Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Procesní a technologické řešení zajištění dat pro zpětné vyšetřování

Bakalářská práce

Autor: Denis Šabacký
Studijní obor: Aplikovaná informatika

Vedoucí práce: doc. Mgr. Josef Horálek, Ph.D.

Hradec Králové duben 2024

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 22.4.2024 Denis Šabacký

Poděkování:

Děkuji doc. Mgr. Josefu Horálkovi, Ph.D. za důležité rady a metodické vedení mé práce.

Abstrakt

Bakalářská práce se zabývá zajištěním a zpracováním digitálních stop pro bezpečnostní dohledy organizací. Analyzuje a porovnává známé publikace a standardy pro zajištění digitálních stop, navrhuje vlastní procesní postupy a nabízí pro ně technologická řešení. Teoretická část práce definuje pojem digitální stopy, vysvětluje jejich význam v rámci bezpečnostních dohledů organizací a popisuje vybrané standardy a doporučení pro zajištění digitálních stop. V praktické části tyto standardy analyzuje a porovnává. Na základě zjištěných informací a výsledků analýzy navrhuje vhodné procesní postupy a technologická řešení pro zajištění digitálních stop. Poslední část práce pak obsahuje table-top cvičení, které simuluje krizový scénář bezpečnostního incidentu a demonstruje význam správně nastavených procesů a technologií popsaných a navržených v předešlých kapitolách práce.

Klíčová slova

Bezpečnostní dohled, bezpečnostní incident, bezpečnostní rámec, digitální stopa, kybernetická bezpečnost, sběr logů.

Abstract

Title: Process and technology solutions for securing data for retrospective investigations

This Bachelor Thesis covers the processing and collection of digital footprints in the security operation centres of organizations. It compares well-known publications and standards for collecting digital footprints and designs its own process of digital footprint collection with technological solutions for it. The theoretical part of the thesis defines the concept of digital footprints, explains their importance in the context of cyber security surveillance of organizations and describes selected standards and recommendations. The practical part analyses and compares these standards. Based on the information found and the results of the analysis, it then designs suitable process and technological solutions for collection and analysis of digital footprints. The last part of the thesis includes a table-top exercise that simulates a crisis scenario of a security incident and demonstrates the importance of the properly set processes and technologies described and designed in the previous chapters of the Bachelor Thesis.

Key words

Cybersecurity, cybersecurity framework, digital footprint, log management, security incident, security monitoring.

Obsah

1 Úvod

Bakalářská práce se zabývá tématem procesních a technologických postupů pro zajištění digitálních stop v rámci bezpečnostního dohledu. Téma považuje autor za aktuální vzhledem k době všeobecně podporované digitalizace a rozvoje technologií napříč všemi odvětvími. Tento rozvoj přirozeně vede k větší závislosti na digitálních datech a IT systémech. Se současně se zvyšujícím počtem kybernetických útoků a jejich narůstající sofistikovaností roste zároveň i potřeba tyto systémy a data chránit. Autorovi práce je z jeho dosavadní praxe známo, že povědomí mnoha organizací o správném kybernetickém zabezpečení je však stále nedostatečné. Tato situace vede autora k výběru tří publikovaných standardů, které vznikly jako průvodce pro společnosti k vytvoření procesu zajištění digitálních stop a implementace bezpečnostního rámce. Záměrem autora je seznámit s informacemi a požadavky, s kterými organizace mohou přijít do styku při řešení této problematiky a navrhnout vhodný proces pro zajištění digitálních stop. Zkoumané publikace jsou autorem vybrány, neboť jsou celosvětově známé a organizacím snadno dostupné.

V teoretické části tato práce popisuje, co jsou to digitální stopy a proč jsou významné z pohledu oddělení bezpečnostního dohledu, který je středobodem práce s digitálními stopami pro zajištění kybernetické bezpečnosti organizace. Dále práce popisuje vybrané standardy a uvádí jejich hlavní charakteristiky a obsah.

V praktické části je provedena SWOT analýza zkoumaných norem a výsledky jsou pro přehled porovnávány v tabulce vlastností. Následně autor navrhuje optimální proces sběru digitálních stop v organizacích. Procesní návrh je v dalších kapitolách doplněn příklady technologií, které se pro zpracování digitálních stop využívají. V poslední části práce je zpracované table-top cvičení, které má za úkol prověřit připravenost společností na kybernetické incidenty a zdůraznit důležitost správně nastaveného procesu sběru a vyhodnocování digitálních stop.

2 Cíl práce

Cílem práce je analyzovat známé standardy spojené se sběrem digitálních stop a navrhnout procesní a technologické postupy pro zajištění digitálních stop a případně vytvořit table-top cvičení, které by účel těchto procesů demonstrovalo.

3 Metodika zpracování

Práce zkoumá obsah a požadavky určených standardů, zahrnuje jejich SWOT analýzu a komparaci výstupů analýzy v tabulce. Na základě výsledků, zjištěných informací a zkušeností ze své praxe poté autor navrhuje vhodný proces a technologie pro sběr a vyhodnocování digitálních stop. Pro demonstraci účelu a užitečnosti postupů z návrhové části je na konci bakalářské práce vytvořeno table-top cvičení.

4 Digitální stopy

Definice pojmu digitální stopa, nebo digitální důkaz, není nikde jednotně stanovena. Na tyto pojmy se pohlíží z různých úhlů pohledu vzhledem k jejich interdisciplinaritě, nebo na základě použití. Nejčastěji se definuje vzhledem k pohledu právnímu spojeného s vyšetřováním kriminálních činů. Například americký NIJ (Novak et al., 2018) uvádí, že digitální důkaz je *„informace uložená nebo přenášená v binární podobě, o kterou se lze opřít u soudu.“* (vlastní překlad)[1]. Pro širší použití, které je vhodnější v technických oborech, jako je kybernetická bezpečnost, se spíše hodí popis, který uvádí Vladimír Smejkal (2018, s. 825) *„Každé technologické zařízení, které získává, zpracovává, předává nebo uchovává data, zanechává záznamy (odrazy) o své činnosti. V oblasti IS/IT jsou tedy především digitální stopy, které lze definovat podle SWGDE (Scientific Working Group on Digital Evidence) jako jakékoliv informace s vypovídající hodnotou, uložené nebo přenášené v digitální podobě.“*

4.1 Význam digitálních stop v rámci bezpečnostního dohledu

Kybernetická prostředí se v dnešní době neustále rychleji vyvíjejí a organizace všech velikostí a sektorů se stávají čím dál častěji terčem různých bezpečnostních hrozeb. Kybernetické útoky, jako jsou phishingové emaily, sofistikované ransomware kampaně a další podobné hrozby, jsou stále více na vzestupu a mají stále kritičtější dopad na fungování organizací, jak vyplývá například i z reportu hrozeb 2023 (ENISA, 2023). Z těchto důvodů je stále více potřebné, aby organizace řešily svou ochranu proti kybernetickým útokům zaváděním opatření skrze vytvoření bezpečnostního rámce pro ochranu svých dat.

Jak popisují Jarpey a McCoy (2017, s. 3–10), základem takovéto ochrany jsou právě kybernetická bezpečnostní centra, která mohou mít různou formu a kompetence. Záleží na velikosti organizace, potřebě a rozsahu, v jakém potřebují kybernetickou bezpečnost řešit. Mohou mít podobu jednoho pracovníka v rámci IT

[1] Originální znění „Digital evidence is information stored or transmitted in binary form that may be relied on in court.”

oddělení, který je aktivní pouze ve standardních pracovních hodinách, ale také se mohou skládat z několika týmů, které spolupracují a fungují v režimu 24/7/365.

Svojí podstatou se ale shodují – jsou to místa určená pro kontinuální monitorování, detekci, analýzu a reakci na bezpečnostní hrozby v síťovém a informačním prostředí organizace. Klasické oddělení bezpečnostního dohledu, tak jak ho popisují například Bhatt et al. (2014), je hierarchicky zorganizované do několika týmů různých úrovní, uspořádaných podle stupně jejich odbornosti, zkušeností a jejich účelu. Týmy úrovně L1 (dále jako týmy L1) mají většinou za úkol aktivní monitoring a vyhodnocování všech upozornění, která jsou generovaná automatizovanými nástroji pro vyhodnocování kyberbezpečnostních událostí a incidentů. Provádí takzvanou základní triáž událostí. To je činnost, při které týmy L1 rozhodují, zda je upozornění takzvaně reálně pozitivní a může se jednat o potenciální hrozbu, nebo je falešně pozitivní, vzniklo například nějakým provozním zásahem a není potřeba se s ním dále zabývat. Týmy na úrovni L2 (dále jako týmy L2) pak provádí detailnější analýzu událostí, které L1 týmy vyhodnotily jako relevantní. Pokud L2 potvrdí a rozhodnou, že se jedná o bezpečností incident, zahajuje se vyšetřování a analýza. Ta může skončit například jen upozorněním uživatele na smazání softwaru z počítače, odpojení zařízení od sítě, karanténou souborů, ale také může pokračovat v odhalení velkého bezpečnostního incidentu. V takovém případě je kompetencí týmů L2 připravit podklady ze své analýzy a dále komunikovat s dalšími pracovníky, jako jsou například týmy na L3 úrovni (dále jako týmy L3). To už jsou zpravidla expertní role a týmy specializované pro reakci na incidenty. Společně tak tyto týmy zaštiťují monitoring, detekci a analýzu kybernetických událostí a tvoří základní prvek celého kyberbezpečnostního rámce organizace.

Pro všechny tyto činnosti jsou právě digitální stopy naprosto nezbytné. Aktivně sbírané digitální stopy, jako jsou zejména logy ze systémů, síťového provozu a aplikací, tvoří základ pro detekční pravidla bezpečnostních nástrojů. S těmi týmy bezpečnostního dohledu pracují a mohou tak zajišťovat detekci událostí a incidentů v reálném čase, od kterých se odvíjí další činnosti popisované výše. Dalším důležitým aspektem je možnost takovéto digitální stopy ukládat dlouhodobě na zabezpečené úložiště v nezměněné formě. Kombinací vyhodnocování a ukládání digitálních stop pak zajišťuje dostatečnou viditelnost v IT prostředí organizace,

možnost detekce událostí a incidentů v reálném čase a možnost digitální stopy využít pro zpětnou analýzu a vyšetřování. (Cichonski et al., 2012)

4.2 Potřeba zajištění digitálních stop pro zpětné vyšetřování a modelování incidentů

Zpětné vyšetřování a modelování incidentů jsou další klíčové činnosti v rámci kybernetické bezpečnosti organizace. V případě, že dojde ke kybernetickému incidentu v síti organizace, je velmi důležité mu porozumět. I v tomto procesu mají hlavní úlohu digitální stopy, protože právě jejich analýzou jsou bezpečnostní oddělení schopné vyšetřit rozsah škod a počet možných napadených zařízení, aby se vyloučila možnost, že v prostředí zůstává škodlivý kód. Dále jsou díky nim schopna bezpečnostní oddělení zanalyzovat a popsat průběh útoku, stanovit jeho počátek, a tím například i zranitelné místo v síti organizace. Tento proces může zahrnovat analýzu digitálních důkazů, jako jsou logy ze serverů, síťového provozu, e-mailů a dalších. Z těchto nálezů se poté mohou vydefinovat další vybraná opatření k zabezpečení těchto slabých míst v systému. Pochopením přesného rozsahu a chování a průběhu incidentu umožňuje organizacím transparentně komunikovat s interními i externími subjekty, jako jsou zákazníci, obchodní partneři i regulační orgány. Díky jasné a včasné komunikaci zvyšuje organizace svoji důvěryhodnost a může zamezit reputačním škodám po kybernetickém incidentu organizace. (Cichonski et al., 2012)

Při sběru digitálních stop je důležitým aspektem také délka jejich uchovávání. V případě bezpečnostního incidentu je totiž možné, že události, které k němu vedly, se mohly stát dlouho před tím, než samotný incident nastal nebo než byl odhalen. (NÚKIB, 2023, s. 23). Digitální stopy je proto vhodné uchovávat po delší časové období, což však může být velmi náročné na kapacitu úložiště. Organizace mohou zvolit pro efektivní uchování logů různé strategie, například určením hodnoty logů vzhledem k bezpečnosti, zvolit dobu uchování podle jejich kritičnosti anebo podle požadavků, které na ně může klást zákon.

Z pohledu digitálních stop použitelných ke zpětnému vyšetřování se nejčastěji používají systémové logy. Jak popisují Schmidt et al. (2012, s. 29–48), logy jsou sbírky záznamů o událostech, které obsahují důležité informace o stavech systému,

chybách, bezpečnostních incidentech a dalších významných informacích o provozu. Mají formu textových záznamů a mohou být v různých souborových formátech. Díky informacím, které logy obsahují, a díky tomu, že se dají snadno sbírat z téměř všech zařízení v síti, se logy stávají ideálními pro ukládání jako digitální stopy.

Pro jejich ukládání existují různá doporučení, která logy rozdělují do kategorií a stanovují jim doporučenou minimální dobu jejich uložení. Například NIST SP 800-92 (Kent, 2006) rozděluje minimální retence logů a dat podle důležitosti zdroje, ze kterého digitální stopy sbíráme.

Tabulka 1: Minimální doba uchování logů podle NIST SP 800-92. Zdroj: Kent (2006)

Důležitost systému	**Minimální doba uchování**
Nízká	1–2 týdny
Střední	1–3 měsíce
Vysoká	3–12 měsíců

Zdroje logů také můžeme rozdělit na kategorie, jak uvádí NÚKIB ve svém minimálním bezpečnostním standardu. (NÚKIB, 2023)

Tabulka 2: Minimální doba uchování logů podle Národního úřadu pro kybernetickou bezpečnost. Zdroj: Národní úřad pro kybernetickou bezpečnost (2023)

Typ logů	**Minimální doba uchování**
Security logy	60 dní
OS logy	30 dní
Aplikační logy	7–30 dní

V české legislativě také existuje vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „vyhláška o kybernetické bezpečnosti“) která v ustanovení § 22 subjektům spadajícím pod zákon o kybernetické bezpečnosti minimální dobu retence logů přímo nařizuje.

Tabulka 3: Minimální doba uchování logů podle vyhlášky o kybernetické bezpečnosti. Zdroj: Vyhláška o kybernetické bezpečnosti (2018)

Provozovatel	**Minimální nařízení doba uchování**
Kritické informační infrastruktury	18 měsíců
Významných informačních systémů	12 měsíců

5 Komparace existujících postupů pro zajištění digitálních stop

Pro pomoc organizacím s vytvořením postupů zajištění digitálních stop existují různé rámce. V následujících kapitolách byla k popsání a komparaci vybrána tři konkrétní doporučení: standard ISO/IEC 27002:2022 vydaný Mezinárodní organizací pro normalizaci ISO a Mezinárodní elektrotechnickou komisí IEC. Průvodce NIST 800-92, který vydal americký Národní institut standardů a technologie; a webový rámec Device Security Guidance, spravovaný Národním centrem pro kybernetickou bezpečnost NCSC ve Velké Británii. Tato doporučení, včetně rámců, byla vybrána z důvodu, že se jedná o snadno dostupná doporučení pocházející z různých institucí, která jsou uznávaná na celosvětové úrovni. Tvoří tak globální vzorek požadavků, obecně přijímaných postupů a doporučení pro zajišťování digitálních stop organizacemi pro kybernetickou bezpečnost.

5.1 Přehled dostupných standardů a doporučení v oblasti bezpečnostního dohledu

5.1.1 ISO/IEC 27002

ISO/IEC 27002 je mezinárodní standard pro správu informační bezpečnosti. Slouží jako doplňkový dokument k ISO/IEC 27001 a poskytuje konkrétní doporučení a návody implementace bezpečnostních kontrol, které ISO/IEC 27001 požaduje v rámci řízení bezpečnosti informací. Dále definuje postupy na zavedení, provádění, udržování a kontinuální zlepšování řízení bezpečnosti informací v organizacích. V rámci těchto požadavků také definuje potřebu zajištění digitálních stop ve formě systémových logů. (ČSN EN ISO/IEC 27002, 2023)

Sběr logů

Prvním krokem v rámci sběru digitálních stop je podle ISO/IEC 27002 určit účel jejich vytváření, jaká data se zaznamenávají a jaké jsou specifické požadavky na ochranu a zpracování těchto dat. To by mělo být zaznamenáno v konkrétních

politikách pro logování. Dále stanovuje, že by logy měly zahrnovat informace, jako jsou identifikátory uživatelů, systémové aktivity, časové údaje a podrobnosti o relevantních událostech, jako přihlášení a odhlášení, identita zařízení, systémové identifikátory, umístění, síťové adresy a protokoly. Z těchto událostí by organizace měly být schopné zaznamenávat podstatné události v jejich IT prostředí. Standard zmiňuje události, jako jsou pokusy o přístup k systému a datům, změny v konfiguraci systému, používání privilegií, alarmy zabezpečovacího systému a deaktivace, nebo i aktivace bezpečnostních systémů. V souvislosti se sběrem logů dále ISO/IEC 27002 klade důraz na časovou synchronizaci zdrojů pro všechny systémy. To je důležité zejména pro správnou korelaci logů mezi jednotlivými systémy a pro správnou analýzu při vyšetřování incidentů. (ČSN EN ISO/IEC 27002, 2023)

Ochrana logů

Z hlediska ochrany logů by uživatelé, včetně těch s privilegovanými přístupovými právy, neměli mít možnost mazat nebo deaktivovat logy svých vlastních aktivit pro udržení jejich dostupnosti. Mezi techniky ochrany logů standard zdůrazňuje kryptografické hašování a manipulaci se soubory omezenou pouze pro přidávání a čtení, díky čemuž se posiluje zachování jejich integrity a nechtěné přepsání dat. Dalším krokem, který by měly brát organizace v potaz, je podle standardu anonymizace logů, například pomocí maskování dat. Logy mohou obsahovat citlivá data a osobní informace osob, prostřednictvím kterých mohou být identifikovány a je potřeba přijmout opatření na ochranu jejich soukromí. (ČSN EN ISO/IEC 27002, 2023)

Analýza logů

Analýza logů by měla dle doporučení zahrnovat správnou interpretaci informačních bezpečnostních událostí, identifikaci neobvyklých aktivit a anomálního chování, které mohou být indikátorem kompromitace. K tomu je potřeba zohledňovat nezbytné dovednosti expertů, kteří ji provádějí. Do analýzy by kromě podezřelých událostí měli experti zahrnovat i další monitorovací aktivity, jako je kontrola úspěšných a neúspěšných pokusů o přístup ke chráněným zdrojům, kontrola DNS logů a prohlížení výkazů od poskytovatelů služeb pro neobvyklou aktivitu. Podezřelé a skutečné incidenty informační bezpečnosti by měly být

identifikovány a stát se předmětem dalšího vyšetřování. (ČSN EN ISO/IEC 27002, 2023)

5.1.2 Device Security Guidance od NCSC

Device Security Guidance NCSC poskytuje doporučení pro zabezpečení koncových zařízení v rámci organizace. Má formu elektronických článků na webových stránkách Národního centra pro bezpečnost v Británii. Přístup doporučení v oblasti sběru logů je srovnatelný s metodami správy logů podle NIST 800-92 a ISO/IEC 27002, ale je zaměřen specificky na zabezpečení zařízení, takže jsou jednotlivá doporučení spíše obecná.

Sběr logů

V oblasti sběru digitálních stop průvodce zdůrazňuje význam shromažďování, analýzy a správy logů jako základní součásti ochranného monitorování. Organizace by si podle něj měly určit, jaké logy jsou pro ně klíčové. Jako příklad kritických logů zmiňuje hostitelské logy, servisní logy a infrastrukturní logy. Klade důraz na sběr dat z co nejvíce různých zdrojů pro efektivní detekci a reakci na bezpečnostní incidenty. (NCSC, 2021)

Pro pomoc organizacím definovat jaké logy pro ně mohou být kritické, nabízí NCSC na doprovodném průvodci také systém kladení otázek, kterými by se organizace měly zabývat při setkání s incidentem, nebo při jeho vyšetřování. (NCSC, 2018)

Ukládání a ochrana

NCSC zdůrazňuje význam používání nástrojů a technik pro obecnou ochranu dat a zařízení před neoprávněnou manipulací a zajištění jejich integrity a dostupnosti. Device Security Guidance doporučuje pokyny pro konfiguraci logovacích úrovní na různých druzích zařízení, jeho hlavním zaměřením pak jsou koncové stanice, které dělí podle jejich operačního systému. V rámci obecných instrukcí doporučuje uchovávání logů a jejich bezpečné archivování, které zajistí organizacím efektivní vyhodnocování bezpečnostních incidentů a připraví je i na případné auditování. (NCSC, 2021)

5.1.3 NIST SP 800-92 - Guide to Computer Security Management

Tato publikace vydaná Národním institutem pro standardy a technologie poskytuje velmi technicky podrobný rámec o tom, jak efektivně spravovat logy z bezpečnostního hlediska. V mnoha ohledech se toto doporučení shoduje s ISO/IEC 27001 a ISO/IEC 27002, avšak NIST SP – 800-92 jde mnohem více do technického detailu.

Sběr logů

Podle NIST 800-92 je důležitým krokem definovat politiky a procedury pro logování. Měly by v sobě obsahovat informace, jaké události se mají logovat a v jakém detailu, jak se mají logy uchovávat a jak se mají analyzovat. Logy z různých typů zařízení obsahují různou hloubku informací a je potřeba přihlížet k tomu, jaké údaje se z nich dají využít pro korelování událostí, které umožňují sledování chování systémů a detekci potenciálních bezpečnostních incidentů.
(KENT, 2006 kapitola 4.2)

Standard doporučuje sbírat autentizační a autorizační logy, systémové logy, aplikační logy, síťové logy a logy ze zabezpečovacích zařízení, jako jsou například firewally, systémy pro detekci a prevenci úniků a antivirové programy. (KENT, 2006, kapitola 2.1)

Ochrana a šifrování logů

NIST SP 800-92 radí, jak zajistit, aby nedocházelo k neoprávněnému přístupu, úpravám nebo odstranění logů. Zahrnuje techniky jako použití kryptografického hašování pomocí funkcí, jako jsou MD5, SHA-1 nebo modernější SHA-256. Díky těmto algoritmům lze ověřovat, že logy po jejich vytvoření nebyly nechtěně upraveny. Standard zmiňuje i důležitost zabezpečení jejich přenosu například při ukládání do centrálního úložiště. Pro takovéto zabezpečení doporučuje například využití kryptografického protokolu TLS. (KENT, 2006, kapitola 3.3.2)

Analýza a monitorování

Pravidelná nebo také kontinuální analýza logů pro identifikaci podezřelé aktivity, bezpečnostních incidentů nebo i nedostatků v konfiguraci je podle

publikace klíčová pro plné využití potenciálu digitálních stop ve formě logů. (KENT, 2006, kapitola 5.2)

Provádět analýzu manuálně je neefektivní, a proto NIST SP 900-92 doporučuje použití automatizovaných nástrojů, jako je SIEM. Ty jsou díky agregačním a korelačním funkcím schopny vyhodnocovat velké množství dat v reálném čase. Důležité je také srovnání a vizualizace logů v různých časových obdobích, díky čemuž je podle tohoto standardu možné identifikovat anomálie v infrastruktuře organizace, které mohou naznačovat bezpečnostní incidenty. (KENT, 2006, kapitola 3.4)

5.2 Hodnocení předností a omezení standardů – SWOT

Každý z těchto standardů nabízí různé pojetí a hloubku detailu metod pro zpracování, ukládání a analýzu digitálních stop ve formě logů. Tato kapitola se zabývá pochopením jejich silných a slabých stránek, příležitostí a potenciálních výzev z pohledu jejich aplikovatelnosti a efektivity pro nastavení sběru logů v organizacích.

5.2.1 ISO/IEC 27002

Silné stránky

Silnou stránkou ISO/IEC 27002 je jeho praktická orientace. Například v oblasti logování poskytuje konkrétní doporučení, jaké typy logů má organizace sbírat, což usnadňuje jejich aplikaci v reálném prostředí.

Stejně jako ISO/IEC 27001 je i tento standard navržen tak, aby byl aplikovatelný napříč různými typy organizací bez ohledu na jejich velikost nebo odvětví, další silnou stránkou je tedy jeho univerzální aplikovatelnost.

Velmi silnou stránkou je vysoká míra takzvané compliance, tedy souladu s pravidly a nařízeními. Aplikování doporučení ISO/IEC 27002 pomáhá organizacím splnit právní a regulační požadavky, díky čemuž tak může organizace potenciálně zvýšit důvěru a postavení u svých zákazníků a partnerů.

Slabé stránky

Přesto, že jeho univerzálnost je výhodou, některá z doporučení mohou být stále příliš obecná nebo vyžadovat specifickou interpretaci pro konkrétní prostředí organizace, což komplikuje jeho aplikovatelnost.

Další slabou stránkou je skutečnost, že pro úspěšnou implementaci standardu jsou zapotřebí hluboké odborné znalosti a porozumění bezpečnostním konceptům. Obecně může být implementace standardů z rodiny ISO/IEC 27000 nákladná, obzvlášť v případě, kdy organizace začíná tvořit procesy sběru logů nově od základů.

Příležitosti

S rostoucím počtem kybernetických hrozeb se klade čím dál větší důraz na robustní bezpečnostní opatření se silnou compliance. To do budoucna zvyšuje relevanci doporučení vydávaných v ISO/IEC 27002 a díky univerzálnosti lze efektivně kombinovat s dalšími standardy a frameworky.

Výzvy

Rychlý vývoj technologií může způsobit neaktuálnost a snížit relevanci některých doporučení v ISO/IEC 27002. Jiné standardy a frameworky, které jsou svojí formou více inovativní nebo jdou do technické hloubky, mohou některé organizace v budoucnu více preferovat.

5.2.2 Device Security Guidance

Silné stránky

Forma jednotlivých stránek NCSC umožňuje pravidelně aktualizovat obsah, a reagovat tak na nejnovější hrozby a moderní postupy v kybernetické bezpečnosti.

Průvodce pokrývá různé typy zařízení, což umožňuje organizacím aplikovat doporučení napříč celým spektrem jejich technologického prostředí.

Slabé stránky

Stránky mají nekonzistentní formu a hloubku obsahu, některá doporučení mohou být pro technologicky méně zdatné organizace obtížně implementovatelná.

Účel těchto doporučení je zejména pro obecnou podporu oblasti kybernetické bezpečnosti v organizacích a nemá prakticky žádné certifikační možnosti. Zabezpečení pouze podle tohoto doporučení může organizacím později způsobit komplikace s plněním regulačních předpisů, a nutnost opřít se nakonec také o jiné standardy.

Příležitosti

Díky formátu, který je možné lehce aktualizovat, může Device Security Guidance přinášet jednotlivá relevantní doporučení bez nutnosti vydávání celého rámce, a tím si tak udržet aktuálnost nad ostatními standardy.

Platforma, na které Device Security Guidance je umístěn, se dá organizacemi využívat i pro spolupráci a sdílení informací o hrozbách. Díky novinkám a událostem sdílených na této platformě se tak posiluje komunita kyberbezpečnosti. To může v budoucnu zvýšit návštěvnost a relevanci těchto doporučení.

Výzvy

Větší důraz na regulatorní předpisy může být výzva pro relevanci Device Security Guidance. Pro plnění compliance bude třeba, aby doporučení sledovalo změny v regulačním a právním prostředí a přizpůsobovalo jim své postupy.

5.2.3 NIST SP 800-92

Silné stránky

NIST je uznávanou autoritou v oblasti bezpečnostních standardů, což dodává SP 800-92 vysokou úroveň důvěryhodnosti.

Rámec poskytuje podrobné a praktické pokyny pro správu logů. Organizace tak mohou najít podrobné návody na implementaci jednotlivých řešení.

I přes velkou míru technického detailu je NIST SP 800-92 navržen univerzálně tak, aby byl aplikovatelný v různých typech organizací a technologických prostředích. V některých kapitolách přímo pojednává o rozdílech velikostí IT infrastruktury, a jaký to může mít dopad pro rozhodování o implementaci jednotlivých doporučení.

Slabé stránky

Detailnost a složitost pokynů rámce mohou být pro některé organizace překážkou. Některé jeho kapitoly zase naopak nezmiňují konkrétní postupy, to může být pro organizace komplikací pro implementaci.

Stejně jako u dalších rámců tohoto formátu může být problém s aktuálností některých doporučení v důsledku rychlého vývoje IT technologií a kybernetických hrozeb.

Příležitosti

Rostoucí důraz na kybernetickou bezpečnost vede k větší poptávce po spolehlivých a osvědčených standardech, jako je NIST SP 800-92. Tento standard také lze účinně kombinovat s dalšími standardy nejen z rodiny NIST, díky čemuž je možné vytvoření komplexního rámce kybernetické bezpečnosti.

Výzvy

Stále se vyvíjející kybernetické prostředí bude vyžadovat rychlejší přizpůsobování a aktualizaci standardu, aby byla zachována jeho relevance a efektivita i v moderních IT prostředí organizace.

5.3 Komparace standardů

Pro přehlednější viditelnost rozdílů je v této kapitole vypracováno porovnání jednotlivých vlastností popisovaných ve SWOT analýze.

Tabulka 4: Komparace vybraných standardů. Zdroj: vlastní zpracování

Vlastnost	ISO/IEC 27002	Device Security Guidance	NIST SP 800-92
Praktická orientace	Ano	Ano	Ano
Univerzální aplikovatelnost	Ano	Ne	Ano
Specifičnost doporučení	Částečně	Ne	Ano
Soulad s předpisy	Ano	Ne	Ano
Certifikační možnosti	Ano	Ne	Ne
Potřeba odborných znalostí	Ano	Ano	Ano
Nákladnost implementace	Vysoká	Nízká	Střední až vysoká
Podpora standardních technologií	Ano	Ano	Ano
Detail technických pokynů	Střední	Nízký	Vysoký
Reakce na nové hrozby	Pomalá	Rychlá	Pomalá
Komunitní spolupráce	Ne	Ano	Ne
Aktualizovatelnost	Pomalá	Rychlá	Pomalá
Udržování aktuálnosti	Výzva	Příležitost	Výzva

Z komparace vyplývá, k jakým účelům se jednotlivé standardy nejlépe hodí.

5.4 Shrnutí nedostatků v současných postupech

Při analýze jednotlivých standardů je zřejmé, že každý z nich plní specifický účel a má své vymezené oblasti pokrytí. Využití těchto standardů pro kompletní proces zajištění digitálních stop izolovaně tak může přinést pro organizace nekompletní pohled a obtížné pochopení rozsahu problematiky správného zajištění digitálních stop.

Například standard ISO/IEC 27002 má velmi obecnou povahu a nezachází do velkých technických detailů ani metodik pro implementaci jednotlivých doporučení. Zavedení doporučení v ISO/IEC 27002 vyžaduje hluboké znalosti a porozumění bezpečnostním konceptům, a proto zavádění pro menší organizace může být podle tohoto standardu složité. Postupy nezmiňují konkrétní technologie možné k využití a naplnění požadavků, které stanovují.

NIST SP 800-92 poskytuje pokyny pro správu logů konkrétněji, ale nepokrývá procesní postupy jako stanovení hlavních informačních aktiv organizace, ani analýzu jejich rizik.

V potaz je potřeba také brát rychlý vývoj IT technologií a prostředí, v kterých organizace svá data spravují. To může vést k tomu, že některé doporučené postupy se mohou stát zastaralými nebo neúplnými.

Aktuálnosti se daří v případě Device Security Guidance, který je vydávaný formou aktualizovaných a revidovaných článků na webových stránkách NCSC. V porovnání s publikacemi ISO/IEC a NIST však není obsah Device Security Guidance tak dobře ucelený a chybí mu další podpora pro compliance a certifikace.

6 Návrh procesních postupů pro zajištění digitálních stop

Následující kapitola obsahuje návrh procesu pro zajištění digitálních stop. Autor vychází z informací, které získal z pracovních konzultací, odborných konferencí, technologických fór nebo podcastů. Využívá ale také informace získané z teoretické části práce, které korespondují s jeho zkušenostmi z praxe.

6.1 Definice vhodného procesu pro zachytávání a ukládání digitálních stop

6.1.1 Počáteční analýza a příprava

Správa aktiv

Řízení aktiv je v rámci správy zabezpečení informačních systémů klíčové, jelikož umožňuje organizaci získat o aktivech komplexní přehled, a díky tomu lépe porozumět a mapovat své IT prostředí. V kontextu zachytávání a ukládání digitálních stop je důkladná administrace aktiv nezbytná pro efektivní identifikaci toho, kde a jak mohou být digitální stopy generovány a v jakém množství je potřeba je sbírat, analyzovat a uchovávat. Kvalitní správou aktiv navíc lze předejít slepým místům při dalším škálování IT infrastruktury.

Najít postup, jakým způsobem řídit svá aktiva, v České republice pomáhá například Národní úřad pro kybernetickou bezpečnost (NÚKIB, 2022), který pro správu aktiv vydal průvodce. V tom ukazuje detailní metodiku včetně praktických příkladů.

V rámci procesu sběru digitálních stop je podstatné určení a inventarizace všech aktiv, což zahrnuje nejen hardwarové a softwarové komponenty, ale i data, informace a služby, mezi které mohou patřit mimo jiné právě i digitální stopy a logy. Tím organizace získá prvotní přehled o možných zdrojích a typech logů. Pro každé aktivum je pak nutné určit jeho význam, umístění, způsoby ochrany a garanta aktiva, který za něj zodpovídá.

Dalším důležitým krokem je klasifikace aktiv podle jejich hodnoty, citlivosti a kritičnosti pro organizaci. Klasifikace umožňuje určit úroveň ochrany, která by měla být pro různá aktiva aplikována, a prioritizovat zabezpečení těch nejcitlivějších a nejkritičtějších aktiv. Efektivní zabezpečení vyžaduje nejen technická opatření, ale i školení zaměstnanců a vytváření bezpečnostního povědomí v rámci organizace. Efektivní správa aktiv je kontinuální proces, který vyžaduje pravidelné aktualizace a dodržování principu neustálého zlepšování.

Analýza rizik

Proces analýzy rizik se zahajuje identifikací všech možných hrozeb a zranitelností, které mohou ohrozit cenná aktiva organizace. To zahrnuje rozpoznání potenciálních zdrojů hrozeb, jako jsou interní chyby nebo vnější útočníci, a identifikaci zranitelných míst v systémech a procesech, jež by mohla být využita k jejich kompromitaci. Následně se provádí hodnocení a klasifikace identifikovaných rizik na základě jejich pravděpodobnosti a potenciálního dopadu na organizaci, což umožňuje prioritizaci rizik a efektivní alokaci zdrojů.

Analýza rizik je také úzce spojena s procesem sběru a analýzy digitálních stop ve formě logů. To je nezbytné pro efektivní detekci a reakci na bezpečnostní incidenty. Porozumění rizikům umožňuje organizacím lépe identifikovat, která aktiva a systémy vyžadují zvýšenou pozornost a odkud a jaké logy je potřeba sbírat a analyzovat, aby bylo možné rychle identifikovat a řešit bezpečnostní incidenty.

Přehled regulatorních a legislativních požadavků

Přehled regulatorních a legislativních požadavků představuje zásadní a závěrečný krok v počáteční analýze procesu zachytávání a ukládání digitálních stop. Tento krok je nezbytný pro zajištění, že všechny aktivity související s logováním nejen splňují technické a bezpečnostní standardy, ale jsou také v plném souladu s platnými zákony a nařízeními. Legislativa může mít značný vliv na rozhodovací procesy organizace týkající se toho, jaká data jsou sbírána, jakým způsobem jsou ukládána, jak s nimi nakládat a jak dlouho je uchovávat.

V kontextu České republiky jsou organizace povinny respektovat řadu právních předpisů, včetně Obecného nařízení o ochraně osobních údajů (Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně

fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)), který klade důraz na principy minimalizace dat a omezení jejich uchovávání. To může vést organizace k tomu, aby zvážily míru logování. Dalším důležitým právním předpisem je zákon o kybernetické bezpečnosti. Ten stanovuje povinnosti pro poskytovatele základních služeb a digitálních služeb v oblasti kybernetické bezpečnosti. Klade zároveň důraz na zabezpečení informačních systémů a nařizuje, aby organizace implementovaly adekvátní technické a organizační opatření pro prevenci kybernetických útoků a incidentů. V rámci procesu zachytávání a uchovávání digitálních stop je důležité, že udává povinnost retence. V současném znění se jedná o 12 a 18 měsíců podle kategorie, kam organizace může spadat. (§ 22 vyhlášky o kybernetické bezpečnosti)

6.1.2 Vytvoření logovací politiky

Stanovení cílů logování

V prvním kroku je potřeba vyspecifikovat účel logovací politiky. Skrze stanovení cílů by měla organizace určit a odpovědět na to, proč vlastně logovací politika vznikla. Informace v této kapitole by měly reflektovat to, co bylo zjištěno v předchozích analýzách. Jeden z účelů tedy může být plnění legislativních a regulačních požadavků, které se vztahují na organizaci. Dále by měla popisovat nalezená rizika, hrozby, kterým organizace čelí, a určit, jak logování může pomoci tyto hrozby mitigovat – například skrze umožnění forenzní analýzy a zpětného vyšetřování. Dále můžou být přidány potřeby operačního monitorování určených aktiv. Cíle logování by měly být pravidelně přezkoumávány a aktualizovány, aby odpovídaly dynamickému prostředí kybernetické bezpečnosti a měnícím se obchodním potřebám organizace, čímž se zajistí, že logovací praxe zůstane relevantní a efektivní.

Určení rozsahu logování

Určení rozsahu logování by mělo obsahovat informace o tom, jaké systémy, aplikace a události budou monitorovány. To je zásadní pro zajištění, že logovací

proces pokrývá všechny klíčové informace, které by mohly být kritické pro organizaci. Rozsah by měl opět vycházet z počáteční analýzy aktiv, rizik a legislativy.

V rámci určení rozsahu je nutné definovat, které typy událostí budou logovány, včetně úspěšných a neúspěšných pokusů o přístup, změn konfigurace systému, bezpečnostních incidentů a dalších událostí, které mohou ovlivnit bezpečnostní stav organizace. Při stanovení rozsahu logování je také důležité vzít v úvahu technologické možnosti a omezení, jako je kapacita úložiště a vliv logování na výkon systémů.

Efektivní rozsah logování nejenže podporuje bezpečnostní a operativní cíle organizace, ale také pomáhá při detekci a reakci na incidenty, zlepšení výkonu systémů a splnění legislativních požadavků.

Výběr úrovně logování

Výběr úrovně logování je rozhodujícím procesem, který určuje, kolik informací bude zaznamenáváno do logů. Tento výběr by měl reflektovat specifické potřeby organizace v oblasti bezpečnosti, provozu a dodržování předpisů. Úroveň logování musí být nastavena tak, aby bylo možné efektivně monitorovat a analyzovat chování systémů a zachytit důležité události, zatímco se minimalizuje objem dat a zátěž na systémové zdroje. Vysoká úroveň detailu může být potřebná pro kritické systémy, kdežto nižší úroveň může být adekvátní pro méně kritické aplikace. Při výběru úrovně logování je klíčové najít rovnováhu mezi potřebou detailních informací pro analýzu a potřebou udržet systém efektivní a reagující.

Retence a rotace logů

Politika retence a rotace logů je klíčová pro správu úložiště logů a zajištění, že logy jsou dostupné pro analýzu a audit po potřebnou dobu. Retence určuje, jak dlouho jsou logy uchovávány před jejich odstraněním nebo archivací, zatímco rotace se zabývá mechanismem obnovy logů pro optimalizaci úložiště. Efektivní strategie musí vyvážit legislativní a provozní požadavky s omezeními úložiště a zabezpečením dat. Nastavení adekvátních intervalů retence a rotace pomáhá v prevenci ztráty důležitých informací a zajišťuje soulad s regulačními požadavky.

Bezpečnostní a ochranná opatření

Zajištění bezpečnosti logů je nezbytné pro ochranu proti neautorizovanému přístupu, modifikaci nebo ztrátě důležitých dat. Bezpečnostní opatření by měla zahrnovat šifrování logů, kontrolu přístupu k logovacím souborům a pravidelné auditování logů. Dále je důležité zvážit využití bezpečných protokolů pro přenos logů a implementaci integritních kontrol pro detekci neoprávněných změn. Tyto kroky pomáhají zajistit, že logy zůstanou důvěryhodným zdrojem informací pro bezpečnostní analýzy a auditování.

6.1.3 Výběr a implementace logovací infrastruktury

Implementace a konfigurace logovací infrastruktury vyžaduje promyšlený výběr a nasazení logovacích nástrojů a řešení. Tento proces začíná rozhodováním mezi interně vyvinutými a externě získanými logovacími nástroji, přičemž každá možnost přináší specifické výhody v kontextu kontroly, nákladů a podpory. Dalším klíčovým rozhodnutím je výběr mezi centralizovaným a decentralizovaným logováním. Zatímco centralizované řešení nabízí lepší přehlednost a usnadnění správy, decentralizované systémy mohou poskytovat větší flexibilitu v určitých provozních situacích.

Důležitým aspektem je také zajištění, že vybraná logovací řešení jsou plně kompatibilní s existující IT infrastrukturou a že se snadno integrují s ostatními systémy pro bezpečnostní monitorování a správu. Výběr nástrojů by měl také zahrnovat úvahy o jejich funkcionalitě a možnostech rozšíření, aby byly schopné plnit aktuální i budoucí potřeby organizace v oblasti logování.

Bezpečnost logovaných dat je přitom kritickou součástí celého procesu, což vyžaduje, aby byla zvolená řešení schopna efektivně chránit logy před neoprávněným přístupem, modifikací a ztrátou. To zahrnuje využití šifrování, kontrol přístupu a pravidelné auditování logů.

Nakonec je nezbytné provést důkladné testování a validaci nasazených logovacích mechanismů, aby se ověřilo, že fungují správně a že logy jsou správně shromažďovány, uchovávány a jsou přístupné pro analýzu a auditování. To zajišťuje, že logovací infrastruktura splňuje všechny požadavky na bezpečnost, provoz a dodržování předpisů organizace.

6.1.4 Sběr a analýza logů

Nastavení sběru logů

Nastavení sběru logů vyžaduje promyšlenou strategii, která zahrnuje identifikaci všech zdrojů logování, jako jsou servery, síťová zařízení, aplikace a bezpečnostní systémy. Pro každý zdroj je nutné určit typy událostí, které jsou pro organizaci nejrelevantnější, a zajistit, aby byly logy shromažďovány v konzistentním a strukturovaném formátu. Důležitým aspektem je také výběr a konfigurace nástrojů pro sběr logů, které mohou automaticky agregovat a normalizovat data z různých zdrojů. To umožňuje efektivnější správu a analýzu logů.

Monitorování a analýza

Monitorování a analýza logů jsou kritické pro detekci bezpečnostních incidentů, monitorování výkonu systémů a sledování dodržování interních a externích politik. Použití sofistikovaných analytických nástrojů, včetně softwaru pro správu logů a bezpečnostní informační a event management systémy (SIEM), umožňuje organizacím automatizovat proces monitorování a rychle identifikovat podezřelé aktivity. Pokročilé techniky, jako je korelace událostí, behaviorální analýza a strojové učení, mohou dále zvýšit schopnost organizace rozpoznávat složité vzorce chování a potenciální hrozby. Efektivní analýza logů také zahrnuje pravidelnou revizi a audit logovacích záznamů, aby se ověřila jejich přesnost a úplnost a zajistilo se, že jsou v souladu s politikami ochrany a zabezpečení dat.

6.2 Specifikace rolí a odpovědností v procesu

Specifikace rolí a odpovědností v procesu logování je dalším důležitým krokem v celém procesu zachytávání stop. Správné rozdělení povinností zajišťuje, že všechny vydefinované body logovací politiky jsou efektivně spravovány a mají určené osoby, které za jejich implementaci a dodržování nesou zodpovědnost. Počet rolí a osob, které budou v procesu figurovat, bude záležet na velikosti a potřebách organizace, důležitý ale zůstává fakt, že je pokrytý celý proces.

Rozdělení rolí ve výše navrhovaném procesu může vypadat například takto:

- **Ředitel pro informační technologie**: Zodpovídá za celkovou strategii IT a integraci technologických řešení v souladu s obchodními cíli.
- **Ředitel bezpečnosti**: Odpovědný za vytvoření a udržování bezpečnostních politik, strategií a programů.
- **Systémový a síťový administrátor**: Spravuje a konfiguruje logování na systémech a síťových zařízeních, zajišťuje sběr a předávání logů.
- **Aplikační vývojář:** Zajišťuje, že aplikace generují logy v souladu s požadavky logovací politiky.
- **Architekt kybernetické bezpečnosti:** Navrhuje bezpečnostní architekturu, včetně logovací infrastruktury, pro splnění specifických bezpečnostních požadavků.
- **Manažer kybernetické bezpečnosti:** Je zodpovědný za dohled nad tím, že jsou informační systémy a operace organizace v souladu se zákony a regulatorními opatřeními.
- **Garant aktiva:** Zodpovídá za určení úrovně ochrany aktiva, za monitorování jeho využívání a udržování jeho bezpečnosti a integrity.
- **Security analytik L2:** Provádí hloubkovou analýzu logů a reaguje na složitější bezpečnostní incidenty.
- **Security analytik L1**: Monitoruje logy na běžné bezpečnostní události a prvotní analýzu incidentů.
- **Tým pro reakci na incidenty:** Specializovaný tým reagující na bezpečnostní incidenty, využívá logy pro analýzu a řešení incidentů.
- **Auditor kybernetické bezpečnosti:** Provádí audit logů a procesů logování pro ověření dodržování interních politik a externích regulací.

Každá role by měla mít jasně definované odpovědnosti, jako je konfigurace logovacích nástrojů, sledování a analýza logů, reakce na incidenty a udržování compliance. Tímto způsobem se zajišťuje, že všechny činnosti spojené s logováním jsou pokryty a efektivně řízeny.

Dále je potřeba brát v potaz i role, které mohou být pevně stanovené legislativou. V České republice například vyhláška o kybernetické bezpečnosti stanovuje bezpečností role, které povinná osoba v rámci systému řízení bezpečnosti

a informací musí určit. (§3 a §7 vyhlášky o kybernetické bezpečnosti). Jsou to role manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti, garant aktiva a auditor kybernetické bezpečnosti. Vyhláška dále stanovuje, jaké musí zaměstnanec splňovat podmínky pro možnosti plnění této role i jaké má povinnosti a zodpovědnosti. Příloha číslo 7 vyhlášky o kybernetické bezpečnosti pak blíže popisuje doporučené klíčové činnosti, znalosti, zkušenosti, vzdělání a příklady relevantních certifikací, ke kterým může organizace přihlédnout při hledání vhodných kandidátů pro tyto role.

6.3 Stanovení kontrolních bodů a audit procesu

Stanovení kontrolních bodů a audit procesu jsou klíčovými kroky k zajištění, že proces zachytávání a ukládání digitálních stop je efektivní, bezpečný a v souladu s interními i externími požadavky. Tato kapitola poskytuje přehled o tom, jak stanovit efektivní kontrolní body a provádět audit celého procesu logování, což zahrnuje sběr, analýzu, uchovávání a ochranu logů.

6.3.1 Vytvoření kontrolních bodů

Kontrolní body by měly být stanoveny na klíčových místech procesu logování, aby bylo možné pravidelně ověřovat jeho správnost a efektivitu. Kontrolní body by měly zahrnovat:

- **Kontrola správnosti konfigurace logování**: Ověření, zda jsou všechny systémy a aplikace správně nastaveny pro logování požadovaných událostí.
- **Ověření úplnosti sběru logů**: Zajištění, že jsou logy shromažďovány ze všech relevantních zdrojů bez výpadků.
- **Kontrola efektivity analýzy logů**: Hodnocení, zda analytické nástroje a procesy efektivně identifikují a reportují bezpečnostní incidenty a jiné významné události.
- **Audit bezpečnostních a ochranných opatření**: Kontrola, zda jsou logy adekvátně chráněny před neautorizovaným přístupem, ztrátou nebo poškozením.

- **Ověření dodržování politiky retence a rotace logů**: Kontrola, zda jsou logy uchovávány a archivovány v souladu s interními politikami a externími regulacemi.

6.3.2 Proces auditu

Audit procesu logování by měl být pravidelně prováděn interními nebo externími auditory s cílem ověřit jeho soulad s nastavenými politikami, bezpečnostními standardy a legislativními požadavky. Audit by měl zahrnovat:

- **Revize dokumentace a politik**: Ověření, že všechny dokumenty a politiky logování jsou aktuální, kompletní a v souladu s nejnovějšími požadavky.
- **Rozhovory s klíčovými osobami**: Diskuse s osobami odpovědnými za různé aspekty logování, aby se získal přehled o praktickém provádění politik.
- **Technická ověření**: Použití nástrojů a procedur k prověření technického nastavení a efektivity logovacích systémů a procesů.
- **Analýza incidentů a reakcí na ně**: Posouzení, jak efektivně organizace reagovala na detekované incidenty, včetně analýzy logů.
- **Vyhodnocení dodržování legislativy a regulačních požadavků**: Kontrola, zda jsou všechny aktivity v souladu s relevantními zákony a nařízeními.

6.3.3 Doporučení a zlepšení

Na závěr auditu by měla být připravena zpráva, která shrnuje zjištění a poskytuje doporučení pro zlepšení. Tato zpráva by měla:

- **Identifikovat slabé stránky a rizika**: Upozornit na oblasti, kde proces logování není dostatečně efektivní nebo bezpečný.
- **Nabídnout konkrétní opatření**: Poskytnout praktické návrhy na zlepšení, včetně technických úprav, aktualizace politik a školení personálu.
- **Stanovit časový plán pro implementaci**: Určit realistické termíny pro provedení doporučených změn a zlepšení.

Stanovení kontrolních bodů a pravidelný audit jsou nezbytné k zajištění toho, že proces logování je aktuální a funkční vzhledem k rozvoji technologií a možných změn v infrastruktuře organizace. Díky těmto bodům se organizace zároveň může připravit na pozdější možné externí audity spojené s compliance a legislativou.

7 Návrh technologických postupů pro zajištění digitálních stop

Aby byly pokryty veškeré body určené v procesu, je zapotřebí taková technologie, která umí bezpečně sbírat a dlouhodobě ukládat digitální stopy ze zařízení organizace, ale také nad nimi umožňovat analýzu v reálném čase.

7.1 Technologie SIEM

Jako nejvhodnější pro tyto účely se ukazuje být technologie SIEM, která spojuje prvky managementu logů a vyhodnocování incidentů. Umožňuje sběr a konsolidaci logů z velkého počtu druhů zdrojů, včetně síťových zařízení, bezpečnostních systémů, databází nebo koncových zařízení, díky čemuž zajišťuje velkou viditelnost v IT infrastruktuře organizace. Nad těmito daty je pak schopná aplikovat sofistikované algoritmy a korelační pravidla, díky kterým umožňuje automatizovaný monitoring a zpracování dat pro IT pracovníky organizace.

SIEM je kombinací dvou technologií:

- **SIM (Security Information Management)** – technologie zajišťující sběr a ukládání logů. (Vielberth, 2021)
- **SEM (Security Event Management)** – slouží k analýze a vyhodnocování kybernetických bezpečnostních incidentů v reálném čase. (Vielberth, 2021)

7.2 Zajištění a zpracování dat technologií SIEM

Sběr dat

Prvním krokem je logy získat. Logy se sbírají ze zařízení pomocí kolektorů. Kolektor může být například formou serveru v síti. Jak dále popisují například Miller et al. (2010), základními vlastnostmi je schopnost logy přijímat ze zdrojů, které je umí odesílat metodou push, aktivně sbírat pomocí metody pull ze zařízení, které odesílat logy samy neumí, a posílat je dál do databází a úložišť. Kolektor by měl umět data i zašifrovat kvůli bezpečnému přenosu.

Normalizace

Logy se do nástroje SIEM získávají z různých zdrojů od odlišných vendorů, a mají tak i různou podobu a formát. Pro jejich další zpracování je nutné informace z logů strukturovat a zařadit do standardizovaných polí tak, aby vyhledávání a analýza mohla probíhat jednotnými dotazy nehledě na vendora.

Ukládání

Ukládání logů je řešeno většinou dvěma databázemi, z čehož je jedna pro zpracování logů v reálném čase. Z ní se data zpracovávají pro vytváření alertů a vyhodnocování incidentů v reálném čase. Tato databáze se také využívá v případě analýzy v krátkém časovém období. Podobnou architekturu doporučuje například i Swift (2006), který popisuje, že v této databázi se ukládají data většinou po dobu 30 dní. Klade se zde důraz převážně na velkou výpočetní rychlost, tedy CPU a RAM.

Druhá databáze bude sloužit pro dlouhodobé ukládání logů, které pak mohou být použity pro forenzní analýzu za dlouhé časové období. Zde se klade důraz převážně na velkou kapacitu. Data se proto také před uložením většinou komprimují. Podle Swifta (2006) zde logy můžeme chtít uchovávat po dobu až 18 měsíců.

Korelace

Velmi silnou vlastností SIEM technologií je možnost odhalit podezřelé chování v síti v reálném čase. To zajišťují korelační pravidla, která jsou schopna zachytit souvislosti mezi různými událostmi i z různých zdrojů. Korelační pravidla mohou být vytvořena například z podmínek spojených funkcemi IF, AND, OR a NOT. Pokud jsou pak všechny podmínky splněny, korelační pravidlo sepne a vytvoří se alert.

Analýza

Alerty poté přebírají L1 pracovníci a dělají takzvanou triage (třídění), při které na základě priorit aletry analyzují a rozhodují, zda se jedná o falešně pozitivní alert, nebo může jít o reálnou hrozbu. Alert vyhodnocený jako relevantní, je eskalován na seniornější úroveň L2, která provádí hloubkovou analýzu a zkoumá, zda událost nemohla vést ke kybernetickému bezpečnostnímu incidentu. V takovém

případě může incident eskalovat na další úrovně a vést k dalším krokům jako je forenzní analýza.

7.3 Příklady technologie SIEM

Technologii SIEM nabízí mnoho poskytovatelů v různých variantách. Díky tomu také umožňuje širokou škálu implementačních možností, od velkých robustních řešení pro velké organizace s rozsáhlou IT infrastrukturou, až po opensource řešení, která mohou být vhodnější pro organizace střední a malé.

Řešení pro velké organizace přinášejí vendoři, jakou jsou Splunk, IBM, QRadar, FortiSIEM nebo ArcSight. Tyto systémy nabízí velkou sadu pokročilých analyzačních funkcí, sofistikovaných korelací s velkým zaměřením na automatizaci, většinou je nabízejí s možností kombinace dalších doprovodných technologií, jako je SOAR. Jejich výhodou je vysoký počet funkcionalit, možnosti vysokého škálování a klientský servis. Nevýhodou je velká pořizovací cena a vysoké poplatky za licence.

Pro malé a středně velké organizace mohou být lepší cestou opensource řešení, která poskytují veškeré potřebné základní funkce, vyžadují však více manuální správy a konfigurace. Příkladem může být OSSIM od AT&T, nebo řešení postavené na sběru logů skrze ELK Stack (Kombinace nástroků ElasticSearch, Logstach, Kibana) doplněné o bezpečnostní analýzy z nástrojů jako je Wazuh, nebo Security Onion. Výhodou těchto systémů je menší pořizovací cena a větší flexibilita pro konkrétní potřeby menších firem.

7.4 Technologie XDR

I když SIEM systémy poskytují vynikající schopnosti sběru a analýzy logů, mohou mít obtíže s detekcí sofistikovanějších hrozeb, které vyžadují pokročilou analýzu chování procesů. XDR může být tak další vhodná doplňující technologie SIEMu.

Stejně jako SIEM mají za účel poskytnutí viditelnosti v kybernetickém prostředí, centralizované vyhodnocování událostí a poskytování alertů. Zaměřuje se však více na hlubokou behaviorální analýzu procesů a dat v IT prostředí organizace. Díky strojovému učení je tak schopný zachytit pokročilé techniky v reálném čase.

Navíc nabízí možnosti takzvané response, což znamená, že vyskytujícím se útokům můžeme automaticky anebo centrálně zabránit, například tím, že koncové stanici zablokujeme přístup k internetu, nebo ji izolujeme od ostatních zařízení v síti. Jedná se o moderní bezpečnostní řešení, které umožňuje L1 a L2 analytikům provádět analýzu mnohem komplexnějšího chování v hlídaném kybernetickém prostředí. XDR je velmi často kombinací a rozšíření nástrojů EDR a NDR.

EDR – Endpoint Detection and Response

EDR se zaměřuje pouze na koncová zařízení, pro která nabízí komplexnější vyhodnocovací mechanismy i za pomocí strojového učení. Data získává pomocí agentu nainstalovaného na koncovém zařízení, a nabízí tak možnost automatické reakce na detekované bezpečnostní hrozby. Velmi často je jeho součástí i antivirus. (Aarness, 2023)

NDR – Network Detection and Response

Funguje podobně jako EDR, je však zaměřený na síťovou vrstvu infrastruktury. Stejně jako EDR umí automaticky reagovat, například zablokováním provozu z určité IP adresy. (Neuman, 2023)

XDR – Extended Detection and Response

Spojením vlastností EDR, NDR a dalších moderních bezpečnostních nástrojů do jednoho řešení dodává nejširší perspektivu a komplexitu vyhodnocování hrozeb napříč kybernetického prostředí organizace. Nabízí monitoring koncových zařízení, síťového provozu, e-mailové komunikace a cloudu. (George et al., 2021, st. 494–495)

Nevýhodou XDR je velká náročnost na úložiště. Metadata, se kterými pracuje, jsou uchovávána pouze po omezenou dobu, než jsou značně agregována. Pro účely dlouhodobého ukládání jsou formáty logů využívané v SIEM vhodnější, protože jsou navrženy tak, aby podporovaly rozsáhlé historické analýzy a možnosti auditního sledování.

7.5 Příklady technologií XDR

XDR je relativně novým konceptem v oblasti kybernetické bezpečnosti a možností nemá tolik jako SIEM. Mezi přední vendory patří společnosti jako, CrowdStrike s Falcon platformou, SentinelOne, Trend Micro a dalších. Tato řešení jsou často zaměřena na velké organizace s rozsáhlými IT prostředími a vyššími bezpečnostními požadavky.

8 Zpětné vyšetřování a modelování incidentů s využitím digitálních stop

Poté, co jsou digitální stopy procesně a technologicky sesbírány a zpracovány, dají se využít pro celý proces zpracování kybernetických incidentů od analýzy až po jejich vyšetřování a modelování. Zpětné vyšetřování je většinou posledním krokem celého procesu zpracování incidentu a jeho účelem je pochopení, jak a proč k incidentu došlo. Umožňuje také identifikování možných kroků pro prevenci podobných událostí v budoucnosti.

8.1 Postup vyšetřování a modelování incidentů

V oblasti zpracování incidentů existují různé postupy a doporučení, kterými se firmy mohou řídit. Například ENISA (2010) rozděluje a popisuje proces vyšetřování incidentu následujícím způsobem:

Registrace

Proces začíná zprávou o možné bezpečnostní události, organizace by měla mít nastavené komunikační matice a prostředky, jako je například e-mail, telefon, nebo tiketový systém. Po přijetí zprávy by měla být událost formálně zaznamenána v systému pro správu incidentů.

Triage

V této fázi probíhá základní ověření události, její klasifikace a rozhodnutí, zda se jedná o takzvaný false-positive, nebo skutečný bezpečnostní incident. Triage je kritickým krokem, protože určuje, jak vážný incident je, jaké má dopady a jak rychle se může šířit. Na základě těchto informací se nastavují priority a rozhoduje se o dalším postupu.

Řešení incidentu

Ve fázi řešení incidentu se shromažďují veškerá dostupná data, analyzují se digitální stopy a provádí se výzkum potřebných opatření. Svolávají se potřebné týmy a specialisté, kteří se snaží incident vyřešit a obnovit normální stav.

Uzavření a post-analýza

Po obnovení normálního stavu a vyřešení aktivního incidentu by mělo proběhnout právě zpětné vyšetřování a modelování útoku. Těmito kroky by se měly identifikovat možná zlepšení a strategie, jak podobným incidentům v budoucnosti předejít.

8.2 Využití rámce MITRE ATT&CK pro modelování incidentů

MITRE ATT&CK je nástroj, který mohou organizace využít při vyšetřování a modelování incidentů. Tento rámec obsahuje globálně uznávanou znalostní databázi, která popisuje různé taktiky a techniky používané kybernetickými útočníky a je založená na skutečných incidentech. (The MITRE Corporation, c2015 - 2024)

MITRE ATT&CK popisuje útoky třemi informacemi:

- **Taktiky:** Představují cíle, kterých se útočníci snaží dosáhnout, například získání přístupu nebo exfiltrace dat.
- **Techniky**: Představují metody, které útočníci používají k dosažení svých cílů. Například šifrování dat.
- **Procedury**: Popisují příklady implementace technik. Každá technika může být realizována různými způsoby. Procedury jsou obvykle založené na skutečných incidentech.

Praktického využití rámce ukazuje například Cindy Ou (2023) rozborem útoku typu spearphishing.[2]

[2] Taktiky a techniky jsou volně přeloženy autorem. Originální anglické názvy jsou dohledatelné podle zmíněných ID na stránkách https://attack.mitre.org/

Tabulka 5: Spearphishing útok – první taktika. Zdroj: Cindy Ou (2023)

Taktika: Počáteční přístup (ID: TA0001)
Technika: Spearphishingová příloha (ID: T1566.001)
Procedura: Útočník odešle vytipovanému zaměstnanci finanční instituce spearphishingový e-mail se škodlivou přílohou.

Tabulka 6: Spearphishing útok – druhá taktika. Zdroj: Cindy Ou (2023)

Taktika: Spuštění útoku (ID: TA0002)
Technika: Spuštění škodlivého souboru uživatelem (ID: T1204.002)
Procedura: Útočník čeká a spoléhá na to, že zaměstnanec otevře škodlivou přílohu v emailu. Po otevření přílohy se spustí kód, který umožní útočníkovy získat vzdálený přístup do sítě společnosti

Tabulka 7: Spearphishing útok – třetí taktika. Zdroj: Cindy Ou (2023)

Taktika: Laterální pohyb (ID: TA0008)
Technika: Laterální přenos nástrojů (ID: T1570)
Procedura: Pomocí nástroje umožňující kopírování souborů z různých systémů útočník ukradne citlivá finanční data.

Tabulka 8: Spearphishing útok – čtvrtá taktika. Zdroj: Cindy Ou (2023)

Taktika: Impakt útoku (ID: TA0040)
Technika: Zašifrování dat jako dopad útoku (ID: T1486)
Procedura: Útočník zašifruje originální data na systémech finanční instituce, a tím je znepřístupní. Poté vyžaduje od firmy peněžní náhradu, výměnou za dešifrovací klíč, který by jim data opět zpřístupnil.

Takto popsaný model umožňuje organizacím identifikovat klíčové body útoku a přijmout odpovídající bezpečnostní opatření. To může být například vytvoření nových korelačních pravidel v technologii SIEM, organizace školení pro zaměstnance na téma phishing, zavedení pravidelných phishingových simulací pro školící účely, nebo vytvoření table-top cvičení se stejným scénářem. Takto proaktivní přístup vede k neustálému zdokonalování a zvyšování odolnosti proti budoucím hrozbám.

9 Table-top cvičení

Table-top cvičení je forma interaktivní simulace ve formátu skupinové diskuse, která slouží k otestování reakce na kybernetické bezpečnostní události. Probíhá tak, že účastníci cvičení, většinou z různých oddělení organizace, jsou uvedeni do příběhu podle předem připraveného scénáře, který simuluje vybraný incident. Scénář by měl být založen na realistických událostech a měl by účastníky vtáhnout do děje.

Na základě získaných informací jsou účastníci vyzváni k diskusi o tom, jak by na situaci reagovali podle stávajících plánů a firemních politik. Na základě jejich reakcí moderátor odkrývá další scénáře, eskaluje situaci, nebo jinak určuje další děj příběhu. Účelem je identifikovat možné slabiny v reakčních plánech, posílit spolupráci a komunikaci mezi týmy a zlepšit připravenost organizace na řešení skutečných incidentů. Důležitým aspektem table-top cvičení je otevřená komunikace a bezpečné psychologické prostředí pro diskusi bez obav z kritiky jejich rozhodnutí a možných chyb.

Role v cvičení

Moderátor: Řídí průběh cvičení, představuje scénáře, zasahuje s dodatečnými informacemi nebo otázkami a zajišťuje správný směr a bezpečné prostředí pro diskusi.

Účastníci: Jednotliví zaměstnanci organizace z různých týmů a oddělení. Jejich úkolem je reagovat na scénář podle svých zodpovědností a plánů.

Pozorovatelé: Ve cvičení mohou být i nezávislí pozorovatelé, například z externí konzultantské firmy, nebo nestranný zástupce organizace. Cvičení se účastní neaktivně s cílem získat přehled o průběhu a poskytnout nezávislou zpětnou vazbu.

Zapisovatel: Zaznamenává klíčové body diskuse, rozhodnutí a dle jeho pohledu slabiny. Takový zápis je poté použit pro zpětné hodnocení a debriefing celého cvičení.

Tabulka 9: Table-top – Úvodní scénář. Zdroj: vlastní zpracování

Úvodní scénář
Jste součástí klíčových pracovníků v „Banka Securita“, která je jednou z vedoucích finančních institucí ve státě Modrá. Vaše banka se pyšní špičkovými systémy a důrazem na kybernetickou bezpečnost. Pro své služby využívá technologie, jako jsou cloudové služby, chytré aplikace pro mobilní bankovnictví, strojové učení pro personalizaci služeb a špičkové zabezpečení transakcí. Zákaznická data a klíčové systémy jsou řízeny v rozlehlé IT infrastruktuře s centrálními servery obsahující nejnovější verzi Windows Server 2022. Banka má také komplexní systém Logamangementu a SIEM pro ukládání digitálních stop a vyhodnocování alertů pomocí korelačních pravidel. Banka se nachází v prostředí, kde v důsledku mezinárodních konfliktů a politického napětí stále roste riziko kybernetických hrozeb a útoků od APT skupin zaměřujících se na klíčovou infrastrukturu organizací ve finančním sektoru. Tyto okolnosti představují hrozbu i pro „Banka Securita“. Jakýkoliv incident, který by mohl vést k porušení důvěrnosti, integrity nebo dostupnosti zákaznických dat a služeb, by mohl mít pro banku devastační reputační následky a mohla by ztratit své postavení na trhu. Je proto nesmírně důležité, aby byl váš tým vždy o krok napřed před útočníky díky rychlé detekci, analýze a adekvátní reakci na jakékoliv neobvyklé incidenty. Jako klíčoví pracovníci „Banky Securita", tedy hrajete zásadní roli v ochraně finančních a osobních údajů zákazníků. Vaše odborné znalosti a rozhodovací schopnosti budou důležité pro zachování bezpečnosti a stability vaší banky a budou rozhodující pro udržení důvěry ve finanční systém ve státě Modrá.

Tabulka 10: Table-top – Úvodní informace pro účastníky. Zdroj: vlastní zpracování

Úvodní informace pro jednotlivé účastníky
Informace SOC tým: V průběhu noci se začaly vyskakovat alerty na dohledu SIEM, ohledně neobvyklé aktivity na kritickém serveru Windows Server 2022. Na tomto serveru jsou uložena zákaznická data a systémy, které spravují základní zákaznické služby.
Informace pro ředitele kyberbezpečnosti: O víkendu si u snídaně přečetl noviny, které odebírá a dočetl se v nich o konfliktu mezi státy Červená a Modrá. Psalo se v nich, že kromě vojenského napjetí se konflikt přenesl také do kyberprostoru, kde se snaží paralyzovat různé klíčové služby státu. CISA vydala varování pro bankovní instituce státu Modrá.
Informace pro manažera kyberbezpečnosti: Z jeho informačních zdrojů přišlo upozornění o zranitelnosti na technologii SMB, která za určitých podmínek umožňuje útočníkům vzdáleně spustit libovolný kód na Windows Server 2022. Na tuto zranitelnost by měl v nejbližší době vydat Microsoft opravný patch.

Tabulka 11: Table-top – Správná reakce dle ISMS. Zdroj: vlastní zpracování

Reakce dle ISMS/standardu/metodik („Správná reakce“)

Raná fáze – počátek incidentu
• Analýza alertů
• Identifikace problému
• Odpojení od sítě/vypnutí systému
• Sběr relevantních logů a dat pro další analýzu (správný postup)
• Informování vedení a doporučení dalšího postupu
 	
Střední fáze – incident response plán
• Svolání Incident Response týmu (Bezpečnost, IT, právní, externí komunikace)
• Aktivování Incident Response plánu:
  ○ Sdělení informací vyzkoumaných z logů
  ○ Zahájení důkladné forenzní analýzy na pochopení rozsahu útoku a jeho zdroje
  ○ IT a bezpečností tým vytvářejí plán obnovy ze záloh
  ○ Příprava interní a externí komunikace
• Aktivování Incident Response plánu
 	
Pozdní fáze – stabilizace incidentu
• Spolupráce s externími partnery (NÚKIB a další případné autority)
• Aktualizace potřebných patchů systémů
• Zvýšené monitorování sítě a systémů
 	
Post fáze – hodnocení incidentu
• Hodnocení incidentu
• Analýza příčin
• Aktualizace řídící dokumentace

Reálné kroky dané role:
Zpětné vyhodnocení kroků:

Tabulka 12: Table-top – Situační událost IT. Zdroj: vlastní zpracování

Situační událost: IT
Ošetřeno: IT je informováno a jedná podle přesně koordinovaných kroků shodně s incident response plánem.
Důsledek: Žádný
Neošetřeno: V důsledku nedostatečné komunikace mezi IT a bezpečnostními týmy dochází k nedorozuměním ohledně rozsahu incidentu a nejsou přijata vhodná opatření. IT tým se snaží server obnovit ze zálohy a zapnout.
Důsledek: Způsobená dvojí práce a zmatek, může vést k dalším škodám a pokračování incidentu.

Tabulka 13: Table-top – Situační událost média. Zdroj: vlastní zpracování

Situační událost: Média
Ošetřeno: V médiích se objevují články o výpadku služby, díky včasné komunikaci mají dostatek informací a popisují událost jako řízený zásah proti možné kybernetické události.
Důsledek: Žádný
Neošetřeno: V médiích se objevují články o výpadku služby a spekulují o příčinách. Veřejnost v komentářích kritizuje výpadek a mlčení organizace.
Důsledek: Veřejnost v komentářích kritizuje výpadek a mlčení organizace, což vede k reputační ztrátě.

Tabulka 14: Table-top – Situační událost forenzní kopie. Zdroj: vlastní zpracování

Situační událost: Forenzní kopie – správný postup
Ošetřeno: Forenzní tým správně zajistil bitovou kopii potřebných dat a logů ze zařízení a může začít s detailní forenzní analýzou.
Důsledek: Více získaných informací o incidentu pro pozdější komunikaci s externími subjekty – zvýšení reputace a důvěryhodnosti.
Neošetřeno: Nedostatkem vybavení nebo špatným postupem byly nezajištěny, nebo dokonce ztraceny data logy ze serverů. Forenzní analýza ztrácí podstatu. Důkazy byly upraveny.
Důsledek: Omezená znalost incidentu, horší podmínky pro pozdější nápravná opatření, komunikaci s externími subjekty.

Tabulka 15 Table-top – Situační událost plán obnovy. Zdroj: vlastní zpracování

Situační událost: Plány obnovy
Ošetřeno: Na jiném serveru úspěšně obnoveny systémy a možnost přepnutí zpět do provozu.
Důsledek: Zvýšení důvěryhodnosti, spokojenost klientů při obnově služby.
Neošetřeno: Neúplné plány obnovy, zálohy se nezdařily, data jsou ztracena.
Důsledek: Ztráta kritických dat a mnohem delší doba obnovy služby vedoucí k finančním ztrátám a poškození pověsti banky.

Debriefing a zpětná vazba

Po skončení simulace scénáře následuje debriefing. Ten je klíčovým momentem pro celé cvičení. Moderátor společně s pozorovateli a zapisovatelem představuje zjištění z cvičení a vede diskusi o tom, jaké kroky se během cvičení podnikly, jaké byly reakce týmu a jak efektivní byly v kontextu daného scénáře. Může se také rozvést celý očekáváný postup a porovnat ho s postupem účastníků.

Při vyhodnocení je velmi důležité uznat úspěchy a pozitivní akce účastníků. Pochvala za dobrou práci a efektivní rozhodování posiluje sebevědomí a motivuje účastníky k dalšímu zlepšování. Je důležité, aby si účastníci odnesli pocit, že jejich

úsilí bylo ceněno a že chyby v simulaci jsou cennými lekcemi, ne důvodem pro kritiku.

10 Závěr

Správné procesní a technologické zajištění digitálních stop a jejich vyhodnocování je základem dobrého kybernetického bezpečnostního rámce organizace. Díky těmto procesům získávají organizace viditelnost událostí v jejich IT prostředí, možnost identifikovat bezpečnostní incidenty v reálném čase a schopnost na ně adekvátně reagovat.

Autor práce ze své praxe v oblasti kybernetické bezpečnosti vnímá, že znalost správných postupů mnoha organizací je nedostatečná. Cílem práce tedy bylo identifikovat možné nedostatky ve známých standardech, ze kterých mohou společnosti vycházet při implementaci procesů sběru a zpracování digitálních stop, navrhnout procesní a technologické postupy pro zajištění digitálních stop a případně vytvořit table-top cvičení, které by účel těchto procesů demonstrovalo.

Z výsledků zkoumání, SWOT analýzy a následné komparace bylo zjištěno, že jednotlivé standardy sice obsahují užitečné informace, návody a doporučení pro zpracování digitálních stop, některé se však zaměřují pouze na omezený účel a některé podstatné kroky popisují nedostatečně. Z výsledků je patrné, že jsou rozdíly také v podrobnosti, obecnosti a technickém popisu jednotlivých doporučení. Informace v nich tak nemusí určité kroky dostatečně pokrývat, což podle autora může způsobit demotivaci organizací vytvářet proces podle uznávaných postupů, může je to vést k zanedbání některých důležitých procesních kroků a mohou se rozhodnout spoléhat na jednodušší nedostatečné řešení.

Informace získané výzkumem korespondují s praktickými zkušenostmi autora práce, který se zjištěné nedostatky pokusil pokrýt vlastním návrhem procesních a technologických postupů.

Poslední část práce se zaměřila na table-top cvičení, které simuluje scénář možného bezpečnostního incidentu. Jeho smyslem je umožnit účastníkům odzkoušet svoji připravenost na řešení takového incidentu a demonstrovat jim důležitost správně nastavených postupů z návrhové části této práce.

10.1 Nástin dalšího výzkumu a rozvoje tématu

Jedním z identifikovaných nedostatků zjištěných výzkumem, který autor nemohl pokrýt ve svých procesních a technologických návrzích, je možnost

standardy udržovat aktuální s rychlým vývojem bezpečnostních hrozeb při zachování jejich compliance pro účely auditu. Dalším rozvojem tématu této práce by mohlo být zkoumání a vývoj vhodné platformy, která by standardům a doporučením umožňovala flexibilní a rychlejší integraci nových nástrojů a postupů, a zároveň jim udržovala vysokou míru compliance a zachovávala možnost použití standardů pro auditní účely.

Jiným pokračováním výzkumu návrhové části by mohlo být provedení studie s použitím navržených procesních a technologických postupů ve více typech organizací různých velikostí, jako jsou například korporáty, malé a střední podniky, státní instituce a neziskové organizace. Metodologie takové studie by mohla zahrnovat rozhovory a dotazníkové šetření, které by zkoumalo efektivitu a uživatelskou přívětivost navrhovaných postupů. Výsledky by mohly identifikovat bariéry a nedostatky při implementaci v různých IT prostředích a umožnily by vznik návrhů změn, které by procesy mohly zlepšit a učinit je intuitivnější.

Stejnou metodikou by se mohlo také zkoumat, jak vytvořené table-top cvičení ovlivňuje vnímání jednotlivých účastníků ohledně důležitosti a užitečnosti správně nastavených procesů a technologií pro zpracování digitálních stop.

11 Seznam použité literatury

[1] AARNESS, Anne, 2023. What is endpoint detection and response (EDR)? Online. Crowdstrike. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/. [cit. 2024-03-24].

[2] BHATT, Sandeep; MANADHATA, Pratyusa K. a ZOMLOT, Loai, 2014. The Operational Role of Security Information and Event Management Systems. Online. IEEE Security & Privacy. Roč. 2014, č. 12, s. 35–41. Dostupné z: https://doi.org/10.1109/MSP.2014.103. [cit. 2023-09-24].

[3] CICHONSKI, Paul; MILLAR, Thomas; GRANCE, Timothy a SCARFONE, Karen, 2012. NIST SP 800-61 Rev. 2. Computer Security Incident Handling Guide. Online. Special Publication. Dostupné z: https://doi.org/https://doi.org/10.6028/NIST.SP.800-61r2. [cit. 2023-09-03].

[4] ENISA, 2010. Good Practice Guide for Incident Management. Online. Dostupné z: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management. [cit. 2024-03-30].

[5] ENISA, 2023 Threat landscape. Online. ISBN 978-92-9204-588-3. ISSN 2363-3050. Dostupné z: https://doi.org/10.2824/782573. [cit. 2024-04-07].

[6] GEORGE, A. Shaji; GEORGE, A. S. Hovan; BASKAR, T. a PANDEY, Digvijay, 2021. XDR: The Evolution of Endpoint Security Solutions – Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future. Online. IJARSCT: International Journal of Advanced Research in Science, Communication and Technology. Roč. 2021, č. 8, s. 494-495. ISSN 2581-9429. Dostupné z: https://doi.org/10.5281/zenodo.7028219. [cit. 2023-09-24].

[7] JARPEY, Gregory a MCCOY, Scott, 2017. Security Operations Center Guidebook. Butterworth-Heinemann. ISBN 978-0-12-803657-0.

[8] KENT, Karen a SOUPPAYA, Murugiah, September 2006. Guide to Computer Security Log Management. Online. Dostupné z: https://doi.org/https://doi.org/10.6028/NIST.SP.800-92. [cit. 2023-09-10].

[9] MILLER, David; HARRHIS, Shon; HARPER, Allen a VANDYKE, Stephen, 2010. Security Information and Event Management (SIEM) Implementation. 1. McGraw-Hill Education - Europe. ISBN 9780071701099.

[10] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

[11] NCSC, 2018. Introduction to logging for security purposes. Online. The National Cyber Security Centre. Dostupné z: https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes. [cit. 2024-04-07].

[12] NCSC, 2021. Device Security Guidance. Online. The National Cyber Security Centre. Dostupné z: https://www.ncsc.gov.uk/collection/device-security-guidance. [cit. 2024-04-07].

[13] NEUMAN, David, 2023. Engineering Effective Network Detection and Response for the Enterprise. Online. TAG CYBER Whitepaper. S. 1-8. Dostupné z: https://www.opentext.com/assets/documents/en-US/pdf/opentext-security-ndr-campaign-tag-position-paper-en.pdf. [cit. 2023-09-24].

[14] NOVAK, Martin; GRIER, Jonathan; GONZALES, Daniel. 2018. New Approaches to Digital Evidence Acquisition and Analysis. In: nij.ojp.gov [online]., 9. února, 2021 Dostupné z: https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis [cit. 2023-09-03].

[15] NÚKIB, 2022. Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti. Online. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Prvodce%20zenm%20aktiv%20a%20rizik%20dle%20vyhlky%20o%20kybernetick%20bezpenosti.pdf. [cit. 2023-12-21].

[16] NÚKIB, 2023 Minimální bezpečnostní standard [online]. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf [cit. 2023-09-09].

[17] OU, Cindy, 2023. Incident Response with MITRE ATT&CK Framework: Write-Up. Online. Dostupné z: https://medium.com/@shunxianou/incident-response-with-mitre-att-ck-framework-write-up-3178be8ee8d2. [cit. 2024-04-07].

[18] SCHMIDT, Kevin; PHILLIPS, Chris a CHUVAKIN, Anton, 2012. Logging and Log Management. Elsevier. ISBN 978-1-59749-635-3.

[19] SMEJKAL, Vladimír, 2018. Kybernetická kriminalita. 3. vydání. Plzeň: Aleš Čeněk. ISBN 978-80-7380-720-7.

[20] SWIFT, David, 2006. A Practical Application of SIM/SEM/SIEM Automating Threat Identification. Online. White Paper. Dostupné z: https://www.sans.org/white-papers/1781/. [cit. 2024-03-23].

[21] THE MITRE CORPORATION, c2015 - 2024. MITRE ATT&ACK. Online. Dostupné z: https://attack.mitre.org/. [cit. 2024-04-03].

[22] VIELBERTH, Manfred, 2021. Security Information and Event Management (SIEM). Online. Encyclopedia of Cryptography, Security and Privacy. ISBN 978-3-642-27739-9. Dostupné z: https://doi.org/https://doi.org/10.1007/978-3-642-27739-9_1681-1. [cit. 2023-09-23].

[23] Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

12 Seznam zkratek

1) APT – Advanced Persistent Threat
2) CERT – Computer Emergency Response Team
3) CISA – Cybersecurity and Infrastructure Security Agency
4) CPU –Central processing unit
5) ČSN – České technické normy
6) DNS – Domain Name System
7) EDR – Endpoint Detection and Response
8) ENISA – The European Union Agency for Cybersecurity
9) GDPR – General Data Protection Regulation
10) IBM – International Business Machines Corporation
11) IDS – Intrusion Detection System
12) IEC – International Electrotechnical Commission
13) IP – Internet Protocol
14) IPS – Intrusion Protection System
15) IS/IT – Informační systémy/Informační technologie
16) ISO – International Organization for Standardization
17) L1 – Level 1
18) L2 – Level 2
19) L3 – Level 3
20) NCSC – National Cyber Security Centre
21) NDR –Network Detection and Response
22) NIJ – National Institute of Justice
23) NIST–National Institute of Standards and Technology
24) NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost
25) OS – Operační systémy
26) RAM – Random-access memory
27) SEM – Security Evenet Management
28) SHA1 – Secure Hash Algorithm 1
29) SIEM – Security Information and Incident Management
30) SIM – Security Information Management
31) SMB – Server Message Block
32) SOC – Security Operations Center

33) SP – Special Publications

34) SWGDE – Scientific Working Group on Digital Evidence

35) SWOT – Strengths, Weaknesses, Opportunities, Threats

36) TLS – Transport Layer Security

37) TLS – Transport Layer Security

38) XDR – Extended detection and response

13 Seznam tabulek

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání bakalářské práce

Autor:	**Denis Šabacký**
Studium:	I2100725
Studijní program:	B1802 Aplikovaná informatika
Studijní obor:	Aplikovaná informatika
Název bakalářské práce:	**Procesní a technologické řešení zajištění dat pro zpětné vyšetřování**
Název bakalářské práce AJ:	Process and technology solutions for securing data for retrospective investigations

Cíl, metody, literatura, předpoklady:

Cílem práce je analyzovat a navrhnout procesní a technologické postupy pro zajištění digitálních stop z bezpečnostního dohledu L1 a L2 pro zpětné vyšetřování a modelování incidentů.

V teoretické části autor zpracuue požadavky na zajitšění digitálních stop z dohledu L1 a L2 dle mezinárodních norem, doporučení a národní legislativy.

V praktické části autor navrhne jednoznačné procesní postupy pro zajitšění požadavklů plynoucích z teoretické části a navrhne vhodná technologická řešení uvedených požadavků.

Národní legislativa v akutálním znění

ISO/IEC 27001

ISO/IEC 27002

Zákon o kybernetické bezpečnosti (v akutálním znění)

vyhláška kybernetické bezpečnosti (v aktuálním znění)

Digital Forensics and Incident Response

Gerard Johansen

"A practical guide to deploying digital forensic techniques in response to cyber security incidents"

Cyber Forensics

From Data to Digital Evidence

Albert J. Marcella Jr.

"An explanation of the basic principles of data This book explains the basic principles of data as building blocks of electronic evidential matter, which are used in a cyber forensics investigations."

Digital forensic process

Gerardus Blokdyk

"What are all of our Digital forensic process domains and what do they do? Can Management personnel recognize the monetary benefit of Digital forensic process?"

Zadávající pracoviště:	Katedra informačních technologií, Fakulta informatiky a managementu
Vedoucí práce:	doc. Mgr. Josef Horálek, Ph.D.
Datum zadání závěrečné práce:	15.10.2021