Анализ на обхвата на концептуален модел за споделен център за операции по киберсигурността на индустриални управляващи системи

В. Димитров[1], К. Спасов[2], С. Сярова[1]

Analysis of the Scope of a Conceptual Model for a Sharing Center for ICS Cyber Security Operations

W. Dimitrov[1], K. Spasov[2], S. Syarova[1]

[1] *Department of Computer Science, Faculty of Information Sciences, University of Library Studies and Information Technologies, Sofia, Bulgaria, v.dimitrov@unibit.bg, s.syarova@unibit.bg*

[2] *Department of Statistics and Econometrics, Faculty of Economics and Business Administration, Sofia University St. Kliment Ohridski, Sofia, Bulgaria, k.spasov@gmail.com*

Key Words: *Cyber; security; operations; center; ICS; shared.*

Abstract. *The article offers a analysis of the scope of a conceptual model for a Shared Industrial Control Sys-tems (ICS) CyberSecurity Operations Center (SOC). The analysis of design of the conceptual model is aimed at bridging the gaps in existing market solutions and meeting the needs of the entire cycle of cybersecurity en-gagements. It ensures continuous proportional ICS protection against malicious actors and in accordance with regulations and standards. The focus of the research is on the three basic functions of cybersecurity cycle – proactive functions, security operations management, and cybersecurity incident response. The aim of the study is to increase the effectiveness of cybersecurity for all Shared SOC subscribers, to overcome the problem of staff shortages, and allow each company to focus on its core business. The applied methodology is based on the Fea-ture Driven Development approach, empirical experience from the implementation of cyber defense systems, and interdisciplinary vision. The proposed analysis provides reference points for synthesizing a private solution for multiple clients of Shared SOC, a basis for concept of operations and preparation for technical design. The idea of a Shared SOC provides a powerful tool for meeting the requirement for multi-layered cyber protection, which is already a fact in many regulatory measures. Shared SOC creates conditions for all subscribers with ICS to increase their level of maturity in cybersecurity.*

Проблеми пред киберзащитата на индустриални управляващи системи

Индустриалните управляващи системи (ИУС) гарантират основни операции за критична инфраструктура от енергетиката, водоснабдяването, транспорта и производството. Важна насока за научни изследвания е темата за споделяне на общи услуги, предоставящи киберсигурност за ИУС [1, 2].

Потенциалът на хакерите расте с изпреварващи темпове пред този на киберзащитниците [1,2,3]. Според някои публикации [4,5] вътрешен нападател, който вече е в корпоративната информационна система, би могъл да проникне в индустриалната мрежа в 82% от случаите.

Ограничения на съществуващите решения за Центрове за операции по киберсигурността (ЦОК). Изследване на предлаганите услуги от продуктите за киберсигурност и реалните потребности в съответствие с правната рамка в областта на ИУС и SCADA [6,7,8] сме публикували в предходна статия [9]. Технологиите за киберсигурност имат ограничен обхват, основан на корпоративния опит на съответния производител. В тези предложения липсват модели за организиране на дейностите на екипите за сигурност. Предизвикателствата се пораждат от множеството технологии и услуги за сигурност от различни доставчици. Съвместяването им в системи за киберзащита води до липса на оперативна съвместимост между различни системи за сигурност, недостатъчна видимост от край до край, неадекватни ресурси за намаляване на рисковете [10], [11].

Конвергенцията на IoT и ИУС доведе до схващането за OT (Operation Technologies), което значително усложни повърхността за заплаха и усилията за киберзащита [12], [13]. Нашият преглед на нарушенията на сигурността на ИУС в областта на критичната инфраструктура обхваща периода след 2003 г. [6,14,15].

Методология на изследването

Споделеният Център за операции по киберсигурността (СЦОК) предоставя услуги за киберзащита на множество ИУС. Този подход позволява организациите да възложат услугите по киберзащита на ИУС и информационните системи, както и комуникационната си свързаност на външна струк-

тура. Това ще доведе до повишаване на ефективността на киберзащитата за всички абонати на СЦОК и преодоляване на проблема с недостига на кадри, а всяка компания ще се съсредоточи върху основната си дейност. Предлаганият модел предоставя опорни точки за синтезиране на споделено частно решение за множество клиенти на СЦОК, база за идейно проучване и съставяне на техническо задание и проект. Нашият принос е в определянето на обхвата на операциите, които се извършват от екипа на СЦОК.

Регулаторни ограничения. При определяне на набора от операции, които са делегирани на споделената ЦОК, вземаме предвид съществуващите закони, директиви и стандарти, прилагани в областта на сигурността на ИУС.

Смятаме, че операциите, необходими за СЦОК, определят функционалностите на СЦОК и техническия дизайн на архитектурата, а елементите на концептуалния модел се основават на набора от функционалности. Натовареността на центъра и изискванията за мащабируемост са тема на техническата архитектура, които излизат извън обхвата на настоящата статия.

Анализираният модел е основан на емпиричен опит от създаване на центрове за управление на кризи при природни бедствия и аварии и решения за киберзащита за големи ИКТ системи. Общото тук е схващането, че инцидентът с киберсигурност, обработван от СЦОК, има естеството и ефектите от криза. Изискванията за управление на процеси и в двата случая са близки [16]. Използваме методология за синтез на функции в зависимост от потребностите за реализиране на процеси (Feature Driven Development, FDD), ефективна на етапите проучване и техническо задание [17], Мултидисциплинарен подход в проектирането на надеждни защитени системи [18].

Предложеният концептуален модел за споделен център за киберсигурност се отличава с пълнота на обхвата на предлаганите услуги, характерна за подхода **umbrella** [19]. Разликите от наличните на пазара технологии за киберсигурност и частните решения, които са интегрирани в корпоративните системи за киберсигурност, обхващат:

- пълния цикъл на киберинцидент;
- контрола върху веригите за доставки на ИКТ активи;
- актуализиране на компетенциите на екипа на СЦОК и екипите на компаниите клиенти.

Визията ни за пълния цикъл на инцидент включва всички процеси, които се инициализират след началото му. В тези процеси участват клиентската организация на споделения център за киберсигурност, различни отдели на самия център и много външни трети страни.

Емпиричният ни опит от управлението на инциденти по сигурността показва, че този процес включва широка екосистема от участващи организации, занимаващи се с различни аспекти на последиците от инцидента. На практика считаме, че инцидентът е завършен само след като всички възможни ангажименти на пострадалата организация към засегнатите трети страни и отделни граждани са окончателно отпаднали заедно с всички институционални регулаторни задължения по отношение на инцидента.

Приемаме, че целта на СЦОК е да предпазва от кибератаки ИУС, които са свързани с организационните информационни системи и съдържат както съвременни, така и остарели технологии за автоматизация.

Централизираните защитни функции ще увеличат ефективността на технологиите, инсталирани в СЦОК. Голяма част от едновременните усилия за управление на киберсигурността и поддържащите активи за абонатите ще бъдат избегнати.

Изисквания към модела. Анализираме функцията на СЦОК въз основа на съществуващите правни рамки, стандарти и отраслови изисквания за сигурност на ИУС, публикувани от водещите институции в световен мащаб. SOC осигурява киберзащита за повече от една инсталации от ИУС, собственикът на всяка инсталация на ICS може да бъде различен.

Целта на анализа е да посочи набор от функционалности, които ще засилят ефекта от ЦСОК. Вземаме предвид много разлики между изискванията за сигурност и нуждите на традиционната ИКТ система и ИУС. Общият набор е изброен например в [7]. Екосистемата за киберсигурност на ИУС вече е далеч извън стандартите и включва множество елементи от цифровото пространство, свързани с интернет сигурността и веригата на доставки [20]. Моделът е оразмерен да предотвратява в пропорционална степен инцидентите с киберсигурност от високо ниво. Според [21] това са прекъсвания, които са най-сериозни и се считат за значителни. Отговорът на тези инциденти трябва да бъде незабавен. Инцидентите от високо ниво включват животозастрашаващи дейности, компрометиране на критични системи или информация, компрометиране на привилегировани акаунти и нарушаване на законите.

Зад термина управление на инциденти разбираме сложен процес, който обхваща превантивни дейности, откриване, анализ, реагиране и възстановяване от разрушителни събития с последваща обратна връзка за недопускане на аналогични ситуации. Целта на управлението на инциденти е да смекчи въздействието на разрушителното събитие. За да постигне тази цел, се установяват процеси, които откриват и анализират събития, за да определят дали даден инцидент е в ход, реагират, премахват последствията и подобряват способностите на организацията да реагира на бъдещ инцидент.

Както при другите стъпки, степента и усилията, необходими за управлението, зависят от въздействието на инцидента и оперативната среда на организацията. След като организацията приключи прегледа си, важно е да затвори инцидента. Приключването на инцидента е официална декларация, че не е необходимо да се предприемат допълнителни действия. Дейностите по закриване на инциденти включват уведомяване на всички заинтересовани страни, засегнати от инцидента, че е разрешен и те не трябва да изпитват допълнителни ефекти. Важните практики за подобряване на възможностите за управление на инциденти включват анализ на първопричината след закриване на инцидента [21] и актуализиране на политиките за киберзащита в рамките на функционалностите за управление на промяната и управление на знанието.

При изграждането на този концептуален модел сме взели предвид общите характеристики на процесите на откриване на инвазии и характерните процеси на възстановяване и елиминиране на последствията от неуспехи в киберсигурността.

Систематизирането на набора от функции, които ИУС СЦОК трябва да изпълнява, сме извършили на основата на анализ на известни от последните двадесет години киберинциденти в обекти от критичната инфраструктура. Полученият набор от функции осигурява намаляване на оперативните разходи на СЦОК за всеки абонат; преодолява недостига на персонал за киберсигурност в отделните организации, управлявани ИУС; фокусирано натрупването на опит и знания, инкорпориране на авангардни технологии, които позволяват проактивни политики за сигурност; откриване на нови заплахи и ранни етапи на атаки; предоставяне на достъп на предприятието до пакет от услуги, включително дистанционно управление на периметъра.

Фиг. 1. Обща визия за ЦСОК

Обхват на концептуалния модел за СЦОК

Предполагаме, че абонатите към СЦОК имат приблизително подобна техническа архитектура в съответните им слоеве на ИУС: сензори, PLC, не-IP мрежи, канали за събиране на данни, портали, бази данни, сървъри и системи за оркестрация, връзки с външни системи към доставчици, подизпълнители и институции. Комуникационната свързаност и основните мрежови услуги DNS, NTP, SMTP за абонатите се осигуряват чрез СЦОК. Трите основни стълба на ЦСОК са агрегати от проактивни функции, оперативно управление и отговор на инцидент, покриващи сечението от необходими за абонатите услуги по киберсигурността (*фиг. 1*).

Проактивни функции. Имат най-голяма тежест при управлението на киберсигурността. Организациите поддържат защитени връзки чрез VPN между обектите с ИУС и производителите на оборудване. Всяка подобна връзка представлява риск, който трябва да се наблюдава.

Управлението на политиките за сигурност включва спазване на регулаторните изисквания, бизнес политиката и организационните цели и спазването на изискванията на стандартите за сигурност. Споделеният СЦОК може да управлява ядрото на политиката, което е общо за всички, и да предоставя методически указания за конкретните раздели, които засягат всеки абонат. Споделянето на защитата на основните мрежови услуги ще увеличи нивото на защита за всички абонати [22,23].

Връзки с външни организации. Регулаторните мерки задължават организациите да поддържат комуникация с множество външни организации през различни етапи от жизнения цикъл на киберзащитата: при комуникации с външни доставчици, при оперативно управление. При справяне с последиците от инцидент в сигурността са необходими комуникации с разследващи органи, външни консултантски компании, застрахователни компании, държавни институции, пресата и други. Ескалацията на инциденти изисква комуникация с правителствени ведомства и браншови организации, подизпълнители за предоставяне на услуги за киберсигурност, връзки с обществеността. Обхваща целия жизнен цикъл на инцидент по сигурността. От първоначално откриване до връщане към стабилно състояние. Екипът е съставен от професионалисти по сигурността, единствено посветени на защитата на бизнеса.

Изследвания и развитие. Екипът на СЦОК управлява тестовата площадка със симулация на общи ИУС и обучение на служителите [24]. Проучва авангардните технологии с цел бъдещо внедряване в СЦОК. Контролира подизпълнителите, които разработват нови решения. Лабораторното тестване на ъпдейтите е предпоставка за избягване на проблеми при налагането на актуализациите по сигурността върху живите системи. Мултиплицира ефекта, тъй като резултатите се използват от всички засегнати абонати.

Гарантиране на сигурност по цялата веригата за доставки. Организациите комуникират с множество контрагенти по веригата на доставки, което увеличава повърхността за атаката. СЦОК предполага защитна стратегия за намаляване на рисковете от трети страни по веригата за доставки. Тя трябва да съдържа технически и организационни мерки, спазване на стандартите, регламентите и контрол върху съдържанието на договорите, които могат да създадат предпоставки за киберинциденти. Това означава приемане на принципа за нулево доверие и необходимостта от постоянен мониторинг на доставчиците [25], контрол при доставка на продукти; управление на договори с доставчици на облачни услуги и телекомуникационни оператори в секциите за сигурност и SLA (Service Level Agreement). Тези функционалности отразяват динамиката на регулаторните мерки, които през последните години се увеличават, дават пълна представа за риска на трети страни за всеки абонат на СЦОК. СЦОК предоставя възможност за проучване на авангардните технологии и навременното им внедряване, обучение на алгоритми за машинно обучение с богати набори от данни, събрани от реални атаки [26].

Оперативното управление на сигурността включва реагиране на събития от системите за мониторинг и регистриране на инциденти в реално време; идентифициране на точки на проникване и премахване на уязвимости, тестване за проникване, управление на активите и комуникационните връзки, обменът, извършен от всеки актив, откриване на проблеми с неправилни конфигурации и други слабости. Точното съвпадение на уязвимостите към контролерите се извършва въз основа на данните за версиите на фърмуера, трафикът от огледални портове в комутаторите се подават в IDS за анализ.

Нашата визия за ангажираността на звената на СЦОК обхваща дейности, които засягат цялата екосистема за сигурност на абонатите. Екипът на СЦОК установява повише-

ните рискове, премахва фалшивите положителни резултати, идентифицира възникналите събитията по сигурността, които са свързани с публикувани вече инциденти, разузнава заплахите. Създава условия за оценка на въздействието на предложената настройка и теста корекцията за некритични активи в лабораторна обстановка – операционни системи, бази данни, табла, защитни стени и други устройства за периферна защита. Това гарантира, че операционните системи не са засегнати неблагоприятно от актуализациите. СЦОК предоставя актуализации на системите за сигурност веднъж вместо всеки абонат. Същото се отнася и за последващи проверки на сегментирането на мрежата и контрола на достъпа. Проактивно извършва регресионно тестване, преди да внедри актуализации на оперативни или критични активи.

Мониторинг на системните конфигурации за недостатъци в сигурността, редовни актуализации и признаци на компрометиране. Получаване на филтрирани нормализирани регистрационни файлове, корелиране и анализ на регистрационни файлове с най-съвременни технологии – анализ на големи данни, ML, AI. Извършване на анализ на аномалии – индикатори за компромис (IoC) за намиране на противникови инструменти или артефакти; създаване на хипотези за тестване; произволно търсене, използване на автоматизирани инструменти за откриване на сигнали, тестване за уязвимости в сигурността в променящия се домейн на ИУС [27].

Автоматизирани дейности по сигурността. СЦОК предоставя единен портал със служители, обучени в използването на инструменти за автоматизация за процесите на сигурност. Литературни източници описват ефектите от умората върху експертите по сигурността в режим 24/7 [28,29].

Отговор на инцидент по киберсигурността. Включва регистриране на инцидента, назначаване на приоритет, проследяване и предоставяне на пълна история на събитията и дейностите през целия жизнен цикъл на инцидента, управление на процесите за елиминиране на последствията от инциденти със сигурността. Активира се предварително изготвен план за реагиране при киберинциденти (служителите трябва да са обучени за неговото прилагане), договарянето на ангажименти на трети страни: външен адвокат, консултанти, разследващи органи, правоприлагащи и регулаторни органи; управление на връзките с обществеността чрез пресконференции и публикации на фирмени уебсайтове. Основните връзки между оперативното управление и отговора на инцидент по сигурността са представени на *фиг. 2*.

Фиг. 2. Функционални връзки

Преглед на реакцията след инцидента и научени уроци. Криминалистични изследвания върху запазени оригинални данни и носители. Събиране на всички подходящи регистрационни файлове: от DNS, защитни стени, прокси, дневник на системните събития, комуникация ДОО за допълнителни данни, извършване на оценка на щетите. СЦОК е институция, отговорна за оценка на инциденти със сигурността, комбинирани технически умения и опит в разследването. Подходящи показатели могат да бъдат избрани от [30].

Разследване на инциденти по сигурността. Организацията може да претърпи последователни успешни кибератаки [31]. Анализът на много инциденти показва, че: (1) те отнемат много време, след като са предприети всички технически мерки в отговор на инцидента; (2) се ангажират трети страни за последващ анализ на инцидента; (3) появят си искове за щети от трети страни; (4) организацията продължава да разпределя ресурси за справяне с тези дългосрочни последици; (5) има нужда за координирано управление на процесите, свързани с тези последици.

Споделената СЦОК трябва да преодолее следващите пропуски в киберсигурността на ИУС: липса на активно разследване и целостта на доказателства и данни; липса на съвместими криминалистични инструменти за полеви устройства. Клиентите на СЦОК по исторически причини поддържат и остарели, и авангардни технологии. Идентифицирането на източници на данни в SCADA и множеството слоеве на свързаност в сложна архитектура е трудна по своята същност задача [8].

Заключение

Днешните ЦОК ще се развият радикално в близко бъдеще, тъй като авангардните технологиите се интегрират от индустрията за киберсигурност. Идеята за СЦОК предоставя мощен инструмент за изпълнение на изискването за многослойна киберзащита, което вече е факт в много регулаторни мерки. СЦОК създава условия всички абонати с ИУС да повишат нивото си на зрялост в киберсигурността [32] – може да бъде от полза за архитекти на системи за сигурност, системни архитекти и интегратори.. В съответствие със стандартите за проектиране логичната следваща стъпки в изследванията е синтезирането на концептуална архитектура и организационно решение за управление на отделните функционалности на СЦОК.

Литература

1. Mathieu Poujol,Wolfgang Schwab. The State of Industrial Cybersecurity, 2018.

2. Samuel Tweneboah-Koduah, Knud Erik Skouby and Reza Tadayoni. Cyber Security Threats to IoT Applications and Service Domains. – *Wireless Personal Communications*, 95, May 2017, 1, 169–185.

3. David Livingstone, Caroline Baylon, Roger Brunt. Cyber Security at Civil Nuclear Facilities. Understanding the Risks. 2015.

4. Evan Reese, Steve Miller. A Totally Tubular Treatise on TRITON and TriStation A Totally Tubular Treatise on TRI-TON and TriStation. 6, 2018 [Online; Accessed 7 Jun. 2019].

5. Positive Technologies. Industrial Companies: Attack Vectors. 2, 2019.

6. Goran Andersson, Peyman Mohajerin Esfahani, Maria Vrakopoulou, Kostas Margellos, John Lygeros, Andre Teixei-ra, Gyorgy Dan, Henrik Sandberg and Karl H. Johansson. Cyber-security of SCADA Systems. In 2012 IEEE PES Inno-vative Smart Grid Technologies (ISGT), IEEE.

7. Karen Scarfone, Keith Stouffer, Joe Falco. Guide to Industrial Control Systems (ICS) Security. Recommendations of the National Institute of Standards and Technology. Special Publi-cation 800-82, June 2011.

8. Sandeep Mittal. The Issues in Cyber-Defence and Cyber-Forensics of the SCADA Systems. 6, 2015 [Online; Accessed 6 Jun. 2019].

9. Willian Dimitrov and Svetlana Syarova. Analysis of the Functionalities of a Shared ICS Security Operations Center. In 2019 Big Data, Knowledge and Control Systems Engineering (BdKCSE). IEEE, Nov. 2019.

10. Managed Security Services. 2013, DDCC-1437/11/13.

11. Peyo Hristov and Teodora Hristova. Explaining the DLT Applications in the Context of a Customers, Facility Manage-ments and Utility Companies Relationship. In 2019 16th Conference on Electrical Machines, Drives and Power Systems (ELMA). IEEE, June 2019.

12. Mauro Conti, Ali Dehghantanha, Katrin Franke and Steve Watson. Internet of Things Security and Forensics: Challenges and Opportunities. https://arxiv.org/pdf/1811.09239.pdf.

13. European Union Agency for Network and Information Security. Baseline Security Recommendations for IOT in the Context of Critical Information Infrastructures. November 2017.

14. Brian Cusack and Amr Mahmoud. Digital Forensics Investigative Framework for Control Rooms in Critical Infra-structure. Australian Digital Forensics Conference, 2018.

15. Andrew Fielder, Tingting Li and Chris Hankin. Defense-in-depth vs. Critical Component Defense for Industrial Control Systems. In 4th International Symposium for ICS & SCADA Cyber Security Research 2016 (ICS-CSR 2016). BCS Learning & Development, 2016.

16. ENISA. Mapping of OES Security Requirements to Specific Sectors. 2017.

17. Zahid Nawaz, Shabib Aftab and Faiza Anwer. Simplified FDD Process Model. – *International Journal of Modern Education and Computer Science*, 9, Sep. 2017, 9, 53–59.

18. Ivan Gaidarski and Zlatogor Minchev. Virtual Enterprise Data Protection: Framework Implementation with Practical Valida-tion. Conference BISEC 2018At, Belgrade, Serbia, 2018.

19. Sihyung Lee, Kyriaki Levanti and Hyong S. Kim. Network Monitoring: Present and Future. – *Computer Networks*, June 2014, 65, 84–98.

20. Andrew Ginter. The Top 20 Cyberattacks on Industrial Control Systems, chapter Andrew Ginter. Waterfall Security Solutions.

21. Funded and Supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University. Crr Supplemental Resource Guide, 5, Incident Management Version 1.1.

22. Alex Cowperthwaite and Anil Somayaji. The Futility of Dnssec. In Proc. 5th Annual Symp. Information Assurance (ASIA, 10), 2010, 2–8.

23. Gurubaran S. Bind Dns Software Flaw Let Remote Attackers to Cause DOS Attack. 4, 2019 [Online; Accessed 26 Apr. 2019].

24. Adrian Pauna (ENISA). Certification of Cyber Security Skills of ICS/ SCADA Professionals. December 2014.

25. Shaun Nichols. Remember Stuxnet? You'll Endure its Hated-by-critics Sequel if You Don't Patch Your Holey Siemens Industrial Kit. 7, 2019.

26. Marcio Teixeira, Tara Salman, Maede Zolanvari, Raj Jain, Nader Meskin and Mohammed Samaka. SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach. – *Future Internet,* 10, Aug. 2018, 8, 76.

27. Steffen Pfrang, David Meier, Michael Friedrich and JGjrgen Beyerer. Advancing Protocol Fuzzing for Industrial Automa-tion and Control Systems. In Proceedings of the 4th Interna-tional Conference on Information Systems Security and Priva-cy. SCITEPRESS, 2018.

28. Maria Bada and Jason R.C. Nurse. Developing Cybersecurity Education and Awareness Programmes for Small- and Medi-um-sized Enterprises (SMEs). – *Information & Computer Security*, 27, July 2019, 3, 393–410.

29. Lee Hadlington. Human Factors in Cybersecurity Examining the Link between Internet Addiction, Impulsivity, Attitudes towards Cybersecurity and Risky Cybersecurity Behaviours. – *Heliyon*, 3, July 2017, 7, e00346.

30. CIS. Center for Internet Security. A Measurement Companion to the CIS Critical Security Controls, 2015.

31. Peter Walker and Alex Hern. Labour Suffers Second Cyber-attack in Two Days. 11, 2019.

32. ENISA Rossella Mattioli, ENISA Konstantinos Moulinos. Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors. 2015.

За контакти:
Доц. д-р **Велиян Димитров**
Факултет по компютърни науки
Университет по библиотекознание
и информационни технологии
e-mail: v.dimitrov@unibit.bg
Доц. д-р **Камен Спасов**
Катедра „Статистика и иконометрия"
Стопански факултет
СУ „Св. Климент Охридски"
e-mail: k.spasov@gmail.com
Светлана Сярова
Факултет по компютърни науки
Университет по библиотекознание
и информационни технологии
e-mail: s.syarova@unibit.bg