ОБЗОР И КЛАСИФИКАЦИЯ НА СЪЩЕСТВУВАЩИТЕ КИБЕРАТАКИ

Николай Митев, Виктория Спасова

Университет по библиотекознание и информационни технологии

Резюме: Съществуващата глобална ИТ инфраструктура, която е основа на съвременното информационно общество, е широко използвана за творческа и иновативна дейност, но освен това може да бъде използвана от различни злонамерени лица, групи и организации за осъществяване на атаки през киберпространството. Знанието за вида и основните характеристики на съществуващите кибератаки и за извършителите и тяхната мотивация позволява на организациите да направят оценка на риска и да предприемат адекватни мерки за защита на своите информационни активи.

Ключови думи: кибератаки, технологии, процеси, хора.

Въведение

„Дигитална трансформация“ на съвременното информационно общество означава създадената глобална ИТ инфраструктура да бъде широко използвана за творческа и иновативна дейност за повишаване на ефикасността и ефективността на производствените, бизнес и управленските процеси, водещи до повишаване на благосъстоянието и осигуряване на просперитета на обществото, но освен това може да бъде използвана от различни злонамерени лица, групи и организации за осъществяване на атаки през киберпространството. Анализът на изследователи, експерти и професионалисти в областта на сигурността, както и данните, публикувани ежегодно от множество водещи ИТ компании, държавни институции, агенции и компании за киберсигурност относно ситуацията с кибератаките и предизвиканите в резултат от тяхното осъществяване пробиви в киберсигурността, показват непрекъснатото увеличение на инцидентите през последните години. Следователно подробно и добре документиран феномен е, че съвременното общество има глобален проблем със сигурността на киберпространството.

Методология на изследването

Методологията на изследването се основава на интердисциплинарния подход. Използвани са общонаучни

методи, като сравнителен анализ и синтез, класификация, систематизация, обобщение.

Кибератаки

Кибератаката (атаката) е опит за разрушаване, разкриване, променяне, забрана, кражба или получаване на неупълномощен достъп до/или неупълномощено използване на информационен актив.[1]

Атаките представляват реализация на рисковете от заплахите от злонамерени външни и вътрешни източници за информационните активи на организациите чрез използване на уязвимости в трите компонента, които са определящи както за нормалното функциониране, така и за сигурността на информационните системи и мрежи на организациите – **технологии, процеси и хора**. С други думи, нарушенията на сигурността в резултат на успешно извършени атаки са резултат на:

- слаби и/или остарели технологии;
- неадекватни, недобре планирани, осъществявани и контролирани процеси;
- хора, които са необучени, наивни или злонамерени.

Атаки, базирани на уязвимости в технологиите

Инцидентите и нарушенията на сигурността, дължащи се **на технологиите**, са тези, възникнали в резултат на атаки, експлоатиращи уязвимости на ИТ инфраструктурата. Поради голямото разнообразие на организации с различен бизнес профил, работещи в различни сфери на икономиката и управлението, на прилаганите ИТ решения, на използваните хардуер и софтуер технологичните атаки са изключително многобройни и разнообразни, но може да се групират в няколко основни категории:

- Denial of Service (DoS) – атаки от типа „отказ на услуга“ (DoS); независимо от начина, по който са извършени, целят да нарушат нормалната работа на системата, която е цел на атаката. Най-често се осъществяват, като атакуващият претоварва целевата система със заявки, така че да изчерпи целия ѝ ресурс за обработка на заявките;
- DDoS (Distributed Denial of Service) – разновидност на DoS атаката, при която „наводняването“ на целевата система със заявки става чрез много устройства. Обикновено това са устройства, които не принадлежат на атакуващия, а са

собственост на потребители, неподозиращи, че изпращат заявки към ресурса, цел на атаката;

- Man-in-the-middle (MitM) – при този тип атаки извършителят се позиционира между потребителя и сървъра, който предлага дадена услуга. При успешно прилагане на такава атака извършителят изгражда две различни сесии – една с потребителя и една със сървъра. Този тип атаки имат различни варианти според начина на реализиране;
- SQL Injection (SQLi) – атаките се състоят във въвеждане или т.нар. „инжектиране“ на SQL заявка, представляваща зловреден код, в посока от клиента към приложението на услугата;
- Cross-site scripting (XSS) – атака, при която извършителите използват уязвимости на лошо проектирани и програмирани уебсайтове и „вмъкват“ нежелан код, който се изпълнява от браузъра на крайните потребители;
- Backdoor (задна врата) – атаката за създаване/използване на backdoor позволява заобикаляне на съществуващия механизъм за оторизация (контрол на достъпа) или на системата за криптиране в компютър или друго устройство. В света на киберсигурността терминът „задна врата“ се отнася до всеки метод, чрез който оторизирани и неупълномощени потребители могат да заобиколят нормалните мерки за сигурност и да получат потребителски достъп на високо ниво в компютърна система, мрежа или софтуерно приложение;
- Нулев ден (нулев час) (zero day или zero hour attack) – използва новооткрита уязвимост на системен или приложен софтуер, която е известна само на един или на ограничен брой атакуващи. За реализирането на атаката създава и използва малуер, т.нар. „нулев ден експлойт“, срещу който няма защита, докато производителят на софтуера не публикува поправка, която елиминира съществуващата уязвимост;
- Атаки, базирани на пропуски при избирането и използването на пароли. Например Credential Stuffing е вид кибератака, при която откраднати идентификационни данни (като потребителско име и парола) се използват за получаване на неоторизиран достъп до потребителски акаунти чрез използване на голям брой автоматични заявки за логване. Password Spraying е атака, целяща

получаване на неоторизиран достъп до потребителски акаунти чрез опити за логване с някои често използвани пароли;

- Атаки, базирани на т.нар. „съвременни упорити заплахи“ (Advanced Persistent Threat – APT) – с този обобщаващ термин се дефинират комплексни, професионално управлявани кибератаки, особено такива, които използват неразкрити познания за уязвимости в сигурността на компютърните системи, платформи или приложения, осъществявани от групи и организации с много големи технически, човешки и финансови ресурси.

В Националната стратегия за киберсигурност „Киберустойчива България 2020“ се обръща особено внимание на този вид атаки, като се подчертава: „Съвременните атаки през интернет са комплексни, организирани и използват широк спектър от наречените „съвременни упорити заплахи“, с продължителен скрит период. Те често са насочени към високо стойностни, но недобре защитени цели и могат лесно да ескалират от киберинцидент в киберкриза“[2].

За определяне на понятието „съвременни упорити заплахи“ може да се използва дефиницията на Националния институт по стандартизация и технологии (NIST 800 – 61) на САЩ: „APT атаката е действия на противник, притежаващ усъвършенствани експертни познания и значителни ресурси, които му позволяват да създаде условия за постигане на целите си, като използва множество направления (вектори) на атаката (например кибер-, физически и измама). Тези цели обикновено включват установяване и разширяване на присъствието на нападателя в ИТ инфраструктурата на целевите организации, което му позволява да извърши изтегляне или компрометиране на информация, подкопаване или възпрепятстване на критични аспекти на мисията, програмата или организацията; или да се позиционира, за да изпълни тези цели в бъдеще. Съвременната упорита заплаха: (1) преследва целите си непрекъснато за продължителен период от време; (2) адаптира се към усилията на защитниците да се противопоставят на това; (3) решена е да поддържа нивото на взаимодействие, необходимо за постигане на набелязаните цели“[3].

Друга основна характеристика на APT атаките се отнася до източниците на APT заплахите, които реализират тези атаки. Според класификацията на ISACA източниците на APT заплахи са[4]:

Таблица 1. Източници на APT заплахи

Заплаха	Какво търсят	Въздействие върху бизнеса
Разузнавателни агенции	Политически, отбранителни, търговски или производствени тайни	Загуба на интелектуална собственост, на търговски и производствени тайни, на конкурентно предимство
Криминални групи	Трансфер на пари, възможности за изнудване, придобиване на лични идентификационни данни или персонална информация с цел потенциална продажба	Финансови загуби, мащабни нарушения на данните за клиентите или загуба на интелектуална собственост и търговски тайни
Терористични групи	Предизвикване и широко разпространение на терор чрез смърт, унищожаване и разрушаване	Прекъсване на производство и услуги, въздействие върху пазарите и потенциални рискове за човешкия живот
Групи на активисти	Придобиване на поверителна информация или прекъсване на услуги	Големи нарушения на данните или прекратяване на услуги
Въоръжени сили	Разузнаване или позициониране за подпомагане на бъдещи атаки срещу критична национална инфраструктура	Сериозни щети на съоръженията и оборудването в случай на военен конфликт

Средства за осъществяване на технологични атаки

Понятието „зловреден софтуер“ (malware – малуер) се използва като събирателен термин за различни видове софтуер, предназначен да повреди, наруши функционирането, открадне, разруши или като цяло да извърши негативни и нелегитимни действия в рамките на компютърните информационни системи и мрежи. Съществуват огромен брой видове и разновидности малуер, които се различават по предназначението си и начина, по който функционират или се разпространяват. Някои от най-често срещаните видове зловреден софтуер са:

- Компютърен вирус – представлява вид компютърна програма, която при изпълнение се репликира, като модифицира други компютърни програми и вмъква свой собствен код към техния;
- Компютърен червей – червеите са самостоятелен софтуер и не изискват приемаща програма или човешка помощ за разпространение. За да се разпространят, червеите

използват или уязвимост на целевата система, или някакъв вид социално инженерство, за да подмамят потребителите да ги изпълнят;

- Троянски кон (или просто Троянец) – зловреден софтуер, който получава достъп до дадена целева система, като се маскира като истинско приложение и изглежда легитимен. Троянските коне често се разделят на категории, отразяващи техните цел и предназначение;
- Spyware (шпионски софтуер) – клас зловреден софтуер, който събира информация за човек или организация без тяхното знание;
- Adware (рекламен софтуер) – клас зловреден софтуер, предназначен да показва реклами (обикновено нежелани) на потребителите;
- Ransomware – клас зловреден софтуер, който заключва или криптира данни или функции и изисква плащане, за да ги отключи;
- Keylogger – клас зловреден софтуер, който тайно записва натисканията на клавишите от потребителя и в някои случаи – съдържанието на екрана;
- Browser Hijacker – софтуер, който променя настройките на уеббраузъра без разрешение на потребителя, за инсталиране на нежелана реклама в браузъра;
- Rootkit – клас зловреден софтуер, който прикрива съществуването на друг злонамерен софтуер, като променя основната операционна система;
- Ботнет („мрежа от роботи“) – разпределена широка мрежа от предварително компрометирани устройства, които могат да бъдат контролирани, за да стартират синхронизирано широкомащабни атаки, такива като отказ от услуга (DDoS), срещу избрани жертви;
- Бот – автоматизиран процес, който взаимодейства с други мрежови услуги. Злонамереният бот е саморазпространяващ се малуер, предназначен да зарази даден хост и да се свърже с централен сървър или сървъри, които действат като център за управление и контрол (command and control (C&C) center) на цялата мрежа от компрометирани устройства;
- Експлойт – софтуерен код или поредица от команди, които се възползват от конкретна уязвимост в хардуерна или

софтуерна компютърна система и предизвикват неочаквано или нежелано поведение на системата.

Атаки, базирани на слабости в процесите

Нарушенията на киберсигурността често са резултат от пропуски в планирането, изпълнението или контрола на процесите. Служителите често извършват нарушения или допускат пропуски при изпълнението на установените процеси, основно поради небрежност, незнание, липса на достатъчно квалификация или защото изпълнението на процесите по някакъв начин им създава трудности. По-долу са изложени процесите, имащи връзка с киберсигурността.

Бизнес процеси. Голяма част от рисковете за сигурността може да бъдат идентифицирани и намалени чрез усъвършенстване и усилване на вътрешните бизнес процеси, които зависят от бизнес профила на организацията – от производствените и бизнес дейности, които се осъществяват с помощта на ИКТ. Нови заплахи и уязвимости възникват при изпълнението и най-вече при промяната на бизнес процесите, като въвеждане на:

- автоматизация и компютризация на съществуващи бизнес и производствени процеси;
- нови външни/вътрешни бизнес услуги, осъществявани чрез ИКТ;
- нови функции на съществуващи бизнес услуги;
- промени в ИТ инфраструктурата – софтуер, системи, мрежи;
- промени в организацията на дейността – преминаване към дистанционна работа; използване на облачни услуги; използване на собствени устройства; използване на собствен софтуер; използване на IoT; използване на социални мрежи;
- процеси по управление на взаимоотношения с клиенти, партньори, доставчици, съизпълнители и други външни лица и организации.

Процеси, свързани със сигурността. При установяването на процесите за сигурност на вътрешните информационни системи и мрежи на организацията може да бъдат използвани различни подходи, като предлагания от серията стандарти ISO/IEC 27000 за създаване, въвеждане, поддържане, наблюдение и усъвършенстване на система за управление на информационната сигурност. Прилагането на процесите и процедурите за сигурност зависи от оценката на организацията за допустимия (приемливия)

риск и наличните ресурси, с които разполага. За мнозинството организации, независимо от профила им, важно значение имат следните процеси, свързани със сигурността:

- управление и контрол на достъпа – идентификация, автентикация, оторизация;
- класификация на информацията според чувствителността ѝ;
- управление и допустимо използване на активите;
- управление на човешките ресурси – образование, квалификация, обучение, информираност;
- осигуряване и сигурност на комуникациите, управление на обмена на информация;
- управление на промените;
- създаване и управление на резервни копия;
- криптиране и управление на ключовете;
- инсталиране, промени и съхраняване на системни и приложни софтуерни продукти;
- разработване, изпитване и внедряване на собствени софтуерни решения;
- защита от злонамерен софтуер
- осъществяване на вътрешни и външни одити за оценка на информационната сигурност;
- управление на инциденти с информационната сигурност;
- осигуряване на физическа сигурност и др.[5]

За намаляване на рисковете от атаки в резултат на уязвимости в бизнес процесите и процесите по сигурността при проектирането, създаването, внедряването, предлагането и поддържането на вътрешни и външни за организацията ИТ услуги и свързаните с тяхната реализация процеси може да се приложат съществуващите стандарти и норми за създаване на система за управление на ИТ услугите (ITSM), като ISO/IEC 20000, ITIL, COBIT, и за система за управление на информационната сигурност (ISMS), предлагана от серията стандарти ISO/IEC 27000.

Атаки, експлоатиращи уязвимости на човешките ресурси

Всяка организация (при наличието на достатъчно ресурси) може да постигне колкото ѝ е необходима техническа сигурност на своите информационни системи и мрежи, но ако не подхожда правилно при подбора, обучението, управлението и контрола на персонала, винаги ще бъде подложена на риск от инциденти. Този факт е известен както на мениджърите на компании, така и на атакуващите. Използването на слабости в характера и

поведението, на недостатъчна квалификация, обучение и информираност на служителите ги прави много по-обещаващ вектор за провеждане на атаки срещу целевите организации. Вместо да изразходват големи ресурси за създаване и изпълнение на сложни технологични атаки, които освен това изискват висока квалификация и технологично оборудване, голяма част от атакуващите, особено такива, които не разполагат с необходимите познания, технологии и ресурси, използват методите на **социалното инженерство** за създаване на атаки, насочени към персонала на организациите. Тези методи използват наличието на слабости, като недостатъчни обучение, тренираност и информираност, а също и недостатъци на характера на хората, като небрежност, нехайство, доверчивост, безотговорност и др.

Социалното инженерство е метод за атаки, експлоатиращ слабостите на човешкия характер и поведение, за създаване на достоверно изглеждащи измами и заблуди с цел придобиване на чувствителна информация или данни, които може да бъдат използвани за несанкциониран достъп до информационни ресурси или за създаване или развитие на бъдещи атаки.

Най-разпространените видове атаки, използващи социалното инженерство, са:

- Фишинг (Phishing) – вид атака с цел измама на атакувания, осъществявана чрез електронни съобщения (електронна поща, есемеси и други типове онлайн комуникации, като социални медии, телефонни обаждания и др.), които претендират, че идват от достоверен източник. Този вид атака има за цел да заблуди потребителите да посетят измамен уебсайт, да отворят прикачен файл, съдържащ малуер, или да споделят лична информация, като пароли и идентификатори за логване;
- Насочен фишинг (Spear Phishing) – разновидност на фишинга, но с персонална насоченост, при който целта на атакуващия е определен човек или компания. За да бъде убедителна измамата, при тази разновидност на атаката се използва предварително събрана информация за атакувания, като персонални и професионални данни, както и данни за организацията, като тип на бизнеса, партньори, местоположение и др.;
- „Примамване“ (Baiting) – метод за измама, при който атакуващият се възползва от човешкото любопитство. Може да се състои в подхвърляне (подаряване, намиране)

на физически устройства, например USB памети. На тези устройства обикновено има малуер, който се активира или при поставяне на устройството в компютър, или при стартиране на програма от него. По подобен начин, експлоатирайки знания за интересите на потребителя и възползвайки се от неговото любопитство, методът може да го насочи да кликне върху рекламни банери или обяви в сайтовете, които посещава, за да го отведат до друг сайт, чието съдържание е злонамерено;

- Смишинг (комбинация от SMS и „фишинг“) – измама чрез фалшив есемес, като целта е да бъде получена лична, финансова или свързана със сигурността информация чрез текстово съобщение. Текстовото съобщение обикновено изисква от получателя да кликне върху линк или да се обади на телефонен номер, за да „потвърди“, „актуализира“ или „активира“ профила си. Но линкът води до фалшив уебсайт и на телефонния номер отговаря измамник, който се представя, че е от реална компания;
- Фарминг – измама, чиято цел е прехвърляне на потребителите на фалшиви уебсайтове, имитиращи истинските сайтове, които са проектирани да инсталират малуер, да крадат идентификатори за логване или друга информация. Фармингът е особено опасен при имитация на легитимни сайтове, където посетителите могат да въвеждат свое съдържание, тъй като много често целта на измамниците е да получат идентификационни данни на потребителите за логване в действителните сайтове.

Заключение

Прегледът и анализът на вида, количеството и характеристиките на осъществените през последните години кибератаки показват, че те се развиват и усъвършенстват бързо. Перспективата за зловреден софтуер, причиняващ глобално въздействие върху нормалното функциониране на ИТ инфраструктурата и комуникациите и прекъсване на производствени, управленски или бизнес дейности, или предизвикващ сериозно физическо бедствие, доскоро беше смятана за малко вероятна не само от повечето политици и обикновени хора, но и от професионалистите в областта на сигурността. Днес заплахата е реална и всички институции на държавното управление и водещи компании и предприятия от критичната инфраструктура са потенциални мишени за

кибератаки. Потенциалните нападатели (разузнавателни агенции, подразделения за кибероперации на въоръжени сили, терористи, хактивисти, престъпни организации) са развили своите възможности до мащабно професионално производство и вече притежават сложни и комплексни софтуерни програми и инструменти за осъществяване на кибератаки. За да отговорят на предизвикателствата и да противодействат на заплахите в динамичната киберсреда, държавите създават структури за киберсигурност към различните държавни институции и ведомства, а бизнес организациите инвестират все повече средства за осигуряване на способности за защита срещу кибератаките и на непрекъснатост на бизнес процесите.

Благодарности: Тази публикация е финансирана от Министерството на образованието и науката в изпълнение на Национална научна програма „Сигурност и отбрана“, приета с РМС № 731 от 21.10.2021 г., и съгласно Споразумение № Д01-74/19.05.2022 г.

Бележки

[1] **Закон** за киберсигурност, обн. ДВ, бр. 94 от 13 ноември 2018 г., изм. ДВ, бр. 69 от 4 август 2020 г., изм. и доп. ДВ, бр. 85 от 2 октомври 2020 г., изм. и доп. ДВ, бр. 15 от 22 февруари 2022 г., изм. ДВ, бр. 25 от 29 март 2022 г.

[2] **Национална** стратегия за киберсигурност „Киберустойчива България 2020“. http://www.cyberbg.eu/.

[3] **NIST 800 – 61:** Computer Security Incident Handling Guide. http://dx.doi.org/10.6028/NIST.SP.800-61r2?

[4] **Information** Systems Audit and Control Association (ISACA). Advanced Persistent Threats. How to Manage the Risk to Your Business. https://svpr-isg-a1.isaca.org/ISGweb/Purchase/ProductDetail.aspx?Product_code=WAPT

[5] **ISO/IEC 27002:2022** Information security, cybersecurity and privacy protection – Information security controls.

References/Литература

1. **Denchev**, S. Informatsia i sigurnost. Sofia: Za bukvite – O pismeneh, 2019. ISBN 978-619-185-369-4.]

[**Денчев**, С. Информация и сигурност. София: За буквите – О писменехъ, 2019. ISBN 978-619-185-369-4.]

2. **Semerdzhiev**, Ts., N. **Mitev**. Upravlenie na informatsionnata sigurnost v organizatsiite. Sofia: Softtreyd, 2020. ISBN 978-954-334-236-5.

[**Семерджиев**, Ц., Н. **Митев**. Управление на информационната сигурност в организациите. София: Софттрейд, 2020. ISBN 978-954-334-236-5.]

За авторите

Николай Митев е доц. д-р, преподавател в катедра „Национална сигурност“ в УниБИТ. Чете лекции, автор е и участва като съавтор при издаването на седем учебника и учебни пособия в областта на ефективното използване на информационните системи и управление и защита на информацията.

За контакт с автора: n.mitev@unibit.bg

Виктория Спасова е докторант към катедра „Национална сигурност“ в УниБИТ. Зачислена е в докторска програма „Национална сигурност“, с тема на дисертационния труд „Сигурността на облачните услуги в областта на образованието, като аспект на националната сигурност“.

За контакт с автора: v.spasova@unibit.bg