Политика за сигурност на сървъра

Дата: 01/03/2021

Версия 1.0

Община: Борован

Съдържание

1. Преглед

Неосигурените и уязвими сървъри продължават да бъдат основна входна точка за участниците в злонамерена заплаха. Последователните политики за инсталиране на сървъра, управлението на собствеността и конфигурацията са свързани с правилното изпълнение.

2. Цел

Целта на тази политика е да установи стандарти за базова конфигурация на вътрешно сървърно оборудване, което е собственост и / или се управлява от Община Борован. Ефективното прилагане на тази политика ще сведе до минимум неоторизираният достъп до Община Борован.

3. Обхват

Всички служители, контрагенти, консултанти, временни и други работници трябва да се придържат към тази политика. Тази политика се прилага за сървърно оборудване, което е собственост, експлоатиран или отдаден под наем на Община Борован

Тази политика определя изискванията за оборудване във вътрешната мрежа на Общината.

4. Политика

4.1 Общи изисквания

4.1.1 Всички вътрешни сървъри, разположени в Община Борован, трябва да са собственост на оперативна група, която отговаря за системното администриране. Одобрените ръководства за конфигурация на сървъра трябва да бъдат създадени и поддържани от всяка оперативна група въз основа на бизнес нуждите и одобрени от Община Борован. Оперативните групи трябва да наблюдават спазването на конфигурацията и да прилагат политика за изключения, съобразена с тяхната среда. Всяка оперативна група трябва да установи процес за промяна на конфигурационните ръководства, който включва преглед и одобрение от Община Борован.

Следните елементи трябва да бъдат изпълнени:

- Сървърите трябва да бъдат регистрирани в системата за управление на корпоративното предприятие. Като минимум е необходима следната информация за положително идентифициране на точката на контакт:
  - Контакт (и) и местоположение на сървъра и резервен контакт
  - Хардуер и операционна система / версия
  - Основни функции и приложения, ако е приложимо
- Информацията в системата за управление на корпоративното предприятие трябва да бъде актуализирана.
- Промените в конфигурацията на производствените сървъри трябва да следват съответните процедури за управление на промени.

4.1.2 За целите на сигурността, спазването и поддръжката, упълномощеният персонал може да наблюдава и одитира оборудване, системи, процеси и мрежов трафик.

4.2 Изисквания за конфигуриране

4.2.1 Конфигурацията на операционната система трябва да бъде в съответствие с одобрените указания на Община Борован.

4.2.2 Услугите и приложенията, които няма да бъдат използвани, трябва да бъдат деактивирани, където е възможно.

4.2.3 Достъпът до услуги трябва да бъде регистриран и / или защитен чрез методи за контрол на достъпа, като защитна стена на уеб приложение, ако е възможно.

4.2.4 Най-новите актуализации за сигурност трябва да бъдат инсталирани в системата възможно най-скоро, като единственото изключение е, когато незабавното приложение би нарушило бизнес изискванията.

4.2.5 Доверителните връзки между системите представляват риск за сигурността и тяхното използване трябва да се избягва. Не използвайте доверителни отношения, когато някакъв друг метод за комуникация е достатъчен.

4.2.6 Винаги използвайте стандартни принципи за сигурност с най-малко необходимия достъп, за да изпълнявате функция. Не използвайте root, когато няма привилегирован акаунт.

4.2.7 Ако е налице методология за сигурна връзка (т.е. технически осъществима), привилегированият достъп трябва да се осъществява по защитени канали (например, криптирани мрежови връзки, използващи SSH или IPSec).

4.2.8 Сървърите трябва да бъдат физически разположени в среда с контролиран достъп.

4.2.9 Изрично забранено е сървърите да работят от неконтролирани помещения

4.3 Мониторинг

4.3.1 Всички събития, свързани със сигурността на критични или чувствителни системи, трябва да бъдат регистрирани, а процедурите за одит да бъдат записани, както следва:

- Всички дневници, свързани със сигурността, ще се съхраняват онлайн най-малко 1 седмица.
- Ежедневните резервни копия ще се запазват най-малко 1 месец.
- Седмичните резервни копия ще се запазват най-малко 1 месец.
- Месечните пълни резервни копия ще бъдат запазени минимум 2 години.

4.3.2 Събитията, свързани със сигурността, ще бъдат докладвани на ИТ Отедла, който ще преглежда регистрационните файлове и ще докладва инциденти на ИТ мениджмънта. При необходимост ще бъдат предписани коригиращи мерки. Събитията, свързани със сигурността, включват, но не се ограничават до:

- Порт сканиране атаки.
- Доказателство за неоторизиран достъп до привилегировани акаунти.
- Аномални събития, които не са свързани с конкретни приложения на хоста.

5. Съответствие с политиката

5.1 Измерване на съответствие

Екипът на Община Борован ще проверява спазването на тази политика чрез различни методи, включително, но не само, периодично тестване, отчети за бизнес инструменти, вътрешни и външни одити и обратна връзка към собственика на политиката.

5.2 Изключения

Всяко изключение от правилата трябва да бъде одобрено от екипа на Община Борован предварително.

5.3 Несъответствие

Служител, за когото е установено, че е нарушил тази политика, може да бъде обект на дисциплинарни мерки, включително до прекратяване на работата.