До
Фирмите
Закупили документация
На вниманието на:

Контакт: Бончо Георгиев
Тел. номер: +359 32 278502
Дата: 08.08.2014
Изх. №:

Относно: Отговор на въпроси свързани с документация по система за предварителен подбор

Уважаеми Дами и Господа,

Във връзка със система за предварителен подбор № С-14-НМ-Д-123 с предмет: Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери" и на основание на получено писмо със запитвания с вх. №6676 от 05.08.2014 г. отговаряме по следния начин:

Въпрос 1: *Във връзка с Eman III: Решение за избор на Изпълнител и сключване на договор до Документацията за участие в системата за предварителен подбор на изпълнители с №* С-14-НМ-Д-123
12.4. *Сертификат за задължително издържан IT секюрити тест(Security Evaluation Smart Meter Infrastructure) издаден от Riscure B.V., Адрес: Delftechpark 49, 2628 XJDelft Nederlands (Холандия), Т:+31 15251 4090, www. Riscure.com, като необходимо условие за изпълнение на поръчката съгласно 3-Н Защита на личните данни. Таксата при изпълнителя на теста е за сметка на Възлжителя*
Въпрос: Моля да представите методиката за тестване по IT секюрити тест.

Отговор въпрос 1: It Security test ще се проведе в следните фази
1.Анализ на рисковете
2.Дефиниция на тестови сценарии
3.Подготовка на тестова среда и провеждане на тестовете
Възможно е да бъдат направени оценки на сигурността от различни гледни точки White Box, Grey Box или Black Box. .
При White Box, тестовете,чрез предоставяне на информация от Участника в процедурата за вътрешното функциониране на продуктите се осигурява възможност за идентифициране на възможни уязвимости в сигурността по-бързо/по-ефективно..
Grey Box penetration тестовете се фокусират ефективно върху най-вероятните слабости(low-hanging fruit).
Black Box тестовете за сигурност се извършват без задълбочени познания за устройствата и по тази причина са необходими усилия за "reverse engineering" на устройствата.Black Box тестването е по-вероятно да не може да установи възможни уязвимости в сигурността затова за Възложителят представлява интерес да извърши поне Grey Box тестване на продуктите
При стъпка 1 анализ на рисковете ще бъдат анализирани и оценени рисковете, които трябва ще бъдат тествани.Анализът е на база техническите изисквания на Възложителя
При стъпка 2 ще бъде изградена тестова среда и ще бъдат проведени тестове.Функционираща end-to-end или частично настроена тестова среда ще бъде използване за да се атакува със средств,а с които и хакер ще може да атакува
Тестовете може да бъдат както физически така и логически атаки:
А) Физическото тестване на компонентите в инфраструктурата Smart електромер,комуникационни модули, концентратори и централна система.То включва например дали хардуерни security функции се прилагат и използват по правилен начин.Тест дали Fuzzing messages към порт се отразяват на работата на устройството
Б) Логическо тестване на компонентите в инфраструктурата Smart електромер,комуникационни модули, концентратор и централна система и техните интерфейси.То включва например тестване на имплементираните протоколи и устойчивостта им срещу невалидни инструкции.Fuzzing на интерфейсите с цел да се установи дали софтуера управляващ интерфейсите е устойчив.

При стъпка 3 ще се изготви тестова среда и ще се проведат тестове

Въпрос 2: *Във връзка с I. Функционални изисквания към Система за дистанционно отчитане от Въпросника за подбор, стр.2*

1. *Автоматично отчитане – В графика за отчитане да се определя кои електромери кога трябва да се отчетат.*
   Въпрос: Моля, разяснете – може би имате в предвид кои профили да се отчитат, а не кои електромери?

Отговор на въпрос 2: Графикът за отчитане, в случай на дефиниране на такъв в централната система при режим на отчитане "PULL", времевите рамки за отчет ,списък от уреди и данните от уредите определени за отчитане, които следва да бъдат доставени съгласно регламентираните в графика срокове. Т.е графикът се отнася за списък от уреди за които се определят необходимите за отчитане данни (регистърни стойности, товарови профили, събития,

Въпрос 3: *Във връзка с V. Изисквания за сигурност за дистанционно отчитане на електромери и системи за управление на ЕВН БГ ЕР от Въпросника за подбор, стр. 30:*
Запазената информация, която вече не е важна/необходима трябва да бъде изтривана.
Въпрос: Моля, разяснете след какъв интервал да се изтрива?

Отговор на въпрос 3: Информацията, свързана с качеството на връзката,logove на комуникация и др.,която е съхранена и вече не е необходима, следва да бъде запазвана не повече от 12 месеца

Въпрос 4: *Във връзка с Изисквания за сигурност за дистанционно отчитане на електромери и системи за управление за ЕВН БГ ЕР от Въпросника за подбор, стр.30:*
4. Деликатни/лични данни от Е-електромер трябва да може в срок от не повече от 12 часа да се прехвърлят и запазват в Централната система.
Въпрос: Моля разяснете кои данни са деликатни?

Отговор на въпрос 4: За деликатни, лични данни, следва да се има предвид товаровите профили регистрирани от средствата за измерване.

Въпрос 5: *Във връзка с Изисквания за сигурност за дистанционно отчитане на електромери и системи за управление за ЕВН БГ ЕР от Въпросника за подбор, стр. 48:*
99. При софтуера следва да се прилага принципа на 4-те очи за особено важните функции на централната система. Най-съществените функции на системата, които се нуждаят от потвърждение преди изпълнението си, трябва да бъдат конфигурирани по начин, който налага присъствието на поне 2 служители, които да одобрят съответните дейности, преди започване на тяхното изпълнение (пример: процес за прекъсване на електричеството).
Въпрос: Моля посочете минималния брой и видове операции, върху които следва да се приложи принципа на 4-те очи?

Отговор на въпрос 5: Принципът на 4_те очи следва да се разглежда по следния начин.Конфигуриране от един оператор на системата действие, параметър или batch job ,след това разрешение от друг оператор Едва с разрешението от втория оператор действието, параметър или batch job трябва да се активират.
Принципът на „4-те очи" следва да бъде прилаган при команди за включване/изключване на потреблението.
Изпращане на групови команди за включване/изключване трябва да бъде възможно единствено след конфигуриране от 1 оператор, потвърждаване на изпълнението от 2-ри оператор на централната система.
Принципът на „4-те очи" следва да бъде прилаган и при конфигуриране на максималния брой електромери, на които може да бъде прекъснато захранването в рамките на един ден.Един оператор конфигурира броя на електромерите, друг оператор одобрява/разрешава/ този брой
Принципът на „4-те очи" следва да бъде прилаган и при актуализация на firmware на електромерите чрез централната система /Отдалечен firmwaredownload/

С уважение,
Бончо Георгиев
Експерт Логистика, отдел Снабдяване

ЕВН България Електроразпределение ЕАД
EVN
1