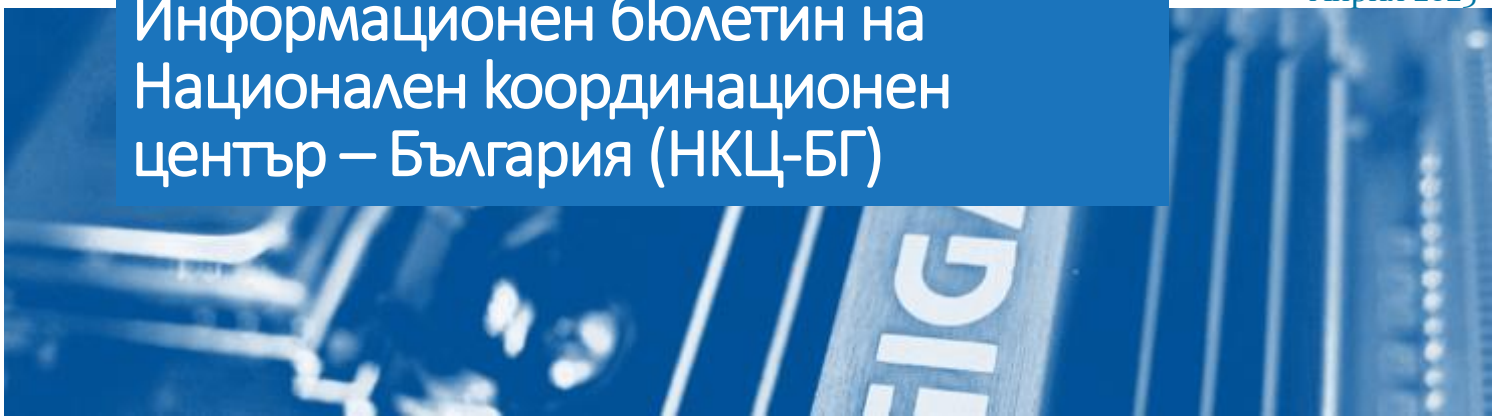
Министерство на електронното управление

Съфинансирано от Европейския съюз

Април 2025

Информационен бюлетин на Национален координационен център – България (НКЦ-БГ)



КИБЕРСИГУРНОСТ И ИНТЕГРИТЕТ НА ИНФОРМАЦИЯТА

Киберсигурност и интегритет на информацията е тема, свързана със защитата на системите за надзорен контрол и събиране на данни (Supervisory Control and Data Acquisition – SCADA). Защитата на критичната инфраструктура е свързана със защитата на основните системи и активи, които са жизненоважни за функционирането на едно общество и неговата икономика. Тези инфраструктури са жизненоважни и прекъсването на нормалното функциониране или унищожаването им би имало съществено негативно въздействие върху националната сигурност, общественото здраве, безопасността или икономическата стабилност.

Критичната инфраструктура обхваща различни сектори като:

1) Енергия – електропреносни мрежи и генератори, нефтопроводи и газопроводи и системи за възобновяема енергия;

2) Водоснабдяващи и канализационни системи – пречиствателни станции и разпределителни мрежи;

3) Транспорт – летища, железопътни линии, магистрали и морско и речно корабоплаване;

ДОБРИ ПРАКТИКИ ЗА ЗАЩИТА НА ОБЛАЧНИ SCADA СИСТЕМИ

• Използване на силно криптиране. Криптирането на данните гарантира, че остават защитени по време на предаване. Това предотвратява неоторизирани потребители да четат или подправят данни.

• Сигурен отдалечен достъп с VPN. Виртуалните частни мрежи (VPN) добавят допълнително ниво на сигурност за отдалечен достъп. Те създават частен и криптиран тунел между потребителя и системата, като предпазват операциите от външни заплахи.

• Многофакторно удостоверяване (MFA). MFA изисква потребителите да потвърдят самоличността си, като използват два или повече



4) Здравеопазване – болници, фармацевтични вериги за доставка и медицински заведения;

5) Информационни технологии – телекомуникационни мрежи, центрове за данни и интернет инфраструктура;

6) Финансови услуги – банкови системи, обработка на плащания и обмен на ценни книжа;

7) Правителство – национални отбранителни системи, служби за спешна помощ и операции на правоприлагащите органи; и др.

ЗАЩИТАТА НА СИСТЕМИТЕ SCADA (НАДЗОРЕН КОНТРОЛ И СЪБИРАНЕ НА ДАННИ) Е ИЗКЛЮЧИТЕЛНО ВАЖНА ПОРАДИ НЯКОЛКО ПРИЧИНИ:

• Сигурност на критичната инфраструктура: SCADA системите контролират основни услуги като електрически мрежи, съоръжения за пречистване на вода, преработка на храни и напитки, нефтопроводи и газопроводи и транспортни системи. Ако тези системи бъдат компрометирани, последствията могат да бъдат катастрофални, вариращи от прекъсване на обслужването до физически щети на инфраструктурата и дори загуба на живот.

• Заплахи за киберсигурността: SCADA системите са все по-уязвими на кибератаки поради връзката им с интернет или възможности за проникване с човешко участие и зависимостта им от наследени системи. Кибернетични заплахи като хакерство, рансъмуер или злонамерен софтуер могат да нарушат операциите, да откраднат чувствителни данни или да повредят оборудването.

• Оперативна непрекъснатост: Много системи, управлявани от SCADA, са отговорни за поддържането на ежедневните операции на индустриите, които влияят на обществото като цяло. Пробив в SCADA система може да доведе до прекъсвания, спиране на производството или влошени услуги, което води до значителни финансови загуби, увреждане на репутацията и намаляване на общественото доверие.

метода, като парола и мобилен OTP.

• Редовни софтуерни актуализации. Поддържането на облачната SCADA система актуална е жизненоважно. Актуализациите често включват отстраняване за уязвимости в сигурността, защитавайки системата от нови заплахи.

• Наблюдаване активността със защитени регистрационни файлове. Дневниците на активността помагат да се проследи кой е имал достъп до системата и какви промени са направени. Редовното наблюдение може бързо да открие необичайна дейност, което позволява да се реагира, преди проблемите да ескалират.

• Обучения на екипа. Операторите и персоналът трябва да разбират важността на киберсигурността. Прости практики, като избягване на подозрителни връзки и използване на силни пароли, допринасят много за поддържането на безопасността на системата.



• Физическо въздействие и въздействие върху околната среда: Успешна атака срещу SCADA системи може да доведе до физическо унищожаване на оборудване или освобождаване на опасни вещества, което може да има дългосрочно въздействие върху околната среда. Например, в случай на съоръжение за пречистване на вода, нападателят може да манипулира химическите нива и да замърси водоснабдяването.

• Национална сигурност: В някои случаи SCADA системите са част от инфраструктурата за национална сигурност. Кибератака, насочена към критични сектори като енергетиката или отбраната, може да се използва за прекъсване на правителствени операции, създаване на хаос или дори за активиране на шпионаж или саботаж.

• Съответствие с нормативните изисквания: Много индустрии разчитат на SCADA системи и трябва да се придържат към стриктни разпоредби относно сигурността и поверителността на данните.

ДЕН НА МРЕЖАТА ОТ НАЦИОНАЛНИ КООРДИНАЦИОННИ ЦЕНТРОВЕ

На 07 април 2025 г. в гр. Варшава (Полша) се проведе среща на Мрежата от национални координационни центрове, чийто домакин беше NCC-PL | Национален координационен център – Полша.
Ключовите теми включваха:
🛡 текущото изпълнение на проекти за киберсигурност по програмите „Цифрова Европа“ и „Хоризонт Европа“;
 сътрудничеството между НКЦ, ЕССС и други заинтересовани страни;
🌐 изграждането на киберобщност и нейният път напред към силна европейска екосистема за киберсигурност.

Лаури Танклер, председател на Мрежата, заяви: „Тези срещи винаги са чудесно време да осъзнаем, че всички работим заедно по обща цел, която е да гарантираме, че екосистемата за киберсигурност в Европа може да расте по-голяма, по-добра и по-силна.“







Министерство на електронното управление

ул. „Ген. Гурко“ № 6

Гр. София 1000

Ел. поща: bnccc@egov.government.bg

Ел. адрес: https://ncc.egov.bg/