Název předmětu: Kybernetická bezpečnost

Téma: 13. Úloha a poslání NÚKIB (exkurze)

Cíl: Cílem je seznámit studenty se základním posláním a úkoly Národního úřadu pro kybernetickou a informační bezpečnost.

Úkoly pro samostatnou práci: zopakovat si základní poslání Národního úřadu pro kybernetickou a informační bezpečnost.

Studijní literatura:

Internetové stránky NÚKIB https://www.govcert.cz/

Obsah:

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku neveřejné služby v rámci družicového systému Galileo. Vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Hlavní oblasti činnosti NÚKIB:

- provozovat Vládní CERT České republiky (GovCERT.CZ)
- spolupráce s ostatními národními CERT® týmy a CSIRT týmy
- spolupráce s mezinárodními CERT® týmy a CSIRT týmy
- příprava bezpečnostních standardů pro informační systémy KII a VIS
- osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti
- výzkum a vývoj v oblasti kybernetické bezpečnosti
- ochrana utajovaných informací v oblasti informačních komunikačních systémů
- kryptografická ochrana
- Národní centrum PRS (NCPRS) - jedna ze služeb evropského satelitního systému Galileo (PRS = Public Regulated Service)

Vládní CERT (GovCERT.CZ) a týmy typu CSIRT hrají klíčovou roli při ochraně kritické informační infrastruktury a významných informačních systémů podle zákona o kybernetické bezpečnosti (181/2014 Sb.) a jeho prováděcích předpisů. Každá země, která má své kritické

systémy připojeny do internetu, musí být schopna efektivně a účinně čelit bezpečnostním výzvám, reagovat na incidenty, koordinovat činnosti při jejich řešení a účelně působit při předcházení incidentům.

Úlohou těchto týmů je zároveň působit jako prvotní zdroj bezpečnostních informací a pomoci pro orgány státu, organizace i občany. Neméně důležitou roli hrají při zvyšování vzdělanosti v oblasti bezpečnosti na internetu.

Orgány a osoby, na které se vztahuje zákon o kybernetické bezpečnosti, musí plnit určité povinnosti vůči vládnímu CERT týmu a orgány a osoby podle § 3 písm. a) a b) plní povinnosti zejména vůči národnímu CERT týmu. Národní CERT tým zaštiťuje organizace CZ.NIC.

POSKYTOVANÉ SLUŽBY

Národní centrum kybernetické bezpečnosti (NCKB) a jeho vládní tým GovCERT.CZ nabízí v rámci své činnosti následující služby, které by Vaší organizaci mohly pomoci v rámci zajišťování kybernetické bezpečnosti:

KOORDINAČNÍ ČINNOST A POMOC PŘI ŘEŠENÍ INCIDENTŮ

Řešení bezpečnostních incidentů patří k hlavním činnostem vládního týmu. Při nahlášení takové události jsou jeho odborníci připraveni pomoci Vašim IT specialistům po technické stránce, včetně poskytnutí rad pro další preventivní opatření. Dojde-li ke zjištění, že některý z incidentů cílí na více subjektů, jsou připraveni koordinovat společný postup na jeho řešení. Pro tento případ se v brněnském sídle připravuje audiovizuální konferenční centrum.

ZPROSTŘEDKOVÁNÍ KONTAKTŮ

Vzhledem k navázané rozsáhlé spolupráci napříč různými institucemi lze poskytnout pomoc při zprostředkování kontaktů jak s českými bezpečnostními týmy, tak se zahraničními partnery při řešení bezpečnostních incidentů s mezinárodním přesahem.

SDÍLENÍ DAT

V rámci úzké spolupráce s různými nadnárodními organizacemi, které se zabývají kybernetickou bezpečností, získává vládní tým velké množství reportů a dat, které se týkají potenciálně infikovaných strojů v České republice. Tyto informace je Vám možné v rámci proaktivní činnosti poskytnout. Vzhledem k různé variabilitě sdílených dat jsou rozdělovány do jednotlivých projektů:

BotnetFeed – pomocí tohoto nástroje jsou zpracovávána data z převzatých C&C serverů o koncových stanicích zapojených do sítí botnetů. Pro identifikaci případně nakažené stanice ve Vašem IP rozsahu, Vám bude předána IP adresa a informace o botnetu, do kterého je začleněna. Pro detailnější analýzu nákazy je možné dodat časové známky komunikace stanice s C&C serverem, cílovou IP adresu a využívaný port. Tyto informace lze po selekci poskytovat partnerům ve formátu xml a csv.

IHAP, MDM* – v rámci těchto projektů jsou sbírány fragmenty indikátorů kompromitace (IoC) z různých serverů. Mezi nejčastější indikátory patří phishing, útoky hrubou silou, ids alerty, spam, pokusy o skenování, zneužívání zranitelností, výskyt malware a mnoho dalších typů. Na základě těchto dat jsou pro partnery připravovány krátké reporty, které vždy obsahují IP adresu kompromitovaného stroje a stručné shrnutí o jaký typ incidentu se jedná.

*IHAP = Incident Handling Automation Project, MDM = Malicious Domain Manager

Shadowserver – tento projekt se zaměřuje na průběžné vyhledávání relevantních informací o zranitelnostech v kyberprostoru a o výskytech těchto zranitelností na konkrétních IP adresách. Tým GovCERT.CZ může zprostředkovat sdílení těchto dat s Vaší organizací nebo jen samotný kontakt se zástupci Shadowserver.

NASAZOVÁNÍ HONEYPOTŮ

Síťové pasti umožňují detekovat pokusy o neautorizovaný přístup do různých systémů, monitorovat chování útočníků a vektory jejich útoků na základě známých zranitelností webových zdrojů (např. XSS, SQL injection). Pro využívání tohoto typu sledování lze nasadit síťovou past na Vámi vyhrazenou IP adresu. V případě, že se rozhodnete v této oblasti s vládním týmem spolupracovat, můžete se zapojit do vzájemného sdílení dat z těchto honeypotů.

PENETRAČNÍ TESTOVÁNÍ

Jednou z forem preventivních aktivit je externí penetrační testování. Jedná se o legální pokus o průnik do testovaných systémů. Výsledkem je zpráva o chybách v zabezpečení testovaného subjektu, která je určena výhradně jeho vlastníkovi, který na základě zprávy učiní příslušná bezpečnostní opatření.

Další možností je provedení skenování zranitelností podle OWASP (Open Web Application Security Project). Pracovníci vládního CERT týmu tak mohou prověřit bezpečnost Vašich webových stránek a upozornit na případná bezpečnostní rizika.

INFORMAČNÍ HUB

Na webových stránkách govcert.cz můžete nalézt informace, rešerše, analýzy a články, které se týkají aktuálních hrozeb a zranitelností se vztahem k systémům v České republice. Ty jsou doplňovány o pravidelné měsíční bulletiny, které shrnují významné bezpečnostní incidenty u nás i ze zahraničí.

V současnosti je připravován i neveřejný informační portál, kde budou smluvním partnerům a spolupracujícím organizacím kromě sdílených dat poskytovány i další informace a hlubší analýzy ve vztahu k jejich systémům.

VZDĚLÁVÁNÍ A VÝZKUMNÁ ČINNOST

Pracovníci NCKB mohou připravit školení či přednášky na různá témata (technické i legislativní) z oblasti kybernetické bezpečnosti.

FORENZNÍ LABORATOŘ A SCADA LABORATOŘ

Odborníci z vládního týmu se také zabývají forenzní analýzou. V případě, že již došlo z jakéhokoliv důvodu ke kompromitaci stroje ve Vaší instituci, nebo máte odůvodněné podezření, že k této kompromitaci mohlo dojít, je možné tuto událost z technického hlediska vyšetřit ve forenzní laboratoři.

GovCERT.CZ nabízí spolupráci i v oblasti technických měření a analýz industriálních a řídicích systémů, pro kterou je pak v objektu NCKB vybudovaná SCADA laboratoř.

HLÁŠENÍ INCIDENTŮ

Při nahlášení kybernetického bezpečnostního incidentu (KBI) jsou odborníci vládního týmu připraveni pomoci po technické stránce, včetně poskytnutí rad pro další preventivní opatření. Dojde-li ke zjištění, že některý z incidentů cílí na více subjektů, jsou připraveni koordinovat společný postup na jeho řešení. V případě, že nám nahlásíte incident, který nespadá do oblasti působnosti vládního týmu (KII, VIS, veřejná správa), postaráme se o jeho předání příslušnému bezpečnostnímu týmu. Pro nahlášení KBI můžete využít některý z níže uvedených způsobů:

E-MAIL

Primárním komunikačním kanálem pro reportování KBI je e-mail cert.incident@nukib.cz. Pro bezpečnější a důvěryhodnou komunikaci doporučujeme použití PGP šifrování. Další podrobnosti k použití PGP jsou uvedeny zde.

Předmět zprávy by měl mimo jiné obsahovat typ incidentu (např. DDoS, hacking, phishing, ransomware, atd.) pro snadnější třídění incidentů mezi jednotlivé analytiky. V těle zprávy je pak potřeba uvést všechny potřebné náležitosti, které jsou popisovány v příloze č. 5 ve Vyhlášce 316/2014 Sb. (vyhláška o kybernetické bezpečnosti). Zpráva by tak měla obsahovat například části logů obsahující záznamy o útoku, časové známky včetně časové zóny, zdrojové a cílové IP adresy a porty. Nezbytnou součástí jsou i základní kontaktní informace, tedy jméno reportujícího a jméno organizace.

FORMULÁŘ

Preferovaným způsobem hlášení KBI je odeslání vyplněného formuláře, který lze stáhnout zde. Tento formulář je k dispozici v editovatelném formátu PDF. Po správném a úplném vyplnění všech položek a textových polí soubor zašlete na e-mailovou adresu cert.incident@nukib.cz.

XML SCHÉMA PRO HLÁŠENÍ INCIDENTU

Toto schéma lze použít pro odeslání všech potřebných detailů incidentu ve formátu XML, nebo jej implementovat do vlastní aplikace pro hlášení kybernetických bezpečnostních incidentů a událostí. Jedná se o platný ekvivalent k dosavadnímu poskytovanému formuláři. Více informací o poskytovaném schématu, včetně konkrétního příkladu fiktivního incidentu a možnosti jeho stažení naleznete zde.

TELEFONICKY

V případě nenadálé a vážné situace, kdy hrozí riziko z prodlení, můžete pro kontaktování týmu GovCERT.CZ v pracovní době využít telefonní spojení na čísle +420 541 110 777. Mimo standardní pracovní dobu pak na telefonním čísle +420 725 502 878.

GovCERT.CZ respektuje soukromí všech kontaktujících osob a institucí a považuje všechny nahlášené incidenty za citlivé informace.