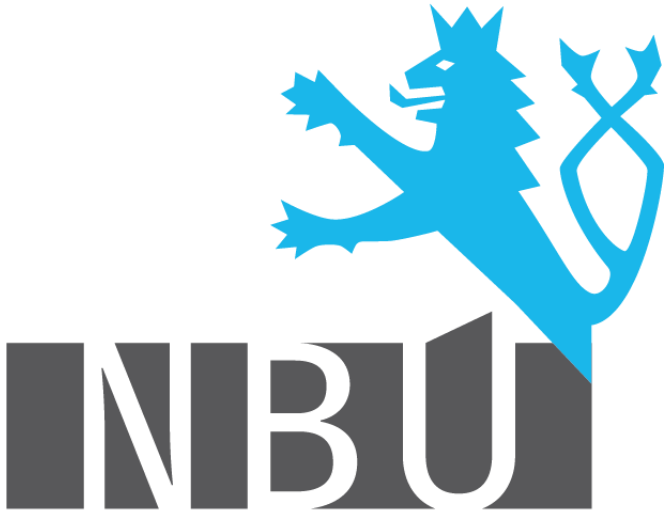

Národní
bezpečnostní
úřad

Národní
bezpečnostní
úřad

Praktické naplňování zákona o kybernetické bezpečnosti

Ondřej Mokoš

OBSAH PREZENTACE

- Kontaktní údaje
- Jak připravit hlášení o kybernetickém incidentu
- Klasifikace incidentu
- Formulace hlášení
- Způsob předávání na NCKB
- Zpětná vazba
- Příklad

ODKAZOVANÉ MATERIÁLY

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů

- Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti

KONTAKTNÍ ÚDAJE

- Zákon o kybernetické bezpečnosti § 16
- Vyhláška o bezpečnostních opatřeních… § 34
- Ohlásit do 30 dnů od
  - určení (systémy kritické informační infrastruktury)
  - dne naplnění určujících kritérií (významné informační systémy)
  - dne nabytí účinnosti zákona (významné sítě, poskytovatelé služeb el. komunikací)
- Forma
  - datová zpráva do datové schránky Úřadu h93aayw
  - listinným hlášením na adresu NCKB

KONTAKTNÍ ÚDAJE 2

- Co jsou kontaktní údaje definuje zákon
- Formulář v příloze č. 7 vyhlášky
  - vzor, seznam nutných polí
- Další užitečné informace
  - rozsah IP adres, adresy webových prezentací, softwarové vybavení…
- Doporučujeme předat veřejné PGP klíče společně s kontaktními údaji
  - předání například emailem
  - otisk klíče ověřit jiným kanálem (osobní předání vizitky, telefon apod.)
  - klíče pro fyzické osoby, které budou za daný subjekt jednat

PGP

- Původní systém Pretty Good Privacy
- Nyní otevřený standard OpenPGP uznaný IETF
- RFC4880
- Pro zabezpečení emailové komunikace
- Asymetrická kryptografie
- Nevyžaduje certifikát od certifikační autority
- De facto standard v komunitě CERT týmů

KONTAKTNÍ ÚDAJE 3

- Udržovat kontaktní údaje aktuální včetně PGP klíčů
- Zodpovědná osoba přejde na jinou pozici, za danou problematiku dále nezodpovídá
- Zodpovědná osoba odejde, emailovou schránku nikdo dále nemonitoruje
- Reorganizace, neplatná telefonní čísla a emailové adresy

JAK PŘIPRAVIT HLÁŠENÍ O KYBERNETICKÉM INCIDENTU

- Povinnost hlásit incidenty vyplývá z § 8 zákona
- Začít plnit do 1 roku od
  - určení (systémy kritické informační infrastruktury)
  - dne naplnění určujících kritérií (významné informační systémy)
  - dne nabytí účinnosti zákona (významné sítě, poskytovatelé služeb el. komunikací)

JAK PŘIPRAVIT HLÁŠENÍ O KYBERNETICKÉM INCIDENTU 2

- Primárním účelem je rychlé předání informací, ne pro kategorizaci v našem systému
- V počátečních fázích řešení incidentu nemusí být všechny informace k dispozici, použít kvalifikovaný odhad
- Čím dříve, tím lépe
  - i za cenu nepřesností

JAK PŘIPRAVIT HLÁŠENÍ O KYBERNETICKÉM INCIDENTU 3

- Hlášení o kybernetickém incidentu je zpravidla počátek komunikace týkající se incidentu
- V hlášení by se mělo objevit, jaká akce se od nás očekává (vzít na vědomí, podílet se na řešení, navázání komunikace s třetí stranou,…)
- Pokud se máme podílet na analýze, je nutné přiložit podpůrné materiály/evidenci (logy, artefakty, apod.)

FORMULÁŘ PRO HLÁŠENÍ

- Úroveň ochrany informace
- Kontaktní údaje
- Detaily incidentu
  - Datum a čas zjištění
  - Časová zóna
  - Kategorie incidentu
  - Typ incidentu
  - Současný stav zvládání kybernetického bezpečnostního incidentu
  - Počet zasažených systémů (odhad)
  - Odhad počtu zasažených uživatelů
  - Popis incidentu
- Systémové detaily
  - Host nebo IP
  - Funkce host (DNS server, stanice atd.)
  - Pokračování

KLASIFIKACE INCIDENTU

- Podle příčiny (vyhláška § 30)
  - KBI způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb
  - KBI způsobený škodlivým kódem
  - KBI způsobený kompromitací technických opatření
  - KBI způsobený porušením organizačních opatření
  - KBI spojený s projevem trvale působících hrozeb
  - ostatní KBI způsobené kybernetickým útokem

KLASIFIKACE INCIDENTU 2

- Podle dopadu (vyhláška § 30)
  - KBI způsobující narušení důvěrnosti aktiv
  - KBI způsobující narušení integrity aktiv
  - KBI způsobující narušení dostupnosti aktiv
  - KBI způsobující kombinaci dopadů uvedených výše

KLASIFIKACE INCIDENTU 3

- Podle závažnosti (vyhláška § 31)
  - Kategorie III
    - velmi závažný KBI, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření KBI včetně minimalizace vzniklých i potenciálních škod.
  - Kategorie II
    - závažný KBI, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření kybernetického incidentu včetně minimalizace vzniklých škod.
  - Kategorie I
    - méně závažný KBI, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření KBI včetně minimalizace vzniklých škod.

FORMULACE HLÁŠENÍ

- Minimální obsah hlášení je dán formulářem
- Popis incidentu by měl obsahovat
  - popis dotčeného systému
  - popis aktuální situace
  - popis průniku
  - podniknuté kroky
  - popis přiložených materiálů (logy, artefakty,…)

ZPŮSOB PŘEDÁVÁNÍ NA NCKB

- Definuje § 32 vyhlášky
- Elektronická podoba
  - elektronický formulář (zatím nedostupné)
  - email cert.incident@nbu.cz
    - preferovaná metoda v kombinaci s PGP
  - datová zpráva do datové schránky Úřadu h93aayw
  - prostřednictvím datového rozhraní (zatím nedostupné)
- Listinná podoba na adresu NCKB

ZPĚTNÁ VAZBA

- Co očekávat od nás?
- Potvrzení přijetí hlášení
- Vyžádání dalších informací
- Průběžné zasílání postupu naší analýzy (pokud požadováno)
- Poskytnutí informací, pokud jsme stejný incident již zaznamenali

ZPĚTNÁ VAZBA 2

- Zprostředkování komunikace s třetí stranou
- Vydání doporučení pro zvýšení zabezpečení
- Ochranné opatření (zákon § 14 a § 15)
- Reaktivní opatření (zákon § 13 a § 15, vyhláška § 33)

NAŠE DALŠÍ SLUŽBY

- Informační servis
  - shrnutí o zranitelnostech
  - doporučení na odstranění
  - identifikátory (CVE, MS Security Bulletin)

DoubleDirect - nový typ útoku Man-in-the-Middle

24. 11. 2014

Velké rozšíření mobilních zařízení vedlo k významnému nárůstu síťových útoků na bezdrátové sítě. DoubleDirect je označení Man-in-the-Middle (M-i-t-M) síťového útoku typu Internet Control Message Protocol přesměrování (ICMP Redirect), který slouží jako alternativa k útoku technikou otravy ARP (ARP poisoning). ICMP přesměrování legálně využívají směrovače k informování zařízení v síti, že je k dispozici lepší trasa pro spojení s určitým konkrétním místem. DoubleDirect byl prozatím zneužit k přesměrování mobilních zařízení, která se snažila připojit k majoritním webovým stránkám jako například Google, Facebook nebo Twitter na zařízení kontrolované útočníkem.

Charakteristika zranitelnosti

Nová metoda spočívá v použití paketů ICMP pro přesměrování, kterými útočník změní směrovací tabulku zařízení patřící oběti tak, aby byl provoz pro konkrétní IP adresu přesměrován přes libovolné síťové cesty. Pokud je do této cesty zahrnut útočníkův stroj, dochází k útoku M-i-t-M. Zatímco dosavadní útoky ICMP Redirect jsou označovány jako polo-duplexní, protože napadený uzel může data pouze přijímat nebo odesílat, útoky DoubleDirect jsou již plně duplexní. To je zajištěno tím, že útočníci jsou schopni například pomocí DNS sniffingu predikovat, na kterou IP adresu oběť bude přistupovat.

Postižené systémy

Zařízení pracující se systémy iOS do verze 8.1.1, Android (včetně Lollipop) a OS X (včetně Yosemite).

Operační systémy Linux a Windows nejsou zranitelností dotčeny, protože nepodporují ICMP pakety pro přesměrování.

Dopad zranitelnosti

Útočník v pozici Man-in-the-Middle může získat přístup k přihlašovacím a citlivým údajům, nebo šířit malware na cílové mobilní zařízení, případně získat přístup k podnikovým sítím.

Řešení

Zakázat ve všech operačních systémech funkci ICMP Redirect.

CVE

N/A

Odkazy

http://blog.zimperium.com/doubledirect-zimperium-discovers-full-duplex-icmp-redirect-attacks-in-the-wild/
http://news.softpedia.com/news/Traffic-from-Google-Facebook-Twitter-Redirected-to-Cybercriminals-Via-New-DoubleDirect-Attack-465607.shtml
http://www.theregister.co.uk/2014/11/21/hackers_snaffling_smartphone_secrets_with_redirection_attack/?mt=1416836489914
http://securityaffairs.co/wordpress/30417/cyber-crime/doubledirect-mitm-attacks.html

NAŠE DALŠÍ SLUŽBY 2

- Předávání informace z dostupných zdrojů
  - CleanMX, Phishtank, MalwareDomainList a další
- Identifikace strojů potenciálně zapojených do botnetů
- Penetrační testování

PŘÍKLAD

- Uvažme blíže neurčenou organizaci
- V této organizaci mají informační systém, který naplnil určující kritéria a stal se významným informačním systémem
- Zodpovědnou osobou za tento informační systém je Alice

PŘÍKLAD – „ROZJEZD“

- Alice do 30 dnů zašle kontaktní údaje a zároveň rozsah IP adres, které organizace používá
- Vygeneruje PGP klíč, veřejnou část nám zašle emailem nebo využije „keyserver“
- Stáhne si naše veřejné klíče
- Telefonicky si vzájemně ověříme otisky klíčů

PŘÍKLAD – „DOBA KLIDU“

- Alici předáváme data získaná z dostupných zdrojů relevantních pro její organizaci
- Rovněž může využívat informace o zranitelnostech publikované na našem webu
- Při výskytu bezpečnostní události můžeme vydat varování pro ostatní organizace
  - vyžaduje rychlou reakci
  - v nejlepším případě můžeme pomoci uchránit před útokem
- V reakci na incident jiné organizace můžeme vydat ochranné opatření a doporučit změny pro zvýšení zabezpečení i v systému Alice

PŘÍKLAD – „MALÝ PROBLÉM“

- Monitorovací nástroje odhalily bezpečnostní problém
- Incident byl velice triviální, Alice jej snadno vyřešila a odeslala hlášení incidentu
- Obdržené hlášení pouze zaevidujeme, tuto informaci můžeme využít k varování ostatních nebo vydání ochranného opatření

PŘÍKLAD – „VELKÉ PROBLÉMY“

- Nastaly velké problémy, Alice odhalila průnik do sítě její organizace se zatím neznámými následky
- Incident řeší podle vypracovaných dokumentů, které tvoří organizační opatření
  - zvládání kybernetických bezpečnostních událostí a incidentů, řízení kontinuity činností apod.
- Bohužel není schopna rychle provést kompletní analýzu
- Odešle hlášení incidentu s přibližným popisem problému a přiloženými některými logy
- CERT tým provede analýzu, případně si vyžádá další záznamy

PŘÍKLAD – „VELKÉ PROBLÉMY“

- Alice ve spolupráci s CERT týmem zanalyzují průnik a objasní celou situaci a doporučí, jak systém lépe zabezpečit
- Alice aplikuje opatření, které zabrání opakovanému zneužití zranitelností
- Incident je vyřešen a může být uzavřen

Národní
bezpečnostní
úřad

Děkuji za pozornost

Ondřej Mokoš
e-mail: o.mokos@nbu.cz
www.govcert.cz