

Politika provozu systému Warden

Úvod

1. Sdružení CESNET, z. s. p. o. (dále jen CESNET), jeho členové a ostatní připojené instituce (dále jen organizace) provozují lokální počítačové sítě. Jejich společným zájmem je zajištění zdraví a bezpečnosti svých sítí a do nich připojených zařízení.
2. Tento dokument vymezuje pravidla pro práci se systémem Warden, který je určen pro sdílení informací o bezpečnostních událostech, které byly detekovány v zapojených sítích. Více informací o systému je možné najít na warden.cesnet.cz.

Definice pojmů

1. **Systém Warden** se skládá z hlavního serveru, obstarávajícího veškeré zásadní činnosti (registrace klientů, rušení klientů, registrace nových událostí atd.) a klientů. Klienti se dělí dle práce s informacemi na dva typy - odesílajícího a přijímajícího klienta.
2. **Událost** představuje v systému Warden informaci o zdroji potenciální hrozby zaznamenanou některou ze zapojených organizací. Informace jsou získávány z detekčních systémů provozovaných v síti zapojené organizace.
3. **Server** zajišťuje přijetí a ukládání informací zasílaných klienty. Poskytuje rozhraní pro přístup ke všem platným uloženým událostem. Přístup k událostem uloženým na serveru je chráněn autentizací a je umožněn pouze zapojeným organizacím.
4. **Odesílající klient** je součástí systému Warden. Odesílá na server události zaznamenané nástroji v síti zapojené organizace a určené pro sdílení v systému.
5. **Přijímající klient** je součástí systému Warden. Stahuje (přijímá) ze serveru události zaznamenané v sítích zapojených organizací, které mu bylo umožněno stahovat provozovatelem systému.

Obecná ustanovení

1. Provozovatelem systému Warden je sdružení CESNET.
2. Poskytovateli a uživateli dat jsou zapojené organizace.

Vymezení rolí a povinností subjektů zapojených do systému Warden

Provozovatel systému Warden

1. Provozovatel systému garantuje bezpečnost a přístupnost dat na serveru systému Warden.
2. Provozovatel poskytuje veškeré potřebné informace o systému Warden pomocí stránek warden.cesnet.cz a dalších na stránkách definovaných komunikačních kanálů. Zejména se jedná o informace o nových verzích, funkcích a změnách.
3. Provozovatel zajišťuje funkčnost komunikačních kanálů pro komunikaci s organizacemi zapojenými do spolupráce v rámci systému Warden.
4. Provozovatel je odpovědný za přístupování a odstupování organizací ze systému Warden. Zpracovává přihlášky, aktivuje a deaktivuje přístup do systému. Přihlašuje a odhlašuje klienty poskytovatelů a uživatelů dat.
5. Provozovatel spolupracuje s uživateli a poskytovateli dat na provozování systému Warden. V rámci „best effort“ poskytuje podporu při běžném provozu systému.

6. Provozovatel je odpovědný za řešení nestandardních situací vyskytujících se při provozu systému Warden bez zbytečného prodlení. Vzhledem ke stanovené odpovědnosti má provozovatel právo vyžadovat řešení těchto nestandardních situací také ze strany poskytovatelů a uživatelů dat.

Poskytovatelé dat (správci odesílajících klientů)

1. Poskytovatelé dat zajišťují, aby jejich data zasílaná na server systému Warden odpovídala svou kvalitou platné Politice čistoty dat.
2. Poskytovatelé dat mají povinnost spolupracovat na bázi „best effort“ s provozovatelem systému Warden na řešení všech nestandardních situací vyskytujících se při provozu systému Warden.
3. V případě zjištění problému v systému Warden mají povinnost poskytovatelé dat hlásit tento problém provozovateli pomocí definovaných komunikačních kanálů, které jsou popsány na stránkách warden.cesnet.cz.
4. Poskytovatelé dat ze sítí nespádajících pod poskytovatele připojení CESNET mohou obdržet pouze události dotýkající se pouze jejich sítě, strojů a služeb do ní spadajících.
5. Poskytovatelé dat mají povinnost používat události systému Warden pouze pro potřeby zajištění bezpečnosti a zdraví počítačové sítě a strojů své organizace. Mimo organizaci je možné publikovat pouze statistické informace odvozené z události systému Warden, a to způsobem, který neohrozí bezpečnost ostatních zapojených organizací.

Uživatelé dat (správci přijímacích klientů)

1. Uživatelé dat mají povinnost spolupracovat na bázi „best effort“ s provozovatelem systému Warden na řešení všech nestandardních situací vyskytujících se při provozu systému Warden.
2. V případě zjištění problému v systému Warden mají povinnost uživatelé dat hlásit tento problém provozovateli pomocí definovaných komunikačních kanálů, které jsou popsány na stránkách warden.cesnet.cz.
3. Uživatelé dat ze sítí nespádajících pod poskytovatele připojení CESNET mohou obdržet pouze události dotýkající se pouze jejich sítě, strojů a služeb do ní spadajících.
4. Uživatelé dat mají povinnost používat události systému Warden pouze pro potřeby zajištění bezpečnosti a zdraví počítačové sítě a strojů své organizace. Mimo organizaci je možné publikovat pouze statistické informace odvozené z události systému Warden, a to způsobem, který neohrozí bezpečnost ostatních zapojených organizací.

Zapojení organizace do systému Warden

1. Organizace požadující přístup do systému Warden kontaktuje za tímto účelem provozovatele systému pomocí jednoho z určených kanálů. Detaily procesu zapojení organizace a přesný návod pro připojení jsou popsány na stránkách warden.cesnet.cz.
2. Žádost o registraci klienta je doručena provozovateli pomocí některého z definovaných komunikačních kanálů. Provozovatel následně provede registraci daného klienta.

Odstoupení organizace ze systému Warden

1. V případě odstoupení organizace ze systému Warden je bez zbytečného prodlení zrušeno právo přístupu k Warden serveru pro všechny její přijímací i odesílající klienty. Události

zaslané organizací na server do doby odstoupení zůstávají k dispozici ostatním zapojeným organizacím.

2. Žádost organizace o zrušení registrace klienta je doručena provozovateli pomocí některého z definovaných komunikačních kanálů. Provozovatel následně provede zrušení registrace daného klienta.

Řešení nestandardních situací při provozu systému Warden

1. V případě neplánovaného pádu systému jej provozovatel v co nejkratší možné době vyřeší a následně informuje zapojené instituce o vyřešení problému a celkové době trvání výpadku.
2. V případě odhalení nevalidních dat v systému Warden musí poskytovatel nebo uživatel dat neprodleně kontaktovat provozovatele systému a oznámit mu všechny známé informace o problému s daty. Provozovatel podnikne nezbytné kroky k vyřešení problému.
3. V případě odhalení chybné konfigurace klienta upozorní provozovatel dotčeného poskytovatele nebo uživatele dat a požádá jej o nápravu situace.
4. V případě odhalení chyby ve zdrojovém kódu systému Warden uvědomí její nálezce provozovatele pomocí určených komunikačních kanálů. Provozovatel zajistí v nejbližším možném termínu její opravu a případnou distribuci opraveného kódu.
5. V případě bezpečnostního incidentu uvědomí osoba, která jej odhalila, bezodkladně bezpečnostní oddělení provozovatele i poskytovatele dat pomocí určených komunikačních kanálů.

Dodržování politiky a pravomoci provozovatele systému

1. Vykonavatelem této politiky je sdružení CESNET jako provozovatel systému Warden.
2. Na členství v systému Warden a ani na využívání jeho služeb nevzniká právní nárok.
3. Konečné rozhodnutí ve všech případech náleží sdružení CESNET jako správci systému Warden.
4. V případě závažného porušení pravidel definovaných v tomto dokumentu může provozovatel sdružení přistoupit k bezodkladnému zrušení členství dotčené organizace a jejímu odpojení od poskytovaných služeb.

Odpovědnost

1. Sdružení CESNET jako provozovatel systému Warden neposkytuje žádné garance týkající se dostupnosti a funkčnosti. Systém je provozován na bázi „best effort“ a jeho služby jsou poskytovány bez záruky. Výjimkou jsou pouze oblasti pokryté politikami uvedenými na stránkách warden.cesnet.cz.

Přechodná a závěrečná ustanovení

2. Dokument nabývá platnosti a účinnosti **7. 7. 2014** a je platný v rámci organizací zapojených do projektu Warden.