Приложение на дигиталната трансформация в обучението по компютърна криминалистика и управление на риска в киберсигурността

Валентина Петрова

Application of digital transformation in training in computer forensics and cybersecurity risk management

Valentina Petrova

Abstract:
Digital computer forensics is a key discipline in overcoming cybercrime. Traditional investigative methods have been greatly enhanced by digital transformation, which includes the use of automated forensic analysis tools and big data. The report explores the application of these innovations in computer forensics to improve the effectiveness of forensic investigations. The technologies that support the collection, analysis and interpretation of digital evidence are analyzed, as well as the advantages and challenges. The interaction of cyber risk management and digital transformation is investigated, highlighting key vulnerabilities and security strategies. Digital transformation is revolutionizing cyber risk management by integrating innovative technologies to detect, prevent and mitigate cyber threats. The application of computer forensics and cybersecurity risk management in digital transformation in the training of students and cadets at the Bulgarian Naval Academy is demonstrated.
Keywords: Digital transformation, Digital computer forensics, Cyber risk.

For contacts: Assoc. Prof. Valentina Petrova, Nikola Vaptsarov Naval Academy, v.petrova@naval-acad.bg

ВЪВЕДЕНИЕ

Дигиталната трансформация променя не само методите на преподаване, но и самото съдържание на обучението в сферата на киберсигурността. С нарастването на киберзаплахите, обучението по компютърна криминалистика и управление на риска трябва да отговаря на новите предизвикателства чрез интегриране на автоматизирани криминалистични инструменти, скенери за уязвимости, симулационни среди и анализи в реално време. В контекста на бързоразвиващите се технологии и все по-сложните киберзаплахи, традиционните форми на преподаване се оказват недостатъчни, за да подготвят ефективно бъдещи специалисти за предизвикателствата на реалния дигитален свят. Дигиталната трансформация не се изразява само в преминаването към електронни платформи за обучение, а включва цялостно преструктуриране на методите на преподаване, учебните програми и технологичната инфраструктура, използвана в обучителния процес. В обучението по компютърна криминалистика това означава интегриране на професионални криминалистични инструменти и реалистични симулационни среди за разследване на инциденти, извличане на цифрови доказателства и анализ на зловредна дейност. В управлението на риска в киберсигурността дигиталната трансформация предоставя възможности за провеждане на практическо обучение с използване на скенери за уязвимости, автоматизирани системи за мониторинг и платформи за оценка на заплахи.

ИЗЛОЖЕНИЕ

Технологии в компютърната криминалистика

С нарастващата цифровизация на обществото престъпната дейност все по-често се премества в дигитална среда. Това налага трансформация и адаптация на методите за разследване на престъпления чрез прилагане на иновативни технологии в сферата на компютърната криминалистика (digital forensics). Целта на настоящото проучване е да се анализират основните технологични иновации, използвани в съвременните криминалистични разследвания, техните предимства и ограничения, както и бъдещите насоки в развитието на цифровата криминалистика. Софтуерни платформи като FTK (Forensic Toolkit), EnCase, Autopsy и X-Ways Forensics дават възможност за бързо извличане на данни от компютри, мобилни устройства, мрежови хранилища и облачни услуги. Автоматизацията значително ускорява процеса на събиране на цифрови доказателства, като едновременно с това се спазват стандартите за доказателствена годност. Алгоритми от изкуствения интелект (ИИ) се прилагат за анализ на големи обеми от данни и за откриване на подозрителни файлове, поведенчески модели или зловреден софтуер. Машинното обучение позволява класификация и предсказване на инциденти въз основа на обучени модели, повишавайки ефективността на криминалистичния анализ. Технологията на разпределената счетоводна книга (DLT) намира приложение в проследяването и верифицирането на цифровите доказателства. Чрез блокчейн може да се гарантира, че цифровите артефакти не са били манипулирани след тяхното събиране. Системи като SIEM (Security Information and Event Management) и NDR (Network Detection and Response) предоставят данни за разследване на киберинциденти, като позволяват проследяване на атаките до техния източник и възстановяване на хронологията на събитията.

Предимствата на цифровизираните криминалистични методи включват:

- Скорост и ефективност: Съвременните инструменти позволяват анализ на терабайти данни за кратко време. Autopsy, FTK Imager и X-Ways Forensics позволяват извличане, индексиране и анализ на огромни обеми данни – включително харддискове с капацитет над 5–10 TB в рамките на часове, а не дни. Предлагат възможности за паралелна обработка, индексиране и търсене в милиони файлове за минути. Това е особено важно при анализ на иззети твърди дискове, мобилни устройства и облачни хранилища.

При разследване на случай с детска порнография в Германия, използването на базирана система на ИИ за откриване на изображения намалява времето за преглед от разследващите с 80%, като класифицира и приоритизира съмнителните файлове. В случай на корпоративен пробив в базата данни на здравноосигурителна компания в САЩ, екип от цифрови криминалисти използват Nuix за сканиране и категоризиране на 7 TB данни, свързани с клиентски записи, в рамките на 36 часа – време, което ръчна проверка не би могла да постигне за седмици.

- Прецизност: Автоматизираните процеси и анализи значително намаляват риска от човешки грешки. Софтуерни модули могат точно да изчисляват времеви марки, да извличат скрити или изтрити файлове и да реконструират комуникации

от чат приложения. Специализираните софтуерни решения използват алгоритми за точна идентификация на файлове, хеш сравнения, времеви анализи и възстановяване на изтрити данни. Това повишава обективността на събраните доказателства и тяхната юридическа стойност.

При киберпрестъпление срещу финансова институция в САЩ, използването на Volatility Framework (инструмент за анализ на RAM памет) довежда до откриването на „временно“ инжектиран зловреден код, който човешкият анализатор би могъл да пропусне. Друг случай е при използването на Volatility Framework за проникване в правителствена мрежа, при който експертите успяват да извлекат зловреден код от оперативната памет на заразен компютър – задача, почти невъзможна за ръчен анализ без висок риск от пропуски.

- Мобилност и дистанционен достъп: Облачните и отдалечени системи позволяват разследване без физическо присъствие. Magnet AXIOM Cloud или Cellebrite Cloud Analyzer, позволяват достъп и анализ на цифрови доказателства от разстояние, включително данни от Google Drive, iCloud, Dropbox и Microsoft OneDrive, като разследващите органи могат да преглеждат доказателства дистанционно от различни географски локации, в синхрон с локални експерти. Това е от особено значение в трансгранични разследвания или при пандемични ограничения. При операция на Европол срещу онлайн трафик на наркотици, експерти от различни държави използват споделена облачна среда, за да анализират и координират действията си в реално време. Платформи като AWS, Azure и Google Cloud предлагат мащабируеми и гъвкави решения за управление на сигурността. Чрез инструменти като AWS Security Hub и Azure Security Center, организациите могат централизирано да наблюдават, анализират и реагират на заплахи [6].

В хибридна инфраструктура Azure Sentinel се използва облачен SIEM подход, който позволява мигновен анализ на големи обеми от данни и интеграция с модели на ИИ за предсказване на заплахи.

- Интегриране с други системи: Съществува възможност за свързване с национални бази данни и полицейски платформи. Съвременните криминалистични инструменти могат да се свързват директно с национални и международни бази данни, като INTERPOL’s I-24/7, AFIS (автоматизирана система за пръстови отпечатъци) или Europol’s EIS (European Information System). При разследване на престъпна група за онлайн измами, автоматичното сравнение на MAC адреси и IP локации с външни бази данни довежда до бързо идентифициране на заподозрени в няколко държави. Инструменти като IBM i2 Analyst’s Notebook и Palantir могат да се свързват със системи за криминални досиета, банки за ДНК профили, биометрични бази данни и други. В рамките на операция на Европол, данни, извлечени от компютър на член на организирана престъпна група, са съпоставени с хронологията на комуникации от платформа за криптирани съобщения чрез интеграция със системата EIS (European Information System), водещи до идентифициране на още петима съучастници.

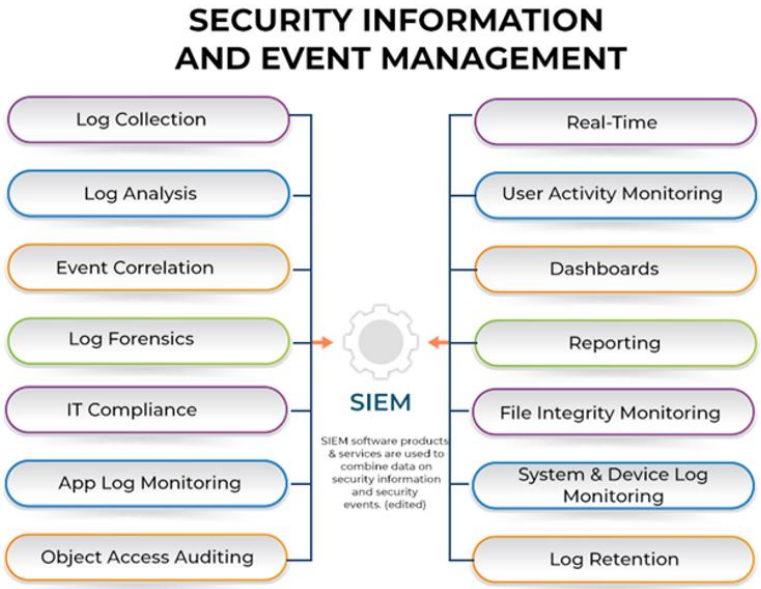
Управление на киберриска в епохата на дигитализация

Управлението на киберриска представлява процес по идентифициране, оценка и смекчаване на рискове, произтичащи от потенциални или реални

кибератаки, уязвимости в системите, човешки грешки и злонамерени действия. При традиционните подходи управлението на риска се фокусира основно върху защитата на ИТ инфраструктурата [2, 3, 4]. С дигиталната трансформация обаче, обхватът на риска се разширява до разпределени облачни среди, устройства с IoT, слабо защитени мобилни и дистанционни модели и изкуствен интелект, който сам може да бъде манипулиран.

Съвременните дигитални технологии не само пораждат рискове, но и създават нови възможности за тяхното ефективно управление:

- Изкуствен интелект и машинно обучение: Изкуственият интелект се превръща в основен компонент за управление на киберриска. Системи за откриване на аномалии (SIEM, показана на фигура 1, SOAR платформи) използват ИИ за идентифициране на подозрително поведение в реално време.



Фиг. 1. Управление на информационната сигурност и събитията [8].

Платформи като IBM QRadar, Splunk, Microsoft Sentinel и Darktrace използват алгоритми за машинно обучение, за да разпознаят аномалии в потребителското поведение, мрежовия трафик и достъпа до ресурси [7]. Ако потребител внезапно започне да изтегля голямо количество чувствителни файлове извън работно време, системата автоматично ще генерира сигнал за инцидент.

В практиката, прилагането на ИИ за поведенчески анализ позволява бързо откриване на атаки тип "insider threat", ransomware или компрометирани акаунти, които биха останали незабелязани от традиционните мерки за сигурност [1].

- Автоматизация: Автоматизирано управление на уязвимости и съответствие чрез инструменти като Tenable Nessus, Qualys Vulnerability Management и Greenbone OpenVAS автоматизират процеса по сканиране, класифициране и отстраняване на уязвимости [5]. С Tenable.io организациите могат да осъществяват непрекъснат мониторинг на облачна инфраструктура и автоматично да създават „тикети“ за екипите по сигурност, когато е открита критична уязвимост (напр. CVE-2023-23397 – zero-click уязвимост в Microsoft Outlook). Автоматизацията значително съкращава времето за реакция (MTTR – Mean Time to Respond) и спомага за постигане на нормативно съответствие, като

тези инструменти са съвместими с изискванията на международните регулации като ISO/IEC 27001, NIS2 и GDPR, и подпомагат процеса по създаване на отчети и автоматизирани мерки.

ЗАКЛЮЧЕНИЕ

В условията на нарастваща дигитализация на всички аспекти от обществения и икономическия живот, образованието в сферата на компютърната криминалистика и управлението на риска в киберсигурността се превръща в стратегически приоритет. Дигиталната трансформация вече не е бъдещ ориентир, а текущ процес, който изисква активна адаптация, иновации и инвестиции в ресурси и компетенции.

Представените в доклада практики от ВВМУ „Н. Й. Вапцаров“ илюстрират как чрез внедряване на съвременни технологии – като скенери за уязвимости, симулационни среди, криминалистични платформи и стандартизирани рамки за оценка на риска – обучението се трансформира от теоретична подготовка в практически ефективен инструмент за изграждане на професионална готовност.

Бъдещите усилия следва да бъдат насочени към разширяване на виртуалните лаборатории, повишаване на цифровата компетентност на преподавателите, въвеждане на обучителни системи, подкрепени от ИИ и засилено партньорство между академичните институции, държавата и индустрията.

ЛИТЕРАТУРА

[1] Zuech, R., Khoshgoftaar, T. M., & Wald, R. (2015). *Intrusion detection and Big Heterogeneous Data: A Survey*. Journal of Big Data, 2(1), 3. https://doi.org/10.1186/s40537-015-0013-4

[2] V. Petrova, “Using the Analytic Hierarchy Process for LMS selection”: 20th International Conference on Computer Systems and Technologies. Ruse, Bulgaria: Pages, ISBN: 978-1-4503-7149-0, Jun. 2019, pp. 332-336. doi:10.1145/3345252.3345297

[3] V. Petrova, "The Hierarchical Decision Model of cybersecurity risk assessment," *2021 12th National Conference with International Participation (ELECTRONICA)*, Sofia, Bulgaria, 2021, pp. 1-4, doi: 10.1109/ELECTRONICA52725.2021.9513722.

[4] V. Petrova, A decision hierarchical model of cyber security risk assessment. Mathematics and Education in Mathematics, 2021, 50: 191-195.

[5] Tenable, Inc. (2023). *Tenable Nessus User Guide*. https://docs.tenable.com

[6] Amazon Web Services (2023). *AWS Security Hub – User Guide*. https://docs.aws.amazon.com/securityhub/

[7] European Union Agency for Cybersecurity (ENISA). (2021). *AI Cybersecurity Challenges*. https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

[8] https://www.linkedin.com/pulse/siem-security-information-event-management-g%C3%BCvenlik-bilgileri-basci