

ТЕХНИЧЕСКИ ИЗИСКВАНИЯ

КЪМ

ОБЩЕСТВЕНА ПОРЪЧКА

С предмет: „Наблюдение, анализ и оценка на кибер сигурността на комуникационната и информационната инфраструктура на ВВС и реакция при кибер инциденти“.

1. Услугата обхваща комуникационната и информационната инфраструктура на ВВС, в които се създава, обработва, съхранява и обменя неklasифицирана информация, в това число и мрежите с достъп до Интернет и включва следните функционалности:

- Наблюдение на комуникационните и информационните ресурси в режим 24/7/365;
- Автоматизиран анализ на метаданни, базирани на журнална информация и тяхното корелиране;
- Оценка на сигурността на комуникационната и информационната инфраструктура при въздействие на кибер атака върху услугите и системите на ВВС;
- Анализ и управление на уязвимостите, чрез ежемесечно сканиране на комуникационно информационната структура;
- Предоставяне на периодични доклади за открити уязвимости и мерките за тяхното преодоляване;
- Откриване на кибер атаки в реално време, с възможност за дефиниране на целта и риска от кибер атаката;
- Изготвяне на препоръки и насоки след възникнал конкретен инцидент, свързан със сигурността;
- Изготвяне и предоставяне на детайлни доклади и препоръки за предотвратяването на злонамерени действия срещу комуникационните и информационните ресурси;
- Изготвяне и предоставяне на разширени анализи за кибер атаките, включващи информация за вектора/източника на атаката, експозиция към атаката и оценка на въздействието;
- Изготвянето на експертизи в случай на кибер престъпления и/или подпомагане на ВВС за тяхното изготвяне;
- Своевременно уведомяване при откриване на критични уязвимости или кибер заплахи;
- Провеждане на специализирани обучения на служители на ВВС на добри практики за кибер сигурност.

2. Дейности за изпълнение:

- Първоначален оглед и оценка на място на съществуващата инфраструктура на ВВС с достъп до Интернет.

- Разполагане (инсталиране) на сензори за събиране и изпращане на метаданни към Център за управление на сигурността (ЦУС).

3. Срок на изпълнение.

- Срок за изпълнение - 1 (една) година, считано от датата на сключване на договора.

4. Съдържание и обем на услугите.

№	Услугата включва следните функционалности	Дейности
1.	Първоначален оглед и оценка на мястото на съществуващата инфраструктура на ВВС с достъп до Интернет	Ще се извърши първоначален оглед, запознаване и оценка на съществуващата инфраструктура на ВВС с достъп до Интернет.
2.	Разполагане (инсталиране) на сензори за събиране и изпращане на метаданни към Център за Управление на Сигурността (ЦУС)	След първоначалният оглед и анализ на съществуващата инфраструктура на ВВС с достъп до Интернет ще се инсталира и интегрира сензор/и за събиране на логове в инфраструктурата на ВВС. По този начин ще се събира и анализира логовете и ще се изпращат мета данни до Центъра за Управление на Сигурността (ЦУС) за по-нататъшен анализ.
3.	Наблюдение на комуникационните и информационните ресурси в режим 24/7/365	Ще се извършва наблюдение на комуникационните и информационните ресурси в режим 24/7/365, чрез колекция, агрегиране и корелиране на логовете, генерирани от ресурсите. Тези действия ще се осъществяват чрез SIEM (Security Incident and Event Management) сензор, разположен в инфраструктурата на ВВС, където ще се съхраняват всички събрани лог-файлове.
4.	Автоматизиран анализ на метаданни, базирани на журнална информация и тяхното корелиране	Ще се осъществява автоматизиран анализ на метаданни, базирани на журнална информация и тяхното корелиране. Ще се извърши този анализ чрез първоначална обработка в самият SIEM сензор, намиращ се в инфраструктурата на ВВС. По-нататъшната обработка, включително разследването от експертния екип ще се извършва в работещият 24/7 „ЦУС“.
5.	Оценка на сигурността на комуникационната и информационната инфраструктура при въздействие на кибер атака върху услугите и системите на ВВС	Специализиран екип ще извършва оценката на сигурността на комуникационната и информационната инфраструктура при въздействие на кибер атака върху услугите и системите на ВВС, на базата на специално разработена методология за оценка, съдържаща контроли свързани с ISO 27001, NIST и COBIT. Тези контроли ще бъдат оценени чрез провеждане на интервюта и технически огледи на комуникационната и информационната инфраструктура.
6.	Анализ и управление на уязвимостите, чрез ежемесечно сканиране на комуникационно информационната структура	Ще се осъществява анализ и управление на уязвимостите, чрез ежемесечно сканиране на комуникационно информационната структура. Ежемесечно ще се извършва сканиране на външните Интернет на IP адреси на ВВС.
7.	Предоставяне на регулярни структурни доклади за открити уязвимости и мерките за тяхното преодоляване	Ще се предоставят регулярни структурирани доклади за открити уязвимости и мерките за тяхното преодоляване. Резултатите от ежемесечното сканиране на

№	Услугата включва следните функционалности	Дейности
		<p>външните Интернет IP адреси ще бъде предоставен във вид на доклад на ВВС, за да могат откритите уязвимости да бъдат адресирани и управлявани от администраторския екип на Възложителя.</p> <p>Всички открити уязвимости ще бъдат придружени с препоръки за възможното им преодоляване.</p>
8.	Изготвяне на препоръки и насоки след възникнал конкретен инцидент, свързан със сигурността	<p>Ще се изготвят препоръки и насоки след възникнал конкретен инцидент, свързан със сигурност.</p> <p>Всеки регистриран инцидент ще бъде анализиран от експертния екип на „ЦУС“ и ще бъде изпратен анализа, както и препоръки за адресирането на инцидента.</p>
9.	Изготвяне и предоставяне на детайлни доклади и препоръки за предотвратяването на злонамерени действия срещу комуникационните и информационните ресурси	<p>Ще се изготвят и предоставят детайлни доклади и препоръки за предотвратяването на злонамерени действия срещу комуникационните и информационните ресурси</p>
10.	Изготвяне и предоставяне на разширени анализи за кибер атаките, включващи информация за вектора/източника на атаката, експозиция към атаката и оценка на въздействието	<p>Ще се изготвят и предоставят разширени анализи за кибер атаките, включващи информация за вектора/източника на атаката, експозиция към атаката и оценка на въздействието.</p> <p>При детектиране на атака от рода на сканиране на портове, сканиране на услуги, brute-force атаки на базата на анализиранияте логове ще се идентифицира източника на атаката и ще се извърши оценка на потенциалното въздействие.</p>
11.	Своевременно уведомяване при откриване на критични уязвимост или кибер заплахи	<p>Ежемесечно ще се изготвя и предоставя доклад, описващ по-важните открити уязвимости и кибер заплахи/атаки в световен мащаб, а когато има оповестена критична атака или уязвимост, ще се изготви доклад незабавно. Тези доклади ще бъдат предоставени на ВВС, за да могат да бъдат взети по-нататъшни мерки от екипа, администриращ системите.</p>
12.	Провеждаме на специализирани обучения на служители на ВВС на добри практики за кибер сигурност	<p>Ще се проведе специализирано обучение по кибер сигурност на служители на ВВС.</p> <p>Темите, периода, броя на служителите и мястото на провеждане на обучението ще бъдат уточнени между Възложителя и Изпълнителя.</p>
13.	Извършване на тестове за предоставяне на услугата	<p>Провеждането на окончателният тест за предоставяне на услугата ще бъде извършен през последните 30 дни от срока за изпълнение на договора.</p> <p>Резултатите от теста ще бъдат отразени в доклад.</p>