ЦАПК ПРОГРЕС ГРУП АД
Адрес за контакти:
София, 1574, бул."Шипченски проход " №69А, п.к. 14, БЪЛГАРИЯ
Microsoft® Златен сертифициран партньор:
Microsoft ® Доставчик на облачни решения
Microsoft® Оторизиран партньор за сферата на образованието
DELL EMC Златен партньор
тел: (02) 8704159; (02) 8709111; (02)8705257
факс: (02) 9733853
Електронна поща: cadrd@progress.bg

CAD R&D CENTRE PROGRESS GROUP
For contacts:
69A, Shipchenski prohod Blvd., Sofia 1574, P.O. BOX 14, BULGARIA
Microsoft® Gold Competency Partner:
Microsoft® Cloud Solution Provider (CSP)
Microsoft® Authorized Education Partner (AEP)
DELL EMC Gold Partner
Phone: +35928704159; +35928709111; +3592 8705257
Fax: +35929733853
E-mail: cadrd@progress.bg

http://www.progress.bg

ЕИК 202604898 **UIN 202604898**

Автоматизиран процес на управление на информационната сигурност съгласно Наредба за минималните изисквания за мрежова и информационна сигурност ма Министерски съвет. № 186 от 19 Юли 2019 г.

Въведение:

На 19.07.2019 г. е обнародвана Наредба за минималните изисквания за мрежова и информационна сигурност (Постановление № 186 на Министерски съвет на Република България). Наредбата се прилага в следните субекти: административните органи; операторите на съществени услуги по смисъла на Закона за киберсигурност относно техните мрежи и информационни системи, използвани при предоставянето на съществени услуги; доставчиците на цифрови услуги по смисъла на Закона за киберсигурност относно техните мрежи и информационни системи, използвани при предоставянето на цифрови услуги; лицата, осъществяващи публични функции, които не са определени като оператори на съществени услуги по смисъла на Закона за киберсигурност, когато тези лица предоставят административни услуги по електронен път; организациите, предоставящи обществени услуги, които не са определени като оператори на съществени услуги или не са доставчици на цифрови услуги по смисъла на Закона за киберсигурност, когато тези организации предоставят административни услуги по електронен път. Изискванията по наредбата за задължителни от 19 Ноември 2019 г..

Настоящото предложение е за автоматизиране на процеса за управление на информационната сигурност съгласно наредбата от доставчик на услуги.

Общо състояние

Мерките за мрежова и информационна сигурност са организационни, технологични и технически и се прилагат в съответствие със спецификата на дейността. Под информационна сигурност се разбира запазване на достъпността, интегритета (цялостност и наличност) и конфиденциалността на информацията по време на целия й жизнен цикъл (създаване, обработване, съхранение, пренасяне и унищожение).

Информационната сигурност не бива да се разглежда като цел, а по скоро като непрекъснат процес изискващ действия и проверки.

Целта на наредбата е разработването, поддържането и функционирането на комплексна система от мерки за управление и поддръжка на информационната сигурност. Условията описани в наредбата, до голяма степен са и изисквания на международния стандарт за информационна сигурност БДС ISO/IEC 27001.

Предложението е за автоматизиране на процеса на изграждане и поддържка на функционираща система за информационна сигурност, в съответствие с наредбата, при множество субекти.

Цели:

Основната цел е изграждане и поддръжка на системи за информационна сигурност удовлетворяващи изискванията на наредбата по автоматизиран способ. Посредством работещите и поддържани системи се очаква намаляване на инцидентите с информационната сигурност, оценка на риска и овладяване на рисковете и възможностите.

Цел на настоящото решение

Да покаже възможностите за автоматизирано привеждане на информационните системи в съответствие с наредбата, както и последващата им поддръжка от страна на доставчик на услуги в множество субекти, включени в обхвата на наредбата.

В дейностите са включени:

1. Извършване на одит на текущото състояние на информационната сигурност на организацията спрямо наредбата;
2. Въвеждане на мерки свързани с информационната сигурност, вследствие на резултатите от одита;
3. Автоматизиран процес на следене изпълнението на мерките по информационна сигурност;
4. Периодични оценки нивото на съответствие на информационната сигурност с изискванията на наредбата;
5. Извършване на одит в края на планиран период.

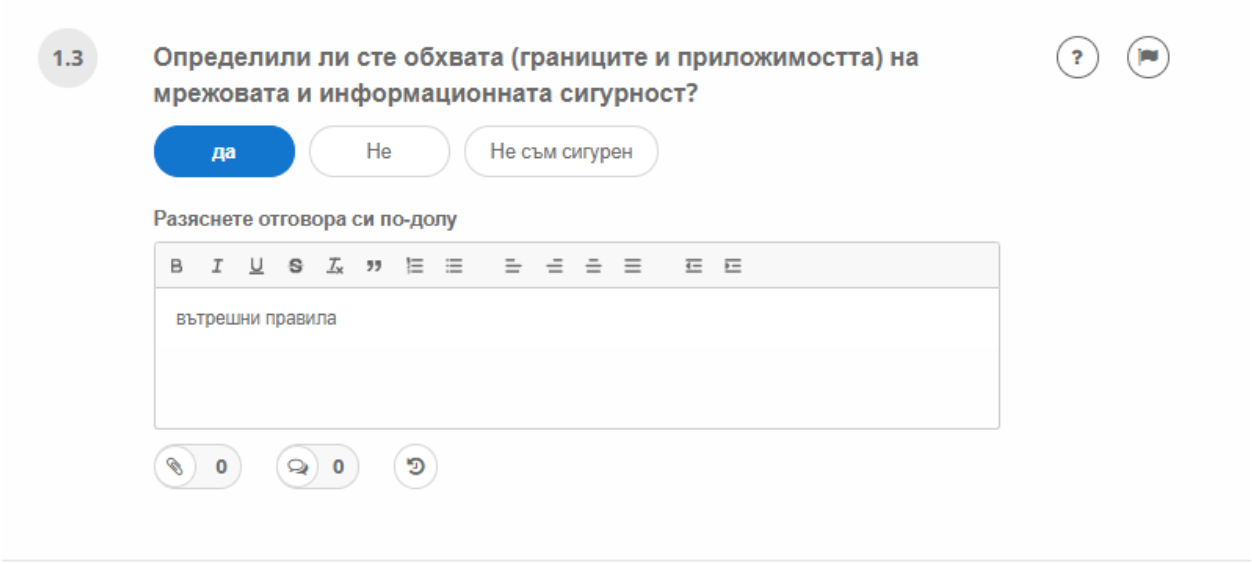
Решение

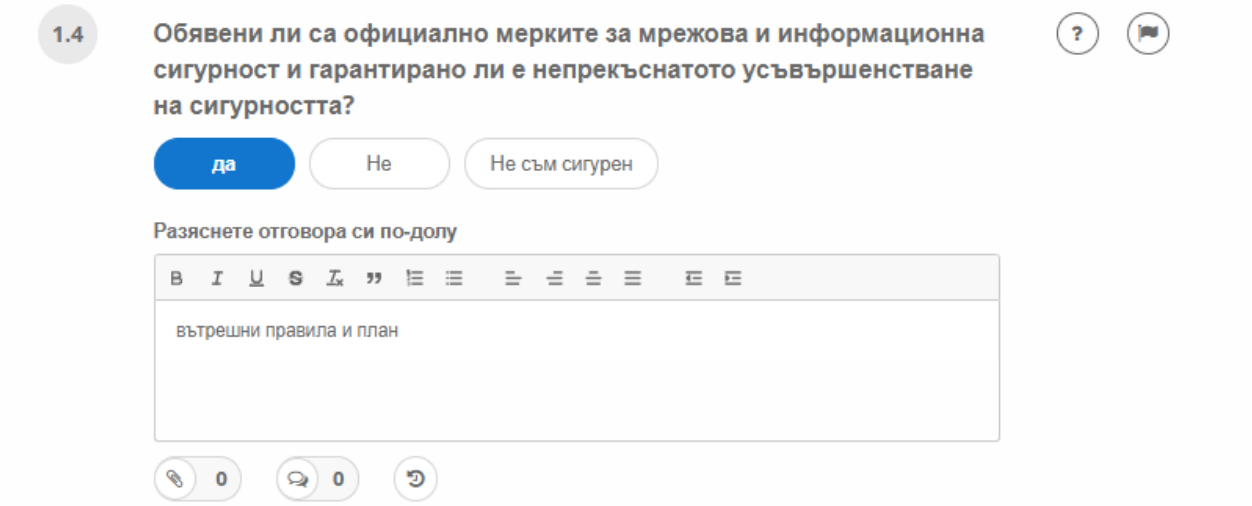
Решението преминава през няколко етапа, свързани в логическа последователност. Извършването на дейности през всички етапи се осъществяват съвместно от доставчика на услугата, както и отговорни лица от субектите.

1. Етап - извършване на одит

Извършването на одит има за цел да се заснеме текущото състояние на информационната сигурност. Одита е насочен към установяване на съответствие на текущото състояние към изискванията на наредбата. Одита се извършва на база на въпроси и отговори. Въпросите са така подбрани, че са обхванати изискванията на наредбата в пълня и обем. Възможните отговори на въпросите са „Да“ или „Не“. Отговорите се получават от оторизирани лица на субекта със съответното ниво на знания за съществуващата ИТ инфраструктура. Одита е съществена и основополагаща част за последващите дейности по управление на информационната сигурност.

Визуализация на интерфейс за въпроси:





2. Етап - Въвеждане на мерки свързани с информационната сигурност.

На база на проведените одити се набелязват мерки за подобряване на информационната сигурност. Набелязването на мерки се извършва от съвместен екип на субекта и консултантите. При набелязването на мерки се дефинират срокове за извършването на дейностите и отговорни лица. Мерките са така планирани, че да бъде постигнато необходимото ниво на информационна сигурност според наредбата. Определянето на конкретните мерки със съответните отговорници и срокове, след съгласие със всички страни, се отбелязва в софтуерния продукт за автоматизация на процеса, управление и поддръжка на информационната сигурност. На този етап е необходимо да се определи и бюджета за набелязаните мерки.

3. Етап - Автоматизиране на процеса на следене изпълнението на мерките по информационна сигурност.

След като мерките за информационна сигурност са набелязани коректно, автоматично се проследяват и отчитат реално извършените действия и резултатите от тях. Периода на проверка може да е свободно избран но препоръчително е три месеца, поради естеството на дейностите. Препоръчителните първи мерки за изпълнение са: полагане на цели за информационна сигурност, описание на активи на субекта/ползвателя, конкретизиране на заплахи и уязвимости, налични или планирани защити, управление на рисковете и план за справяне с инциденти.

Примерна извадка от детайлен отчет за проверка (първоначална или периодична):

Детайли на оценката

ID 9

Наименование Одит към Наредба за минималните изисквания за мрежова и информационна сигурност - Областна администрация Добрич

Организация CAD R&D Progress Group JSC

Описание

Утвърждаващ Boris Hristov

Отговарящ Plamen Stanev

Шаблон ISO 27001 Audit Checklist - 1.1 BG

Създаден от Borislav Kalchev

Дата на създаване 02/20/2020 05:57 PM

Краен срок

Дата на завършване

Дата на подаване 02/26/2020 10:08 PM

Етап Преглед

Брой рискове много високо ниво 0

Брой рискове високо ниво 0

Брой рискове средно ниво 52

Брой рискове ниско ниво 0

Общ брой рискове 52

Общо ниво на риск Средно

Обща оценка на риска 2.0

Резултат

Коментари на резултата

Основен идентификатор на записа

Основно име на записа

Версия на шаблона 2

Версия на проекта 1

Брой идентифицирани рискове 52

Брой отворени заявки за допълнителна информация 0

Маркери

Въпросник

1 4 Контекст на организацията

1.1 **Документирали ли сте външните и вътрешните фактори свързани с целите на организацията и влияещи на мрежовата и информационната сигурност?**

Отговор

Не съм сигурен

Разяснения

н/а

Рискове

Присъщо ниво на риска
2.0

Ниво на остатъчен риск
2.0

Описание на риска

Заплаха

State
IDENTIFIED

Собственик на риска

Краен срок за отстраняване на риска

План за оздравяване

Оздравяване

Резултат

Дата на затваряне

4. Етап - Текущи оценки нивото на съответствие на информационната сигурност с изискванията на наредбата.

Текущите проверки на нивото на информационната сигурност и съответствието спрямо наредбата може да са планирани и непланирани. Планираните проверки се извършват по предварително утвърден график или при изпълнение и приключване на дейностите по някоя от мерките. Непланираните проверки се извършват при нововъведения свързани с дейността и касаещи информационната сигурност или при сериозни инциденти. Текущите проверки могат да бъдат само върху областта на информационната сигурност, която е засегната от мерките, промените или инцидентите.

5. Етап - Извършване на одит в края на планиран период.

Съгласно наредбата, пълен одит на информационната сигурност и спазването на указанията на наредбата, се извършва планирано, минимум веднъж годишно. Извършва се и съпоставка на нивата на информационната сигурност в началото и в края на планирания период.

Роли и отговорности

Собственик на проекта – Възложител, организацията която финансира процеса на автоматизирано управление на информационната сигурност.

Субект на проверката – организациите, в които е задължително да се прилага наредбата, отговорни за извършване на дейностите по информационна сигурност, за постигане на съответствие с наредбата.

Контролиращ дейностите орган – Организация с делегирани административни правомощия върху субектите.

Доставчик на услуги - извършва дейности по одитиране, консултантски услуги, набелязване на мерки, следене на графика за извършване на набелязаните мерки, отчитане на извършените мерки, извършване на повторни одити.

Срокове

Периода за извършване на дейностите е минимум една година.

Поради комплексността на мерките и изпълнението им, препоръчителният период е три години

Поддръжката на информационна сигурност е постоянен процес и автоматизирането на поддръжката би спомогнало за осъществяване на целите през целия период на съществуване на субекта.

В автоматизирания продукт са налични разработени въпроси за съответствие на текущото състояние към изискванията на наредбата и дейностите по предложения модел, които могат да стартират веднага.

Рискове и ограничения

Различни нива на информационна сигурност в различните субекти.

Недостатъчно време за изпълнение на дейностите по превеждане на информационната сигурност според изискванията на наредбата.

Отказ от съдействие от страна на субектите.

Подаване на некоректна информация по време на одитите.

Недостиг на средства в планираните бюджети за информационна сигурност при субектите.

Необходимост от допълнителни консултантски услуги при субектите.

Компетентност на персонала при субектите.

Финансова стойност

Стойността на предложеното решение се базира на следните елементи:

Абонаментна такса за поддръжка на средството за автоматизация – абонаментната такса е фиксирана за 1 година и не се влияе от броя на субектите.

Консултантски услуги от страна на доставчика на услуги – измерват се в часове.

Заетост на персонала на субектите, свързана с информационната сигурност - измерват се в часове.

За ЦАПК ПРОГРЕС ГРУП АД

ЦАПК ПРОГРЕС ГРУП АД е водеща българска компания с дългогодишен опит в сферата на Информационните Технологии.

Основните дейности на компанията са предоставянето на комплексни решения в сферата на ИКТ, които включват: софтуерна и хардуерна поддръжка; разработка; инженеринг; инсталиране, обслужване, промяна, корекции, поддръжка на компютърни инфраструктури, бази данни и програмни системи на клиенти и на водещи в областта на ИКТ производители; хостинг и колокация; обучение и образование в сферата на ИКТ; консултантски услуги в областта на ИКТ; търговия с техническо и програмно осигуряване за ИКТ.

През последните години, компанията се фокусира в предоставянето на консултантски услуги и извършване на одит на информационната среда, в съответствие с изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност. Също така, компанията предоставя консултантски услуги, във връзка с изискванията на Общата Регулация за защита на личните данни (GDPR).

През текущата 2020 г., фирма ЦАПК ПРОГРЕС ГРУП АД изпълни два консултантски проекта с предмет: „Извършване на одит на информационната среда, в съответствие с изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност“:

- Извършване на одит на информационната среда на Администрацията на Народното събрание, в съответствие с изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност;
- Вътрешен одит на мрежовата и информационната сигурност на Комисията за защита от дискриминация, в съответствие с чл. 35, ал. 1, т.1 от Наредбата за минималните изисквания за мрежова и информационна сигурност.

Два пилотни проекта за извършване на одит на информационната среда, в съответствие с изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност, са в процес на изпълнение от страна на фирма ЦАПК ПРОГРЕС ГРУП АД към настоящия момент. Бенефициенти на проектите са Областна администрация Бургас и Областна администрация Добрич.

През м. Ноември 2019 г., служители на фирма ЦАПК ПРОГРЕС ГРУП АД, проведоха учебни курсове (workshops) на служители на Електроенергиен Системен Оператор ЕАД

Дейностите на компанията се изпълняват в съответствие с международно-приети стандарти за управление на качеството БДС EN ISO 9001:2008, управление на сигурността на информацията ISO/IEC 27001:2017 и управление на услугите ISO/IEC 20000-1:2011. ЦАПК ПРОГРЕС ГРУП АД е сертифицирана по съответните международно-приети стандарти и разполага със сертифицирани специалисти, които редовно преминават съответните обучителни курсове и сертификационни изпити. Фирма ЦАПК ПРОГРЕС ГРУП АД стриктно спазва изискванията на Общата Регулация за защита на личните данни (GDPR), налице са стриктни политики и вътрешно-фирмени процедури за спазването на регламента, както и съответните отговорни служители. Регулярно се провеждат обучения на служителите на компанията, във връзка с горе-цитираните международни стандарти и регулации.