MANAGING RISKS ACCORDING TO ISO/IEC 27001

Veronika Doubková
Master Degree Programme (2), FEEC BUT
E-mail: vdoubkov00@vutbr.cz

Supervised by: Tomáš Horváth
E-mail: horvath@feec.vutbr.cz

Abstract: This paper is dealing with risk assesment on a organization scope using Verinice. Verinice is a open-source tool for managing information security risks and creating risk assesment complying with ISO/IEC 27000 series. Based on risk assesment are implemented security precautions for lowering risks in optical fiber networks.

Keywords: Information Security Management System (ISMS) , Software Verinice

1 ÚVOD

Optická vlákna tvoří páteřní sítě všech moderních telekomunikačních sítí, ať už se jedná o datové, hlasové, bezdrátové, televizní nebo jiné přenosy. Organizace v prostředí kybernetické bezpečnosti usilují o bezpečnost informací a dat přenášených v optických sítích. S počátečním zavedením optických sítí se předpokládalo, že jsou bezpečné. S postupem času se však ukázalo, že i tyto sítě jsou rizikové a je potřeba zavádět bezpečnostní opatření ke snížení rizik. Ekonomiky a společnosti patřící do kritické infrastruktury jsou přímo nuceny zákonem o kybernetické bezpečnosti zavádět systém řízení bezpečnosti informací. V tomto směru je využita sada norem řady ISO/IEC 27000 pro oblast bezpečnosti informací.

2 SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

Zavedení systému řízení bezpečnosti informací je pro organizace patřící do kritické informační infrastruktury nutností vyplývající ze zákona č.181/2014 Sb., o kybernetické bezpečnosti, a jeho prováděcích předpisech [1].
Pro každou organizaci je klíčová bezpečnost informací, znamenající uplatnění obecných bezpečnostních opatření a postupů sloužících k zajištění ochrany před ztrátou integrity, dostupnosti a důvěrnosti. Systém řízení bezpečnosti informací, dále jen ISMS, představuje základní přístup pro vytvoření podmínek v organizaci, které zajistí potřebnou ochranu informací před ztrátou důvěrnosti, dostupnosti a integrity. ISMS lze aplikovat jak na celou organizaci, tak na organizační složku v rámci organizace nebo na specificky určený komunikační a informační systém. Procesem a řízením rizik v kybernetické bezpečnosti zaměřené na organizace se specifikuje sada norem ISO/IEC 27000 [2].

3 SOFTWARE VERINICE

Je Open Source nástroj pro řízení rizik bezpečností informací a tvorbu ISMS v souladu s řadou norem ISO 27000, umožňující následující procesy [3]:

- řízení rizik podle ISO/IEC 27005 – Řízení rizik bezpečnosti informací,
- importování vlastního katalogu rizik a součástí ve formátu XML,
- exportování vytvořeného katalogu rizik ve formátu .VNA.

3.1 PROCES ŘÍZENÍ RIZIK BEZPEČNOSTI INFORMACÍ

Software Verinice umožňuje modelovat celý proces řízení rizik bezpečnosti informací a následné hodnocení rizik, dle automatické metriky stanovené softwarem. Výstupem ze softwaru je registr rizik obsahující výsledky hodnocení rizik, identifikovaná rizika pro všechna aktiva, dále pak matice rizik, znázorňující hodnoty rizik, která jsou pro organizaci přijatelná, mírná nebo nepřijatelná. V případě mírných nebo nepřijatelných rizik následuje ošetření rizik. V tomto případě by měla být vybrána vhodná opatření pro snížení rizik.
Prvním krokem v procesu řízení rizik je stanovení kontextu zahrnující určení základních kritérií pro řízení bezpečnosti informací, definici rozsahu a hranic, a stanovení příslušné organizační struktury pro řízení rizik bezpečnosti informací. Dále se posuzují rizika, tato činnost zahrnuje identifikaci rizik, analýzu rizik a vyhodnocení rizik. Posouzení rizik zahrnuje hodnotu informačních aktiv, identifikují se možné hrozby a zranitelnosti, které existují nebo by mohly existovat. Pokud je dostatek informací pro efektivní určení akcí nutných k modifikaci rizik na přijatelnou úroveň, pak je úkol splněn a následuje ošetření rizik. Pokud se organizace rozhodne pro důkladnější posouzení, nebo chybí dostatek informací, tento proces se opakuje. Výstupem posouzení rizik je seznam hodnocených rizik [2].
Po této fázi následuje ošetření rizik, jedná se o neustálý opakující se cyklus. Opakování vede k zajištění, že rizika s vysokou úrovní jsou náležitě posouzena. Vstupem je seznam rizik, kterým byla přidělena priorita podle kritérií pro hodnocení rizik v souvislosti se scénáři incidentů. Měla by být vybrána vhodná opatření pro snížení rizik, podstoupení, vyhnutí se nebo sdílení rizik s vypracovaným plánem pro ošetření rizik. Ošetření rizik nemusí vést k okamžité přijatelnosti úrovně zbytkového rizika. Zbytkové riziko je takové riziko, které zůstává i po zavedení příslušných opatření, ale je snížen na příslušnou úroveň a nadále se monitorují. Výstupem ošetření rizik je plán ošetření rizik a zbytková rizika, která vyžadují rozhodnutí vedoucího pracovníka organizace pro jejich akceptaci. Dále následuje akceptace rizik. Zde by měla být učiněna formální rozhodnutí o akceptaci rizik a odpovědnosti za toto rozhodnutí v souvislosti s ISO/IEC 27001 – Systémy řízení bezpečnosti informací – Požadavky [2].
Komunikace rizik zahrnuje informace o rizicích a prováděných akcích v celém průběhu řízení rizik mezi zainteresovanými stranami. Monitorování a přezkoumání rizik slouží k identifikaci změn v kontextu organizace a udržení přehlednosti komplexního obrazu rizik [2].

4 REALIZACE SCÉNÁŘŮ

V prostředí softwaru Verinice byly vytvořeny tři scénáře zaměřené na optické sítě. V každém scénáři je dána hodnota pravděpodobnosti, která je automaticky softwarem stanovena na základě individuálního ohodnocení úrovně hrozby a zranitelnosti. Výsledkem je stanovení hodnoty rizik a následné ošetření rizik vhodnými opatřeními.
Příkladem motivací útočníků pro páchání trestné činnosti, tedy realizaci uvedených scénářů může být vidina zisku peněz, prestiž mezi útočníky, zvýšení ega, zničení konkurence, nebo jako výzva k tomu nalézt zranitelnosti v sítích nebo systémech.

4.1 ODPOSLECH (WIRETAPPING)

Cílem odposlechu obecně je získat neoprávněný přístup k datům za účelem sběru dat nebo analýzy provozu. V dnešní digitální éře dochází k odposlouchávání ve všech síťových vrstvách od aplikační po fyzickou vrstvu, přičemž nové útoky jsou odhaleny téměř denně [4].
Běžným způsobem realizace útoků odposlechu je přímý přístup k optickému vláknu. Útočník připojí splitter/coupler, který rozdělí vstupní optický signál do více výstupů. Za použití vhodného vybavení je možné tento vyvázaný signál vyhodnocovat, například pomocí fotodetektoru. Útočník se pak může vrátit na místo připojené kabelem a provést odposlech. Po rozdělení vlákna splitterem však dochází ke zvýšení celkového útlumu na trase v závislosti na použitém dělicím poměru [5].

4.2 Odepření služby

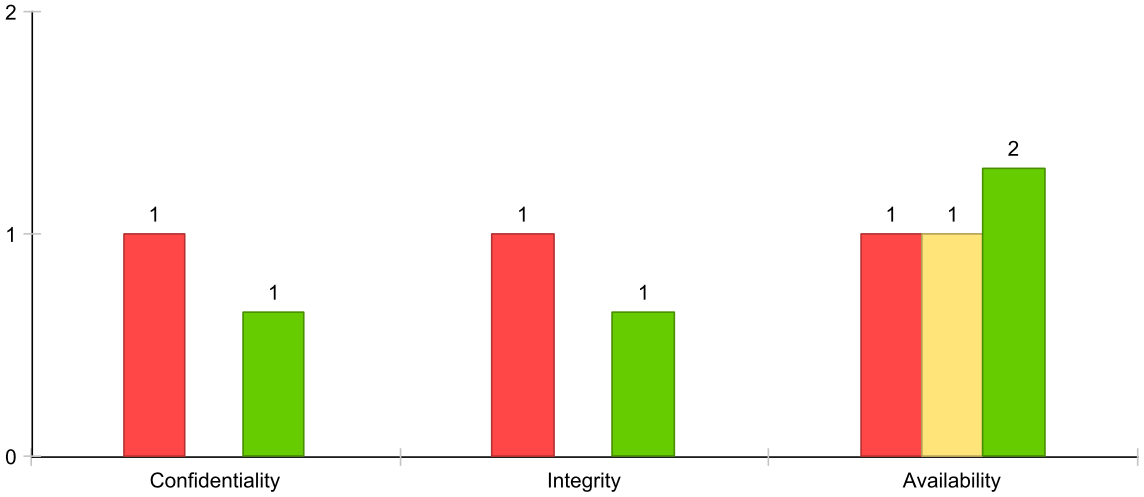
Ačkoli optická vlákna jsou imunní vůči elektromagnetickému rušení a nevyzařují přenášené signály do okolí v případě dostatečného ohnutí optického vlákna může docházet k úniku signálu.
V případě ohnutí optického vlákna lze zrealizovat útok známý jako Denial of services. Příkladem realizace takového útoku je potřebné do ohnutého optického vlákna zasvítit laserovým paprskem. Laserový paprsek musí být na stejné nebo blízké vlnové délce jako je signál v optickém vláknu, aby docházelo k degradaci signálu, která směřuje k úplnému znemožnění služby.

4.3 Fyzické poškození optického kabelu

Nejspíš jeden z nejjednodušších útoků je fyzické přerušení optických vláken. Tento útok nevyžaduje znalost optických vláken, jako například při útoku odposlechem nebo vydělení optického signálu spliterrem.
Nedávný útok na optické kabely přerušil přístup k internetu v částech východní Evropy, Íránu a Turecka. Problém, který trval nejméně dvě hodiny byl způsoben fyzickým poškozením více optických vláken současně, což byla velmi neobvyklá věc. Google uvedl, že jeho služby byly nedostupné v uvedených regionech po dobu třiceti minut [6].

5 Ošetření rizik

Na základě ohodnocení rizik v prostředí softwaru Verinice s ohledem na vytvořené scénáře, definované hrozby, zranitelnosti a aktivum bylo nutno zavést bezpečnostní opaření pro snížení rizik. Nejzávažnější rizika plynou z odposlechu s dopadem na důvěrnost a integritu. Dále odepřením služby s dopadem na dostupnost. Tyto rizika jsou pro organizaci nepřijatelná a jsou znázorněna na obrázku 1 červenou barvou. Žlutá barva zobrazuje rizika mírná vyplývající z fyzického poškození optického kabelu s dopadem na dostupnost. Po zavedení bezpečnostních opatření bylo dosaženo snížení rizik z nepřijatelné a mírné úrovně na přijatelnou. Přijatelná úroveň rizik je vykreslena zelenou barvou.
Pro snížení rizik v případě odposlechu byly například implementovány firewally, kryptografické prostředky, logování, virtuální privátní sítě (VPN), systémy pro monitorování optických tras, které dokáží lokalizovat krátkodobé změny v síti a další. Některé z uvedených opatření jsou implementovány i pro odepření služby a nadále rozšířeny o implementaci anti-spamového softwaru, kontrolu síťových zařízení a síťový load balancing. Rozdělení sítě, rerouting, zálohování a fyzické kontroly jsou implementovány pro snížení rizik u fyzického zničení optické sítě.



Obrázek 1: Hodnoty rizik

6 ZÁVĚR

Sítě, komunikační a informační systémy hrají bezpochyby zásadní roli ve společnosti, proto je pro tyto systémy klíčová bezpečnost a spolehlivost. Článek poskytuje základní informace o zavedení systému řízení bezpečnosti informací a následný proces řízení rizik bezpečnosti informací vycházející z řady norem ISO/IEC 27000, pro zajištění ochrany před ztrátou dostupnosti, důvěrnosti a integrity.
Cílem práce bylo identifikovat aktivum, hrozby, zranitelnosti a scénáře v prostředí softwaru Verinice, který postupově vychází z normy ISO/IEC 27005 a následné vyhodnocení možných rizik v optických sítích.
Výstupem ze softwaru Verinice byl registr rizik ve formátu .VNA, který poskytuje náhled na rizika s ohledem na požadavky normy ISO/IEC 27001. Na základě posouzení rizik byla implementována bezpečnostní opatření směřující ke snížení rizik na úroveň přijatelnou.

REFERENCE

[1] *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. In: . 2014, číslo 181.

[2] *ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. 2013.

[3] *Verinice. User Guide 1.19*. SerNet, 2019.

[4] FURDEK, Marija, Nina SKORIN-KAPOV, Szilard ZSIGMOND a Lena WOSINSKA. *Vulnerabilities and Security Issues in Optical Networks.* [online]. 2014 [cit. 2019-12-21]. Dostupné z: https://www.researchgate.net/publication/269268194_Vulnerabilities_and_security_issues_in_optical_networks

[5] DAHAN, David a Uri MAHLAB. *Security Threats and Protection Procedures for Optical Networks.* [online]. In: . 2017, s. 186-200 [cit. 2020-03-12]. DOI: 10.1049/iet-opt.2016.0150. ISSN 1751-876. Dostupné z: https://www.researchgate.net/publication/316970468_Security_Threats_and_Protection_Procedures_for_Optical_Networks

[6] *Google goes offline after fibre cables cut.* [online]. London: BBC, 2019 [cit. 2019-12-21]. Dostupné z: https://www.bbc.com/news/technology-50851420