ISSN 2738-7089 https://doi.org/10.11610/cybsec16bg

Funded by the European Union

ПРОГРАМА НАУЧНИ ИЗСЛЕДВАНИЯ, ИНОВАЦИИ И ДИГИТАЛИЗАЦИЯ ЗА ИНТЕЛИГЕНТНА ТРАНСФОРМАЦИЯ

Digital Innovation Hub Trakia

ИИКТ
ИНСТИТУТ ПО ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

Информационен бюлетин за киберсигурност и интегритет на информацията

Бюлетин Март 2025 Номер 16

Цели и обхват

Настоящият брой на информационния бюлетин за киберсигурност и интегритет на информцията е с водеща 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; 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.

Като се имат предвид тези фактори, осигуряването на SCADA системи е от съществено значение за поддържане на безопасността, надеждността и устойчивостта на критичната инфраструктура, опазване на общественото здраве и безопасност и защита на националната сигурност. В допълнение към осигуряване защитата на SCADA системите е представена информация относно разбирането на рисковете за киберсигурността, свързани със системите за охранителни камери.

В бюлетина традиционно са представени важни събития през изминалия тремесечен период, свързани с изпълнението на проекта Киберсигурност за всички заинтересовани страни (CYBER4ALLSTAR), както и полезни връзки за общността.

Редактор на броя: **проф. д.н. Даниела Борисова**

Съдържание:

Фокус на изданието: Защита на SCADA системи

проф. д.н. Даниела Борисова,
ИИКТ-БАН

SCADA – Supervisory Control and Data Acquisition

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.
- **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. Защитата на SCADA системите гарантира съответствие със закони като NIST Cybersecurity Framework, GDPR и специфични за индустрията стандарти.

Примери за заплахи и уязвимости за сигурността на SCADA

Специфичните видове заплахи за SCADA мрежите попадат в следните четири категории:

1. **Хакери**: Умишлени, злонамерени лица или групи, които възнамеряват да получат достъп до ключови компоненти в SCADA мрежи. Тези хакери също могат да бъдат част от правителствен план като вид кибервойна.

2. Зловреден софтуер: Зловреден софтуер ще включва вируси, шпионски софтуер и други програми, които не са непременно насочени към SCADA мрежи. Въпреки че може да не са насочени конкретно към тези мрежи, зловредният софтуер все още представлява заплаха за работата на ключова инфраструктура.

3. Терористи: Хакерите може да искат достъп за злонамерени намерения, но обикновено са мотивирани от престъпна печалба. Терористите обикновено се стремят да причинят възможно най-много щети на критичните системи на определени услуги.

4. Вътрешна грешка: Работниците са често срещана причина за проблеми с мрежата на SCADA или умишлено (поради вътрешни работни проблеми), или по-често чрез грешка на оператора. Повечето проблеми в тази категория се дължат на лошо обучение или небрежност.

Слабости в сигурността на системата SCADA

1. Лошо обучение: Повечето служители разбират жизненоважната природа на системите и как да работят и наблюдават контролите. Въпреки това, мнозина, които работят със SCADA системи, са недостатъчно обучени за предотвратяване, наблюдение и идентифициране на потенциални заплахи за сигурността.

2. Пропуски в разработката на приложения: Приложенията стават все по-голяма част от индустриалните системи за контрол. И все пак много приложения, които се разработват, нямат нивото на сигурност, което може да се очаква за такива жизненоважни системи.

3. Проблеми с наблюдението: Един вид наблюдение е да се гарантира, че системите работят правилно. Друг е да се търсят потенциални заплахи за мрежата. В много случаи заплахата не се открива, докато хакерите не получат достъп до определени системи и не започнат да ги използват.

4. Липса на поддръжка: Софтуерът остарява, създават се нови актуализации на приложения, за да се подобри функционалността или сигурността, а грешките в програмирането се коригират. Ако тези актуализации не се администрират бързо и правилно, възникват уязвимости.

Как да подобрим сигурността на SCADA системите?

1. Мрежово сегментиране: Тази стратегия включва създаване на „зони“ в рамките на SCADA мрежата, всяка със свои специфични контроли за сигурност. Това може да означава отделяне на критични системи за контрол от останалата част от мрежата или разделяне на голяма система на по-малки, по-управляеми сегменти. Това намалява риска нападателят да може да се движи хоризонтално / странично през мрежата и да има достъп до чувствителни зони, след като е нарушил по-малко сигурна секция.

2. Контрол на достъпа и автентификация: SCADA системите трябва да включват цялостно управление на потребителските привилегии като контроли за достъп, базирани на роли, при които на потребителите се предоставят права за достъп в зависимост от длъжността им, и контроли за достъп, базирани на време, ограничаващи достъпа до определени часове за конкретни потребители. Силните методи за удостоверяване също включват биометрична проверка или

използването на токени за сигурност заедно с традиционните пароли. Целта е да се създаде здрава бариера, където достъпът е строго регулиран и наблюдаван.

3. Редовни актуализации и корекции: Тази стратегия трябва да бъде част от по-широк подход за управление на риска. Редовното актуализиране и корекция на системи включва не само прилагане на най-новите корекции, но и тестване на тези актуализации в контролирана среда, за да се гарантира, че те не нарушават стабилността на системата. За SCADA системи, където времето за непрекъсната работа е от решаващо значение, корекциите трябва да се прилагат по начин, който минимизира времето за престой. Също така е важно да има план за връщане назад, в случай че актуализация въведе нови уязвимости или несъвместимост на системата.

4. Обучение и информираност на служителите: Този аспект включва създаване на култура на осъзнаване на сигурността в организацията. Програмите за обучение трябва да бъдат редовни, ангажиращи и съобразени с различните роли в компанията. Например, симулирани фишинг упражнения, семинари за разпознаване на тактики за социално инженерство и обучение за специфичните типове заплахи, насочени към SCADA системите. Целта е да се гарантира, че служителите не само са запознати с протоколите, но и са продобили практически умения за гарантиране на сигурността на системата.

5. Оценки на уязвимостта и тестове за проникване: Редовните оценки трябва да включват както автоматизирано сканиране за известни уязвимости, така и ръчно тестване за разкриване на неизвестни слабости. Тестването за проникване, от друга страна, включва симулиране на кибератака при контролирани условия, за да се тества устойчивостта на системата. Това трябва да се прави от опитни професионалисти, които могат да имитират тактиките и техниките на нападателите от реалния свят. Този подход помага да се разбере не само къде са уязвимостите, но и как атакуващият може да ги използва и как системата ще реагира.

6. Криптиране на данни: Криптирането трябва да се реализира с помощта на усъвършенствани алгоритми и трябва да обхваща всички данни, свързани със системата SCADA. Това включва оперативни данни, регистрационни файлове и всякаква комуникация между устройства и контролни центрове. Прилагането на криптиране от край до край гарантира целостта и поверителността на данните, особено когато се предават през потенциално несигурни мрежи. Също така е жизненоважно ключовете за криптиране да се управляват сигурно, като се гарантира, че те се съхраняват и обработват със същото ниво на сигурност като данните, които защитават и дори по-високо.

7. Защитни стени и системи за откриване на проникване (intrusion detection system – IDS): Защитните стени за SCADA системи трябва да бъдат нещо повече от стандартни корпоративни защитни стени; те трябва да могат да обработват уникалните типове трафик и протоколи, използвани в индустриалните системи за контрол. По подобен начин IDS трябва да бъде пригодна да разпознава специфичните модели и аномалии, които показват кибер заплаха в SCADA среда. Това трябва да включва интегрирането на базирани на поведение системи за откриване, които могат да идентифицират необичайни дейности, които означават потенциално нарушение или злонамерена дейност.

8. Редовни одити и оценки на сигурността: Те трябва да се извършват както вътрешно, така и от експерти на трети страни, за да се гарантира обективност и задълбоченост. Одитите трябва да включват преглед на всички политики и процедури, мерки за физическа сигурност, нива на потребителски достъп и мрежова архитектура. Оценките на сигурността могат също да включват тестове за проникване и упражнения за симулиране на сценарии за атака в реалния свят.

9. План за реагиране при инциденти: Изчерпателният план за реагиране при инциденти за SCADA система трябва да включва специфични процедури за различни видове инциденти, ясни роли и отговорности и комуникационни стратегии за вътрешни и външни заинтересовани страни. Трябва да се провеждат редовни тренировки и симулации на сценарии за кибератаки, за да се осигури готовност. Планът трябва също така да включва процедури за криминалистичен анализ, за да се разбере векторът на атаката и да се предотвратят бъдещи инциденти.

10. Съответствие с индустриалните стандарти и разпоредби: Това включва поддържане и спазване на стандарти като NERC CIP, ISA/IEC 62443 и др., свързани със SCADA системите. Съответствието гарантира базова линия на сигурност, но организациите трябва да се стремят да надхвърлят тези стандарти, когато е възможно. Редовните прегледи на състоянието на съответствие, включително анализ на пропуските спрямо най-новите стандарти и регулаторни изисквания, помагат да се гарантира, че SCADA системите са съвместими и следват най-добрите практики за сигурност.

Добри практики за защита на облачни SCADA системи

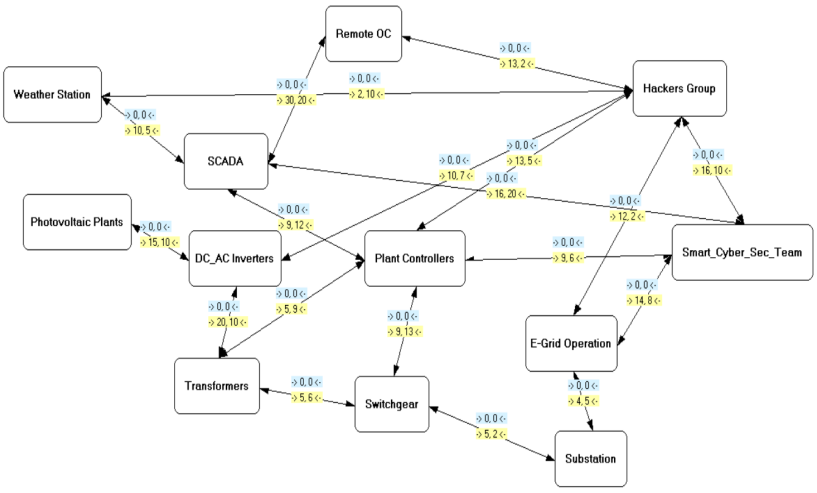
- Използване на силно криптиране. Криптирането на данните гарантира, че остават защитени по време на предаване. Това предотвратява неоторизирани потребители да четат или подправят данни.
- Сигурен отдалечен достъп с VPN. Виртуалните частни мрежи (VPN) добавят допълнително ниво на сигурност за отдалечен 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 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.

Проактивно моделиране и изследване на SCADA системи в смесена реалност

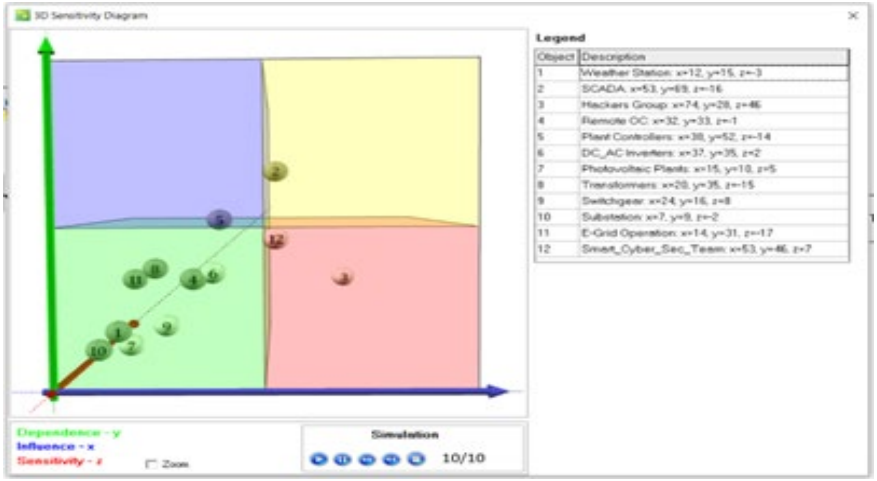
Доц. д-р Златогор Минчев
ГМИС, ИИКТ-БАН

С развитието на съвременната Индустрия 4.0/5.0 се очаква обработването на големи обеми от данни и последващо смесване на информацията от различните сензорни системи с цел мониторинг и управление да се осъществява посредством системно интегриране в добавена или смесена реалност, която позволява включване на машините/роботите и обективната реалност по качествено нов начин в една своеобразна, интелигентна производствена екосистема. При това използването на облачните технологии и високоскоростните безжични комуникации (5G/6G) е от ключово значение за гарантирането на гъвкавост на тези нови, производствените системи. При все това, гарантирането на киберсигурността в тази нова екосистема е сериозно предизвикателство, предвид нейната иновативност и голяма гъвкавост, пораждащи множество неизвестни и известни вектори за атаки. От своя страна SCADA системите навлизат все повече в тези нови Индустрии на бъдещето 4.0/5.0, добавяйки редица интелигентни функционалности, базирани на алгоритми с изкуствен интелект.

Разработеният динамичен модел за проактивно изследване на имплементацията на SCADA системи е с фокус върху все по-широко навлизащите в новата енергийна инфраструктура на Европа, малки фотоволтаични паркове. При това, като основна тяхна уязвимост се

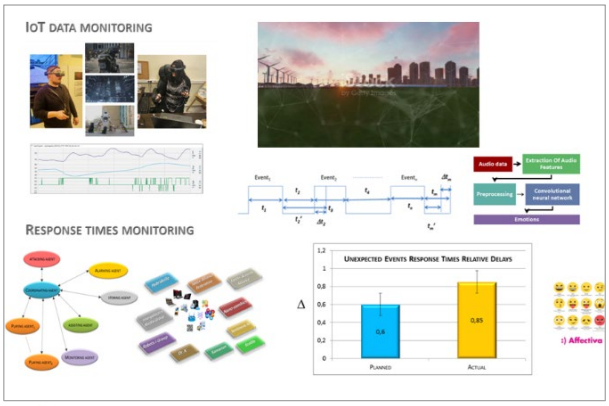


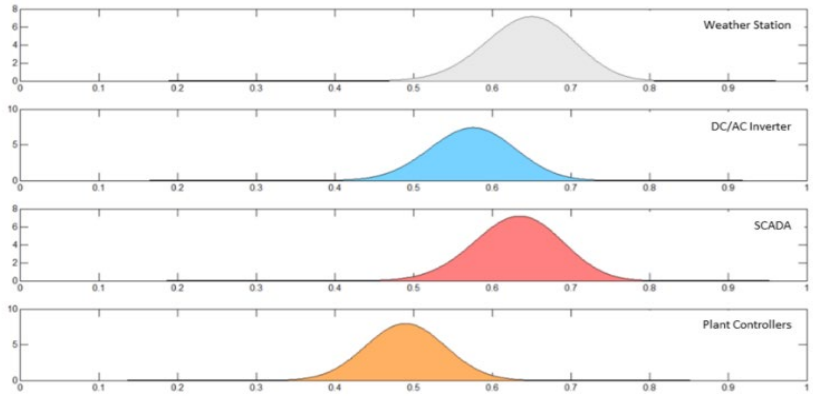
проявява, отдалечения достъп до средата, който не е достатъчно защитен и позволява генерирането на редица сценарии (основани на DDoS атаки, използване на малуер, или пролуки в комуникационните

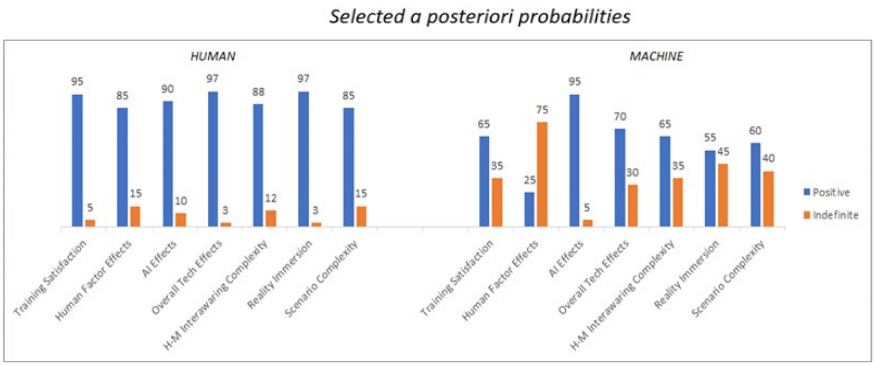


протоколи) за ескалиране на неоторизиран достъп до управлението и сензорните им системи отвън. Това от своя страна най-често засяга или външни сензорни системи, които биват компрометирани целево, или инверторните системи, които биват умишлено повредени и се налага тяхната своевременна замяна.

Предложеният модел е изследван и оценен едновременно и независимо чрез вероятностни симулации на авторски алгоритми с изкуствен интелект върху високопроизводителни GPU архитектури и с реални ползватели, експериментално в смесена реалност, като постигнатите резултати дават много добри допълнения на машинните оценки спрямо тези на експертите.







Като основен извод от направеното изследване може да се предложи една своеобразна мярка за защита на тези нови фотоволтаични решения, чрез въвеждането на допълнителни защитни интелигентни стени и IDS системи, частни VPN мрежи и слой за допълнително криптиране и защитена оторизация, които да гарантират по-надеждни цялостни фотоволтаични интелигентни решения, срещу увеличена обща себестойност на инвестицията в краткосрочен план. Друг важен момент е апробирането на използваните интелигентни алгоритмични решения за отказоустойчивост и надеждност, (показатели които са особено важни за съвременните SCADA решения) преди тяхното фактическо инсталиране.

Нови курсове в европейският цифров иновационен хъб Тракия

Европейският цифров иновационен хъб Тракия (EDIH Trakia) представя новия си курс „HPC & AI – Основи на изкуствения интелект и високопроизводителните изчисления“, предназначен за професионалисти, които искат да придобият основни знания и практически умения за приложението на изкуствения интелект в публичния сектор, бизнеса и индустрията. Курсът се осъществява по проект Cyber4AllSTAR с финансовата подкрепа на програма „Дигитална Европа“ на Европейския съюз и националната програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ 2021-2027).

Пълният текст може да прочетете тук.

Социалното инженерство остава най-използваният метод за киберпрестъпления, засягащ както бизнеса, така и гражданите, техните организации и публични институции. В отговор на тази нарастваща заплаха, Европейският дигитален иновационен хъб Тракия (ЕЦИХ Тракия) стартира нова обучителна услуга – онлайн курс „Кибер защита“ (Cyber Defense) – услуга № 20 от Каталога с безвъзмездни услуги на ЕЦИХ Тракия, предназначен за лица и организации, които искат да изградят ключови умения за защита срещу кибератаки. Курсът се осъществява по проект Cyber4AllSTAR с финансовата подкрепа на програма „Дигитална Европа“ на Европейския съюз и националната програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ 2021-2027).

Пълният текст може да прочетете тук.

Киберсигурност в областта на научните изследвания

На 4-5 март 2025 г. в Тракийския университет – Стара Загора се проведоха консултантските събития „Европейски цифрови иновационни дни в научните изследвания“, организирани от ЕЦИХ „Тракия“ по проект Cyber4AllSTAR, които бяха посветени на дигиталната трансформация и киберсигурността в сферата на научните изследвания. Двудневният форум събра на едно място водещи експерти в областта на киберсигурността, изкуствения интелект и дигиталните технологии, които представиха най-новите тенденции и иновации. Участниците имаха възможност да се включат в дискусии, семинари и презентации, с широк спектър от теми.

Събитието започна с встъпителни думи от д-р Христиан Даскалов, председател на Управителния съвет на ЕЦИХ „Тракия“, и проф. д-р Добри Ярков, ректор на Тракийския университет. Те подчертаха значението на иновациите в дигиталната ера и необходимостта от тясно сътрудничество между различните сектори.

Пълният текст може да прочетете тук.

Обучителен семинар за одитори

На 21-23 февруари 2025 г., в хотел „Ландмарк Крийк“ в Пловдив, се проведе обучителен семинар, организиран от Техникъл Трейнинг България ЕООД, Си Ай България ООД и Европейски цифров иновационен хъб „Тракия“ (ЕЦИХ Тракия). Събитието събра водещи експерти, сертифицирани одитори и представители на бизнеса, за да обсъдят актуалните тенденции, регулаторните промени и най-добрите практики в одиторската дейност.

Семинарът обхвана разнообразни теми, свързани с акредитационните изисквания, новите възможности за сертификация и подобряване на процесите по външен одит. Сред основните акценти бяха:

- **Развитие на акредитационните процеси и обратна връзка от проверките** – водещи експерти анализираха предизвикателствата и възможностите за подобрение в управлението на одити.
- **Предстоящи проектни инициативи, финансирани от ЕС** – бяха представени нови възможности за дигитализация, технологична модернизация и обучителни програми.
- **Киберсигурност и информационна сигурност** – акцент върху сертифицираните обучения в тази област, водени от експерти като Ясен Танев и Радостина Даковска.

Пълният текст може да прочетете тук.

Новата гореща тема в киберсигурността: Застраховането

В периода 30-31 януари 2025 г. в София Тех Парк се проведоха „Европейски цифрови иновационни дни в застраховането“, организирани от ЕЦИХ Тракия по проект Cyber4AllSTAR с финансовата подкрепа на програма „Дигитална Европа“ на Европейския съюз и националната програма „ПНИИДИТ 2021-2027“, в партньорство с водещи организации от сектора като Академията „Cyber360“ и „CyberOne“ – учредители на ЦИХ Тракия, както и ЗК ЛЕВ Инс, с които Хъбът си партнира още от 2023 г. по линия на националната кампания „Пази детето в интернет“.

Събитията бяха посветени на иновациите в киберсигурността и цифровизацията в застрахователния сектор, като целта бе да бъдат информирани и вдъхновени представителите на застрахователни компании, брокери и бизнеси, които активно търсят начини за дигитална трансформация и сигурност..

Пълният текст може да прочетете тук.

Безвъзмездна и експертна подкрепа за DORA съответствие

От 17 януари 2025 г., влиза в сила Регламентът за дигитална операционна устойчивост (DORA), който поставя нови изисквания пред финансовите институции и застрахователните компании в ЕС. В отговор на това предизвикателство, Цифровия иновационен хъб Тракия обявява пакет от специализирани услуги за подпомагане на организациите в техния път към съответствие с регламента, чрез предоставяне на безвъзмездни услуги необходими за постигането на целта. Всички услуги на хъба са достъпни като безвъзмездна помощ за допустимите организации, което прави прехода към съответствие с DORA по-достъпен за малките и средни предприятия.

Пълният текст може да прочетете тук.

Иноваторите говорят: Поглед отвътре към света на QSA

Иновационната екосистема на ЕЦИХ Тракия включва в себе си стотици от най-успешните и креативни компании и организации от гражданския и публичен сектор, които лидират цифровото бъдеще на България. Днес Ви представяме информационен материал по актуална тема от дигиталния дневен ред на България и Европа, подготвен от приятелите ни от 7 Security- водещ доставчик на одитни услуги в обхвата на PCI DSS. Ако и Вие желаете да публикувате в рубриката “Иноваторите говорят“, заявете своя интерес за присъединяване към нашата екосистема и споделете с аудиторията на ЕЦИХ Тракия своята гледна точка по важен за Вас въпрос.

Кои са QSA?

QSA са специалисти, сертифицирани от Съвета за стандарти за сигурност на индустрията за разплащателни карти (PCI SSC). Тяхната мисия е да помогнат на бизнеса да се съобрази със стандарта за сигурност на данните в сектора на разплащателните карти (PCI DSS) — световно призната рамка, предназначена да защитава данните на разплащателните карти.

Независимо дали става въпрос за малък бутик или мултинационална корпорация, QSA-ите се гмуркат дълбоко в техните системи, политики и процедури, за да гарантират, че отговарят на строги стандарти за сигурност. Но не става въпрос само за отбелязване на квадратчета. QSA са и консултанти, както и системни архитекти в някои случаи, като насочват организациите към по-силни защити и им помагат да се ориентират в непрекъснато променящия се пейзаж от заплахи за киберсигурността.

Пълният текст може да прочетете тук.

Академични инициативи на ЕЦИХ Тракия и стипендианти на БАК

В края на м. декември 2024, по време на форума „Европейски цифрови иновационни дни в местното самоуправление“, бяха обявени стипендиантите на Българската асоциация по киберсигурност – пилотна инициатива в подкрепа на млади експерти от различни академични сфери и нива на професионално развитие, но със сходни интереси в областта на киберсигурността.

В партньорство с Европейски цифров иновационен хъб „Тракия“ се връчват поименни стипендии в памет на доц. д-р Алексей Петров – изп. директор на Съюза за стопанска инициатива и ръководител на

катедрата „Политически науки и национална сигурност“ към Пловдивски университет «Паисий Хилендарски» в периода 2019 – 2023 г. и г-н Светлин Илиев, председател на Сдружение «ЦИХ Тракия» в периода 2021 – 2023 г. Инициативата получи подкрепата на Европейската организация по киберсигурност (ECSO) и на Европейската мрежа на цифровите иновационни хъбове към Европейската комисия (EDIH Network).

Стипендиантите за учебната 2024-2025 г. са:

- Мартин Русинов – възпитаник на Национална търговска гимназия, гр. Пловдив, специалност «Икономическа информатика». По настоящем се обучава в Национален военен университет „Васил Левски”;
- Алек Калинов – възпитаник на професионална гимназия по високи технологии „Александър С. Попов», гр. София, специалност «Приложно програмиране»;
- Стефани Тодорова – възпитаник на Технически университет – София, специалност „Киберсигурност“;
- Атанас Атанасов – възпитаник на Пловдивски университет „Паисий Хилендарски“, специалност „Киберсигурност“;
- Йоан Иванов – възпитаник на Технически университет – Варна, специалност „Софтуерни технологии“;
- Симеон Аргиров – възпитаник на Пловдивски университет „Паисий Хилендарски“, специалност „Национална сигурност“.

Обучението на стипендиантите стартира на 21.01.2025 г. и ще продължи една календарна година, през която те ще имат осигурен безплатен достъп както до над 200 курса и 60 специализации в сферата на киберсигурността, подбрани от екипа на БАК, така и до останалите над 10,000 обучителни ресурса, предоставени от водещи университети и компании през платформата „Coursera“.

Пълният текст може да прочетете тук.

Нови партньорства на ЕЦИХ Тракия в сектор „Сигурност“

Европейският цифров иновационен хъб „Тракия“ взе участие в организирания на 16 януари в Букурещ работен семинар на тема „Defensive Frontlines: Strengthening Cyber Resilience in Evolving Threat Landscapes“. Събитието се организира от Евроатлантическия център за устойчивост (E-ARC) към Външното министерство на Румъния в рамките на проекта „ECYBRIDGE: Укрепване на взаимодействието в областта на отбраната и гражданската киберсигурност“, финансиран по програма „Дигитална Европа“. В проекта от българска страна участва Висшето военноморско училище „Н.Й.Вапцаров“, а доц. Велизар Шаламанов от ИИКТ-БАН и ръководството на „Cyber4AllSTAR“ (ЕЦИХ Тракия) с координатор Съюза за стопанска инициатива е сред ключовите академични експерти, направляващи дейността на международния консорциум, съставен от военни и цивилни организации и кибер-специалисти.

Семинарът е предназначен специално за експерти в областта на киберсигурността, като например специалисти в областта на отбраната и гражданската киберсигурност, ръководители на сектори в критичните инфраструктури, експерти, участващи в междусекторни сътрудничества в областта на сигурността, представители на неправителствени организации, действащи в сектори, свързани с

киберсигурността, и т.н., и обхваща няколко основни теми: картографиране на съвременната кибервойна, устойчивост чрез сътрудничество, разбиране на киберустойчивостта и др.

Пълният текст може да прочетете тук.

Цифровите хъбове на Южен и Северен Централен Регион обявиха стратегическо сътрудничество

Подписването на споразумение за сътрудничество между базирания в гр. Пловдив Европейски цифров иновационен хъб „Тракия“ (Cyber4AllSTAR) с координатор Съюза за стопанска инициатива и Европейския цифров иновационен хъб за ускорена дигитализация на МСП от Северен Централен Регион (ADi4SMEs) с координатор Регионален иновационен център – Габрово се състоя в началото на м. януари 2025 в Бизнес център „Сиентия“ – Габрово.

Това се случи по време на организираната от Регионален иновационен център – Габрово информационна среща „Киберсигурност за МСП“. Поводът бе Директивата относно мерките за високо общо ниво на киберсигурност в Европейския съюз (Директивата NIS2), а паневропейската мрежа от цифрови хъбове в сферата на киберсигурността бе представена от страна на ЕЦИХ Тракия като възможност за получаване на безвъзмездна помощ от страна на малките и средни предприятия в процеса на постигане и доказване на съответствие с новите изисквания.

Пълният текст може да прочетете тук.

Разбиране на рисковете за киберсигурността на системите за охранителни камери

Тъй като все повече електроника или устройства изискват достъп до интернет, те стават лесни мишени за хакери и киберпрестъпници. Системите за охранителни камери не са изключение от този повишен риск. Ако трябва да се преглеждат камерите от разстояние или получаване на сигнали, свързването им с интернет ги излага на потенциални заплахи за киберсигурността. Ето някои прости, но важни стъпки, които да се предприемат, за да се намали риска от киберзаплахи в системите за сигурност:

- **Изолиране мрежата на камерите.** Един от най-ефективните начини за защита на система от камери за сигурност от кибернетични заплахи е сегментирането на мрежата, известно още като мрежова изолация. Тази стратегия включва създаване на отделна мрежа за охранителни камери, така че те да не споделят същата връзка като вашите компютри, принтери или други устройства.
- **Идентификация за вход в системата за охранителни камери.**Тази стъпка може да изглежда очевидна, но паролите по подразбиране остават един от най-големите рискове за хакване на системата за охранителна камера. Повечето съвременни системи изискват промяна на паролата по време на настройка, което намалява риска.
- **Създаване на потребителски роли в системата за охранителна камера**. Създаването на вторични потребителски акаунти, различни от основния администраторски потребител, за ежедневна употреба е наложително, ако има необходимост от достъп на други потребители.

- **Актуализиране на фърмуера**. Актуализациите на фърмуера на устройствата е от ключово значение, тъй като те обикновено се отнасят до новооткрити експлойти, наред с други неща, като подобряване на функциите. Поддържането на фърмуера на рекордера и IP охранителна камера актуален ще гарантира, че те имат най-новите корекции за сигурност.
- **Ограничаване на отдалечения достъп и наблюдаване на активността**. Най-ефективният начин да защита на системата за охранителните камери е като се ограничи или деактивира изцяло отдалечения достъп. Въпреки че това може да не е най-удобната опция, това е най-сигурният начин за предотвратяване на неоторизиран достъп.
- **Избор на марка**. Когато избирате система за охранителна камера, важно преди да направим покупката, да проверим за новини за текущи уязвимости или пробиви на данни, свързани с избраната марка. Ако една компания има повтарящи се проблеми със сигурността, трябва да потърсим друга.

Пълният текст може да прочетете тук.

Връзки към събития по киберсигурност

- Gartner Security & Risk Management Summit, 7-8 April 2025, Dubai, UAE
- CYBERUK, 6-8 May, 2025, Manchester, UK
- Cybersec Europe, 21-22 May, 2025, Brussels
- InfoSecurity Europe, 3-5 June, 2025, London, UK

Редакционен съвет

Публикуването на настоящия брой на бюлетина се реализира с финансовата подкрепа на проект: **#101083793 – CYBER4All STAR – DIGITAL-2021-EDIH-01 на ЕК**

British Embassy Sofia

СЪЮЗ ЗА СТОПАНСКА ИНИЦИАТИВА
UNION FOR PRIVATE ECONOMIC ENTERPRI

ИИКТ
ИНСТИТУТ ПО ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

BCA
BULGARIAN CYBERSECURITY ASSOCIATION
Българска асоциация по киберсигурност

ОБЩИНА ПЛОВДИВ