ISSN 2738-7089 https://doi.org/10.11610/cybsec08bg

Funded by the European Union

Digital Innovation Hub Trakia

Институт ИИКТ
Институт по информационни и комуникационни технологии

Информационен бюлетин за киберсигурност

Бюлетин Юни 2023 Номер 8

Цели и обхват

Съдържание:

Настоящия брой на информационния бюлетин за киберсигурност е фокусиран върху най-често срещаните видове кибератаки и инструментите за симулация на кибератаки.

Основна задача пред компаниите е осигуряване на сигурността на данните на фирмата и тези на клиентите. Прогнозите показват увеличаване на киберинцидентите, като същевременно се увеличава и броя на потребителите, които стават все по-запознати с подобни рискове. Ако се абстрахираме от техническата част, то основният елемент на защитата за предотвратяване на последиците от такъв инцидент е обучението, което е и една от дейностите на ЕЦИХ ТРАКИЯ. Комплексно решение може да се търси в комбинацията между обучение, технически средства и киберзастраховане.

В броя са описани едни от най-често срещаните кибератаки, а именно: Phishing; Malicious Software (malware); MITM (Man In The Middle); SQL Injection; Denial-of-Service (DoS) и Distributed denial-of-service (DDoS); Ransomware; Cross-site scripting (XSS); Supply Chain Attacks; и IoT Attacks. Представени са и някои практични съвети как да поддържаме данните в безопасност.

Представен е списък на 10 най-добри инструмента за симулация на кибератака за подобряване на сигурността. Дадена е и класацията на инструменти за симулация на кибератаки според Gartner, приложими за малки компании. Продуктите за киберсигурност могат да бъдат скъпи, но има много отлични инструменти с отворен код, които да помогнат за защитата на системите и данните. Списък на някои от най-популярните сред кибер професионалистите безплатни инструменти за киберсигурност е представен.

В настоящия брой е отразено официалното откриване на Европейския цифров иновационен хъб (ЕЦИХ) ТРАКИЯ в град Пловдив, състояло се на 20 април 2023 . Показан е напредъка от проведените обучения от лектори на ЕЦИХ ТРАКИЯ в областта на киберсигурността и е дадена информация за предстоящо лятно училище.

Представен е Законът за цифровите услуги (Digital Services Act) и Законът за цифровия пазар (Digital Market Act), формиращи единен набор от правила, които се прилагат в целия ЕС.

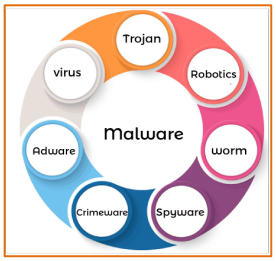
Редактор на броя: **проф. д.н. Даниела Борисова**

Фокус на изданието: Кибератаки – същност и основни видове

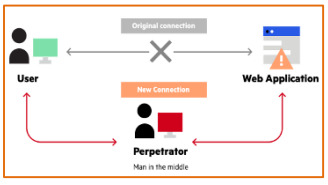
Digital Innovation Hub Trakia

Кибератаките по своето естество представляват целенасочени и зловредни опити за пробив в информационните системи на индивиди и организации. Обикновено целта е финансова облага, но все по-често унищожаването на информация се превръща в основна цел на атаките. Най-често срещаните видове кибератаки са както следва:

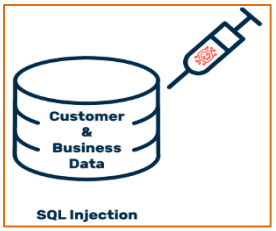
Фишинг (Phishing) е най-разпространеният вид кибератака днес – разпращане на масови имейли до нищо не подозиращи получатели, които привидно идват от доверен източник. Това е типичният им почерк и сценарий. Ключовото при тях е, че самите имейли изглеждат легитимни и изключително достоверно. А това логично води и до много сериозно успех за атаки от подобен тип. Зловредното съдържание на тези имейли обикновено позволява достъп до устройствата, може да инсталира зловредни файлове, както и да извлече чувствителна информация – лична и финансова. След възходът на социалните мрежи, фишингът вече не се ограничава само до имейлите. Не рядко фишингът разчита и на т. нар. социално инженерство (social engineering), за да повлияе така на мишените, че да кликнат на съмнителен линк или файл, получен чрез директно съобщение.



Зловредният софтуер (**Malicious Software**) е събирателен термин за разнообразие от атаки като вируси, шпионски софтуер (spyware), червеи и други, които използват съществуващи уязвимости, за да компрометират дадена система. Малуерът е способен да ограничи достъпа до системата и дори до такава степен да наруши функционирането на една система, че да я разруши напълно. Този тип вируси могат да нанесат страховити щети на заразените системи, а също така да извлекат и огромно количество чувствителна информация. Най-често получават достъп до системите при кликване на опасни линкове и отваряне на зловредни файлове, получени по имейл.



MITM (Man In The Middle) атаки се характеризират с прихващането на комуникация между две системи. Обмяната на данни между тях може да бъде нарушена, а споделяната информация дори изменена, без двете страни в процеса да подозират нищо. Една от водещите уязвимости, от които хакерите се възползват за целта, са публични Wi-Fi мрежи, а самите атаки са много трудни за засичане. За осъществяване на MITM атака много често спомагат малуерът и фишингът.



SQL Injection е друг много разпространен тип кибератаки и може би най-използваният за хакване на бази данни. Хакерите използват зловреден SQL код, който буквално инжектират (оттам и името) в полета, които позволяват въвеждането на данни в уеб страниците. Базите данни получават

информация точно през тези полета, което ги прави и изключително уязвими към атаки с SQL инжекции. Една такава атака може да открадне ценна информация, а в най-лошия случай – и напълно да унищожи базата данни.

Denial-of-Service DoS атаките по своето естество това са атаки, които целят претоварването на ресурсите на системи, мрежи и сървъри до степен, в която не могат да изпълняват заявките, които получават. Най-честите мишени на подобни атаки не са индивиди, а популярни уеб сървъри. **Distributed denial-of-service (DDoS)** атаките от своя страна имат няколко източника на трафик, а крайната цел е „свалянето“ на дадената система, така че да може друг тип зловредна атака да си проправи път. За целите на DDoS атаките се използват ботове.

Ransomware може да се определи като вид кибератака, при която всички файлове на системата се кодират и хакерът изисква от организацията да плати, ако искат да си върнат достъпа до тези файлове. След като системата бъде атакувана успешно, използвайки този начин на атака, остава единствената възможност да платите на хакера, което може да струва твърде много на организацията.

Cross-site scripting (XSS) или скриптове между сайтове, нападателят предава злонамерени скриптове, използвайки съдържание с възможност за кликване, което се изпраща до браузъра на целта. Когато жертвата кликне върху съдържанието, скриптът се изпълнява. Тъй като потребителят вече е влязъл в сесията на уеб приложение, въведеното от него се разглежда като законно от уеб приложението. Изпълненият скрипт обаче е бил променен от нападателя, което е довело до нежелано действие, предприето от „потребителя“.

Supply Chain Attacks е вид кибератака, която е насочена към доверен доставчик трета страна, който предлага услуги или софтуер от жизненоважно значение за веригата за доставки. Атаките по веригата за доставки на софтуер инжектират злонамерен код в приложение, за да заразят всички потребители на приложението, докато атаките по веригата на доставки на хардуер компрометират физически компоненти със същата цел. Веригите за доставка на софтуер са особено уязвими, тъй като съвременният софтуер не е написан от нулата: по-скоро той включва много готови компоненти, като API на трети страни, код с отворен код и патентован код от доставчици на софтуер.

IoT Attack е всяка кибератака, която е насочена към устройство или мрежа на Интернет на нещата (IoT). Веднъж компрометиран, хакерът може да поеме контрол над устройството, да открадне данни или да се присъедини към група от заразени устройства, за да създаде ботнет за стартиране на DoS или DDoS атаки.

Ето някои начини как поддържаме данните в безопасност:

- Инвестиране в надеждна система за киберсигурност.
- Наемане на ИТ администратори, които ще следят отблизо всички мрежи в рамките на фирмата.
- Използване на система за двустепенно или многофакторно удостоверяване, което да гарантира, че всички акаунти, които имат достъп до системата са проверени служители.
- Образоване на служителите чрез текущо вътрешно обучение за кибератаките и киберсигурността и за това какви стъпки да предприемат, ако възникне пробив в данните.
- Наемане на външен екип за защита, който да подпомага вътрешния ИТ отдел при наблюдението на бизнес мрежите и системите.

10 най-добри инструмента за симулация на кибератака за подобряване на сигурността

Симулацията на кибератака е сравнително нов инструмент за ИТ сигурност, който може автоматично да открие дупки в киберзащитата на институцията. Въпреки че симулацията на кибератака звучи много като автоматизирано тестване за проникване на повърхността, този тип симулация включва повече от тестване с писалка. Симулацията на кибератака включва предлагане на решения за максимизиране на ресурсите за сигурност и намаляване на кибер рисковете.

Тъй като необходимостта от киберсигурност продължава да расте, се появяват повече методи за защита срещу кибератаки. „Симулацията“ се отнася до способността за имитиране на техники, процедури и тактики на злонамерени участници. Повечето инструменти и платформи за симулация на атаки предоставят автоматизирани или полуавтоматизирани средства за постигане на гледната точка на нападателя за мрежата на жертвата. Симулацията на кибератака е най-новата в линията на киберотбраната.

Как инструментите за симулация на кибер атаки тестват сигурността? Инструментите за симулация на кибератаки или инструментите за мрежови атаки тестват сигурността, като имитират техниките на злонамерени агенти и пътищата на атака, използвайки различни методи за тестване. Тестът за проникване (известен като „pentest“ или „pen-test“) търси и използва пропуски в сигурността в мрежите и услугите на фирмата. Експертите използват тактики за атака от реалния свят върху целевата система, за да постигнат предварително определена цел по време на пентест. Тестването за проникване се използва за проверка и локализиране на уязвимости, преди потенциални хакери да получат достъп през споменатите пропуски. Фирмите могат също така да копират целия процес на нападение срещу мрежи в реално време, като използват софтуера BAS (Breach and Attack Simulation), виртуални компютри и други методи. BAS автоматизира и извършва непрекъснато тестване.

10 най-добри инструмента за симулация на кибератаки (пълен текст).

Класацията на инструменти за симулация на кибератаки според Gartner, приложими за малки компании е както следва: AttackIQ; Picus; Cymulate; SafeBreach; XM Cyber; Threat Simulator; Chariot Detect; FortiTester.

20 безплатни инструмента за киберсигурност

Инструментите за киберсигурност вече не са само за предприятията; те са от съществено значение за всеки тип и размер организация. Някои инструменти са специализирани в антивирусни програми, докато други се фокусират върху фишинг, мрежова сигурност или скриптове. Ефективните продукти, съчетани със задълбочено планиране на киберсигурността, са задължителни за всички. Независимо дали фирмите имат вътрешен екип за сигурност или възлагат тези услуги на външни изпълнители, всеки субект се нуждае от професионалисти в областта на киберсигурността, за да открият и поправят всякакви слабости в компютърните системи. За щастие има много безплатни инструменти за киберсигурност като:

Aircrack-ng; Burp Suite; Defendify; Gophish; Have I Been Pwned; Kali Linux; Metasploit Framework; Nmap; Nikto; Open Vulnerability Assessment Scanner; OSSEC; Password managers; PfSense; P0f; REMnux; Security Onion; Snort; Sqlmap; Wireshark; Zed Attack Proxy (ZAP).

Реализирани дейности по проекта CYBER4All STAR #101083793

550 обучени лица и над 92% успеваемост на тестовете – обученията през първото полугодие на ЕЦИХ ТРАКИЯ се радват на широк интерес и висока резултатност

Обученията по проект CYBER4ALLStar на Европейския Цифров Иновационен Хъб ТРАКИЯ жънат успехи и могат да се похвалят със сериозни резултати само година след стартирането си. Основи на киберсигурността е най-търсената тема сред обученията. На интерес се радват също тези за изкуствен интелект, както и младежката програма по дигитално гражданство.

Основи на офанзивното проникване и обучението на обучители също са неразделна част от портфолиото на проектните тренинги.

Резултатите от тях говорят красноречиво за качеството на програмите (97.7 %) от обучените лица декларират, че биха препоръчали обучението на свои приятели и колеги. Изключително висока е и успеваемостта на теста по „Основи на киберсигурността“ (92 %).

Проведените 39 обучения обхващат както фирми, представители на малкия и средния бизнес в България, така и публични организации и училища.

Публични изяви

На 20 април 2023 се състоя официалното откриване на Европейския цифров иновационен хъб (ЕЦИХ) ТРАКИЯ в град Пловдив.

Съюзът за стопанска инициатива и всички партньори в ЕЦИХ ТРАКИЯ са си поставили амбициозната цел ЕЦИХ ТРАКИЯ да поведе към дигитална трансформация и мрежова сигурност общинските структури, малките и средни предприятия в южен централен район в България.

Събитието продължи с два дискусионни панела: “ЕЦИХ ТРАКИЯ – мост в публично-частното партньорство” и “Възможности за финансиране за дигитална трансформация и киберсигурност”.

Предстоящи събития

Обучителите на ЕЦИХ ТРАКИЯ планират и провеждането на лятно училище с най-мотивираните и напреднали младежи по програмата за дигитално гражданство.

То ще се проведе през месеците юли и август и включва прилагането на реални сценарии по етично хакерство в кибер полигона на хъба.

В него ще вземат участие две групи по 18 младежи на възраст между 14 г. и 18 г. от Националната търговска гимназия и от ОУ "Паисий Хилендарски" в гр. Пловдив

Закон за цифровите услуги (DSA) и Закон за цифровия пазар (DMA)

Законът за цифровите услуги (Digital Services Act) и Законът за цифровия пазар (Digital Market Act) формират единен набор от правила, които се прилагат в целия ЕС. Те имат две основни цели:

1. да се създаде по-безопасно цифрово пространство, в което основните права на всички потребители на цифрови услуги са защитени;
2. за създаване на равнопоставени условия за насърчаване на иновациите, растежа и конкурентоспособността, както на европейския единен пазар, така и в световен мащаб..

Вижте цялата статия тук.

Връзки към институции и инициативи

- Съюз за стопанска инициатива
- ДИХ-Тракия
- Българска асоциация по киберсигурност
- ИИКТ-БАН
- ПУ „Паисий Хилендарски“
- Община Пловдив
- DTA
- ECSO
- Cyber Competence Network
- Cyberwatching.eu
- DIGILIENCE 2023

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 ENTERPRISE

ПЛОВДИВСКИ УНИВЕРСИТЕТ 1961 ПАИСИЙ ХИЛЕНДАРСКИ

BCA
BULGARIAN CYBERSECURITY ASSOCIATION
Българска асоциация по киберсигурност

ОБЩИНА ПЛОВДИВ