Úvod do kybernetické bezpečnosti - přehled

Karel Velička

10. ledna 2024

Obsah

1 Úvod

Informační bezpečnost ≡ Ochrana informací v jakékoliv podobě (digitální i papírová)

Kybernetická bezpečnost ≡ Ochrana informací pouze v digitální podobě

Kybernetická událost ≡ může způsobit narušení bezpečnosti

Kybernetický incident ≡ narušení bezpečnosti

Technická opatření ≡ zajišťuje hardware a software, detekce a zamezení kybernetických událostí a incidentů

Organizační opatření ≡ zajišťují procesy, podpora a doplnění pro technická opatření.

SoD – Separation of Duty

- Jedna osoba nemůže přistoupit, upravit, spustit proces bez toho, aniž by toto někdo schválil
- Jsou rozděleny práva/povinnosti

Least Privilege / Need-to-know

- Zamezení přístupu do systémů, které daný uživatel nepotřebuje k práci

Zero trust

- Neexistuje "důvěrný" uživatel, systém nebo zařízení

Fail secure

- Pokud selže nějaká ochrana, tak tím nevznikne prostor pro útočníka, protože výchozí stav je bezpečný

2 Rizika

Analýza rizik

- *Primární aktiva*: informace, nebo procesy (služby), které organizace potřebuje pro své fungování (receptura)
- *Podpůrná aktiva*: co potřebují primární aktiva pro své fungování
- *Skupinová aktiva*: pokud se záměrně sdružujeme více podpůrných aktiv dohromady (Linux/ Win servery)
- *Riziko*: co se může našim primárním aktivům stát a proti čemu je musíme zabezpečit
  událost, která s určitou pravděpodobností může (ne)nastat. Hrozba zneužije zranitelnost a vznikne incident.

Úrovně detailu

- *Malá úroveň*: Jednoduše vytvořená analýza rizik + lehce spravovatelná - ALE - malá přidaná hodnota
- *Velká úroveň*: Přesný popis procesů + pokrývá hodně rizik - ALE - dlouhá analýza rizik + nelze jednoduše aktualizovat

PDCA – Plan-Do-Check-Act ≡ Začneme na malém detailu a v příštím běhu procesu jdeme o úroveň níže do většího detailu, nebo zahrneme více systémů.

CIA Triad

- *Confidentiality*: data nebudou dostupná neoprávněné osobě (krádež firemní databáze, ...)
- *Integrita*: data nejsou pozměněna a mohu se na ně spolehnout (MITM, Změna čísla bankovního účtu, ...)
- *Availability*: data jsou dostupná v čase, kdy jsou potřebná (DDoS, Ransomware ...)

Hodnocení aktiv ≡ jak jsou pro mě jednotlivá aktiva důležitá z pohledu důvěrnosti, integrity a dostupnost

3 Threat Intelligence, Kybernetický zločin a jeho ekonomika

Threat Intelligence ≡ porozumění hrozbám, před tím, než se objeví

Pravidlo tří otázek

- *Hrozba*: Co nám hrozí?
- *Dopad*: Jaký bude dopad?
- *Akce*: Jaká opatření navrhnout?

Typy

- *Taktická*: Bezpečnostní provoz a monitoring - popis akcí a opatření
- *Operativní*: Vedení informační bezpečnosti, Threat Hunting - popis chování útočníků a skupin
- *Strategická*: Vedení organizace/ informační bezpečnosti - popis dopadu hrozeb na organizac

Kybernetický zločin jakákoliv kriminální aktivita která zahrnuje využití výpočetních zařízení, síťových zařízení nebo sítě

Advanced Persistent Threat (APT)

- Dlouhodobé, nedetekované hrozby
- Cílí na organizaci/ stát s cílem získat cenná data (špionáž)
- Úmyslně pomalý progres, nepozorované vniknutí

4 Protokoly v kybernetické bezpečnosti

Protokol Série kroků/akcí, zahrnující dvě nebo vice stran, navržených za účelem dosažení cíle/splnění úlohy. Kryptografie v protokolech pro zajištění CIAutentizace.

4.1 Autentizační protokoly

Selfie útok

- Autentizace prostřednictvím předem dohodnutého tajemství, které musí znát oba účastníci
- Např. TLS 1.3 umožňuje mód Pre Shared Key (PSK)

Diverzifikace klíčů ≡ kompromitace jednoho uživatelského klíče nesmí ovlivnit bezpečnost ostatních klíčů

Útok na pseudonáhodný generátor

- V každém okamžiku je generátor ve stavu
- Útočník se pokusí rekonstruovat tento stav z výstupu $\implies$ stejný stav vede ke stejné generované sekvenci
- Stejný stav bude použit více než jednou (např. 2+ virtuálních strojů nabootuje ze stejného snapshotu)
- Zdroj entropie je nevyhnutný pro iniciální seed hodnotu

4.2 SSL/TLS Protokol - Secure Socket Layer, Transport Layer security

Zajišťuje důvěrnost a integritu dat mezi dvěma komunikujícími aplikacemi a garantuje bezpečnou komunikaci v přítomnosti útočníka na síťové vrstvě

Handshake protokol

- Dvě komunikující strany (klient a server) - dojednání verze protokolu a sady kryptografických algoritmů
- Autentizace serveru, ustanovení tajného klíče

Record protokol

- Přenos a odeslání zprávy z aplikace - fragmentace do bloků, komprese, počítání MAC, šifrování, hlavičky

Truncation útok (zkracování)

- Útočník manipuluje TCP spojení pro ukončení přenosu dat
- Strany budou předpokládat, že přenášená zpráva je kratší, než je ve skutečnosti
- Řešením je mít různé typy bloků (0 - data, 1 - uzavření spojení)

5 Bezpečnost sítí

Model síťové bezpečnosti

- Internet - zaměstnanci, klienti
- DMZ - VPN gateway
- Trusted - soukromé služby, App server
- Privileged - PCI server

Zero trust

- důvěra není nikdy garantována
- Princip minimálních oprávnění
- Rozšířené řízení identit, Mikro segmentace, Softwarově definovaný perimetr

Zdroje data

- Sběr packetů - Zachycení přesné kopie provozu (paketů, tak jak byly přenášeny po síti)
- NetFlows - IP packety přenesené po síti během daného intervalu (v jedné NetFlow mají všechny společné vlastnosti)
- Logy - Síťová zařízení (směrovače, přepínače), Firewally, ...

Packetová analýza ≡ hledání vzorů, parsování specifických příznaků, filtrování

SPF (Sender Permitted From) ≡ pouze vybrané systémy mohou posílát emaily jménem mé domény

DKIM (Domain Keys Identified Email) ≡ emailový server domény kryptograficky podepíše zprávu (info v hlavičce, klíč v txt)

PDMARC ≡ autentizace emailu, politika, a protokol pro reportování. Spoléhá na SPF a DKIM

Statistická analýza NetFlows

- Identifikace kompromitovaných zařízení - kompromitovaná zařízení mohou posílat/ přijímat více dat než obvykle
- Potvrzení či vyvrácení úniku dat - je možné provést analýzu objemu odeslaných dat pro ověření zda mohlo dojít k úniku dat
- Profilování uživatelské aktivity - data z uživatelských zařízení mohou odhalit standardní pracovní dobu, časy neaktivity, apod.

6 Opeační Systémy

6.1 UEFI (Unified Extensible Firmware Interface)

- Nástupce původního rozhraní BIOS (grafické prostředí, možnost ovládání myší)
- hrozby: Buffer overflow, Úprava proměnných UEFI (SecureBoot), SMM code injection, Disclosure of SMRAM contents, ...

6.2 Firmware

program pro provádění základních nízkoúrovňových operací (mezi HW a SW)

SecureBoot ≡ brání načtení nedůvěryhodného (bez certifikátu) operačního systému (klíče uloženy na TPM)

TPM ≡ standard bezpečného čipu pro uložení šifrovacích klíčů; umožňuje používání SecureBoot, Šifrování disku, Biometrické autentizace, ...

Buffer overflow ≡ do zásobníku zapsáno více, než je kapacita $\implies$ zápis do sousedního úseku operační paměti $\implies$ možnost zápisu dat do prostoru paměti jiné aplikace

6.3 Operační systémy

Hardening ≡ bezpečné nastavení operačních systémů a aplikací (snaha o snížení Attack surface $\implies$ vypnutí/blokování nepotřebných služeb apod.)

Ochrana Windows

- *UAC*: bez potvrzení uživatele nemůže aplikace eskalovat oprávnění
- *Smart App Control*: kontrola spouštěných aplikací.
- *Virtualization-based security*: aplikace v separátních virtualizovaných prostředích (izolace)

Ochrana Linux

- *SELinux*: lze nastavit přístupová oprávnění pro každého uživatele, aplikaci, process a soubor na disku
- *chroot*: technika posunutí kořenu souborového systému (ztráta/ nabytí oprávnění)
- *Fail2ban*: opakované pokusy o přihlášení (brute force) způsobí zablokování síťového prostupu

6.4 Virtualizace

HW hypervisor ≡ slouží k emulaci HW (např. VMware, KVM, ...),

SW hypervisor ≡ instalován na OS hosta (Virtualbox, ...), méně bezpečné než HW hypervisor

6.5 Kontejnery

- Virtualizace OS, instalace až na OS (Docker, ...)
- *chroot*: technika posunutí kořenu souborového systému (ztráta/ nabytí oprávnění)
- *Fail2ban*: opakované pokusy o přihlášení (brute force) způsobí zablokování síťového prostupu

Namespaces a cgoups

- *Namespaces*: umožňuje oddělení jednotlivých procesů na tzv. jmenné prostory (user ID, process ID, network, mount)
- *cgoups*: umožňuje řídit zdroje (CPU, RAM, HDD, síť), omezovat přidělené zdroje, prioritizovat jeden proces před druhým, měřit spotřebované zdroje

7 Webová a mobilní bezpečnost

Statické stránky ≡ pouze front-end, žádná logika na straně serveru, žádný vstup od uživatele

- Obsah přímo v HTML kódu (resp. + CSS, JS), do kódu stránek nelze sáhnout
- *Útok*: DDoS, změna HTML souboru (přes FTP/SCP)

Dnyamické stránky ≡ front-end i back-end, logika, vstup od uživatele, obsah načítán z databáze

- Vykonává se na straně PHP serveru, práce s proměnnými
- *Útok*: podvržený vstup, špatně napsaný back-end

Server Side Includes (SSI) ≡ možnost při načítání stránky vložit (element) do statické HTML další kód; částečně dynamické

7.1 Vstupy od uživatele

> "Každý vstup je nebezpečný"

- *Formuláře*: kontrolovat HTTP POST; např. vyhledávání, přihlášení, vložení do košíku, ...
- *URL adresy*: back-end PHP volání `$_GET` - ovlivnění chování stránky; přístup k jinému účtu, ...
- *Cookies*: posílá se HTTP Request požadavku + cookies; obstarává historii, zajišťuje identifikaci
- *HTTP hlavičky*: Request (user) a Response (server); obsahují HTTP headers (Referrer-Policy, X-XSS-Protection, HTTP Public Key Pinning (HPKP)...)

7.2 HTTP headers

CSP (Content-Security-Policy)

- Určí politika, odkud se mohou nahrávat externí zdroje (obrázky, JS, fonty)
- Ochrana proti XSS, data injection

HSTS (HTTP Strict Transport Security header)

- Vynutí přístup pouze přes HTTPS
- Ochrana proti Man-in-the-middle

HPKP (HTTP Public Key Pinning)

- Prohlížeč přijímá odpověď serveru pouze když přijde i s certifikátem s odpovídajícím public key
- Zabraňuje vystavení falešných certifikátů pro doménu

7.3 Šifrování spojení

- Přesměrovat HTTPS na HTTP, přepnout komunikaci na „slabé šifrování“, přesměrovat komunikaci přes svoji doménu

7.4 OWASP TOP 10

A05:2021 – Security Misconfiguration

- *Popis*: špatná konfigurace prostředí, ve kterém je web-aplikace provozována (nastavení serveru, zapomenuté konfigurační/instalační skripty, výchozí adresáře a hesla, přístupová práva hostingu/cloudu)
- *Ochrana*: hardening webového, aplikačního serveru; aktualizace knihoven + frameworků, změna výchozího nastavení; nastavení oprávnění; odinstalace nepoužívaných komponent/portů/frameworků
- Security through obscurity - Změna výchozího nastavení; vhodné proti automatizovaným útokům

A06:2021 – Vulnerable and Outdated Components

- *Popis*: zastaralá a zranitelná komponenta (webový server, databáze, ...), neprovedení okamžitého upgrade platformy
- *Ochrana*: pravidelné a okamžité patchování a skenů zranitelností; sledování nově zveřejněných zranitelnost

A09:2021 – Security Logging and Monitoring Failures

- *Popis*: nezaznamenávání logů (neúspěšné přihlášení, podezřelá aktivita); logy se ukládají pouze lokálně;
- *Ochrana*: zajistit logování ve správném a čitelném formátu; logování úspěšných i neúspěšných přihlášení

7.5 Testování webových aplikací

SAST (Static Application Security Testing)

- Testování zdrojového kódu aplikace (inside-out)
- Nevyžaduje běžící systém k provedení scanu; rychlé; navede na konkrétní řádku kódu
- Hodně false-positives; nedokáže najít zranitelnosti u služeb třetích stran; musí mít přístup ke zdrojovému kódu

DAST (Dynamic Application Security Testing)

- Testování skrze front-end; simuluje chování uživatele (outside-in)
- Nevyžaduje přístup ani změny ve zdrojovém kódu; málo false-positives; tester nemusí o aplikaci nic vědět
- Neidentifikuje zranitelnost ve zdrojovém kódu; riziko incidentu v produkčním prostředím; trvá dlouho

IAST (Interactive Application Security Testing)

- Kominace SAST a DAST; pracuje nad běžící aplikací; nepotřebuje přístup ke zdrojovému kódu

7.6 Mobilní bezpečnost

- pravidelně aktualizovat, mít antivirus, zálohovat, nepřipojovat se k nedůvěryhodným wifi, zámek displeje
- instalovat z ověřených zdrojů, číst podmínky, nepovolovat nepotřebná oprávnění

Mobile Device Management (MDM)

- Nástroj pro zajištění kontroly nad mobilními zařízením
- Kontrola bezpečnostních firemních politik
- správa a kontrola nad aplikacemi, které jsou na zařízen nainstalovány
- Uzamknoutí, smazání, skenování zařízení, vypnout kameru/NFC/GPS, ...

8 Legislativa v kybernetické bezpečnosti

8.1 Organizační opatření

- řízení rizik a aktiv, bezpečnostní politika, organizační bezpečnost, stanovení bezpečnostních požadavků,

ISMS - Systém řízení bezpečnosti informací

- Soubor pravidel, cílem je zachovat důvěrnost, integritu a dostupnost informací aplikováním procesu řízení rizik

Řízení rizik

- Otázku řízení rizik jako činnost zahrnující hodnocení rizik

Technická opatření

- Fyzická bezpečnost; kryptografické prostředky; nástroj pro ověřování identity, řízení přístupových oprávnění, ochranu před škodlivým kódem, detekci, sběr a vyhodnocění kybernetických bezpečnostních událostí
- Je součást procesů a celkového systému řízení organizace
- Aplikace na organizaci, Specifický informační a komunikační systém

9 Digitální stopa

Cookies prvních stran ≡ preference uživatele, provoz stránky, analýza

Digitální stopa ≡ soubor informací o činnosti uživatele ve virtuálním prostředí

- *Aktivní*: záměrně sdílená informace (sociální sítě, ...)
- *Pasivní*: bez vědomí, někdy i bez souhlasu (IP adresy, ...)

Lze díky ní sestavit identita každého člověka.

10 Bezpečný software

Splňuje CIA, závislý na modelu hrozeb,

11 Kyber-fyzikální systémy, IoT

Většinou je cílem způsobit fyzickou škodu; přístupy z IT bezpečnosti nelze vždy aplikovat; nízké náklady na bezpečnost

IoT ≡ jakékoliv zařízení, které sbírá data z fyzického světa a sdílí přes Internernet za účelem poskytnutí služeb a informací

CPS - Kyber-fyzikální systémy ≡ snímání, výpočty, řízení, komunikace a analýza za účelem interakce s fyzickým světem

Architektura CBS a vektory útoku

- *Kompromitace senzoru* - falešný signál
- *Útočník mezi senzorem a kontrolérem* - DoS, zpožďování, blokování
- *Kompromitovaný kontrolér* - škodlivé příkazy
- *Útočník zpozdí/ zablokuje řídící příkazy* - DoS
- *Kompromitace akčního členu* - škodlivé/náhodné akce nezávisle na kontroléru
- *Fyzický útok*

11.1 Mirai Botnet

- Botnet z IoT zařízení běžící na linuxu; cílem byly DDoS útoky
- *Fáze skenování* - Rychlé skenování asynchronně; packety na generované IPv4
- *Fáze Brute-force* - zkokuší přihlašovací údaje
- *Fáze instalace* - nahrán malware
- Mirai snaží zakrýt svou přítomnost - maže binárky, kill procesy,

11.2 Detekce útoků proti CPS

- *Remote attestation* - ověření aktuálního vnitřního stavu (RAM)
- *Network intrusion detection* - sledování interakcí zařízení CPS (jednoduché síťové chování)
- *Active detection* - detekuje anomálie v systému

11.3 Mitigace

Zmírnění poruch

12 Kritická infrastruktura

Modbus

- protokol zasílání zpráv aplikační vrstvy
- *Chybějící autentizace* - vyžaduje pouze platnou adresu a platný kód funkce
- *Chybějící šifrování.* - vše v otevřeném textu
- *Chybějící kontrolní součet zpráv* - možnost poslat podvržené příkazy
- *Chybějící zamezení broadcast zpráv* - možnost DoS
- *Programovatelnost.* - možnost vložení škodlivé logiky

ICCP

DNP3

Stuxnet

Ransomware