IT4Sec Reports 133
http://dx.doi.org/10.11610/it4sec.0133

Топ 10 заплахи за киберпространство през 2019

Златогор Минчев, Павлин Кутинчев, Иван Гайдарски

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

София, май 2019 г.

Златогор Минчев, Павлин Кутинчев, Иван Гайдарски, Топ 10 заплахи за кибер пространство през 2019**,** *IT4Sec Reports* 133, https://doi.org/10.11610/IT4Sec.0133

IT4Sec Reports 133 „Топ 10 заплахи за киберпространство през 2019“. Направените разглеждания в настоящото изследване имат за цел да представят основните направления, в които ще се развиват заплахите за киберпространството през 2019 година. Като основна тенденция се очертава запазването на приоритетна роля за кибер атаки върху иновативните технологични решения, касаещи клауд услуги, смарт мобилни решения и IoT приложения, върху които ще бъдат съсредоточени различните зловредни действия и опити за влияние по отношение на човешкия фактор, хардуера и програмното осигуряване. Като тези действия се развиват в смесената дигитална реалност на бъдещето, основана на интелигентни социални и хетерогенни комуникационни мрежи, и с активното участие на хората. При това допълнителен акцент се очаква да бъде поставен и върху регулациите и политиките за защита на личните и корпоративни данни, системи и услуги.

Ключови думи: киберпространството, обобщена картина на значимост, топ 10 актуални заплахи, смесената дигитална реалност, дигитално бъдеще

IT4SecReports 133 “Top 10 live threats to cyberspace in 2019”. The outlined overviews in the present study are aiming to mark the key assets for development of threats in the cyberspace for 2019. The major trend is outlining a priority role for cyberattacks on innovative technological solutions, concerning cloud services, smart mobiles and IoTs that are addressed by different malware activities and negative attempts from human factor, hardware and software perspectives in the mixed digital reality of the future. Encompassing at the same time both social and heterogeneous communicational smart networks with the active role of the humans. Additional accent is expected to emerge also from the regulations and policies for personal and corporate data, systems and services protection.

Keywords: cyberspace, generalized landscape of significance, top 10 live threats, mixed digital reality, digital future

Благодарност: Резултатите в настоящото изследване са получени в рамките на Национална научна програма „Информационни и комуникационни технологии за единен цифров пазар в науката, образованието и сигурността (ИКТвНОС)“, 2018-2020, финансирана от МОН, Р България.

ISSN 1314-5614

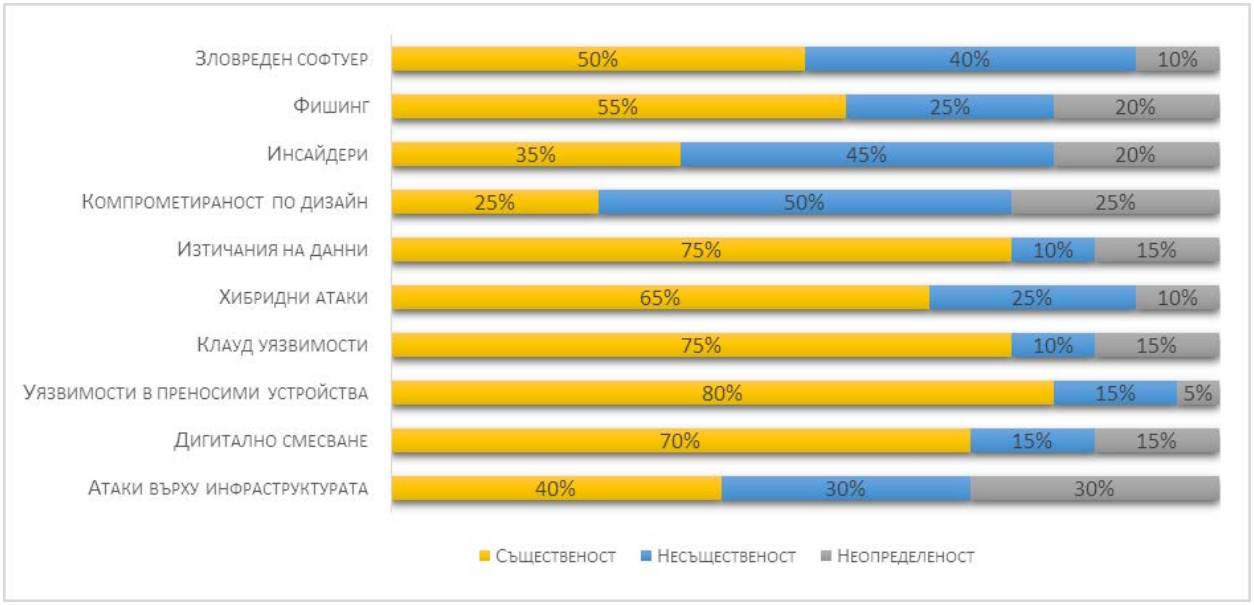
СЪДЪРЖАНИЕ

1. ВЪВЕДЕНИЕ

Все по-нарастващото значение на онлайн услугите в нашето ежедневие и развитието на клауд технологиите, превръща киберсигурността в сфера с голяма важност за сигурността в дигиталната ера. Всяка година кибер инцидентите струват милиарди долари на засегнатите страни и въздействат на значителен обем от чувствителни данни и устройства. В настоящия анализ е направен кратък преглед на очакванията за десетте най-актуални заплахи в кибер пространство през 2019 година. Използвани са както литературни данни от водещи технологични източници (като напр. Symantec [1], Verizone [2], [3], Cisco [4], Sophos [5]), така и експертен индустриален, и изследователски опит събран в рамките на инициативата Securing Digital Future 21 [6].

2. ОБОБЩЕНА КАРТИНА НА ЗНАЧИМОСТ

По подобие на SysSec Red Book [7], основните резултати от настоящото изследване могат да бъдат обобщени графично около десет направления: „Зловреден софтуер“, „Фишинг“, „Инсайдери“, „Компрометираност по дизайн“, „Изтичания на данни“, „Хибридни атаки“, „Клауд уязвимости“, „Уязвимости в преносими устройства“, „Дигитално смесване“, „Атаки върху инфраструктурата“. При това оценките са направени с отчитане, като на „Съществеността“ и „Несъществеността“ на тези направления, така и при отразяване на „Неопределеността“ за това.



Обобщена картина на значимост за 10-те направления на изследване на заплахи в киберпространството през 2019 година

Представените данни от анализа, дават очакван приоритет на проблеми свързани с „Уязвимости в преносими устройства“, отнесени главно към мобилни смарт решения и развиващата се тенденция за Интернет на нещата. Друг забележим момент са „Клауд уязвимостите“, които са свързани също с развитието на облачните услуги от различен тип. По-сложни заплахи, произтичат от проблемите около „Дигиталното смесване“ на обективната и машинно симулирана реалност, както и ефектите върху човешкия фактор. Тук е важно да се отчете и комбинацията на тези заплахи с „Изтичанията на данни“ от различен характер и „Хибридните атаки“, свързани с понятия като: „информационна война“, „фалшиви

новини“, „социален инженеринг“ и Advanced Persisten Threats – APT. При това не бива да пренебрегваме ролята на „Зловредния софтуер“ и „Фишинга“ от различен тип. Проблемите по отношение на „Компрометираността по дизайн“, „Инсайдерите“ и „Атаките върху инфраструктурата“ също са изследвани, въпреки не толкова високата им приоритизация.

3. КОНКРЕТНИ ЗАПЛАХИ И ПОЯСНЕНИЯ

В следващата част от изследването ще бъдат посочени и по-конкретни заплахи към вече очертаните 10 направления от киберпространството за 2019 година. За всяка от тези заплахи е даден кратък коментар, по отношение на представената вече обобщена картина за очаквана значимост в киберпространството през годината.

3.1. ЕКСПОЗИЦИИ КЪМ ТРЕТИ СТРАНИ

Водещата тенденция при малкия и средния бизнес за използване на външни услуги (обработка на плащания, счетоводство, маркетинг, реклама и др.) от т. нар. „трети страни“ ще се запази и през 2019 г. Това на практика означава, че външни за компанията субекти имат достъп до нейните данни. Възникването на кибер-инциденти при използването на този тип услуги е пряко свързано със заплахи касаещи „Инсайдери“, „Хибридни атаки“, „Зловреден софтуер“ и „Фишинг“. Така възникват реални възможности за „Изтичания на данни“ към трети страни, а чувствителните и личните данни на компаниите, използащи външни услуги са поставени под риск. Наред с различните последствия от изтичането на тези данни (като например: нарушаване на търговска тайна, изтичане на ноу-хау към конкуренти, репутационни рискове), значителна тежест вече имат и юридическите последствия. Тук трябва да отбележим и положителната роля на въведената наскоро (от м. май, 2018) у нас, като член на ЕС, GDPR регулация [8] и налагането на глоби върху големи компании като Facebook, Microsoft, и Google, предоставящи основно маркетингови и рекламни услуги, във връзка с някои нарушения по отношение на личните данни на потребителите [9].

3.2. УПРАВЛЕНИЕ НА СОФТУЕРНИТЕ АКТУАЛИЗАЦИИ (UPDATES) И КРЪПКИ (PATCHES)

Редовното актуализирането на фърмуъера на хардуерните устройства, актуализациите и кръпките при софтуерните системи е абсолютно задължително в наши дни. Всяка уязвимост в хардуера или софтуера не остава незабелязана и се превръща в открита покана за атака от страна на недоброжелателите, които атакуват целта с т. нар. „експлоити“. Тук е важно да се отбележат направленията „Компрометираност по дизайн“, „Зловреден софтуер“ и „Атаки върху критичната инфраструктура“, тъй като актуализациите с нови кръпки и ъпдейти крие опасности от поява на нови, непредвидени заплахи и отваря възможност за нерегламентирано обновяване със системен софтуер, който реално не е официален. Това поставя и въпроса за контрол върху масовите устройствата, произведени основно в Китай, по отношение на регулациите в ЕС. Ще отбележим че на практика това са специализирани инструменти за кибер атака чрез новооткрити уязвимости в операционните системи, фърмуера и системните приложения. Две от най-мащабните кибер атаки напоследък се основават именно на такава уязвимост – използва се критична уязвимост в

операционната система Windows, известна като EternalBlue [10]. След пускането на ъпдейт, закърпващ тази уязвимост от Microsoft, организациите, които не са актуализирали софтуера си, бяха изложени на риск от нови атаки. Подобна е и ситуацията с популярната система Android и нейните реплики, предвид активното й навлизане в интелигентната среда на обитание [5]. Същевременно е важно да отбележим, и че обновяването на фърмуера в индустриална среда крие опасности за реализиране на атаки върху критичната инфраструктура, вкл. комуникационна (напр. някои съвсем скорошни случаи със Cisco и Huawei, [11]) и преносимите устройства, които не винаги могат да бъдат идентифицирани бързо, лесно и навременно. През 2019 година се очаква запазване на тези тенденции от заплахи, свързани със софтуерните ъпдейти и кръпките, които особено по отношение на новите комуникационни безжични решения от тип 5G, могат да предизвикат значителни проблеми.

3.3. КЛАУД УЯЗВИМОСТИ

Данните и приложенията, които компаниите съхраняват и инсталират в cloud (от англ. „облак“) решенията днес се увеличават експоненциално [15]. По същия начин нарастват и рисковете от кибер атаки по отношение на клауд решенията през 2019 г. Облачните услуги са уязвими към широк кръг от кибер инциденти [1], [3]. Такива са например: account hijacking („отвличане на профил“), Denial of Service – DoS (атака тип „отказ на услуга“, вкл. и „разпределен“ – Distributed DoS – DDoS), чрез които компаниите могат да загубят достъп до своите данни или приложения за определен период от време, а евентуално дори и част от самите тях, като тук може да се говори и за „Компрометираност по дизайн“.

Друг вид уязвимости са Advanced Persistent Threats (APT) – атаки при които атакуващия прониква във вътрешната мрежа и чрез различни, комбинирани техники успява да се изплъзне на вътрешните мерки за сигурност и да получи достъп до чувствителните данни в облака.

Интересен вид уязвимост е Shared Technology Vulnerabilities (Уязвимости в споделената технология). Инфраструктурата за облачните услуги се основава на т.нар. multi-tenancy технологии, при които различните потребители споделят общи изчислителни и storage (съхраняващи) ресурси. Поради слабости в проектирането, уязвимости в хардуерните компоненти изграждащи инфраструктурата или неправилна конфигурация, може да се стигне до споделени уязвимости, свързани с технологии като Виртуални машини (Virtual Machines – VM), операционни системи, хипервизори и др. Това би позволило на хакерите да компрометират сигурността на данните на потребителите на клауд услуги [12].

Много от потребителите на тези услуги се доверяват на мерките за сигурност, взети от самите доставчици, но на практика те не са достатъчни, за да се елиминират и контролират сложни заплахи, каквито са „Инсайдерите“ [2]. Технологичните мерки за сигурност са само част от решението. Необходими са и редица организационни мерки, включително архивиране (back-up), обучение за повишаване на кибер-сигурността (security awareness training) и разработване на специален план за управление на идентифицираните кибер рискове в компанията използваща клауд услуги.

3.4. WHALING АТАКИ

Една от най-актуалните заплахи днес са Business E-mail Compromise (BEC) атаките, по-известни като “whaling” (от англ. „китоловство“). Този вид spear phishing атаки имат пряко

отношение към „Изтичанията на данни“, като се стремят да убедят жертвата, използвайки специфични детайли и стил в писмото, че атакуващата страна е легитимен и надежден партньор, за да се спечели доверието й, и съответно – осигури достъп и контрол до нейните данни и устройство. Whaling атаките адресират високопоставени корпоративни служители, които използват електронните съобщения за официална комуникация и вярват, че позицията им е добре защитена по подразбиране по отношение на кибератаки. Допълнително включеният „Зловреден софтуер“ е организиран под формата на прикачени документи или хипер връзки. Този вид атаки стават все по-сложни и по-масови напоследък, използвайки смарт решения като Snapchat и се превръщат в сериозна заплаха за компании от различни сектори и размери. Неотдавнашен доклад на ФБР [13] показва над 100% увеличение на загубите в световен мащаб за периода декември 2016 – май 2018, като почти една четвърт от тези загуби са възникнали на територията на САЩ. Тенденцията за използване на този тип фишинг атаки, с известни модификации, се очаква да се запази и през 2019.

3.5. RANSOMWARE АТАКИ

Ransomware (от англ. „откуп“ и „софтуер“) атаките днес са сред най-сериозните и актуални кибер заплахи, които основно могат да бъдат отнесени към „Зловредния софтуер“. За момента те заразяват главно машини от корпоративни мрежи (като има и версии за мобилни устройства, чиито дял постоянно нараства), криптират твърдите им дискове и изнудват своите жертви за откуп срещу декриптиращ ключ, чрез който те да достъпят отново своите данни. Самият откуп обикновено не е сериозна сума, която се заплаща в дигитална валута (най-често биткойни) и използване на електронен блокчейн потфейл. Това обаче не гарантира единственост на откупения достъп до данните, дори при реалното му заплащане. Този тип атаки причиняват значителни щети, които произтичат основно от блокирането на бизнес-процесите, намаляване на производителността на работа и най-вече – от загубата на чувствителни данни, представляваща по същество „Изтичане на данни“ [3]. Допълнително тези атаки могат да инсталират и софтуер за crypto mining („копаене“ на електронни пари), който компрометира и забавя работата на заразените устройства. Ransomware атаките са много популярен и лесен начин за печелене на пари в dark web и способ за негативно въздействие срещу компании и организации от различни мащаби и сектори на икономиката. Според годишни доклади на Cisco за киберсигурността [14], [15] атаките от ransomware се увеличават с темпове от 350% годишно. През 2019 се очаква те да разширят своя мащаб на действие, както по отношение на „Атаки върху инфраструктурата“ (комуникационна, енергийна и др.), така и към начините за проникване, основаващи се вече на сложни „Хибридни атаки“, „Уязвимости в преносими устройства“ и „Инсайдери“. Очаква се ransomware атаките да се реализират и чрез използване на компрометирани преносими устройства, памети, социални мрежи, клауд услуги (вкл. протоколи за отдалечено администриране, като RDP) и чатове. Възможно е и начините за плащане на откуп също да еволюират с цел по-трудното им проследяване (напр. към искане на данни и акредитиви).

3.6. ОБЪРКВАНЕ МЕЖДУ ПОНЯТИЯТА „СЪОТВЕТСТВИЕ СЪС СТАНДАРТИ И РЕГУЛАЦИИ“, И „РЕАЛНА ЗАЩИТА НА ИНФОРМАЦИОННИТЕ АКТИВИ“

Съответствието със стандартите и регулациите за информационна сигурност като напр.: ISO 27001, ISO 27002 [16], Gramm-Leach-Bliley Act (GLBA) [17], Sarbanes-Oxley [18], HIPAA [19] и EU GDPR [8] не е еквивалентно на осигуряването на непрекъсната и стабилна защита на информационните активи. То обаче е важна предпоставка за адекватна тяхна защита и има пряко отношение към направлението „Изтичания на данни“. За пример може да се посочат организации, които трябва да отговарят на стандарта Payment Card Industry Data Security Standard – PCI DSS [20] за своя годишен одит. Съвместимостта с този стандарт не гарантира нивото на защита на техните данни. Според доклада на Verizon за PCI DSS [21], четири от пет компании не успяват да запазят съответствието си със стандарта при междинната оценка. Това по своята същност са своеобразни „Хибридни атаки“, въвеждащи компаниите ползватели на стандарта PCI DSS в заблуждение. Те фактически се превръщат в жертви, които считат съответствието със стандарта за достатъчно. Тук е важно да се отбележи, че де факто съществува ясна разлика между съвместимост и реална информационна защита на активите. За 2019 година се очаква да се запази и тази тенденция, особено по отношение на личните данни с въвеждане на редица иновации в социалните мрежи [22], пряко влияещи върху „Дигиталното смесване“ и засилената тенденция от корпоративни изтичания на данни по отношение на малките и средни компании с преобладаваща финансова мотивация, но не само [3].

3.7. ЗАПЛАХИ ЗА МОБИЛНАТА СИГУРНОСТ

В края на 2018 година броя на активно използваните мобилни устройства премина 12.1 милиарда, а всяка пета организация страда от пробиви в сигурността на мобилните мрежи [23]. Мобилните технологии могат да предложат както значителни предимства за бизнеса, така и да го изложат на редица потенциални заплахи по отношение най-вече на „Изтичания на данни“ [3]. По-голямата част от атаките върху мобилните устройства идват от „Зловреден софтуер“ и „Атаки върху инфраструктурата“ [15], най-често заразени Wi-Fi мрежи. В близо 39% от анкетираните организации се съобщава, че мобилните корпоративни устройства са изтеглили „Зловреден софтуер“ и впоследствие са установили проблеми със сигурността. Според [23], до 2019 г. Wi-Fi мрежите ще пренасят почти 60% от мобилния трафик на данни, достигайки над 115 000 PB (петабайта). Този растеж носи със себе си и нови уязвимости, възникващи когато мобилните устройства се свързват с компрометирани Wi-Fi мрежи и произтичащите от това евентуални загуби или кражби на корпоративни данни. Една от констатациите на проучването е, че само 38% от организациите вземат мерки за унищожаване на данните от мобилните устройства при смяна на потребителя или при изваждане от употреба на самото устройството с цел предотвратяване на „Изтичания на данни“. В този случай върху мобилните устройства остават стотици хиляди имейли, SMS/IM съобщения, снимки, видеоклипове и друга чувствителна информация, лесно достъпни за кибер престъпниците или за случайни лица при загуба на устройството. Тази констатация подчертава колко е важно през 2019 година, организациите да се стремят да управляват своите чувствителните данни през целият им жизнен цикъл. Допълнително ще отбележим и рисковете с „Компрометираност по дизайн“ (вж. напр. [24]) и „Уязвимости в преносими

устройства“ (вж. напр. [25]) по отношение на корпоративните мобилни устройства и проблемите отбелязани вече в т. 3.2.

Най-популярните мерки за сигурност на мобилните устройства включват защита с парола (63%), последвана от дистанционно изтриване на устройства (49%) и криптиране на устройства (43%). Удостоверенията (сертификатите) често са компрометират в резултат на „Фишинг“ атаки. За да ограничат риска от неоторизиран достъп, организациите трябва да въведат по-сигурни средства за удостоверяване, като единична регистрация, контекстно многофакторно удостоверяване и пароли за еднократна употреба. Друга изключителна ефективна мярка е използването на специализиран софтуер за изтриване на данните от мобилните устройства (като напр. [26]). С въвеждането на новите политики за сигурност при мобилните устройства и 5G технологиите се очаква да се постигне решение на част от тези проблеми, но и да възникнат някои нови [27].

3.8. BRING YOUR OWN DEVICE (BYOD)

Днес много компании насърчават служителите си да използват лични мобилни устройства (смартфони, таблети и дори преносими компютри) на работното си място, като част от своята BYOD политика. Тази политика има доста предимства, сред които повишена гъвкавост и удобство, повишаване на производителността и мобилността на служителите, както и по-ниска себестойност на инвестициите в офис инфраструктура [23]. Въпреки ползите, BYOD политиките могат да изложат компаниите и на сериозни рискове от гл. т. на информационната сигурност най-вече по отношение „Изтичания на данни“, и недостатъчната яснота за тяхната надежност, позволяваща компрометиране от типа „Атаки върху инфраструктурата“. Изтичането и загубата на данни е най-сериозното грижа за сигурността при BYOD – около 72%. Същевременно, 56% от респондентите се притесняват от неоторизиран достъп до корпоративни данни и системи, а 54% са загрижени, че потребителите ще изтеглят опасни приложения или съдържание. Личните устройства могат да бъдат по-лесна плячка за хакери и недоброжелатели, в сравнение с корпоративните устройства, създавайки условия за проникване и компрометиране на чувствителните данни на базата на „Уязвимости в преносими устройства“, които BYOD потребителя не администрира достатъчно компетентно. Тук е важно да се отбележи и използването на лични устройства за достъп до нерегламентирани източници на данни, най-често за забавление (торент сайтове, dark web и др.), които могат да ги компрометират, дори без знанието на техните собственици [28].

Предвид гореизложеното, през 2019, BYOD политиките се очаква да станат по-сериозно обмислени и съобразени с корпоративните политики за ИТ сигурност при отчитане на проблемите свързани с клауд услугите и експозицията към трети страни (вж. т. 3.1 и т. 3.3), с оглед избягване на атаки организирани от „Инсайдери“, които имат напълно регламентиран достъп до вътрешната корпоративна мрежа. За целта е необходимо да се увеличи интензитета и периодичността на обучението на служителите по отношение използването на подходящи софтуерни инструменти за постигане на цялостна защита, както и да се извършва редовен преглед на състоянието на BYOD устройствата при спазване на съответните стандарти и политики за сигурност на мобилните устройства (вж. т.3.7 и т.3.6).

3.9. ИНТЕРНЕТ НА НЕЩАТА (IoT)

Internet of Things – IoT (от англ. „Интернет на нещата“) представляват „жива“, интелигентна мрежа от свързани чрез ad-hoc мрежа обекти (смарт устройства, сензори, импланти и др.), които могат да съхраняват, изпращат и получават данни, вкл. и автономно по различни комуникационни канали (напр. Wi-Fi, Bluetooth, 4G, ZigBee [29]). Съвременната IoT технология (наричана още от Cisco – “Internet of Everything” – „Интернет на всичко“) позволява използване и вграждане в редица иновативни и широкомащабни решения, целящи улесняване на нашето ежедневие в дигиталната ера – умни домове, офиси и селища, медицински приложения – биометрия, дистанционна диагностика, телемедицина, доставки, наблюдение и ранно предупреждение за природни катаклизми и т.н. [30], ориентирани около идеята за дигиталното общество на бъдещето – Society 5.0 [31].

Именно свързаността с мрежата обаче създава предпоставки за използването на IoT устройствата като своеобразни точки за достъп от хакери и недоброжелатели [25] по отношение на „Хибридни атаки“ и „Изтичания на данни“ за 2019. Поради експоненциалното нарастване на броя на IoT устройствата и тяхното приложение с различни цели, много експерти прогнозират, че те ще бъдат и източнник на едни от най-големите кибер заплахи през следващите години [32]. Заради своята конструктивна специфика IoT устройствата изискват усложнени, автоматизирани процедури за настройка, конфигуриране и актуализация. Това ги отнася също и към заплахите свързани с направленията „Компрометираност по дизайн“, „Уязвимости в преносими устройства“ и „Зловреден софтуер“. Единичната грешка може да се умножи в пъти, чрез използването на автоматизирани инструменти за управление на IoT и да се генерират милиони нови уязвимости за кибер атака. Интелигетната мрежа, свързваща обектите, която може да бъде и хетерогенна, играе съществена роля по отношение на тяхната кибер сигурност и т. 3.3.

Ето защо през 2019, ползвателите на IoT решения е необходимо да вземат и допълнителни превантивни мерки за повишаване на мрежовата сигурност, чрез провеждане на периодични одити и обучения. Това ще позволи те да бъдат добре информирани по отношение на необходимите програмни настройки, кръпки и актуализации на системно и оперативно равнище, което ще гарантира високото им нивото на сигурност в новото, постоянно прогресиращо дигиталното общество на бъдещето.

3.10. ОСТАРЯЛ ХАРДУЕР

Не всички заплахи за кибер-сигурността са причинени от софтуерни уязвимости. Темпото с което се пускат нови софтуерни актуализации и кръпки, може да затрудни значително и използваните хардуерни платформи [33]. Това от своя страна създава условия за излагане на риск на данните на компаниите. Заради неизбежното остаряване на хардуера и невъзможността понякога за замяна с актуален, за много от устройствата няма възможност за реализиране на актуализации с последните софтуерни версии и кръпки по изцяло конструктивни несъвместимости. Устройства, които разчитат на по-стар софтуер, са по-податливи на кибератаки, създавайки потенциални уязвимости в направленията „Компрометираност по дизайн“ и „Изтичания на данни“. Затова е важно в политиката за кибер-сигурност на компаниите през 2019, този факт да бъде съобразен и да се вземат всички възможни мерки за намаляването и контролирането на този риск.

ДИСКУСИЯ

От изброените 10 направления за изследване на киберпространството и заплахите асоциирани с тях става ясно, че през 2019 година се очаква да се запазят тенденциите за зловредно въздействие както върху иновативните технологични решения, така и по отношение на данните и информацията, пряко или опосредствано. От друга страна трябва да отбележим, че сложни APT заплахи като: корпоративен шпионаж, социален инженеринг и използване на инсайдери се очаква да запазят своята значимост. Съществен момент при това е и ролята на социалните мрежи в съчетание с дезинформацията, реализирана посредством машинно генерирани или асистирани фалшиви новини за медийни кампании, информационни войни и хибридни въздействия с различни цели. Друга среда за реализация на вече отбелязаните заплахи ще бъдат и множеството геймърски платформи, иновативни мобилни смарт решения и комуникационни протоколи ориентирани към IoT и клауд решенията в съчетание с очакваните 5G услуги, които предвид силно иновативния си характер и растяща популярност, предоставят значима област за реализиране на сложни кибер атаки в дигиталното общество на бъдещето.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

[1] “ISTR Internet Security Threat Report,” Symantec, Vol. 24, Feb, 2019.

[2] “Insider Threat Report,” Out of sight should never be out of mind, Verizon, 2019

[3] “2019 Data Breach,” Investigations Report, Verizon, 2019.

[4] “Defending against today’s critical threats,” a 2019 Threat Report, Cisco, Feb, 2019.

[5] “SophosLabs 2019 Threat Report,” Sophos, 2019.

[6] Secure Digital Future 21 Web Page, http://securedfuture21.org, Laccessed 2019/05/13.

[7] SysSec Red Book Web Page, http://www.red-book.eu/, accessed 2019/05/13.

[8] “Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета, на Европейския Съюз” EUR Lex, 27 април 2016, https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32016R0679, accessed 2019/05/13.

[9] “GDPR Fines and Penalties,” Nathan Trust, 2018, https://www.nathantrust.com/gdpr-fines-penalties, accessed 2019/05/13.

[10] Ondrej Kubovič, “One Year Later: EternalBlue Exploit More Popular Now than During WannaCryptor Outbreak,” Welive Security - ESET, May 10, 2018, https://www.welivesecurity.com/2018/05/10/one-year-later-eternalblue-exploit-wannacryptor/, accessed 2019/05/13.

[11] Iain Thomson, “Sinister Secret Backdoor Found in Networking Gear Perfect for Government Espionage: The Chinese are – Oh no, wait, it's Cisco again,” The Register, May 2, 2019, https://www.theregister.co.uk/2019/05/02/cisco_vulnerabilities/, accessed 2019/05/13.

[12] P.S.Suryateja, “Threats and Vulnerabilities of Cloud Computing: A Review,” *International Journal of Computer Sciences and Engineering* 6, no. 3, March 30, 2018.

[13] Public Service Announcement FBI Web Page, https://www.ic3.gov/media/2018/180712.aspx, accessed 2019/05/13.

[14] Cisco Blog, https://blogs.cisco.com/financialservices/ransomware-lessons-for-the-financial-services-industry, accessed 2019/05/13.

[15] Steve Martino, “Anticipating the Unknowns: 2019 Cisco CISO Benchmark Study,” Cisco Benchmark Report, February 28, 2019, https://blogs.cisco.com/security/anticipating-the-unknowns-2019-cisco-ciso-benchmark-study, accessed 2019/05/13.

[16] “ISO/IEC 27000 Family - Information Security Management Systems,” International Organization for Standardization (ISO), https://www.iso.org/isoiec-27001-information-security.html, accessed 2019/05/13.

[17] ”Gramm-Leach-Bliley Act (GLBA) Resources,” Federal Trade Commission, Mar 15, 2019, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act, accessed 2019/05/13.

[18] Juliana De Groot, ”What is SOX Compliance? 2019 SOX Requirements & More,” Digital Guardian, April 26, 2019, https://digitalguardian.com/blog/what-sox-compliance, accessed 2019/05/13.

[19] Juliana De Groot, ”What is HIPAA Compliance? 2019 HIPAA Requirements,” Digital Guardian, April 26, 2019, https://digitalguardian.com/blog/what-hipaa-compliance, accessed 2019/05/13.

[20] PCI Security Standards, https://www.pcisecuritystandards.org/pci_security/, accessed 2019/05/13.

[21] “2018 Payment Security Report,” Verizon, September, 2018, https://enterprise.verizon.com/resources/reports/2018/2018_payment_security_report_en_xg.pdf, accessed 2019/05/13.

[22] Maggie Tillman, “Facebook F8 2019 Event Recap: All the Announcements that Matter,” Pocket-lint, April 30, 2019, https://www.pocket-lint.com/apps/news/facebook/137297-facebook-f8-all-the-announcements-that-matter, accessed 2019/05/13.

[23] “BYOD & Mobile Security: 2016 Spotlight Report,” Information Security, 2016, https://crowdresearchpartners.com/wp-content/uploads/2017/07/BYOD-and-Mobile-Security-Report-2016.pdf, accessed 2019/05/13.

[24] “Android Devices Ship with Pre-installed Malware,” Avast Threat Labs, May 24, 2018, https://blog.avast.com/android-devices-ship-with-pre-installed-malware, accessed 2019/05/13.

[25] “Cyber Attack Trends Analysis: Key Insights to Gear up for in 2019,” Security Report 01,Check Point Research, 2019, http://www.snt.hr/boxcontent/CheckPointSecurityReport2019_vol01.pdf, accessed 2019/05/13.

[26] *Smartphone Factory Resets: The Benefits vs. Limitations*, Blancco e-Book, May, 2018.

[27] “The Promise and Pitfalls of 5G: Will It Kill Cable?” Knowledge@Wharton, Apr 29, 2019, https://knowledge.wharton.upenn.edu/article/the-push-for-5g/, accessed 2019/05/13.

[28] “Game of Threats. How Cybercriminals Use Popular TV Shows to Spread Malware,” Kaspersky Lab, April 1, 2019, https://securelist.com/game-of-threats/90116/, accessed 2019/05/13.

[29] “IoT Standards and Protocols,” Postscapes, 2019, https://www.postscapes.com/internet-of-things-protocols/, accessed 2019/05/13.

[30] Varshita Muddana, “What is the Future of IoT or Internet of Things in next 5 years?” SoftScript, IoT, Latest News, Marketing Trends, Jan 18, 2019, https://www.softscripts.net/blog/2019/01/future-of-iot/, accessed 2019/05/13.

[31] Zlatogor Minchev, et al, *Future Digital Society Resilience in the Informational Age*, (Sofia: SoftTrade, 2019).

[32] “A Guide to IoT: Security Basics,” CSO, Summer 2018, https://images.idgesg.net/assets/2018/06/cso_ie_iot20security20basics20guide20002.pdf, accessed 2019/05/13.

[33] Swarup Bhunia and Mark Tehranipoor, *Hardware Security: A Hands-on Learning Approach*, 1 edition (San Francisco, US: Morgan Kaufmann; November 16, 2018).