					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P40					Заглавие на документа: **Политика за тестване на сигурността и red teaming**							
Версия: 1.0		Дата на влизане в сила: 01.01.2025			Собственик на документа:							
X	Политика		Стандарт		Процедура		Формуляр		Регистър		Друго	

История на редакциите				
Номер на редакцията	**Дата на редакцията**	**Промени**	**Прегледано от**	**Собственик на процеса**

Одобрения			
Име	**Длъжност**	**Дата**	**Подпис**

Съгласуване със стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	9.1, 9.2, 9.3	
ISO/IEC 27002:2022	5.7, 5.36, 8.8, 8.29, 8.30, 8.1	
NIST SP 800-53 Rev.5	CA-2, CA-7, CA-8, RA-5	
GDPR на ЕС	Чл. 32(1)(d)	
NIS2 на ЕС	Чл. 21(2)(f)	
DORA на ЕС	Чл. 25–27	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Цел

1 Да се определи структурирана програма за регулярно тестване на сигурността на мрежите, системите и приложенията на организацията, включително анализ на уязвимости, тестове за проникване и упражнения тип red team, с цел изпълнение на изискванията на член 21(2)(f) от NIS2 относно оценяването на ефективността на мерките за киберсигурност.

1.1 Да се гарантира, че слабостите в техническите и организационните мерки се идентифицират и отстраняват проактивно чрез контролирано тестване, като по този начин се осигурява непрекъснато подобрение на рисковата позиция на организацията по отношение на сигурността.

2. Обхват

2 Тази политика обхваща всички критични информационни системи, приложения и поддържаща инфраструктура, които са собственост на организацията или се експлоатират от нея. Тя включва и тестване на физическата сигурност на обекти, когато това е относимо към киберсигурността (напр. социално инженерство или физически тестове за проникване, ако попадат в обхвата на упражнения тип red team).

2.1 Политиката се прилага за вътрешните екипи по сигурността, всички външни изпълнители по договор, ангажирани с тестване на сигурността, и съответните собственици на системи/приложения. Всички дейности по тестване трябва да бъдат разрешени и да се изпълняват в съответствие с процедурите по тази политика, за да се избегнат непредвидени прекъсвания.

3. Цели

3 Да се провери ефективността на контролите и на приложените мерки за киберсигурност (технически, оперативни и организационни) чрез периодично тестване и симулации, в съответствие с изискването на NIS2 за измерване на ефективността.

3.1 Да се идентифицират уязвимости или пропуски, които редовните оперативни процеси може да не открият, включително zero-day уязвимости или проблеми в конфигурацията, при реалистични сценарии на атака (red teaming), преди те да бъдат използвани от противник.

3.2 Да се предостави на ръководството увереност относно ефективността на контролите и приложими препоръки чрез докладване на констатациите от тестовете, като по този начин се подпомага вземането на решения, основано на риска, относно третирането на риска и непрекъснатото подобрение на програмата за сигурност.

4. Роли и отговорности

4 Координатор по тестването на сигурността (STC): определя се от директора по информационна сигурност (CISO) и отговаря за планирането и надзора на всички дейности по тестване на сигурността. Осигурява, че тестовете са с ясно определен обхват, надлежно разрешени и че резултатите се докладват и по тях се предприемат действия.

4.1 Вътрешен екип по сигурността (Blue Team): съдейства при тестовете (напр. предоставя информация за определяне на обхвата, наблюдава системите по време на тестовете). При упражнения тип red team Blue Team реагира на симулирани атаки и се оценяват неговите способности за откриване и реагиране.

4.2 Red Team / тестери за проникване: могат да бъдат вътрешен екип по offensive security или външни консултанти. Изпълняват тестовете съгласно договорените правила за изпълнение, документират всички установени уязвимости и пътища за експлоатация и спазват поверителността.

[... Раздели 4.3–8 не са включени в тази предварителна версия. Закупете пълния документ за достъп до пълното съдържание. ...]

9. Мониторинг и одит

9 STC поддържа календар и журнал на всички извършени дейности по тестване на сигурността. Този журнал трябва да включва дата, обхват, кой е извършил теста и обобщение на резултатите. Той се преглежда, за да се гарантира спазването на изисквания график (напр. нито една критична система да не остане без тестване след изтичане на годишния цикъл).

9.1 Напредъкът по отстраняването на констатациите от тестовете се наблюдава и докладва ежемесечно. Неприключените проблеми с висока степен на сериозност се преглеждат на срещи на ръководството до тяхното затваряне.

9.2 Вътрешният одит или независим одитор преглежда ежегодно програмата за тестване на сигурността, за да провери, че тестовете са надлежно разрешени, проведени и докладвани, че критичните констатации са адресирани и че програмата отговаря на регулаторните очаквания (например одиторите могат да проверят дали е проведен тест за проникване преди пускането на нова онлайн услуга, когато това се изисква). Всяко отклонение води до изготвяне на планове за коригиращи действия.

10. Преглед и поддръжка

10 Тази политика и общият план за тестване се преглеждат най-малко веднъж годишно. При прегледа се отчитат промените в средата на заплахите (напр. поява на нови техники за атака, които текущото ни тестване може да не обхваща) и съответно се адаптират обхватът и честотата.

10.1 След всеки съществен инцидент по киберсигурност или нарушение тази политика трябва да бъде преразгледана, за да се определи дали допълнително или по-често тестване е можело да предотврати или открие проблема. След това политиката се актуализира, за да включи необходимите промени (например добавяне на нов сценарий в упражненията тип red team въз основа на наблюдавани модели на атака).

10.2 Актуализациите на тази политика трябва да бъдат одобрени от директора по информационна сигурност (CISO) и отбелязани от Управителния съвет. Всички съответни служители се уведомяват за промените, а външните партньори по тестване се уведомяват, ако промяната засяга условията на техния ангажимент.

11. Свързани политики и връзки

11.1 P06 – Политика за управление на риска. Резултатите от тестовете подпомагат оценката на риска и третирането на риска.

11.2 P22 – Политика за регистриране и мониторинг. Валидира покритието на откриването по време на упражнения.

11.3 P24 – Политика за сигурна разработка. Интегрира констатациите от тестовете в контролите по жизнения цикъл на разработката на софтуер (SDLC).

11.4 P25 – Политика за изискванията за сигурност на приложенията. Осигурява изискванията да отразяват изводите от тестовете.

11.5 P30 – Политика за реагиране при инциденти. Сценариите тип red team усъвършенстват наръчниците за реагиране и самото реагиране.

11.6 P31 – Политика за събиране на доказателства и форензика. Осигурява безопасно събиране на артефакти по време на тестване.

11.7 P32 – Политика за непрекъсваемост на дейността и аварийно възстановяване. Упражненията проверяват устойчивостта при атака.

11.8 P33 – Политика за одит и мониторинг на съответствието. Осигурява независим надзор върху ефективността на програмата за тестване.

12. Референтни документи

12.1 Директива NIS2 (ЕС 2022/2555), член 21(2), буква (f) (политики и процедури за оценяване на ефективността на мерките за управление на риска за киберсигурността)

12.2 Регламент за изпълнение (ЕС) 2024/2690 на Комисията, приложение, раздел 7 (изисквания за мониторинг, тестване и оценяване на ефективността на мерките за киберсигурност)

12.3 Технически указания на ENISA (2025) – приложение относно тестването на сигурността и одита (насоки за провеждане на упражнения по киберсигурност и технически тестове)

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:

12.5 Най-добри практики в индустрията: OWASP Testing Guide, NIST SP 800-115 (Technical Guide to Security Testing), CBEST/GREEN Team (рамки за red teaming във финансовия сектор за справка)