuje své schopnosti, aby dodavatelům pomáhala posuzovat a ověřovat jejich bezpečnostní úroveň, včetně interního penetračního testování, externího penetračního testování, auditů hesel v Active Directory, testování dopadu phishingu a testování známých (N-day) zranitelností.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Závěr

Rychle se vyvíjející prostředí kybernetických hrozeb vyžaduje robustní a proaktivní přístup k zabezpečení dodavatelského řetězce. **NodeZero pro řízení bezpečnostní úrovně dodavatelů** stojí v čele této výzvy a nabízí inovativní, perspektivní řešení, které je nepostradatelné pro ochranu komplexních dodavatelských řetězců.

Implementací této platformy jsou organizace schopny nejen komplexně posuzovat a řešit zranitelnosti ve svých dodavatelských sítích, ale také posilovat svou celkovou odolnost vůči kybernetickým hrozbám. Strategická hodnota NodeZero přesahuje rámec okamžité bezpečnosti – funguje jako katalyzátor pro posílení provozní spolehlivosti, ochranu kritických dat a zajištění kontinuity podnikání v době, kdy je dodavatelský řetězec klíčovou tepnou zdraví organizace.

Díky nepřetržité bdělosti a pokročilému penetračnímu testování umožňuje NodeZero organizacím zůstat o krok napřed a proměnit zabezpečení dodavatelského řetězce z potenciální slabiny v pevnou konkurenční výhodu.