МЕПСО

ПРИРАЧНИК

Технички прирачник за администратори

Систем за откривање и спречување на сајбер напади базиран на вештачка интелигенција

Придружен материјал за обуката:
„Техничка обука за администратори"

Документ бр. МЕПСО-ПРИ-АДМ-005 · Класификација: Интерна употреба
Сектор за информатичка и сајбер безбедност · МЕПСО АД Скопје

Содржина

1. Вовед

Системските администратори се на првата линија на техничката одбрана на организацијата. Вашите одлуки и практики директно ја определуваат безбедносната положба на целата инфраструктура.

Овој прирачник е наменет за технички персонал одговорен за администрирање и заштита на системите. Ќе покриеме напредни концепти на мрежна и системска безбедност, со посебен акцент на модерните пристапи вклучувајќи вештачка интелигенција во откривањето на закани.

Како оператор на критична инфраструктура, МЕПСО има зголемени безбедносни барања. Заштитата на системите не е само техничка задача — таа е одговорност со последици за безбедноста на националната енергетска мрежа.

Важност на улогата. Администраторите имаат привилегиран пристап и голема одговорност. Една безбедносна пропуст на администраторско ниво може да ја изложи целата инфраструктура. Затоа највисоките безбедносни стандарди се задолжителни.

2. Улогата на системскиот администратор во безбедноста

Администраторот не е само оператор на системи — тој е чувар на безбедноста.

2.1 Клучни одговорности

- ✓ Конфигурирање и одржување на безбедносните контроли
- ✓ Мониторинг на системите за сомнителна активност
- ✓ Управување со пристап и привилегии
- ✓ Применување на безбедносни ажурирања
- ✓ Одговор на безбедносни инциденти
- ✓ Одржување на резервни копии и планови за опоравување

2.2 Принцип на најмала привилегија

Секој корисник и процес треба да има само оние права што му се неопходни. Ова го ограничува потенцијалниот ризик ако сметка биде компромитирана.

> **Критично.** Администраторските привилегии треба да се користат само кога е потребно. Секојдневната работа треба да се извршува со обичен кориснички профил, а административните права да се активираат само за конкретни задачи.

3. Основи на мрежна безбедност

Мрежата е поврзувачкото ткиво на инфраструктурата и честа мета на напади.

3.1 Сегментација на мрежата

Поделбата на мрежата на сегменти ја ограничува можноста напаѓач да се движи слободно. Критичните системи треба да бидат изолирани од помалку безбедните зони.

3.2 Заштитни ѕидови

Заштитните ѕидови ја контролираат мрежната комуникација според дефинирани правила. Правилната конфигурација дозволува само неопходен сообраќај.

Концепт	Намена
Сегментација	Изолација на критични зони
Заштитен ѕид	Контрола на мрежниот сообраќај
VPN	Безбеден далечински пристап
Мониторинг	Следење на мрежната активност

4. Системи за откривање упади (IDS/IPS)

Системите за откривање упади (IDS) и спречување упади (IPS) го следат сообраќајот за знаци на напад.

4.1 Разлика помеѓу IDS и IPS

Систем	Функција
IDS (Detection)	Открива и предупредува за сомнителна активност
IPS (Prevention)	Открива и активно блокира закани

4.2 Методи на откривање

- **Базирано на потписи** — препознавање на познати шеми на напад;
- **Базирано на аномалии** — откривање отстапувања од нормалното однесување;
- **Хибридно** — комбинација на двата пристапа.

> **Предизвик.** Традиционалните системи базирани на потписи не можат да откријат нови, непознати напади. Тука доаѓа предноста на вештачката интелигенција.

5. Вештачка интелигенција во сајбер одбраната

Вештачката интелигенција (ВИ) револуционизира начинот на кој откриваме и одговараме на закани, овозможувајќи откривање на дотогаш непознати напади.

5.1 Предности на ВИ пристапот

- ✓ Откривање на нови, непознати закани преку анализа на однесување
- ✓ Обработка на огромни количини податоци во реално време
- ✓ Намалување на лажни тревоги преку учење
- ✓ Автоматско прилагодување на нови видови напади
- ✓ Брз одговор без човечка интервенција за познати шеми

5.2 Како функционира

Системите базирани на ВИ учат од нормалното однесување на мрежата и системите. Кога ќе забележат отстапување — необичен сообраќај, невообичаени модели на пристап, сомнителни активности — тие предупредуваат или автоматски реагираат.

> **Предност.** За разлика од традиционалните системи што бараат претходно познавање на секоја закана, ВИ може да препознае сомнително однесување што никогаш претходно не било видено, што е клучно против новите напади.

5.3 Улогата на администраторот

ВИ системите се моќни алатки, но бараат стручно управување. Администраторот ги конфигурира, ги следи резултатите, ги истражува предупредувањата и презема соодветни мерки. Технологијата помага, но човечката експертиза останува неопходна.

6. Анализа на логови и мониторинг

Логовите се записи на активностите во системите — непроценлив извор за откривање и истрага на инциденти.

6.1 Што да следите

- ✓ Обиди за најавување (успешни и неуспешни)
- ✓ Промени во конфигурацијата
- ✓ Пристап до чувствителни ресурси
- ✓ Невообичаен мрежен сообраќај
- ✓ Активности со административни привилегии

6.2 Централизиран мониторинг

Собирањето на логови на едно место овозможува подобра анализа и корелација на настани. Систем за управување со безбедносни информации и настани (SIEM) е клучна алатка за ова.

> **Важно.** Логовите се корисни само ако се прегледуваат. Редовниот мониторинг и анализата се клучни за навремено откривање на инциденти.

7. Управување со пристап и привилегии

- ✓ Применувајте го принципот на најмала привилегија
- ✓ Редовно ревидирајте ги правата на пристап
- ✓ Отстранувајте пристап веднаш по престанок на потреба
- ✓ Користете силна автентикација за административни сметки
- ✓ Одвојте ги административните од обичните сметки
- ✓ Евидентирајте ги сите активности со привилегиран пристап

8. Зајакнување на системите (hardening)

Зајакнувањето е процес на намалување на површината за напад преку отстранување на непотребни функции и примена на безбедносни конфигурации.

- ✓ Оневозможете непотребни сервиси и функции
- ✓ Отстранете стандардни сметки и лозинки
- ✓ Применете безбедни конфигурациски поставки
- ✓ Ограничете го мрежниот пристап на минимум
- ✓ Инсталирајте само неопходен софтвер

> **Принцип.** Секоја непотребна функција е потенцијална ранливост. Помалку функции значи помала површина за напад.

9. Управување со безбедносни ажурирања

Навременото применување на безбедносни ажурирања е една од најважните задачи, но бара внимание за да не се наруши работењето.

9.1 Процес на ажурирање

- ✓ Следете ги објавите за безбедносни пропусти
- ✓ Тестирајте ги ажурирањата во контролирана средина прво
- ✓ Планирајте го применувањето за да минимизирате прекини
- ✓ Одржувајте резервна копија пред критични ажурирања
- ✓ Документирајте ги применетите промени

Рамнотежа. Критичните безбедносни ажурирања треба да се применат брзо, но на критична инфраструктура секое ажурирање мора внимателно да се тестира за да не се наруши работењето. Балансот помеѓу безбедност и стабилност е клучен.

10. Одговор на инциденти

Кога ќе се случи инцидент, структуриран одговор ја ограничува штетата.

10.1 Фази на одговор

1. **Идентификација** — препознавање дека се случува инцидент;
2. **Ограничување** — спречување на ширење на штетата;
3. **Искоренување** — отстранување на причината;
4. **Опоравување** — враќање на нормално работење;
5. **Поуки** — анализа за спречување на идни инциденти.

11. Резервни копии и континуитет

- ✓ Одржувајте редовни и тестирани резервни копии
- ✓ Чувајте копии на одвоено, безбедно место
- ✓ Тестирајте го процесот на враќање редовно
- ✓ Имајте план за континуитет на работењето
- ✓ Документирајте ги процедурите за опоравување

12. Најдобри практики

- ✓ Принцип на најмала привилегија насекаде
- ✓ Одбрана во длабочина — повеќе слоеви заштита
- ✓ Редовен мониторинг и анализа на логови
- ✓ Навремено но тестирано применување на ажурирања
- ✓ Силна автентикација за сите привилегирани сметки
- ✓ Редовни и тестирани резервни копии
- ✓ Документирани процедури и планови за одговор

Најчесто поставувани прашања

Дали ВИ системот целосно ја заменува човечката анализа?

> Не. ВИ е моќна алатка што ги открива и приоретизира заканите, но човечката експертиза е неопходна за истрага, одлучување и одговор на сложени ситуации.

Колку често треба да ги прегледувам логовите?

> Критичните предупредувања треба да се прегледуваат веднаш. Редовниот преглед на логовите треба да биде секојдневна практика, поддржана од автоматизирани алатки за корелација и предупредување.

Како да балансирам безбедност и достапност на критична инфраструктура?

> Секое безбедносно ажурирање или промена мора внимателно да се тестира пред примена. Планирајте ги промените за периоди со минимален импакт и секогаш одржувајте резервна копија за брзо враќање.

Што е одбрана во длабочина?

> Стратегија на повеќе слоеви заштита, така што ако еден слој откаже, другите продолжуваат да штитат. Не се потпирате на една единствена мерка.

Зошто административните сметки бараат посебно внимание?

> Затоа што имаат највисоки привилегии. Компромитирана административна сметка му дава на напаѓачот широк пристап. Затоа бараат најсилна заштита и внимателно управување.

Речник

Поим	Значење
IDS	Систем за откривање упади — предупредува за закани
IPS	Систем за спречување упади — активно блокира закани
SIEM	Управување со безбедносни информации и настани
Hardening	Зајакнување — намалување на површината за напад
Сегментација	Поделба на мрежата на изолирани зони
Најмала привилегија	Доделување само на неопходни права
Одбрана во длабочина	Повеќеслојна безбедносна стратегија
Аномалија	Отстапување од нормалното однесување

Безбедност на индустриски контролни системи (SCADA)

Како оператор на електропреносен систем, МЕПСО управува со индустриски контролни системи (SCADA) што го надгледуваат и контролираат преносот на електрична енергија. Овие системи бараат специјализиран безбедносен пристап.

Особености на SCADA безбедноста

- ✓ Достапноста е критична — прекините имаат сериозни последици
- ✓ Многу системи се проектирани пред современите сајбер закани
- ✓ Ажурирањата бараат исклучително внимателно планирање
- ✓ Изолацијата од корпоративните мрежи е клучна
- ✓ Специјализиран мониторинг за оперативните технологии

Заштитни мерки

- ✓ Строга сегментација помеѓу IT и OT (оперативна технологија) мрежите
- ✓ Контролиран и евидентиран пристап до контролните системи
- ✓ Мониторинг специјализиран за индустриски протоколи
- ✓ Планови за одговор прилагодени на критичната природа

> **Критична одговорност.** Безбедноста на индустриските контролни системи има импликации надвор од самата организација — таа влијае на стабилноста на националната енергетска мрежа. Затоа бара највисоко ниво на внимание и експертиза.

Континуирана едукација

Сајбер заканите постојано еволуираат, а нападите на критична инфраструктура стануваат посложени. Администраторите мора континуирано да ги надградуваат своите знаења, да следат нови закани и да ги применуваат најдобрите практики. Оваа обука е дел од таа континуирана професионална надградба.

Практични сценарија за администратори

Сценарио 1: Необичен мрежен сообраќај

ВИ системот за откривање предупредува за необичен модел на сообраќај од внатрешен систем кон непозната надворешна адреса, во невообичаено време.

> **Правилен пристап:** Не го игнорирате предупредувањето. Истражувате го изворот, ја изолирате засегнатата машина ако е потребно, анализирате што предизвикало сообраќајот, и документирате. Ова може да биде знак за компромитиран систем.

Сценарио 2: Барање за итно ажурирање

Објавен е критичен безбедносен пропуст што бара итно ажурирање, но системот е дел од критичната инфраструктура во работен режим.

> **Правилен пристап:** Проценувате го ризикот, тестирате го ажурирањето во контролирана средина, планирате го применувањето за минимален импакт, обезбедувате резервна копија, и применувате со можност за брзо враќање ако настане проблем.

Сценарио 3: Сомнителна административна активност

Логовите покажуваат административна активност од сметка во време кога соодветниот вработен не бил на работа.

Правилен пристап: Веднаш истражувате. Ова може да биде компромитирана сметка. Проверувате со сопственикот на сметката, разгледувате што било направено, и преземате мерки за обезбедување ако се потврди неовластен пристап.

> **Заеднички именител.** Во сите сценарија, клучот е да не се игнорираат предупредувањата, да се истражува темелно, и да се документира. Будноста и структуираниот пристап се основа на ефикасната одбрана.

Заклучок

Како администратор, вие сте клучен чувар на безбедноста на критичната инфраструктура. Комбинацијата на солидни основни практики, модерни алатки вклучувајќи вештачка интелигенција, и постојана будност ја формира ефикасната одбрана.

> **Клучна порака.** Технологијата, вклучувајќи ВИ, е моќна алатка, но вашата експертиза, будност и одговорност се незаменливи. Најдобрата одбрана комбинира напредна технологија со стручно човечко управување.

МЕПСО АД Скопје — Оператор на електропреносниот систем на Северна Македонија
Документ бр. МЕПСО-ПРИ-АДМ-005 · Класификација: Интерна употреба