HODNOCENÍ ODOLNOSTI PRO OBLAST ENERGETIKY

PŘÍPADOVÁ STUDIE

EVALUATION OF RESILIENCE LEVEL FOR ENERGETIC SECTOR

CASE STUDY

Lukáš KRÁLÍK, David MALANÍK
Univerzita Tomáše Bati ve Zlín, Fakulta aplikované informatiky
Nad Stráněmi 4511, 76005 Zlín
{kralik,d_malanik}@utb.cz

Abstrakt: *Tento článek se zabývá studií události, která se odehrála v prosinci roku 2016 na Ukrajině. Cílem není nalézt příčiny události, ale s využitím již známých informací analyzovat vývoj odolnosti systému v závislosti na čase. Zmíněný útok je rozdělen do fází a ke každé fázi je uveden stručná charakteristika. Na závěr je s využitím analýzy stromem událostí proveden rozbor se zaznamenáním změny odolnosti napadeného systému. Hodnoty uvedené v této studii jsou orientační, jejich konkrétní hodnotu lze získat s využitím připravované metodiky, na jejímž základě tato studie byla vytvořena.*

Klíčová slova: *kybernetický útok, analýza stromem událostí, blackout, kybernetická bezpečnost, konvergovaná bezpečnost.*

Úvod

Pro zajištění bezpečnosti je nezbytné zabývat se samotným řízením bezpečnosti. Pod pojmem řízení bezpečnosti se rozumí zajištění integrity, dostupnosti a důvěrnosti aktiv. Aktiva jsou klíčovým prvkem pro správné fungování systému a narušení jedné z výše vyjmenovaných vlastností může vést ke snížení efektivity nebo dokonce k úplnému znemožnění základní funkcionality systému. V organizaci je pak myšleno zajištění bezpečnosti aktiv zejména z pohledu jejich možného ohrožení jak ze světa fyzického, tak z toho elektronické-ho (kybernetického). S pojmem řízení bezpečnosti velice úzce souvisí i pojem řízení rizik, jehož cílem je vytvoření takových podpínek, které mohou předcházet vzniku nežádoucích situací, které ohrožují aktiva, nebo snižovat případný dopad těchto situací v případě, kdy nastanou. To je dosahováno s využitím řady metod, postupů, procesních rámců, standardů, směrnic a bezpečnostních nástrojů jako je např. analýza rizik.

1 Způsoby zajišťování bezpečnosti

Způsoby zajištění bezpečnosti jsou v zásadě dva základní. Naneštěstí jejich definice v českém jazyce je značně komplikovaná. V anglickém jazyce lze tyto dva způsoby definovat jako Security a Safety. Pod pojmem Security můžeme chápat zajištění bezpečnosti pro hmotná a nehmotná aktiva s využitím technický, technologický, administrativních a legislativních postupů. Na druhé straně je Safety, kterou lze chápat jako bezpečnost a ochranu života a zdraví osob. V mnoha ohledech se tyto dva způsoby vzájemně doplňují a překrývají. Jako konkrétní způsoby zajištění bezpečnosti lze vybrat:

- Fyzická bezpečnost
- Informační bezpečnost
- Požární bezpečnost
- Provozní bezpečnost
- Organizační bezpečnost

- Procesní bezpečnost
- a další.

1.1 Narušení bezpečnosti a vliv na odolnost

Bezpečnost jako takovou lze chápat jako soubor preventivních opatření s cílem zajištění integrity, dostupnosti a důvěrnosti aktiv. Na základě tohoto faktu je pak narušením bezpečnosti jakákoliv událost, která narušuje nebo dokonce překonává preventivní opatření – zvyšuje pravděpodobnost újmy na aktivu. Typickým příkladem může být pravidelné školení na bezpečnost a ochranu zdraví při práci (BOZP). I přes pravidelné školení (preventivní opatření) dělník (chráněné aktivum) nepoužije ochranné prostředky, tím se zvyšuje pravděpodobnost úrazu při práci (narušení bezpečnosti).

Schopnost systému snášet působení negativních vlivů (událostí) je vyjadřována jako odolnost. Odolnost systému je individuální pro každý systém a nelze ji tak generalizovat. Stejně tak je důležité si uvědomit, že jedna a ta samá událost, může ovlivnit odolnost dvou různých systémů zcela odlišně. Příkladem může být požár. V prvním případě je kromě elektrické požární signalizace (EPS) použito i stabilního hasicího zařízení (SHZ), ve druhém případě pouze EPS. Pokud by vznikl požár, odolnost prvního systému je díky použití SHZ mnohem vyšší, jak u druhého systému, kde budou zasahovat jednotky hasičského záchranného sboru (HZS). Pravděpodobnost újmy na aktivu se ve druhém případě značně zvyšuje. Odolnost systému proti negativnímu působení (hrozby) je detailněji popsána níže a demonstrována několika scénářem podle reálné situace.

2 Útok na řídící systém rozvodny VVN a VN

Tato kapitola blíže rozebírá a analyzuje scénář narušení bezpečnosti s ohledem na odolnost systému. Analyzovaná událost vychází ze skutečné události, kdy následkem kybernetického útoku došlo k blackoutu části Kyjeva.

Hrozba: Cílený útok na ovládací systém SCADA rozvodny (Advanced Persistence threat – APT)

Charakteristika: V prosinci 2016 došlo k cílenému útoku na rozvodnu VNN a VN, která dodává el. energii do Ukrajinského města Kyjev. Útok byl zacílen na konkrétní systém s OS Windows XP, který byl použitý na řízení distribuční soustavy. Nejprve došlo k ovládnutí OS pomocí slabě zabezpečeného VNC přístupu, následně bylo ovládání odepřeno obsluze, která systém dozorovala. V druhé fázi došlo k postupnému odpínání jednotlivých větví a odstavení dodávky proudu pro cca. 30 tis. Obyvatel města. Na závěr útočníci poškodili ovládací systém a jemu přidružené prvky takovým způsobem, že jejich obnovení ze zálohy nevedlo k získání přístupu k funkčnímu ovládacímu prostředí. Obnovení dodávek energie muselo být nakonec realizováno ručním připojováním konkrétních stykačů na distribuční cestě, což vzhledem k mrazům a špatnému dohledání odpojených stykačů trvalo 4 dny. Po tuto dobu zůstávala zmíněná část Kyjeva bez proudu. Vyčíslení přímých škod se odhaduje na desítky mil. Kč, obnova systému a jeho zabezpečení na cca. 50 mil. Kč.

Aktivum: Odběratelé energie, distribuční síť, obslužný HW, obslužný SW, obsluha zařízení.

Popis újmy:
kybernetická bezpečnost – odepření přístupu a neoprávněná manipulace s ovládacím SW. Vlivem nedostatečného zabezpečení ovládacího SW došlo k jeho převzetí další osobou a k neoprávněné manipulaci, která měla za následek tzv. blackout pro část města, který se přímo dotkl cca. 30 tisíc lidí. Přímě škody jsou odhadovány na desítky mil. Kč. Nepřímé škody nebyly kalkulovány.
provozní bezpečnost – porucha technologií

Na základě dostupných informací je tento blackout spojován s podobným incidentem z roku 2015. Těmto velkým incidentů vždy předcházela série menších, méně nápadných útoků (hacků), kdy se útočníci pokoušeli aktivně sbírat informace a přístupy. Bohužel první fáze, která je pouze pasivní je těžko zjistitelná a proto je možné, že realizace zmíněného blackoutu započala již v roce 2014. Celý útok na rozvodnou stanici, včetně obnovy dodávek el. energie je tak možné rozdělit do 7 fází, přičemž z pohledu časové náročnosti jsou první dvě fáze nejdelší:

1) ***Průzkum cíle útočníkem pomocí pasivního scanování***
2) ***Průzkum cíle útočníkem pomocí aktivního scanování***
3) ***Útok na konkrétní službu***
4) ***Odepření přístupu pro obsluhu***

5) ***Odpojení stykačů***
6) ***Manuální připojení stykačů.***
7) ***Obnovní dodávky proudu***

1. Fáze: Průzkum cíle útočníkem pomocí pasivního skenování

- **Charakteristika fáze**: Útočník si vytipoval objekt a začíná sbírat informace k možnému útok a připravovat podrobný plán útoku.

- **Jak je poškozováno aktivum?**: Samotná aktiva objektu zatím narušována nejsou. Existuje zde výjimka, pokud např. útočník při pasivním sběru dat použije identitu některého za zaměstnanců. Pak již dochází k ovlivnění aktiva.

- **Jak je narušována odolnost?**: Jedná se pouze o pasivní sběr informací z veřejně dostupných zdrojů. Mezi takové zdroje velice často patří sociální sítě, jako je např. Facebook nebo Twitter. Odolnost objektu není touto aktivitou prozatím vůbec narušována – dochází k nepatrnému snížení, ovšem jedná se o latentní fázi a proto není možné snížení odolnosti detekovat.

- **Jaké informace (údaje) popisují narušení odolnosti**?: Vzhledem ke skutečnosti, že sběr informací probíhá z veřejně dostupných zdrojů, není příliš pravděpodobné, že útočník bude odhalen v této fázi, protože zpravidla nejsou dostupné žádné informace.

2. Fáze: Průzkum cíle útočníkem pomocí aktivního skenování.

- **Charakteristika fáze**: Útočník cíleně kontaktuje systém a snaží se detekovat běžící služby a zranitelnosti v nich. Zkouší triviální hesla ke službám. V této fázi také probíhají útoky sociálním inženýrstvím s cílem získat přístupové údaje do systému od samotných uživatelů. Typickým je phishingový útok, kdy se rozesílá podvržený email.

- **Jak je poškozováno aktivum?**: Aktiva chráněného systému již mohou být poškozována, jelikož sken může vyvolat nežádoucí odezvu systému, která může způsobit nestabilitu.

- **Jak je narušována odolnost?**: Odolnost objektu je již v tomto případě narušována. Sken může způsobit nestabilitu systému a jeho případné nestandartní chování.

- **Jaké informace (údaje) popisují narušení odolnosti**?: Typickým zdrojem informací v této fázi jsou logy ze systémů, jako jsou: Intrusion Detection Systems (IDS), Intrusion Prevention System (IPS) a Security Information and Event Management (SIEM) systém. Minoritním zdrojem informací mohou být i cílové stanice, ovšem vzhledem k velkému množství koncových stanic je vhodné využít jejich logy jen jako podpůrné informace pro výše zmíněné systémy.

3. Fáze: Útok na konkrétní službu

- **Charakteristika fáze**: Vzhledem k identifikaci služby VNC nejprve útočník zkouší slovníková hesla a snaží se ke službě připojit. Následně nachází exploit pro danou verzi VNC a exploitem naruší funkci VNC..

- **Jak je poškozováno aktivum?**: Aktivum – ovládací SW již může být porušován, jelikož využití exploit může vyvolat nežádoucí odezvu systému, která může způsobit nestabilitu a ovlivnit tak dostupnost aktiva. Další možností je, že umožní útočníkovi vzdálený přístup do systému.

- **Jak je narušována odolnost?**: Odolnost objektu je již narušena, exploit otevírá nezabezpečené spojení s cílovým systémem a umožňuje jeho neoprávněné ovládání.

- **Jaké informace (údaje) popisují narušení odolnosti**?: Log z cílového PC a vizuální pohyb ovládacích prvků na obrazovce bez manipulace obsluhy. V prvním kroku nevhodně vyhodnoceno jako autorizovaný přístup zvenčí.

4. Fáze: Odepření přístupu pro obsluhu – nahrání payloadu.

- **Charakteristika fáze**: Zamezení zásahu obsluhy do systému, chráněné aktivum (řídicí systém) je v tuto chvíli nedostupné a je plně pod kontrolou útočníka.
- **Jak je poškozováno aktivum?**: odepřením přístupu obsluze a převzetím kontroly řídícího systému je chráněné aktivum nedostupné a není možné ovládat distribuci el. energie.
- **Jak je narušována odolnost?**: Systém je již kompromitován a napaden, přestává plnit svou základní funkci a řídí se příkazy útočníka nikoliv legitimní obsluhy.
- **Jaké informace (údaje) popisují narušení odolnosti**?: Nedostupnost služby pro legitimní obsluhu. Neoprávněná manipulace s ovládacími prvky.

5. Fáze: Odpojení stykačů.

- **Charakteristika fáze**: Fyzické odpojení napájecích prvků soustavy pomocí jejich systému vzdáleného ovládání. Výpadek proudu ve městě.
- **Jak je poškozováno aktivum?**: Blackout pro cca. 30 tis. lidí. Odepření přístupu pro legitimní obsluhu. Skrytá manipulace se systémem.
- **Jak je narušována odolnost?**: Systém je již v moci útočníka, obsluha se dostala na pozici pozorovatele.
- **Jaké informace (údaje) popisují narušení odolnosti**?: Blackout energetické sítě. Výpadek všech ovládacích systémů.

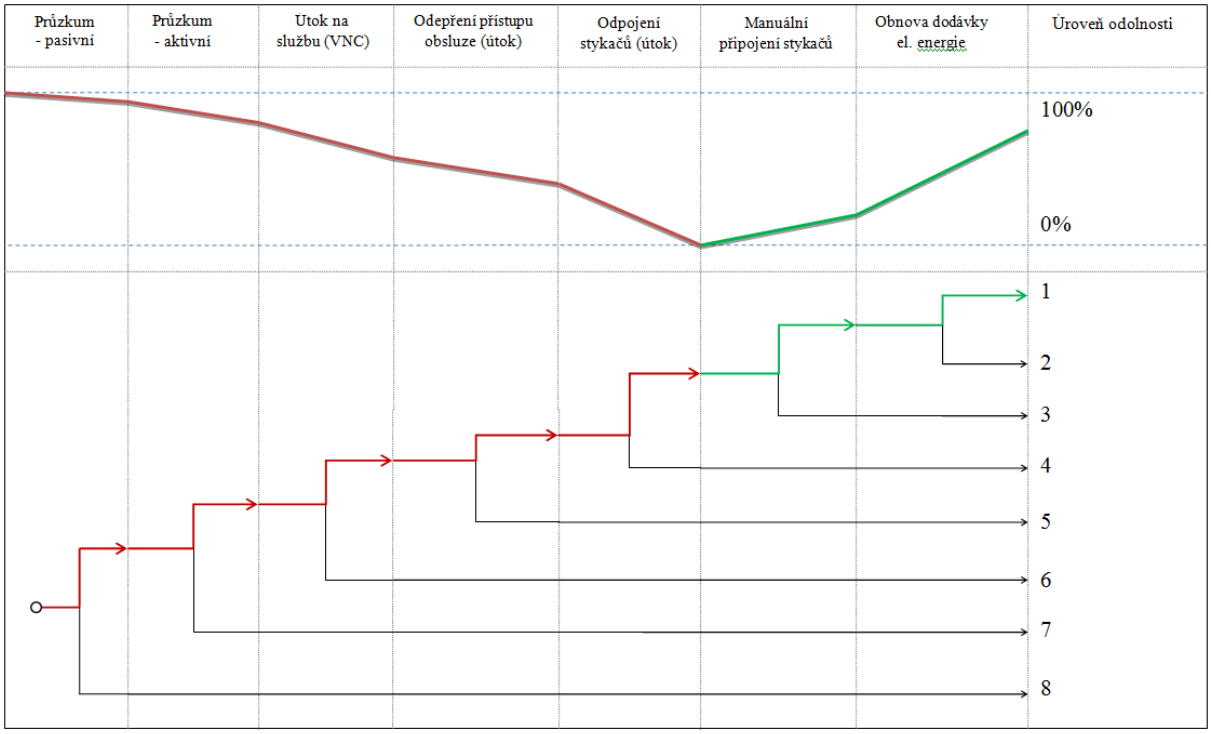
6. Fáze: Manuální připojení stykačů.

- **Charakteristika fáze**: Po inspekci systému došlo k manuálnímu zapojování stykačů z důvodů modifikace kódu ovládacího SW útočníkem. Ovládací SW se během 2 dnů nepodařilo obnovit do použitelného stavu.
- **Jak je poškozováno aktivum?**: Blackout pro cca. 30 tis. lidí. Ohrožení obsluhy z důvodů neznámé manipulace s ovládacím SW. Je možné další poškození SW pomocí skrytých payloadu.
- **Jak je narušována odolnost?**: Systém se začíná zapojovat ručně, nicméně stále je vzdálené ovládání použito pro kontrolu zapojení. Je možná opětovná neoprávněná manipulace např. skrytým payloadem.
- **Jaké informace (údaje) popisují narušení odolnosti**?: Nedostupnost ovládacích prvků systémů. Postupně ustupující blackout.

7. Fáze: Obnovní dodávky el. energie

- **Charakteristika fáze**: Obnovení dodávky el. energie do postižených oblastí. Předpokládá se přechod na bezproblémový provoz, ovšem stále je zde možnost skrytého payloadu nebo backdooru pro případný další útok.
- **Jak je poškozováno aktivum?**: Poškození reputace dodavatele. Ztráta důvěry v ovládací systém. Možné ohrožení obsluhy skrytými payloady.
- **Jak je narušována odolnost?**: Objekt se navenek nalézá ve funkčním stavu, nicméně bez důkladné analýzy všech prvků systému a bez dodatečného zabezpečení je jeho odolnost nižší než před útokem.
- **Jaké informace (údaje) popisují narušení odolnosti**?: Žádné, do doby aktivace payloadu. A to jen v případě, že se payload viditelně projeví.

Níže uvedený Obr. 1. popisuje a zobrazuje vývoj odolnosti v jednotlivých fázích útoku. Přestože v první fázi není možné detekovat snížení odolnosti chráněného systému, tak již v okamžiku, kdy se zahájí pasivní sběr informací, tak jejich agregací dochází k nepatrnému snížení odolnosti. Naneštěstí toto snížení není možné pozorovat a probíhá skrytě. Prvním viditelným snížením odolnosti je fáze aktivního skenu, který může vyústit v útok, jako v tomto případě.



Obr.1: ETA analýza ovládnutí řídícího SW distribuce el. energie

Na základě vytvořeného stromu událostí lze definovat 8 různých stavů:

1) Kybernetický útok vzdáleně vyřadil rozvodnu z provozu odepnutím stykačů a zablokováním řídicího systému; obnovení dodávky el. energie manuálním zapojením stykačů.
2) Kybernetický útok vzdáleně vyřadil rozvodnu z provozu odepnutím stykačů a zablokováním řídicího systému; obnovení dodávky elektrické energie selhalo.
3) Kybernetický útok vzdáleně vyřadil rozvodnu z provozu odepnutím stykačů a zablokováním řídicího systému; obnovení dodávky elektrické energie selhalo.
4) Kybernetický útok znemožnil automatické ovládání rozvodny; distribuce elektrické energie OK.
5) Kybernetický útok na službu (VNC) nebyl úspěšný, distribuce elektrické energie OK.
6) Kybernetický útok v přípravné fázi – aktivní skenování systému.
7) Pasivní skenování systému – bez narušení odolnosti systému (nelze monitorovat).
8) Systém je v kybernetickém „bezpečí“ – ideální stav.

Závěr

Jak ukazuje tato studie, odolnost z pohledu bezpečnosti není statická veličina a dynamicky se v čase mění. Každá změna, každá nově vzniklá událost, bez ohledu na to, zda je klasifikována jako incident, má vliv na odolnost a to jak pozitivní tak negativní. Působení těchto událostí je třeba důsledně monitorovat, aby bylo možné stanovit konkrétní úroveň odolnosti pro daný objekt. Možností jak stanovit odolnost je řada, jednou z nich je připravovaná metodika pro konvergovanou bezpečnost, která bere v potaz nejen bezpečnost kybernetickou, ale řeší i průnik do

dalších oblastí jako je fyzická bezpečnost a naopak. Výsledné hodnocení odolnosti objektu je pak komplexní s vypovídající hodnotou o aktuálním stavu odolnosti v čase.

Tento článek vznikl za podpory grantového projektu VI20172019054 "Analytický programový modul pro hodnocení odolnosti v reálném čase z hlediska konvergované bezpečnosti ", podpořeného Ministerstvem vnitra České republiky v letech 2017-2019.

Literatura

[1] STYCZYNSKI, Jake, Scott STABLES a Nate BEACH-WESTMORELAND. When the lights went out: A comprehensive review of the 2015 attacks on Ukranian critical infrastructure. 1. McLean, USA: Booz Allen Hamilton, 2016.
[2] METZGER, Max. Ukraine confirms December Kiev blackout was cyber-sabotage. *The Cyber-Security source* [online]. Twickenham, UK: SC Media UK, 2017 [cit. 2019-10-08]. Dostupné z: https://www.scmagazineuk.com/ukraine-confirms-december-kiev-blackout-cyber-sabotage/article/1475533