IT4Sec Reports 150
http://dx.doi.org/10.11610/it4sec.0150

Киберсигурност в мрежови системи за управление

Николай Найденов Хранов

Институт по информационни и комуникационни технологии – БАН
секция “Информационни технологии в сигурността”
www.IT4Sec.org

София, юни 2024

Николай Найденов Хранов, Киберсигурност в мрежови системи за управление**,** *IT4Sec Reports 150* (юни 2024), http://dx.doi.org/10.11610/it4sec.0150

IT4Sec Reports 150 „Киберсигурност в мрежови системи за управление". Настоящето изследване е свързано със система за миграция/асимилация на хибридна корпоративна мрежова система с възможност за внедрена идентификация, чрез дистанционна криптирана връзка към нова кибернетична екосистема, без активния процес да преустанови функционирането си, докато първата система не бъде окончателно асимилирана в новата такава, при нарушаване баланса на нейната киберсигурност.

Ключови думи: система за миграция/асимилация, хибридна корпоративна мрежова система, внедрена цифрова идентификация; дистанционна криптирана връзка, кибернетична екосистема, асимилиране на мрежова система, киберсигурност

IT4SecReports 150 "Cybersecurity for Network Management Systems". The present research is related to the migration/assimilation system of a hybrid corporate network system with the option of embedded identification, through a remote encrypted connection to a new cybernetic ecosystem, without the active process function ceasing, while the first system is finally assimilated into the new one, while breaking the balance of its cybersecurity.

Keywords: Migration/Assimilation System, Hybrid Enterprise Network System, Embedded Digital Identity, Remote Encrypted Connection, Cyber Ecosystem, Network System Assimilation, Cybersecurity

ISSN 1314-2119

ИЗЛОЖЕНИЕ

Автоматизирането на дейностите на корпоративната мрежа, като правило, започва с внедряване на различни системи, по-специално за съхранение, обработване и менажиране на критична работна информация, счетоводни и кадрови системи, изграждане на електронна система за управление на документи, създаване на системи за подкрепа и договорни дейности. В случая се визира наличието на няколко информационни системи в предприятието, които могат да работят автономно и са компоненти на „пачуърк “ автоматизацията [2]. В основата на изграждането на мрежовите системи за управление е концепцията за единично информационно пространство, с което трябва да работят всички подсистеми в единна база данни.

„Пачуърк“ автоматизация на мрежовите системи за управление се формира, като правило, на базата на собствени разработки с добавяне на определено количество готов софтуер, който може да поддържа различни операционна система. В мрежовите системи за управление се създава базата на единни интегрирани платформи. Създаването на мрежовите системи за управление в рамките на една инструментална среда, значително подобрява ефективността на системата.

Днес широко се използва процесният подход към управлението дейностите на мрежовата система на управление. Той определя степента на автоматизация на основните и поддържащи бизнес процеси в корпоративните мрежи. В основата на работата на информационните системи на предприятието е функционалният подход, докато при мрежовите системи за управление е интегрираният набор от програми или информационни системи, които поддържат основните процеси на информационната екосистема.

Корпоративната информационна система не е само съвкупност от програми за автоматизиране на информационни процесите: управление производство, ресурси, финансови и икономически дейности.

Характерна особеност на мрежовите системи за управление е интегрирането от край до край, в чиято основа е системният модул, отговорен за бизнес процеса на цялата мрежова система на управление.

Аналогично избраната хибридна информационна система е насочена към решаване на частни задачи, докато мрежовите системи за управление е инструмент за повишаване на ефективността от всички гледни точки.

Хибридната информационна мрежа е отворена интегрирана система в реално време, която автоматизира информационните процеси на всички нива и области на дейност, включително бизнес процеси за вземане на управленски решения.

Основната цел на мрежовите системи за управление е да се повиши ефективността и съхранението на информацията, т.е. задачите, които трябва да бъдат решени за постигане на тази цел са следните:

- свързване на информационните потоци на отделни единици и услуги в единно информационно пространство;
- повишаване на ефективността на получаването на информация, както и подобряване на нейните качества;
- увеличаване на скоростта на вземане на управленски решения и намаляване на рисковете, дължащи се на обработката на надеждна висококачествена входна информация.

Функционалността на информационната система се определя от естеството и вида дейност, организационната и правна структура, географско разположение, характера на информационен обмен;

В мрежовите системи за управление следва да включва компоненти, които гарантират промяна на информационното пространство в корпоративните мрежи:

- редактиране на базата данни, промяна на структурата, полетата на таблици, връзки, индекси и др.;
- модификация на интерфейсите за въвеждане, преглед и корекция на информация;
- управление на структурата и функциите на бизнес процесите;
- промяна в организационното и функционално съдържание на потребителските места;
- генериране на отчети, сложни бизнес сделки и форми;
- разрешение на информация (за целите на информационната сигурност), регистрация на часа на въвеждане и промяна на данни, водене на записи промени / изтривания на данни;
- инструменти за анализ на състоянието на системата по време на работа.

Анализът на състоянието на системата включва изследвания относно:

- оптималност на архитектурата на базата данни;
- ефективността на алгоритмите и програмите;
- статистика: броят на записите, документите, транзакциите, транзакциите;
- дневници на извършените операции;
- използваната дискова и оперативна памет.

ОПИСАНИЕ НА ЕКСПЕРИМЕНТА

Алгоритъм на процедиране на схема на асимилиране/миграция без прекъсване на работният процес

В миграционният процес на съществуваща компютърна архитектура, ведно с приложният и софтуер и критична информация е важно и поетапното превключване на входно изходната точка на свързаност към интернет пространството, от където се осъществяват 95% от софтуерните атаки към сигурността на мрежата и нейният актив, под формата на критична информация. Функционирането на системите и базата данни в сървърната архитектура се запазва, докато се изменят всички процеси в свързаността на системата към интернет, изразено в няколко нива: интелигентни превключватели “SW1[1]” и “SW2”, реагиращи на натоварването от входно/изходният трафик, които реално не позволяват успешно въвеждане на DDoS [2] атака. Второстепенен входно/изходен интерфейс NAT [3], свързан директно с ядрото на системата, ведно с публични превключватели “Pub SW [4]”, грижещи се за категоризиране на трафика – генерират текущи отчети в реално време към мениджмънт ресурс сегментите с човешко участие, при което се предотвратява нежелан (входно/изходен) трафик в рамките на до 15 секунди. Входен модул - “BGP AS” на хибридната мрежа към интернет свързаността, притежаващ външен протокол, осигурява безциклична маршрутизацията между домейни, който представлява интелигентен и сигурен

[1] интелигентни превключватели

[2] атака отказ от услуга

[3] входно изходен интерфейс

[4] публични превключватели

маршрутизиращ протокол с цел предотвратяване на успешно реализиране на атаки от вида “MitM [5]”, базиран на правила за киберсигурност RFC 1771.

RFC 1771 дефинира текущата четвърта версия външен протокол като маршрутизиращ протокол между автономни системи. Интернет използва BGP като основен протокол, за да поддържа пренасянето на трафик по голямата супермагистрала. Разширенията, залегнали във използваната версия 4, VLSM и Classless Inter-Domain Routing (CIDR) дават възможност на външният протокол за справяне с експоненциалното разрастване на интернет. BGP е използвана в конфигурация и обратна връзка с ядрото „kernel“ на системата за миграция, в следствие на следните предимства:

- Наличие на множество изходни точки, свързващи към едни ISP (за споделяне на натоварването).
- Наличие на множество пътища по различни ISP когато искате да управлявате начина за препращане на трафика по тези връзки.
- Интегриране на методи за маршрутизацията в реално време в зависимост от текущите нужди, избор на интелигентен път и конкретни критерии, продиктувани от промяна в архитектурата на мрежата и / или софтуерната ѝ обезпеченост.

Инфраструктурата на мрежа се използва като транзитна област за трафик на данни от различни йерархични информационни нива, без да се нарушава цялостният входно изходен поток.

Концептуален модел: за преодоляване на заплахи, превенция и повишаване нивото на защита в мрежова система за управление при определени основни характеристики:

- Система на самообслужване при поискване: Предоставя се източник на ресурси за самообслужване при поискване. Това е важна характеристика на изчислителните облаци, тъй като това позволява на процесите да променят използваните услуги като пространство и компютинг за изчисления, според необходимостта на системната и нейното натоварване без да се нарушават операциите на хоста.
- Широк достъп до мрежата: Да се използват ресурси тип cloud computing (Облачна изчислителна мощност), които могат да бъдат достъпни и осигурени, чрез основни мрежова връзка и за няколко вида устройства.
- Предложение за събиране на ресурси: Да бъдат обединени ресурсите на системата за повече ефективно и ефикасно използване. Чрез multitenancy (архитектура на софтуерно мултинаемане) и виртуализация, много потребители могат да се обслужват от един и същ физически хардуер.

ПРЕДСТАВЯНЕ НА РЕЗУЛТАТИ

Методика за изчисление на уязвимости в предложените модели и преодоляване на заплахи, в мрежова система за управление

Като методика за пресмятане на уязвимост е използвана Common Vulnerability Scoring System (CVSS) - Общата система за оценка на уязвимостите, предоставя начин за улавяне и установяване на основните характеристики на уязвимостта и изготвяне на числена оценка, отразяваща нейната сериозност. След това числовата оценка бива преведена в качествено представяне (като ниско, средно, високо и критично) чрез алгоритмично представяне, с цел правилно управление на процесите в киберсигурността на мрежовата система на управление. Анализираните стойности на установени уязвимости се калкулират според вида им и в

[5] атака „човек по средата“

процентно съотношение на засегнати данни. Използваните метрики за оценка – „показатели на уязвимости“, представени като качествена оценка за сериозност на заплахата. Оценката е групирана в три вида показатели: Основни (оценява основните показатели: обхват на мрежите; видове информационни потоци) ; Темпорални (оценяват уязвимостите при злоупотреба, които могат да се променят с времето, но остават постоянни в потребителските среди) и Микро среда (оценка защитеността на средата, предоставен като векторен низ). На база показателите се калкулира резултат, вариращ от 0 до 10, които реферира като средна стойност с общата оценка – Фиг .1:

$$\sum \text{обща оценка} = \frac{\text{Основни} \; + \; \text{Темпорални} \; + \; \text{Микросреда}}{3}$$

Фиг. 1.

Алгоритъм на оценка (използвана логика) към фиг.1:

Основни уравнения

Основният (Базов) резултат е функция на уравненията за под резултати за въздействие и експлоатация на грешките. Където основният резултат се определя като,

If (Impact sub score <= 0) 0 else,

Scope Unchanged4 $Roundup(Minimum[(Impact + Exploitability), 10])$

Scope Changed $Roundup(Minimum[1.08 \times (Impact + Exploitability), 10])$

Под резултат на въздействието към системата (ISC) е дефиниран като,

Ако резултат е непроменен 6.42 × $ISC\ Base$

Scope Changed $7.52 \times [ISCBase - 0.029] - 3.25 \times [ISCBase - 0.02]15$

Където,

$$ISCBase = 1 - [(1 - ImpactConf) \times (1 - ImpactInteg) \times (1 - ImpactAvail)]$$

Под резултат от експлоатация на грешките е:

$$8.22 \times AttackVector \times AttackComplexity \times PrivilegeRequired \times UserInteraction$$

Темпорални

Темпоралният резултат е дефиниран като,

$$Roundup(BaseScore \times ExploitCodeMaturity \times RemediationLevel \times ReportConfidence)$$

Микросреда

Стойността на оценката на Микросредата е дефинирана като:

If (Modified Impact Sub score <= 0) 0 else,

Ако модифицираният резултат е непроменен

Round up(Round up (Minimum [(M.Impact + M.Exploitability) ,10]) × Exploit Code Maturity × Remediation Level × Report Confidence)

Ако модифицираният резултат е променен

Закръгляне на стойности от резултати(Round up (Minimum [1.08 × (M.Impact + M.Exploitability) ,10]) × Exploit Code Maturity × Remediation Level × Report Confidence)

Модифицираният резултат на въздействие на средата е дефиниран като:

Ако модифицираният резултат е непроменен

6.42 × [$ISCModified$]

Ако модифицираният резултат е променен на

7.52 × [$ISCModified$ − 0.029]-3.25× [$ISCModified$ × 0.9731 − 0.02] 13

Където,

$ISCModified = Minimum$ [[1 − (1 − $M.IConf$ × CR) × (1 − $M.IInteg$ × IR) × (1 − $M.IAvail$ × AR)], 0.915]

Където модифицираният под резултат от Степента на въздействие върху средата е дефиниран като:

8.22 × $M.AttackVector$ × $M.AttackComplexity$ × $M.PrivilegeRequired$ × $M.UserInteraction$

Където „Закръгляването“ се дефинира като най-малкото число, посочено до един знак след десетичната запетая, което е равно или по-голямо от въведеното. Например, закръгляване нагоре (4.02) е 4.1; и Закръгляване нагоре (4,00) е 4,0.

Алгоритъм – дърво на дефинициите:

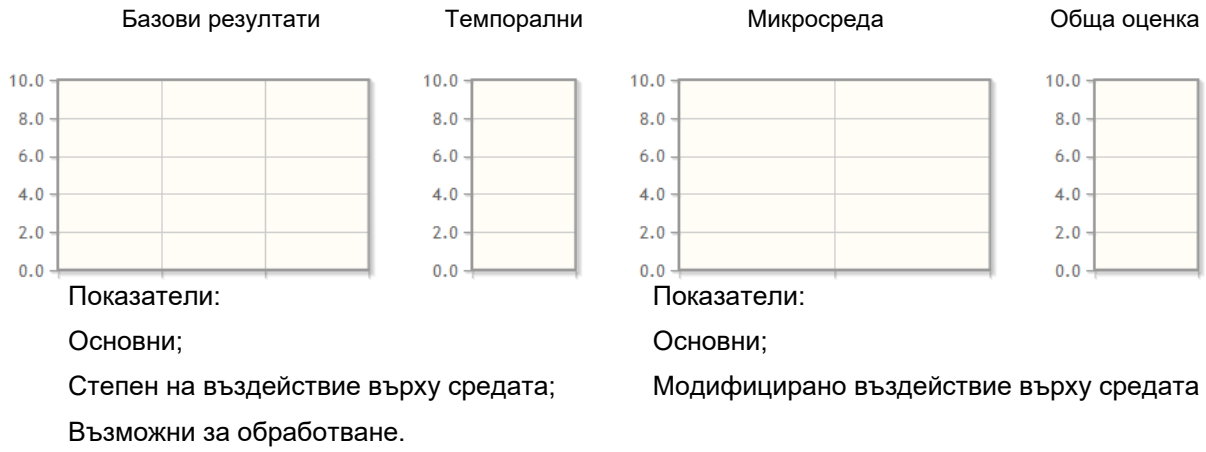
```
(Калкулиране на общият резултат)
                  |
                  |
                  \/
<BaseScore Дефиниране?> ---Не---> [OverallScore = "Не е Дефиниран"] -------
                  |
|
                Да
                  |
|
                  \/
|
    [OverallScore = BaseScore]
                  |
|
                  \/
|
<EnvironmentalScore Дефиниране?> ---Да---> [OverallScore = EnvironmentalScore
                  |
|
                  Не
|
                  |
                  \/
|
        <TemporalScore Дефиниране?> ---Да---> [OverallScore = TemporalScore]
                  |
|
                  Не
                  |
|
                  \/
|
(Връщане към общ резултат) <-----------------------------------------------
```

Резултатите за оценка на тежестта на уязвимостите се отразяват, чрез следното индексиране на математически стойности в определените интервали:

Таблица 1.

Ниво на значимост	Диапазон на резултатите (математическа стойност в интервала 0-10)
Нулево до Ниско	0.0-3.9
Средно	4.0-6.9
Високо до Критично	7.0-10.0

Изразява се таблично по следният начин – фиг. 2:



Фиг. 2.

За целите на настоящата оценка е разработен алгоритъм на пресмятане с заложените математически функции, който заимства метриките CVSS версия 2, версия 3, версия 3.1, версия 4 и версия 4.1, като предлага най-оптимално оценяване от гледна точка на максимално анализирани критерии, изразени и обобщени в цялостен резултат, който от своя страна може да бъде разгледан поетапно при необходимост от подробен анализ на всички критерии и установени данни на оценката.

Представяне и избор на модел на мрежови системи за управление:

1. Предложение за функционален модел (Модел №1: идеална среда) на мрежова система за управление:

Системни компоненти на предлаганата мрежова системи за управление:

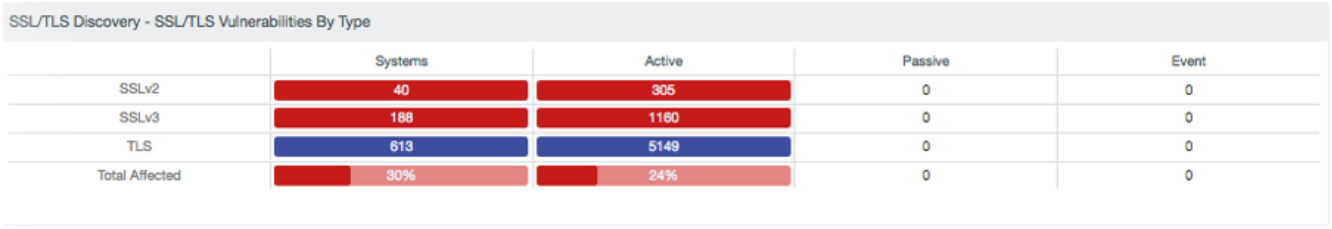
- Платформата като услуга - PaaS[6]
- Софтуер като услуга - SaaS[7]
- Инфраструктура като услуга - IaaS[8]

[6] Облачна услуга – Platform as a Service (PaaS) (от англ.) – Изработване на платформа като услуга

[7] Облачна услуга – Software as a Service (от англ.) – Софтуер като услуга

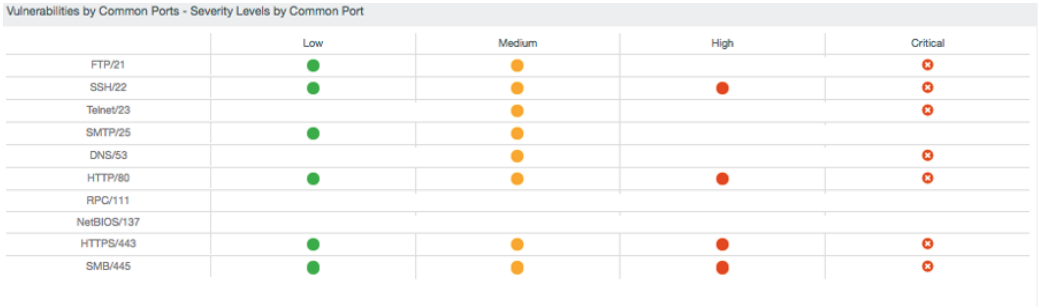
[8] Облачна услуга - Infrastructure as a Service (от англ.) – Цялостна инфраструктура като услуга

Проведен експеримент: Показания на процесите при неутрализиране на атаката (табличен вид – експорт от системата – уязвимости според вида си и в процентно съотношение на засегнати) - Установени връзки фиг. 3:

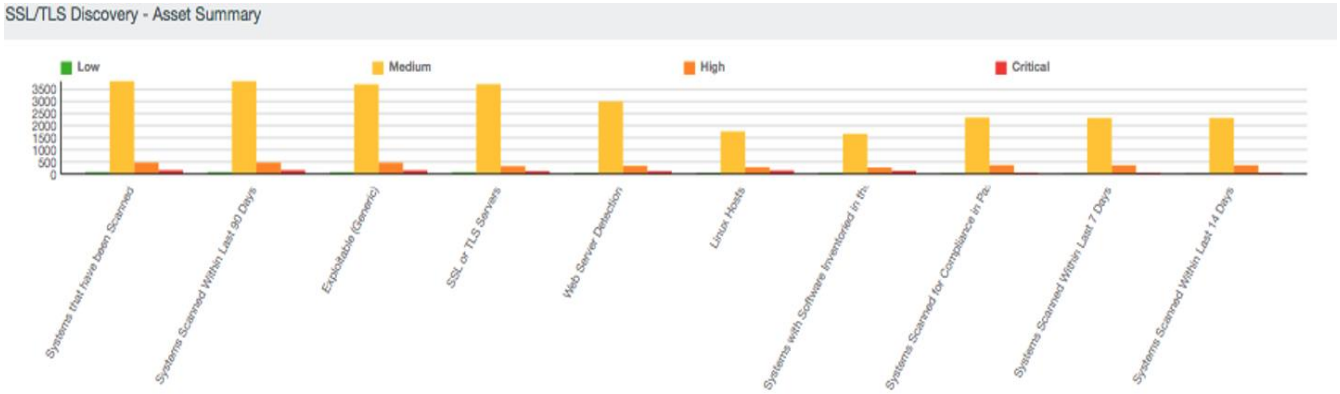


Фиг. 3.

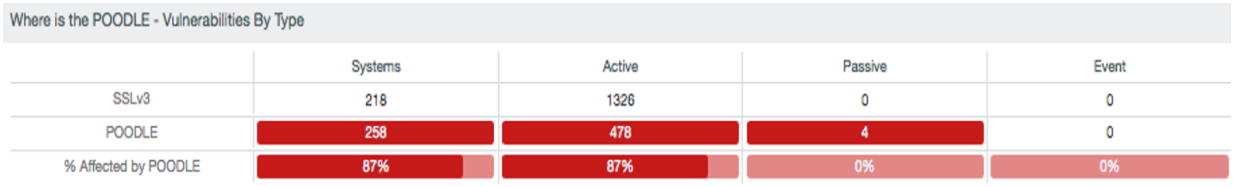
Дефиниция: Установени слабости в SSL/TLS сертификати за комуникационна сигурност, посочване на системни и текущо активни, при калкулация на Общо засегнати точки:



Фиг. 4 – Уязвимости от отворени по подразбиране комуникационни портове – средна натовареност с нива в скала Ниска, Средна, Висока и Критична заплаха

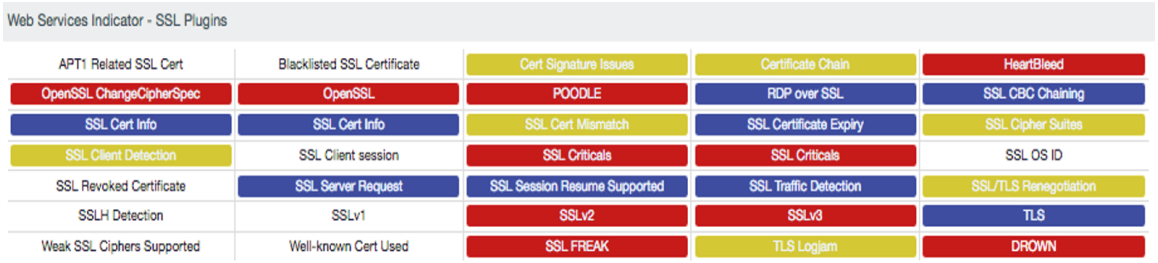


Фиг. 5 – Сумарна активност на установените и предотвратени заплахи в хронологичен ред: седмичен, двуседмичен, тримесечен

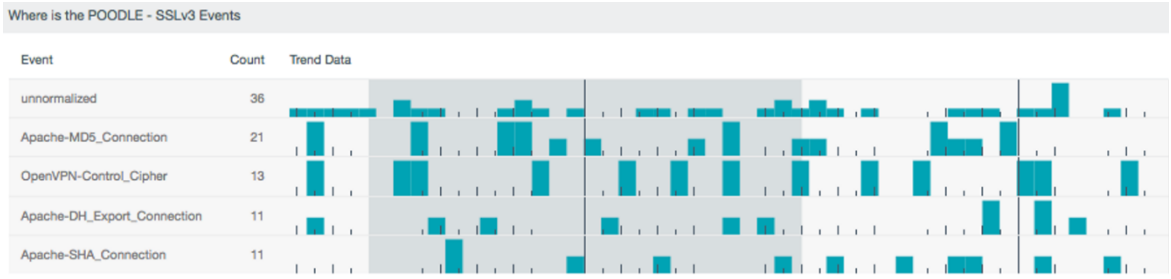


Фиг. 6 – Категоризиране на установените и предотвратени заплахи според вида им с представяне в математическа стойност и процентно съотношение

Фиг. 7 – Топологично разпределение съгласно мрежовата система за управление на установените и предотвратени заплахи в брой и цветова индексация: Ниско, Средно, Високо, Критично



Фиг. 8 – Интернет базиран индикатор на услугите, относими към SSL[9] внедрени интегратори на установените и предотвратени заплахи, с цветна индексация: Червено (Критична заплаха, Висока заплаха), Жълто (Средна заплаха, Ниска заплаха), Синьо (Процес, за който е необходимо подобрение на конфигурацията по защита)



Фиг. 9 – Матрица на активността – събития, с установените и предотвратени заплахи. Показатели съгласно използваните метрики за оценка – „показатели на уязвимости“; тенденция на събитието като заплаха

Таблица №2, резултати от оценка на нивата на сигурност на общ хибриден модел, зададен по условие и изпълним в идеална стерилна среда и затворена екосистема (виртуална лабораторна тестова среда) на мрежовата система.

Оценка на предложеният общ модел – идеална среда

[9] *Secure Sockets Layer – защитен протокол*

Таблица 1

	Стойности 0-10
Базова оценка (обобщава цифрово резултата от анализа)	10
Времева оценка (обобщава резултата от време за реакция и справяне с проблем в сигурността)	9,3
Оценка околна среда (цифрова стойност на запазената цялост на функционалността на цялата система на управление)	8,4

За избор на модел с необходимите характеристики за достигане на ниво максимална киберсигурност в съответствие със идеалният модел в стерилна среда е предложен освен базов хибриден модел и още 2 модела:

2. Предложен МОДЕЛ №2 (Хибридна система)

Проведен експеримент: Показания на процесите при неутрализиране на атаката (табличен вид – експорт от системата). Базова матрица на риска с включени Вектор на достъпа (AV), Автентификация (AU), Сложност на достъпа, Рисков анализатор /съдържа съотношението на установените уязвимости към тези подлежащи на въздействие/ Фиг. 10:

CVSS Base Risk Matrix - Access Vector (AV), Authentication (Au), AccessComplexity(AC) Risk Analysis

Access Vector (AV)	Local (L)	Adjacent Network (A)	Network (N)
Vulnerabilities	8084	164	119278
Exploitable	59%	26%	44%
Access Complexity (AC)	High (H)	Medium (M)	Low (L)
Vulnerabilities	17333	70847	39346
Exploitable	49%	56%	25%
Authentication(Au)	Multiple (M)	Single (S)	None (N)
Vulnerabilities	0	2292	125234
Exploitable	0%	55%	45%

Фиг. 10

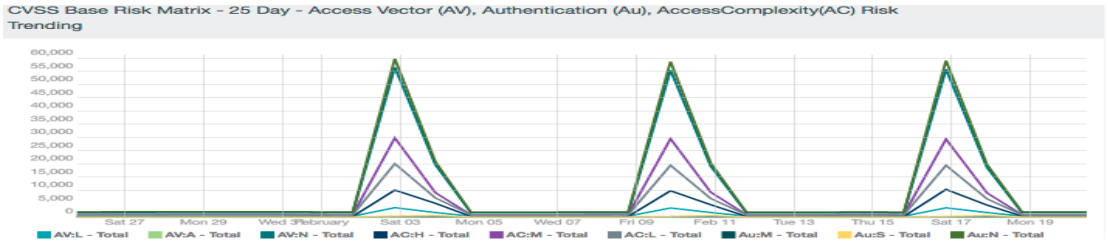
Базова матрица на риска с включени общата система за оценка на уязвимостите. Съдържа конфиденциалност, наличност и интегритет на информацията, с добавяне на анализ на риска от въздействието: измерването е съгласно стойности от съотношението на установените уязвимости към тези подлежащи на въздействие - Фиг. 11:

CVSS Base Risk Matrices - Confidentiality (C), Availability (A), Integrity (I) Impact Risk Analysis

	None (N)	Partial (P)	Complete (C)
Confidentiality Vulns	9044	37476	81006
Confidentiality Exploit	16%	31%	55%
Integrity Vulns	24805	22496	80225
Integrity Exploit	27%	29%	56%
Availability Vulns	40135	6243	81148
Availability Exploit	21%	65%	56%

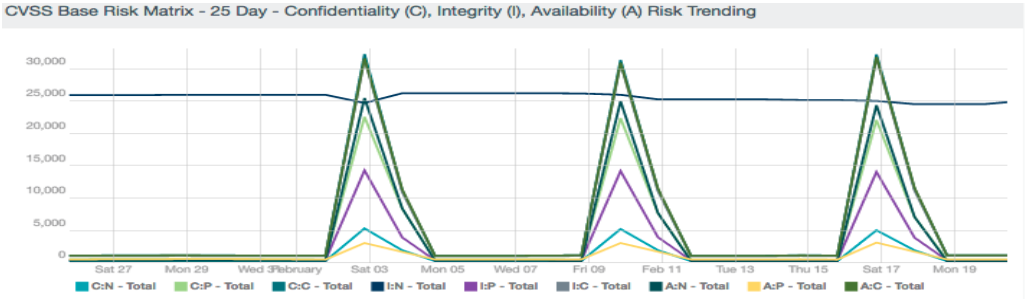
Фиг. 11

Графично представяне на измерването - Графично изобразяване базова матрица на риска в хронологична последователност от 25 дни: с включени Вектор на достъпа (AV), Автентификация (AU), Сложност на достъпа, Рисков анализатор /съдържа съотношението на установените уязвимости към тези подлежащи на въздействие/:



Фиг. 12

Графично изобразяване базова матрица на риска в хронологична последователност от 25 дни: с включени конфиденциалност, наличност и интегритет на информацията, с добавяне на анализ на риска от въздействието: измерването е съгласно стойности от съотношението на установените уязвимости към тези подлежащи на въздействие - Фиг. 13



Фиг. 13

Оценка на предложеният общ модел – хибридна система

Таблица 3, резултати от оценка на нивата на сигурност - хибриден модел №2

Таблица 2

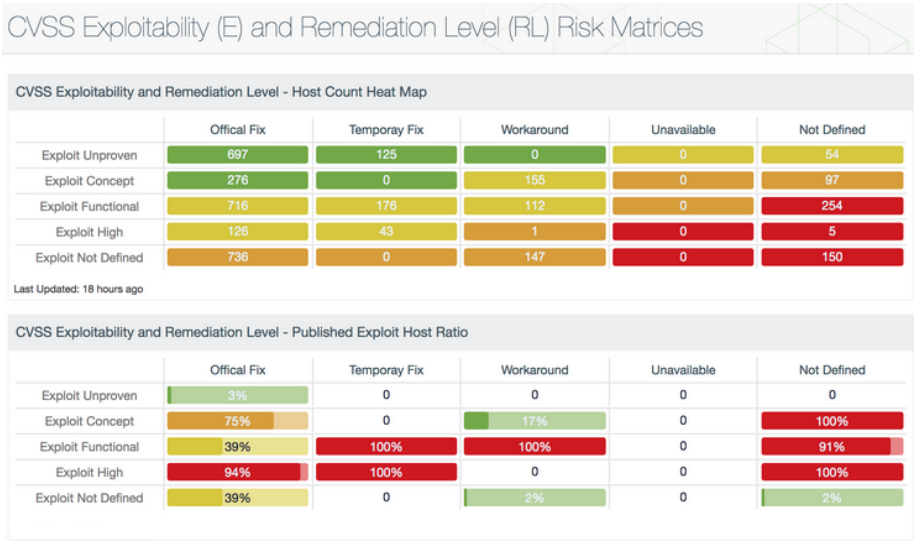
	Стойности 0-10
Базова оценка (обобщава цифрово резултата от анализа)	4,0
Времева оценка (обобщава резултата от време за реакция и справяне с проблем в сигурността)	3,5
Оценка околна среда (цифрова стойност на запазената цялост на функционалността на цялата система на управление)	5,6

3. Предложен функционален модел №3 с интегриран модул за контрол на сигурността, чрез външно администриране, акумулира всички характеристики на Модел №2 (Хибридна система) и допълнителните [1]:

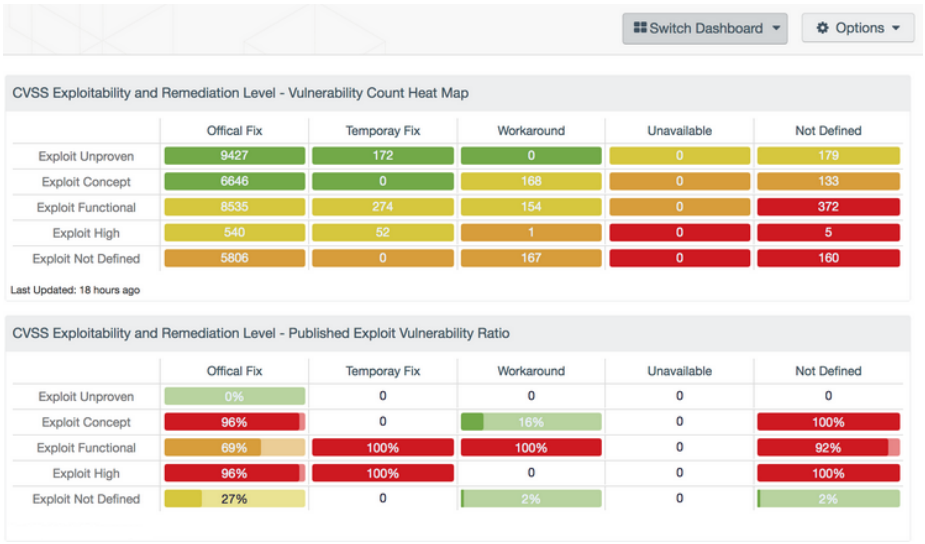
- Checkpoints: шлюзове към база данни за противодействие на известни зловредни кодове
- Автоматизирано възстановяване: платформа за критично възстановяване на системата при тотален срив.

- Dynamic Device Association: процес, по мениджмънт протичащ в реално време, отговорен за адаптация на устройствата в средата.
- Controller-Switch Trust: предоставяне и снемане на доверие от външни програми при работа с базата данни вътрешна за системата.
- Controller-App Plane Trust: мениджмънт на правила на външни програми при работа с базата данни вътрешна за системата.
- Security Domains: класификацията на актива на мрежата, нивата на достъп и свързаността ѝ.
- Дистанционен пряк достъп до паметта (RDMA): Мениджмънт подход с цел превенция от зловреден код.
- Получаване на мащабиране на страниците (RSS): софтуерен механизъм за обмен на информация между два интернет базирани сайта.
- Опашка на виртуална машина (VMQ):
- Обединяване на мрежовия адаптер: физическият мрежов адаптер, който прехвърля данните, директно към паралелна опашка за изпълнение.
- Вмъкване на комутатори (SET): Мениджмънт на множество физически мрежови адаптери.
- Packet Direct: оптимизирана технология за прехвърляне на пакети към външни оторизирани приложения и системи от iOS и Android.
- Server Gateway: сървърен шлюз, с който комуникира интегрираният модул за контрол на сигурността, осигурен чрез външно администриране.
- Внедряване на Distributed Firewalls: разпределена защитна стена с множество потребители, която се предлага като услуга от доставчика на интернет свързаност.
- SMB Multichannel: конфигурация, позволява]а на файловите сървъри да използват множество мрежови връзки едновременно.
- SMB Direct: конфигурация, поддържаща използването на мрежови адаптери, които имат отдалечен директен достъп до паметта (RDMA).
- SMB Encryption: защитаване на SMB Direct конфигурацията.
- Storage Quality of Service (QoS): функция за наблюдение и управление на производителността на ресурсите за съхранение чрез: разпределени на отделни виртуални машини.
- Data Deduplication: анализ на дублиращ се информационен поток или масив
- App-V: среда за виртуализация на приложения, спомагаща за работата на екосистемата като цяло
- RemoteApp: Достъпът до съответните програми съобразно рестрикциите и правата на всеки потребител/служител
- Single Sign On: Система за оторизиране на потребител към акаунт, чрез автентификация на трета независима страна – определена от системата за „доверена“.

Установени показания на процесите при неутрализиране на атаката (табличен вид – експорт от системата) Фиг. 14 и Фиг. 15 (уязвимости към тези подлежащи на въздействие ведно с нивата на сканиране). Показанията са съобразени съобразно установените, дефинирани и недефинирани заплахи:



Фиг. 14



Фиг. 15

Оценка на предложеният общ модел – с интегриран модул за контрол на сигурността чрез външно администриране

Таблица 4 резултати от оценка на нивата на сигурност - хибриден модел №3

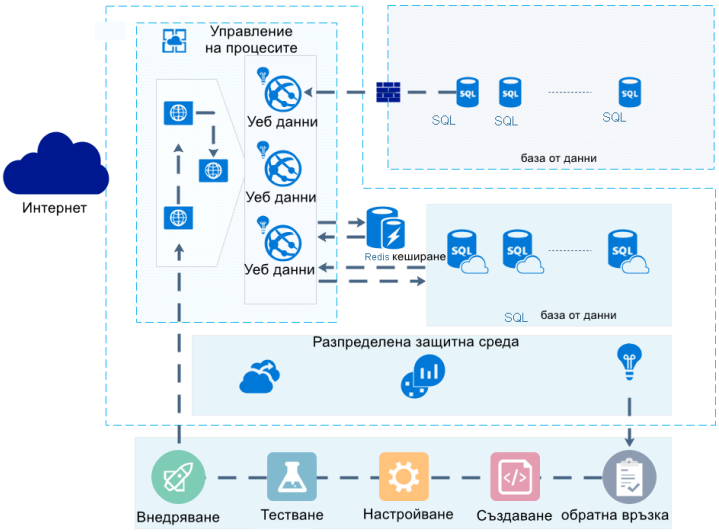
Таблица 3

	Стойности 0-10
Базова оценка (обобщава цифрово резултата от анализа)	7,5
Времева оценка (обобщава резултата от време за реакция и справяне с проблем в сигурността)	6,3
Оценка околна среда (цифрова стойност на запазената цялост на функционалността на цялата система на управление)	6,4

ОБСЪЖДАНЕ НА РЕЗУЛТАТИТЕ:

Сравнителен анализ на установените в хода на изследването предимства и недостатъци в предложените модели на киберсигурност в мрежовите системи на управление

Предимствата на предложените модели са ключовите компоненти за контрол, превенция и мониторинг в реално време на сигурността в предложените модели на мрежовите системи за управление. Но като следващо поколение на архитектура може да бъде посочен използван модел №2 (хибридна система) и №3 (контрол на сигурността с външно администриране) с внедрена разпределена защитна структура, приложима чрез “Distributed Firewalls” - Фиг.17, [3]:

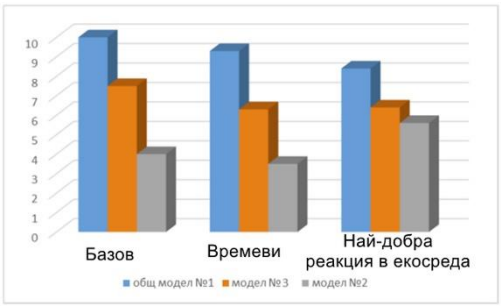


Фиг. 17

- Констативни заключения и избор спрямо направените тестове и експерименти:

В резултат на проведеното изследване между трите приети модела – общ №1; №2 (хибридна система), и №3 (интегриран модул за контрол на сигурността чрез външно администриране) се установи, че в метрика „базова“ - най-ниска стойност има модел №2(хибридна система), в метрика „времева“ - най ниска стойност има облачен модел №2 (хибридна система) и в метрика „Най-добра реакция в екосистема“ има №2 (хибридна система). В следствие на резултатите от проведеното изследване максимално оптимизиран модел в текущо поставената среда има следните характеристики:

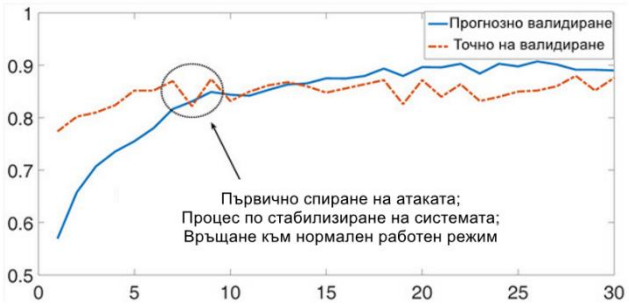
Обобщени групи метрики на трите модела в таблично представяне на резултатите от проведеното тестване - Фиг. 18:



Фиг. 18

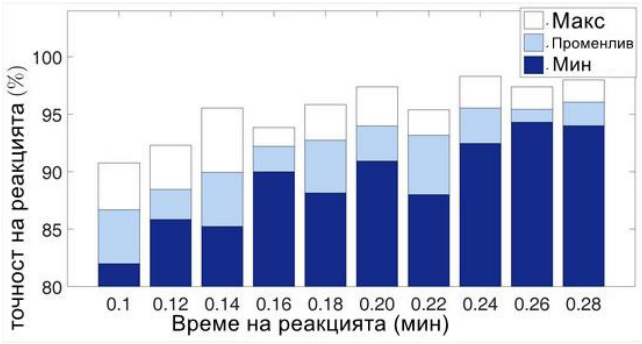
Като Извод от направеното изследване се установиха предимствата на избраният хибриден модел на киберсигурност в мрежовите системи за управление, а именно: Модел №2:

Графично представяне оптимална времева реакция и привеждане на системата в стабилност след атака при Модел №2 на база допълнително проведени симулации – Фиг. 19:



Фиг. 19

Вариацията на точността на самообучението на средата и точността на валидиране на информацията - Фиг. 20:



Фиг. 20

ЗАКЛЮЧЕНИЕ

Изследвания хибриден модел №2 на киберсигурност в мрежовите системи за управление, предложен в настоящето изследване, използва като решение установяване на потенциални заплахи на системата за управление самообучаващи се алгоритми, разполагащи с изкуствен интелект. Самия процес на самообучение е непрекъснато развиваща се база за установяване на слабости и заплахи в системата, автоматично предприемане на решения, съобразени с вече установената конфигурация на системата за управление на мрежата. В допълнение се предлагат и нови конфигурационни методи за тестване в изолирана виртуална среда.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

[[1] Andrea Bianchi, Ian Oakley and Dong Soo Kwon, „Open Sesame: Design Guidelines for Invisible Passwords,“ *IEEE Computer Society*, April, 2012, p.p. 58-65, ISSN 0018-9162.

[2] Harold Joseph Highland, „Computer Virus Handbook,“ Advanced Technology, 2018.

[3] Hafedh Chourabi, et al., „Understanding Smart Cities: An Integrative Framework, System Science (HICSS),“ 45th Hawaii International Conference on System Sciences, 2020, p.p. 2289-2297, DOI: 10.1109/HICSS.2012.615.