

КИБЕРЗАПЛАХИ И ПРОТИВОДЕЙСТВИЕ В ЦЕНТРОВЕ ЗА ДАННИ

Rosen Pasarelski

CYBER THREATS AND COUNTERACTION IN DATA CENTERS

Rosen Pasarelski

Резюме: С бързото развитие на комуникационните и информационните технологии, центровете за данни се утвърждават като критична инфраструктура, изложена на комплексни и еволюиращи киберзаплахи. Настоящото изследване анализира основните категории заплахи, включително злонамерен софтуер, рансъмуер атаки, вътрешни заплахи, разпределени атаки за отказ от услуга (DDoS), както и уязвимости в мрежовата и физическата сигурност. Подчертава се нарастващата роля на автоматизацията и изкуствения интелект в съвременните кибератаки, което усложнява процесите по тяхното откриване и неутрализиране. Целта на статията е да изследва характеристиките на съвременните киберзаплахи и да формулира ефективни подходи за защита на центровете за данни чрез интегрирани модели за киберсигурност. Научните приноси включват систематизация на актуалните заплахи, идентифициране на критични уязвимости и разработване на концептуален модел за многостепенна защита, съчетаващ технологични и организационни механизми. Резултатите от изследването показват, че прилагането на интегрирани решения, базирани на ранно откриване, анализ на аномалии и ефективно управление на достъпа, води до съществено повишаване на сигурността и надеждността на центровете за данни, както и до редуциране на времето за реакция при инциденти.

Ключови думи: киберзаплахи, киберсигурност, центрове за данни, DDoS, MW, RW, APT, Zero-day, IAM.

Abstract: With the rapid development of communication and information technologies, data centers are becoming a critical infrastructure exposed to complex and evolving cyber threats. This study analyzes the main categories of threats, including malware, ransomware attacks, insider threats, distributed denial of service (DDoS) attacks, as well as vulnerabilities in network and physical security. The increasing role of automation and artificial intelligence in modern cyber-attacks is emphasized, which complicates the processes of their detection and neutralization. The aim of the article is to examine the characteristics of modern cyber threats and to formulate effective approaches to protect data centers through integrated cybersecurity models. The scientific contributions include the systematization of current threats, identification of critical vulnerabilities, and development of a conceptual model for multi-layered protection, combining technological and organizational mechanisms. The results of the study show that the implementation of integrated solutions based on early detection, anomaly analysis and effective access management leads to a significant increase in the security and reliability of data centers, as well as a reduction in incident response time.

Keywords: cyber threats, cybersecurity, data centers, DDoS, MW, RW, APT, Zero-day, IAM.

1. Въведение

В условията на интензивно развитие на комуникационните и информационни технологии и експоненциален ръст на генерираните и обработвани данни, центровете за данни се утвърждават като ключов компонент на съвременната дигитална телекомуникационна инфраструктура. Те осигуряват надеждно съхранение, обработка и разпространение на информация, като поддържат функционирането на критични услуги в публичния и частния сектор. Паралелно с това, тяхната стратегическа значимост ги превръща в приоритетна цел на широк спектър от киберзаплахи. Съвременната киберсреда се характеризира с нарастваща сложност и динамика, като атаките стават все по-

ROSEN PASARELSKI

целенасочени, автоматизирани и трудни за откриване. Сред най-разпространените заплахи се открояват разпределените атаки за отказ от услуга (DDoS), атаките тип ransomware (RW), усъвършенстваните устойчиви заплахи (APT), както и експлоатирането на уязвимости от тип “zero-day”. Тези заплахи могат да доведат до компрометиране на чувствителна информация, прекъсване на услугите и значителни икономически щети. В този контекст необходимостта от ефективни механизми за киберзащита на центровете за данни придобива критично значение. Изграждането на надеждни и адаптивни системи за сигурност изисква интегриран подход, съчетаващ съвременни технологични решения, адекватни организационни политики и непрекъснат мониторинг на заплахите. В допълнение, развитието на облачните изчисления, виртуализацията и разпределените архитектури значително увеличава повърхността за атаки, като създава нови предизвикателства пред сигурността на центровете за данни. Интеграцията на хибридни и мултиоблачни среди изисква прилагането на унифицирани политики за сигурност и ефективни механизми за управление на достъпа, които да обезпечат защита на данните независимо от тяхното местоположение. Особено съществено значение придобиват и вътрешните заплахи, произтичащи от неоторизирани действия или грешки на служители, както и недостатъчно ефективни процедури за контрол и мониторинг. Човешкият фактор остава един от най-слабите елементи в системите за сигурност, което налага необходимостта от повишаване на осведомеността и провеждане на регулярни обучения. Наред с това, регулаторните изисквания и стандартите за информационна сигурност, като ISO/IEC 27001 и други добри практики, поставят допълнителни изисквания към управлението и защитата на данните. Спазването на тези стандарти не само подпомага минимизирането на риска, но и повишава доверието на потребителите и партньорите. В този контекст, изследването на съвременните киберзаплахи и разработването на ефективни стратегии за противодействие се явяват ключов фактор за осигуряване на надеждност, непрекъсваемост и устойчивост на центровете за данни в условията на динамично променяща се киберсреда.

2. Класификация на киберзаплахите

Киберзаплахите, насочени към центровете за данни, се характеризират с разнообразие, динамичност и висока сложност, което изисква систематично класифициране за ефективно управление на риска. В практиката по киберсигурност като съвременни киберзаплахи се разграничават следните основни категории:

- Разпределени атаки за отказ от услуга (DDoS) – тези атаки целят претоварване на мрежовата инфраструктура на центъра за данни чрез масивен и координиран трафик от множество източници. Ефектът е временно или продължително блокиране на услуги, което може да доведе до загуба на бизнес и нарушаване на достъпа до критични ресурси. Съвременните DDoS атаки използват автоматизирани ботнет мрежи, IoT устройства и облачни ресурси за увеличаване на мащаба и сложността на атаката.
- Злонамерен софтуер (Malware – MW) – включва вируси, троянски коне, червеи, кейлогъри и шпионски софтуер. Тази киберзаплаха може да компрометира системи, да модифицира или унищожава данни и да създава задни врати за бъдещи атаки. Често се използва за кражба на чувствителна информация, например лични данни, корпоративни тайни или кредити за достъп до облачни услуги. Някои модерни MW атаки включват саморазпространяващи се червеи и използване на изкуствен интелект за адаптиране към защитните механизми на системата. Проникването става чрез изпълними файлове, прикачени към имейли, заразени сайтове или уязвимости в софтуерната инфраструктура.
- Рансъмуер (Ransomware – RW) – представлява софтуер, който криптира данните на центъра за данни и изисква финансова компенсация за възстановяването им. Често това се предлага като услуга от хакери (RaaS – Ransomware-as-a-Service), което

позволява на по-малко технически квалифицирани нападатели да провеждат мащабни кампании. Рансъмуерът може да бъде комбиниран с изтичане на данни (data leak), което увеличава психическия натиска върху жертвата и повишава финансовата стойност на откупа. Типични примери са атаки, насочени към критични облачни услуги, здравни системи и финансови институции. Проникването обикновено започва чрез фишинг, компрометирани уеб страници или уязвимости от тип zero-day. След като изпълнимият файл се стартира, RW криптира данните и оставя искане за откуп. Механизмът на атака включва използване на силни криптографски алгоритми, които правят възстановяването на данните невъзможно без ключ.

- Усъвършенствани устойчиви заплахи (Advanced Persistent Threats – APT) – целенасочени и продължителни атаки, насочени към стратегически данни или системи. Атаките от типа „АПТ“ използват комбинация от технически средства и социално инженерство, за да останат незабелязани за дълъг период. Тези заплахи могат да включват проникване чрез фишинг имейли, експлоатация на уязвимости, компрометиране на IAM системи и внедряване на задни врати. Целта на АРТ е не просто краткотрайно нарушаване на работата на системата, а дългосрочно събиране на информация или контрол над инфраструктурата.
- Уязвимости от тип „Zero-Day“ – експлоатират непознати или нерешени софтуерни уязвимости, за които производителят все още не е пуснал официално издание или обновление на софтуера, което поправя грешка или проблем в системата. Тези атаки са особено опасни, тъй като обичайните антивирусни и защитни системи не могат да ги открият. Киберзаплахите от типа „Zero-Day“ могат да бъдат използвани за проникване в центрове за данни, кражба на критична информация или инсталиране на MW за по-нататъшни действия.
- Управление на идентичности и достъп (Identity and Access Management – IAM) – слабости в IAM системите позволяват неоторизиран достъп, ескалация на привилегии и компрометиране на чувствителни данни. Недостатъците могат да бъдат както технологични (слаби пароли, липса на двуфакторна автентикация), така и организационни (неактуализирани роли и права, липса на мониторинг на действията на потребителите).
- Фишинг и социално инженерство (PH) – атаки, насочени към служители или потребители, които целят извличане на пароли, ключове за достъп или други чувствителни данни. Методи включват измамни имейли, подправени линкове и фалшиви портали, които изглеждат легитимни. Фишингът често се използва като първа стъпка за проникване в системите на центрове за данни и може да бъде комбиниран с MW или RW заплахи. Атаката се реализира чрез подвеждащи съобщения, които мотивират потребителя да разкрие чувствителна информация или да стартира MW.
- Съвременни комбинирани заплахи – тенденцията е към мулти-векторни атаки, които комбинират няколко типа заплахи. Примерите включват RW + DDoS, APT + Zero-Day или фишинг атаки, подпомагащи разпространение на MW. Тези комбинирани подходи затрудняват откриването и противодействието и налагат използването на интегрирани системи за защита и мониторинг.

Тази класификация осигурява основа за анализ на рисковете и разработване на многостепенни стратегии за киберсигурност, включително превантивни, детективни и корективни мерки, насочени към защитата на центрове за данни.

3. Механизми на реални кибератаки

Разбирането на механизма на кибератаките е от ключово значение за ефективното изграждане на стратегии за защита на центрове за данни. В тази част на статията се разглеждат реални методи за проникване, разпространение и експлоатация на уязвимости, характерни за съвременните заплахи.

3.1.Разпределени атаки за отказ от услуга (DDoS)

Атаката DDoS се осъществява чрез координирано изпращане на огромен обем заявки от множество компрометирани устройства (ботнет) към даден сървър. Основният механизъм включва засичане на слабости в мрежовите протоколи, претоварване на сървъри и маршрутизатори, както и използване на аномалии в трафика за блокиране на легитимни заявки. В някои случаи DDoS се комбинира с компрометиране на DNS сървъри или CDN услуги за максимално въздействие.

Пример 1: Механизъм на DDoS атака (псевдокод)

Атаката се осъществява чрез множество компрометирани устройства, които изпращат заявки към целеви сървър:

```
initialize botnet_devices
set target_server
set attack_duration
set request_interval_range

function generate_request():
    request = create_generic_network_request()
    randomize_headers(request)
    return request

function send_traffic(device):
    start_time = current_time()

    while current_time() - start_time < attack_duration:
        request = generate_request()

        send_request_to_target(device, target_server, request)

        wait(random_value(request_interval_range))

parallel_for each device in botnet_devices:
    send_traffic(device)
```

Разширеният модел представя реалистична структура на DDoS атака. Всеки компрометиран възел (бот) функционира независимо и генерира заявки с вариращи параметри, което затруднява откриването на атаката чрез стандартни филтри. Използването на паралелно изпълнение симулира едновременен трафик от множество източници. Включването на случайни интервали между заявките и модификация на параметрите (например заглавни полета) отразява реални техники за избягване на механизми за защита от типа „rate limiting и signature-based detection“. Ограничаването чрез времеви параметър (attack_duration) показва контролирано провеждане на атаката. Този модел демонстрира как координираното генериране на голям обем трафик може да доведе до изчерпване на

ресурсите на целевата система (CPU, памет, мрежова пропускателна способност), което е основната цел на DDoS атаките срещу центрове за данни.

Пример 2: Механизъм на рансъмуер атака (псевдокод)

Рансъмуер атаката се реализира чрез проникване в системата (често чрез фишинг или уязвимост), последвано от криптиране на критични данни и изискване на откуп за тяхното възстановяване:

```
initialize target_system
initialize encryption_key

function scan_files(system):
    return list_of_critical_files(system)

function encrypt_files(files, key):
    for each file in files:
        encrypt(file, key)

function display_ransom_note():
    show_message("Данните ви са криптирани. Платете откуп, за да възстановите достъпа.")

files = scan_files(target_system)
encrypt_files(files, encryption_key)
display_ransom_note()
```

Посоченият модел представя типичната логика на рансъмуер атака, при която първоначално се идентифицират критичните файлове в системата, след което те се криптират със силен криптографски алгоритъм. Показването на съобщение за откуп цели психологически натиск върху жертвата. В реални условия атаката може да включва и експулзация на данни (data exfiltration), което допълнително увеличава въздействието. Подобни атаки представляват сериозна заплаха за центрове за данни, поради потенциалната загуба на достъп до критична информация и прекъсване на услуги.

Пример 3: Механизъм на АРТ атака (псевдокод)

Атаките АРТ представляват дългосрочни и целенасочени кампании, насочени към проникване и устойчиво присъствие в системата:

```
initialize target_network

function initial_access():
    exploit_vulnerability() or execute_phishing_attack()

function establish_persistence():
    install_backdoor()
    create_hidden_access()

function lateral_movement():
    discover_internal_systems()
    gain_additional_access()

function data_exfiltration():
    collect_sensitive_data()
    transfer_data_to_external_server()
```

```
initial_access()  
establish_persistence()  
lateral_movement()  
data_exfiltration()
```

Този модел илюстрира многоетапния характер на АРТ атаките. След първоначален достъп се установява дългосрочно присъствие чрез бекдори, което позволява странично придвижване в мрежата и постепенно разширяване на контрола. Основната цел е извличане на чувствителна информация без да се предизвиква подозрение. В контекста на центровете за данни това може да доведе до продължителна компрометация на инфраструктурата.

Пример 4: Механизъм на Zero-Day атака (псевдокод)

Атаките Zero-Day използват неизвестни уязвимости в софтуера преди наличието на защитен механизъм:

```
initialize target_application  
  
function discover_vulnerability():  
    analyze_application_behavior()  
    identify_unpatched_flaw()  
  
function exploit_vulnerability():  
    execute_malicious_input()  
    gain_unauthorized_access()  
  
function escalate_privileges():  
    obtain_higher_access_rights()  
  
function deploy_payload():  
    install_malware()  
    maintain_access()  
  
discover_vulnerability()  
exploit_vulnerability()  
escalate_privileges()  
deploy_payload()
```

Логиката на модела показва как атакуващият първо идентифицира неизвестна уязвимост, след което я експлоатира за получаване на достъп до системата. Ескалацията на привилегии позволява по-дълбок контрол, а внедряването на зловреден код осигурява устойчив достъп. Липсата на официално издание или обновление на софтуера прави този тип атаки особено трудни за предотвратяване.

Пример 5: Механизъм на атака чрез компрометиране на IAM (псевдокод)

Атаките срещу системи за управление на идентичности и достъп се базират на кражба или злоупотреба с потребителски идентификационни данни:

```
initialize login_system  
  
function obtain_credentials():  
    perform_phishing() or use_leaked_data()  
  
function authenticate(credentials):  
    if valid(credentials):  
        grant_access()
```

```
function escalate_privileges():  
    access_admin_functions()  
    modify_permissions()
```

```
function access_resources():  
    retrieve_sensitive_data()
```

```
credentials = obtain_credentials()  
authenticate(credentials)  
escalate_privileges()  
access_resources()
```

Този модел демонстрира как чрез компрометирани идентификационни данни може да се осъществи неоторизиран достъп до системата. След успешна автентикация атакуващият може да ескалира привилегиите си и да получи достъп до критични ресурси. В центровете за данни подобен тип атака е изключително опасен, тъй като може да остане незабелязан дълго време.

Пример 6: Механизъм на фишинг атака (псевдокод)

Фишинг атаките (РН) представляват една от най-разпространените форми на социално инженерство, при които атакуващият манипулира потребителите с цел получаване на чувствителна информация, като потребителски имена, пароли или други идентификационни данни, чрез имитиране на доверени източници и създаване на измамни комуникационни канали:

```
initialize target_user
```

```
function create_fake_message():  
    message = imitate_trusted_source()  
    include_malicious_link(message)  
    return message
```

```
function send_message(user, message):  
    deliver_email(user, message)
```

```
function capture_credentials():  
    redirect_to_fake_login_page()  
    store_input_data()
```

```
message = create_fake_message()  
send_message(target_user, message)  
capture_credentials()
```

Този модел показва как чрез социално инженерство се манипулира потребителят да предостави чувствителна информация. Основният механизъм разчита на доверие и невнимание, което прави фишинг атаките особено ефективни. В контекста на центровете за данни те често служат като входна точка за по-сложни атаки като RW или APT.

4. Стратегии и технологии за противодействие на киберзаплахите

Защитата на центровете за данни е комплексен процес, който изисква интегриране на технологични решения, организационни мерки и непрекъснат мониторинг на

ROSEN PASARELSKI

сигурността. Основната цел е да се намали вероятността от успешна атака, както и да се минимизират последиците при компрометиране.

4.1.Защита срещу DDoS атаки

Атаките DDoS претоварват сървъри, мрежови устройства и инфраструктура, като целят отказ на легитимни заявки. Механизми за противодействие се използват, както следва:

- устройства за намаляване на DDoS (DDoS mitigation appliances) - Специализирани хардуерни или софтуерни решения, които анализират трафика в реално време и блокират подозрителни пакети. Те използват техники като филтриране по IP, проверка на сесии и поведенчески анализ на трафика.
- Cloud-базирани решения - CDN (Content Delivery Network) и Load Balancers разпределят трафика между множество сървъри, като разтоварват целевия ресурс. Така дори при голям обем заявки услугите остават достъпни.
- Ограничаване на броя заявки (Rate limiting) - Ограничаване на броя заявки от един източник за определен период, за да се предотврати претоварване.
- Анализ на аномалии - Системи за мониторинг на трафика използват модели на нормално поведение (baseline) и сигнализируют при отклонения.

Реални примери за DDoS mitigation устройства и решения:

- Fortinet (FortiDDoS) - устройството FortiDDoS е специализирано решение (част от портфолиото на Fortinet), което анализира трафика при мрежов периметър и автоматично открива и неутрализира различни видове DDoS атаки (включително volumetric, application-layer и DNS-базирани атаки), без да прекъсва легитимен трафик.
- Cisco DDoS Protection (Cisco Guard XT и Traffic Anomaly Detector) - Решението на Cisco включва набор от устройства и модули като Cisco Guard XT 5650 и Traffic Anomaly Detector, които анализират мрежовия трафик за аномалии и предоставят защита срещу DDoS кампании, интегрирани в мрежовите инфраструктури на доставчици на услуги или корпоративни центрове за данни.
- Radware DDoS Protection (DefensePro и Cloud DDoS Protection) - Radware предлага хибридна защита, която комбинира устройства в помещенията за вградено филтриране с облачни „scrubbing“ центрове за справяне с големи обеми атаки. Тези решения използват поведенчески анализ и машинно обучение, за да откриват както volumetric, така и атаки на приложния (Layer 7) слой.
- Cloudflare DDoS Protection - Cloudflare не е традиционен хардуерен уред, но представлява облачна Anycast-базирана платформа, която абсорбира атаки през глобална мрежа от точки за присъствие, анализира трафика в реално време и филтрира злонамерени заявки, преди те да достигнат центровете за данни на клиента.
- Akamai Prolexic (често срещан в по-големи корпоративни среди) - Akamai предлага една от най-големите платформи за DDoS защита с мащабна инфраструктура и „scrubbing centers“ по света, които абсорбират злонамерен трафик, преди да достигне локалната инфраструктура.

Техниките за противодействие, които използват тези решения са:

- Поведенчески анализ за разпознаване на аномалии;
- филтриране на ниво IP/сесии;
- почистване „scrubbing“ на трафика в облака;
- автоматично откриване и блокиране на много типове DDoS вектори;
- интеграция с мрежови и CDN услуги.

4.2. Защита срещу злонамерен софтуер (MW) и рансъмуер (RW)

Атаките чрез MW и RW могат да компрометират данни, да създадат задни врати или да криптират информация срещу откуп. За защита се прилагат:

- Антивирусни решения и EDR (Endpoint Detection & Response) - Осигуряват откриване и блокиране на зловредни файлове и аномалии на крайните устройства. EDR включва мониторинг на поведението на софтуера, анализ на процеси и автоматична реакция.
- Резервно копиране и Disaster Recovery (DR) - Регулярни бекъпи на данни, както локално, така и в облака. Това позволява възстановяване на информацията при успешна RW атака без да се плаща откуп.
- Сегментация на мрежата - Разделяне на инфраструктурата на логически сегменти, за да се ограничи разпространението на MW и RW. Например сървърите с критични данни могат да бъдат отделени от външния достъп.
- Принцип на най-малко привилегии (Least Privilege) - Всеки потребител и процес получава само минималните права, необходими за изпълнение на задачите, за да се намали потенциалният обхват на атаката.

Реални решения за Endpoint Detection and Response (EDR) системи, които следят поведението на процеси и файлове на крайни устройства, откриват аномалии и реагират автоматично:

- CrowdStrike Falcon - Облачна EDR платформа с поведенчески анализ и машинно обучение. Открива сложни MW кампании, включително без файлове (fileless malware).
- Microsoft Defender for Endpoint - Интегрирана защита на Windows среди със поведенчески анализ и защита в реално време.
- SentinelOne Singularity - Автоматично открива, блокира и възстановява компрометирани файлове.

Антивирусни и анти-MW платформи, които осигуряват традиционно откриване на подписи, комбинирано със съвременни анализи:

- Bitdefender GravityZone - Комбинира базиран на сигнатури и поведенчески анализ, подходящ за центрове за данни и виртуални среди.
- Sophos Intercept X - Използва машинно обучение за откриване на подозрителни поведения, предотвратява експлойти.
- Kaspersky Endpoint Security - Надеждна защита срещу широк спектър MW заплахи с централизирано управление.

Реални системи от типа „Network-based malware detection“, които анализират мрежовия трафик, за да открият MW комуникации:

- Cisco Secure Network Analytics (Stealthwatch) - Открива аномалии в мрежовия трафик, свързани с MW и ботнет комуникации.
- Darktrace Enterprise Immune System - Използва AI за моделиране на нормално поведение и индикация на отклонения (MW включително).

Реални специализирани анти-рансъмуер технологии:

- Acronis Cyber Protect - Комбинира анти-рансъмуер, бекъп и възстановяване, защитавайки данните дори ако главна система е компрометирана.

ROSEN PASARELSKI

- Trend Micro Apex One - Предпазва от рансъмуер чрез множество механизми: антивирус, поведенчески анализ и rollback функционалност.
- SentinelOne Ranger + Rollback - Открива рансъмуер поведение и автоматично възстановява компрометирани файлове.
- Veeam Backup & Replication - Поддържа immutable реплики на данни (не могат да бъдат променяни, дори ако системата е компрометирана).

4.3.Защита срещу APT и Zero-Day експлойти

Атаките APT са продължителни и целенасочени, докато Zero-Day експлойтите използват непознати уязвимости. Основните мерки включват:

- Системи SIEM (Security Information and Event Management) - Системите за събиране и анализ на логове позволяват откриване на подозрителни поведения, като необичайни достъпи или сканиране на мрежата.
- Технология за изолирано изпълнение „Sandboxing“ - Технологията за изолирано изпълнение на подозрителни файлове, която предотвратява заразяване на продукционни системи и позволява анализ на поведението на MW.
- Регулярни актуализации - Прилагането на актуализации намалява броя на уязвимостите, достъпни за атакуващите. Дори Zero-Day уязвимости се намаляват чрез мониторинг на новите заплахи и бързо реагиране с временно блокиране на потенциално рискови услуги.

Реални усъвършенствани SIEM / XDR платформи с поведенчески анализ:

- Splunk Enterprise Security - Събира и анализира логове от множество източници за ранна индикация на атаки.
- IBM QRadar - Класически SIEM с ML за подозрително поведение.
- Microsoft Sentinel (Cloud SIEM) - Съвременен облачен SIEM, интегриран със Defender за Endpoint.

4.4.Защита на IAM системи

Компонетът IAM (Identity and Access Management) е ключов за предотвратяване на неоторизиран достъп. Механизмите за защита са:

- Двухфакторна и многофакторна автентикация (2FA/MFA): Изисква комбинация от парола и допълнителен фактор (SMS код, токен, биометрия).
- Ревизия на потребителски права: Редовно проверяване на ролите и привилегиите на служителите и автоматично премахване на излишни права.
- Мониторинг на активност: Логове и анализ на поведението на акаунтите за откриване на необичайни операции, като опити за достъп до административни функции.

Реални решения за IAM системи:

- Платформа Microsoft Azure Active Directory (Azure AD / Entra ID) - Облачна IAM платформа която поддържа единичен вход (Single Sign-On - SSO), многофакторно удостоверяване (Multi-Factor Authentication - MFA) и условен достъп. Интегрира се с множество облачни и локални приложения. Позволява управление на идентичности в хибридни инфраструктури (локални и облачни).
- Платформа Okta Identity Cloud - Осигурява централизирано управление на достъпа до приложения. Поддържа SSO, MFA и управление на жизнен цикъл на потребители. Отличава се с лесна интеграция и висока степен на автоматизация.
- IBM Security Verify - Предоставя управление и администриране на идентичността (Identity Governance and Administration - IGA). Поддържа управление на роли и

политики за достъп. Използва AI за откриване на аномалии в поведението на потребителите.

- Oracle Identity Management - Включва компоненти за управление на достъп, удостоверяване и одит. Подходящ за сложни инфраструктури и критични системи. Поддържа интеграция с бази данни, ERP системи и облачни услуги.
- CyberArk Identity - Платформа, която се фокусира върху защита на привилегирован достъп (PAM). Управлява администраторски акаунти и чувствителни кредитенши. Предотвратява злоупотреби с високи привилегии. Осигурява мониторинг и запис на сесии.
- Auth0 - IAM платформа, широко използвана за уеб и мобилни приложения. Осигурява лесна интеграция чрез API. Поддържа OAuth, OpenID Connect и SSO. Подходяща за модерни облачни приложения.

4.5.Превенция на фишинг и социално инженерство

Механизми използвани за защита от фишинг и социално инженерство:

- Обучение на персонала - Периодично обучение за разпознаване на измамни имейли и фалшиви уебсайтове.
- Филтриране на имейли и защита от спам - Автоматично блокиране на подозрителни линкове и прикачени файлове.
- Тестове и симулации - Контролирани фишинг кампании за повишаване на информираността и устойчивостта на служителите.

Много корпорации използват платформите KnowBe4 или Cofense за симулации на фишинг, което значително намалява успеха на реални атаки.

4.6.Мулти-векторна защита и интегрирани системи

Механизми използвани за мулти-векторна защита:

- Интегрирани системи за сигурност: Комбинират антивирус, SIEM, DDoS защита и IAM в единна платформа. Това позволява централизирано наблюдение и реакция.
- Автоматизация на инциденти (SOAR): Автоматично блокира подозрителни действия, уведомява екипите и започва процедури за възстановяване.
- Тестове за проникване и симулации: Редовно се проверява устойчивостта на центровете за данни чрез безопасни тестове за проникване.

Реални системи за защита от мулти-векторни атаки:

- Palo Alto Networks Cortex XDR - Цялостна XDR платформа, която интегрира данни от крайни устройства, мрежи и облачни среди. Открива сложни атаки (APT, MW, RW) чрез корелация на събития. Използва поведенчески анализ и машинно обучение. Поддържа автоматизирана реакция на инциденти.
- Cisco SecureX - Платформа за интеграция на различни Cisco защитни решения. Обединява мрежова сигурност, EDR и анализ на заплахи. Осигурява централизирана видимост и автоматизация (SOAR функционалности). Позволява координирана реакция при мулти-векторни атаки.
- IBM QRadar Suite - Разширена SIEM/XDR платформа за анализ и корелация на събития. Открива сложни атаки чрез събиране на логове от различни източници. Използва AI за анализ на поведение и откриване на аномалии. Поддържа автоматизирани процеси за реагиране.

5. ЗАКЛЮЧЕНИЕ

Настоящото изследване разглежда съвременните киберзаплахи, насочени към центровете за данни, както и техните механизми на реализиране и възможностите за ефективно противодействие. Анализът показва, че заплахи като DDoS, MW, RW, APT и „Zero-day“ уязвимости се характеризират с висока сложност, автоматизация и често се реализират чрез мулти-векторни атаки. Резултатите от изследването подчертават необходимостта от интегриран подход към киберсигурността, включващ съвременни технологии като DDoS защита, EDR/XDR, SIEM и IAM системи, както и прилагане на организационни политики и механизми за мониторинг. В заключение, ефективната защита на центровете за данни изисква многостепенна и адаптивна стратегия, която да осигури надеждност и непрекъсваемост на услугите в условията на динамично развиваща се киберсреда.

ИЗПОЛЗВАНА ЛИТЕРАТУРА REFERENCES

- [1] STALLINGS, W. *Network security essentials: Applications and standards*. Pearson, 2018. ISBN 978-0134527338.
- [2] KIM, D. and M. SOLOMON. *Fundamentals of information systems security*. Jones & Bartlett Learning, 2016. ISBN 978-1284031621.
- [3] EASTTOM, C. *Computer security fundamentals*. Pearson IT Certification, 2019. ISBN 978-0135774779.
- [4] SINGER, Peter and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2014. ISBN 978-0199918096.
- [5] ZARGAR, Saman Taghavi et al. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Communications Surveys & Tutorials* [online]. 2013, vol. 15(4), pp. 2046 - 2069 [viewed 06.06.2026]. eISSN 1553-877X. Available from: 10.1109/SURV.2013.031413.00127.
- [6] KSHETRI, Nir. *Cybercrime and Cybersecurity in the Global South*. London: Palgrave Macmillan, 2013. ISBN 978-1-137-02193-9.
- [7] CONTI, Mauro et al. Internet of Things Security and Forensics: Challenges and Opportunities. *Future Generation Computer Systems* [online]. 2017, vol. 78(2), pp. 544-546 [viewed 06.06.2026]. Available from: 10.1016/j.future.2017.07.060.
- [8] DOBREVA, A. Impact of new technologies and artificial intelligence in brand management. *Yearbook Telecommunications* [online]. 2024, vol. 11, pp. 107-117 [viewed 11.06.2026]. eISSN 2534-854X. Available from: <https://doi.org/10.33919/YTelecomm.24.11.11>
- [9] АНГЕЛОВ, К. Анализ на сигурността в комуникационни мрежи за интернет на нещата. *Годишник Телекомуникации* [онлайн]. 2024, год. 11, с. 131-141 [прегледан 11.06.2026]. eISSN 2534-854X. Достъпен на: <https://doi.org/10.33919/YTelecomm.24.11.13>
- [10] PASARELSKA, T. Research of the implementation of modern wireless broadband electronic communication services. *Yearbook Telecommunications* [online]. 2024, vol. 11, pp. 69-79 [viewed 11.06.2026]. eISSN 2534-854X. Available from: <https://ojs.nbu.bg/index.php/YT/issue/view/84>
- [11] PASARELSKA, T. Analysis of radio frequency spectrum planning and allocation for the deployment of new modern broadband networks and technologies. *Yearbook Telecommunications* [online]. 2023, vol. 10, pp. 79-88. [viewed 11.06.2026]. eISSN 2534-854X. Available from: <https://doi.org/10.33919/YTelecomm.23.10.8>
- [12] СИМЕОНОВА, Цв. Подход за анализ и моделиране на надеждността на мрежовата свързаност от гледна точка на ефективност и неговата приложимост. *Годишник Телекомуникации* [онлайн]. 2020, год. 7, с. 57-63. [прегледан 11.06.2026]. eISSN 2534-854X. Достъпен на: <https://doi.org/10.33919/YTelecomm.20.7.7>
- [13] PASARELSKI, R., G. PETROV, T. PASARELSKA, K. ANGELOV. Neural Network Architecture to Predict Radio Wave Attenuation in a 5G Network. In: *31st National Conference with International Participation „Telecom 2023“, November 16 - 17, 2023, Sofia, Bulgaria* [online]. 2023, pp. 1-5 [viewed 21.03.2025]. ISSN 2837-5246. Available from: <https://ieeexplore.ieee.org/xpl/conhome/10409594/proceeding>
- [14] СТЕФАНОВА, Тереза. *Новите технологии: приложения, професии, умения: монография*. София: Аскони-издат, 2024. ISBN 978-954-383-151-7. [STEFANOVA, Tereza. *Novite tehnologii: prilozhenia, profesii, umenia: monografia*. Sofia: Askoni-izdat, 2024. ISBN 978-954-383-151-7.]
- [15] IVANOVA, Y. A methodology for empirical research and analysis in the field of cybersecurity. *Yearbook Telecommunications* [online]. 2022, vol. 9, pp. 45-52 [viewed 11.06.2026]. eISSN 2534-854X. Available from: <https://doi.org/10.33919/YTelecomm.22.9.4>

- [16] IVANOVA, Y. Trends in the use of high technology solutions for cybersecurity of critical infrastructure. *Yearbook Telecommunication* [online]. 2019, vol. 6, pp. 37-44 [viewed 11.06.2026]. eISSN 2534-854X. Available from: 10.33919/YTelecomm.19.6.4.

Информация за авторите:

проф. д-р Росен Пасарелски, НБУ департамент „Телекомуникации“, rpasarelski@nbu.bg

Contacts:

Prof. Rosen Pasarelski, PhD, New Bulgarian University, Department „Telecommunications“, rpasarelski@nbu.bg

Дата на постъпване на ръкописа (Date of receipt of the manuscript): 26.06.2025

Дата на приемане за публикуване (Date of adoption for publication): 30.09.2025