CSDM Views 37

Кибер рискове, заплахи и мерки за защита, свързани с COVID-19

Златогор Минчев, Иван Гайдарски

април 2020 г.

Златогор Минчев, Иван Гайдарски, *Кибер рискове, заплахи и мерки за защита, свързани с COVID-19*

Резюме: В настоящия анализ е направен кратък преглед на десетте най-актуални рискове и заплахи от техно-социален тип, свързани с COVID-19 за 2020 година. Предложени са и практически мерки за защита. При това са използвани както литературни данни, така и експертен индустриален, и изследователски опит събран от инициативата “Secure Digital Future 21” и някои скорошни активности на европейската мрежа от центрове по кибер сигурност – ECHO. Представените обобщени данни от анализа, дават текущ приоритет на заплахи и рискове свързани с атаки върху ключови онлайн услуги и уязвимости при работна организация “Home Office”. Други значими към момента са: фишинг заплахите и малуеър атаките. Растеж в значимостта, но в по-малка степен, се очаква и по отношение на: крипто-вирусните атаки, уязвимостите в популярни приложения, robocall измамите, фалшивите приложения и новини, измами от сивия пазар и зловредни домейни. Предвид този факт, е добре въвеждането на мерките за защита да става при максимално автоматизиране, като се разчита на интелигентни системни решения за сигурност и защита с многократно осигуряване. Така от една страна ще се предотвратят загубите на данни, информация, технологични и икономически ресурси, а от друга – ще се улеснят ежедневните социални процеси, чрез интелигентна технологична подкрепа за ефективно трансформиране на обществото в новата дигитална реалност.

Ключови думи: техно-социални рискове и заплахи, мерки за защита, COVID-19, комплексни кризисни ситуации, дигитална трансформация

Zlatogor Minchev and Ivan Gaydarski, *Cyber risks, threats & security measures associated with COVID-19*

Abstract: This analysis provides a brief overview of the ten live techno-social risks and threats associated with COVID-19 for 2020. Practical security measures are also presented. Literature data, industrial experience and research expertise gathered from “Secure Digital Future 21” initiative with some recent activities of the European Network of Cyber Security Centers – ECHO are jointly accomplished. The presented generalized results are giving current priority to threats and risks associated with: attacks on key online services and vulnerabilities in Home Office work organization. Other important issues are: phishing threats and malware attacks. Increased importance, but less expected one is going to emerge from: crypto-virus attacks, vulnerabilities in popular applications, robocall scams, fake apps and news, gray-market scams and malicious domains. Taking in mind these analytical findings, the security measures implementation should be organized with maximum automation, relying on intelligent security systems with multilevel organization. This from one hand will prevent the loss of data, information, technological and economic resources and, from another – is expected to facilitate the everyday social activities through intelligent technological support for effective society transformation in the new digital reality.

Keywords: techno-social threats & risks, protection measures, COVID-19, complex crisis situations, digital transformation

Редактори: проф. Тодор Тагарев, доц. Велизар Шаламанов,
доц. Венелин Георгиев, посл. Валери Рачев

ISSN 1314-5622

1. ВЪВЕДЕНИЕ*

Навлизането на интелигентните технологични решения и клауд услуги в дигиталната ера в съчетание с тенденциите за ускорена глобална свързаност, създава редица предизвикателства пред сигурността в съвременната кибер-физическа реалност. В допълнение трябва да отбележим и появата на нови външни (очаквани и неочаквани) въздействия, като настоящата пандемия от *COVID-19*[1].

Тези фактори способстват за създаването на комплексни кризисни ситуации от качествено нов техно-социален тип, влияещи на развитието на технологиите, социалните процеси и ресурси, биотопа и адаптацията на човешкия фактор в новата трансформирана реалност.

В настоящия анализ (подобно на *Top 10 live threats to cyberspace in 2019*[2]) е направен кратък преглед на десетте най-актуални рискове и заплахи от този нов техно-социален тип, свързани с COVID-19 за 2020 година. Предложени са и практически мерки за защита. При това са използвани както литературни данни, така и експертен индустриален, и изследователски опит събран от инициативата *Secure Digital Future 21*[3] и някои скорошни активности на европейската мрежа от центрове по кибер сигурност – *ECHO*[4].

2. ОБОБЩЕНА КАРТИНА НА ЗНАЧИМОСТ

Основните резултати от настоящия анализ могат да бъдат обобщени графично около следните десет най-актуални рискове и заплахи от техно-социален тип: „Крипто-вирусни атаки“, „Фишинг заплахи“, „Кибер-атаки върху ключови онлайн услуги“, „Измами от сивия пазар”, „Зловредни домейни“, „Малуеър атаки“, „Фалшиви приложения“, „Уязвимости в популярни приложения“, „Уязвимости по работата в Home Office“, „Robocall измами“.

При това оценките за интензитета на въздействие са направени в четиристепенна интервална скала (*Нисък* – [0, 25], *Среден* – [30, 45], *Висок* – [50, 100], *Неопределен* – [0, 15]) с отчитане на „Настоящата значимост“ и „Бъдещата значимост“ (до края на 2020 година), за идентифицираните заплахи и рискове при включване на фактора „Неопределеност“. Ще отбележим, че така се осигурява постигане на по-голям реализъм в направените прогнози и се решава проблема с припокриване на стойностите в оценъчните интервали.

---

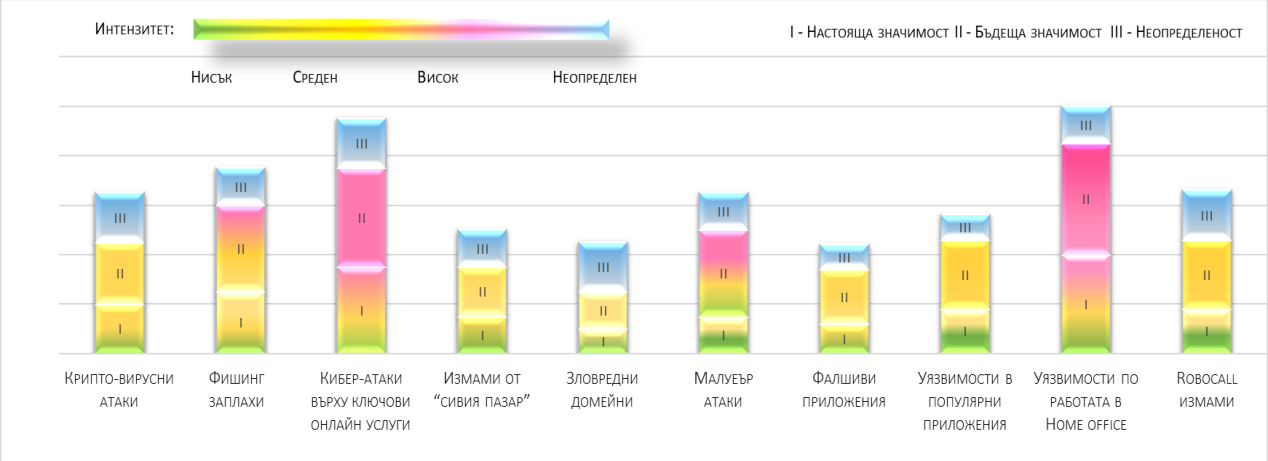
[1] “COVID-19 Pandemia,” [Online]. Available: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen [Accessed 26 April 2020].

[2] Z. Minchev, P. Kutinchev, & I. Gaydarski, “Top 10 live threats to cyberspace in 2019,” IT4Sec Reports, No. 133, Sofia, Institute of Information and Communication Technologies, 2019. [Online]. Available: http://dx.doi.org/10.11610/it4sec.0133 [Accessed 26 April 2020].

[3] “Securing Digital Future 21 Initiative,” 2017. [Online]. Available: http://securedfuture21.org [Accessed 26 April 2020].

[4] “The COVID-19 Hackers Mind-set,” ECHO WHITE PAPER #1. [Online]. Available: https://echonetwork.eu/wp-content/uploads/2020/04/20200408-ECHO-WhitePaper-Hackers-Mindset-FINAL.pdf [Accessed 26 April 2020].

* Предвид сложния и чуждоезиков произход на редица термини и понятия в доклада, които нямат точен аналог или буквален превод на български език, някои допълнителни пояснения са достъпни на адрес: https://bit.ly/3aMDsLu



Обобщена картина на настоящата и бъдеща значимост за 10-те най-актуални рискове и заплахи от техно-социален тип, свързани с COVID-19 през 2020 година

Представените обобщени данни от анализа, дават текущ приоритет на заплахи и рискове свързани с „Кибер-атаки върху ключови онлайн услуги“ и „Уязвимости по работата в Home Office“. Други значими към момента са: „Фишинг заплахи“ и „Малуеър атаките“. Растеж в значимостта, но в по-малка степен се очаква и по отношение на: „Крипто-вирусни атаки“, „Уязвимости в популярни приложения“, „Robocall измами“, „Фалшиви приложения“, „Измами от сивия пазар” и „Зловредни домейни“.

3. ОПИСАНИЕ НА РИСКОВЕТЕ И ЗАПЛАХИТЕ

В настоящата част от изследването ще бъде посочен и коментиран основния фокус и сфера на въздействие на идентифицираните рисковете и заплахи, отбелязани вече в т.2.

3.1. Крипто-вирусни атаки[5,6]

Фокус и сфера на въздействие: Обществени институции с критична важност (административни центрове за услуги, болници, банки и др.) са към момента актуалния обект за този тип атаки от страна на кибер престъпниците. Поради факта, че по време на пандемията те не могат да си позволят нефункциониращи информационни системи, вероятността да платят откупа е значителна.

3.2. Фишинг заплахи[5]

Фокус и сфера на въздействие: Винаги актуалните фишинг атаки се възползват от голямото внимание, което се обръща на всяка информация, свързана с COVID-19, за да примамят жертвите да отворят прикачени файлове или да активират линк, водещ до злонамерен сайт. Обикновено тези атаки могат да бъдат част от криптовирусните или дори елемент на по сложни атаки за социален инженеринг. Това не е единична атака или кампания, а повсеместно използване на темите свързани с пандемията.

---

[5] R. Olson, “Don’t Panic: COVID-19 Cyber Threats,” [Online]. Available: https://unit42.paloaltonetworks.com/covid19-cyber-threats/ [Accessed 26 April 2020].

[6] “COVID-19 cyberthreats,” [Online]. Available: https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats [Accessed 26 April 2020].

3.3. Кибер-атаки върху ключови онлайн услуги, свързани със здравеопазването и обекти от критичната инфраструктура[7]

Фокус и сфера на въздействие: Обектите, свързани със здравеопазването (болници, медицински и изследователски центрове, обществен институции), както и обектите от критичната инфраструктура (далекосъобщителни и електрически мрежи, ютилити (енергийни) компании, институции свързани с националната сигурност) са актуалната цел на кибер-атаките. Разчита се, че информационните системи и системите за ИТ сигурност са претоварени и това увеличава шанса за успешна атака.

3.4. Измами от „сивия пазар", обещаващи лекарства или защитни средства срещу COVID-19[8]

Фокус и сфера на въздействие: Поради трудности в закупуването и наличие на дефицит на надеждни лични предпазни средства, лекарства, дезинфекционни материали или други помощни устройства, непрекъснато се увеличават измамите от т. нар. „сиви търговци". Те предлагат всевъзможни стоки, свързани със заразата на нереални цени и със съмнително качество, които обикновено не могат да се върнат и формално отговарят на направената заявка, която често е предварително платена.

3.5. Зловредни домейни, прикрити зад термини, свързани с пандемията[5,6]

Фокус и сфера на въздействие: Актуалността на думи и изрази, свързани с пандемията от COVID-19 води до процъфтяването на регистрация на всевъзможни зловредни уеб-сайтове, свързани с думите: "corona", "coronavirus", "corona-virus", "covid19" и "covid-19", сайтове със зловреден код, измамни електронни магазини, сайтове обещаващи актуална информация и т.н. За последните няколко седмици са регистрирани над 100 000 такива домейна.

3.6. Малуеър атаки чрез зловреден код, скрит в интерактивни карти или уебсайтове, свързани с COVID-19[6]

Фокус и сфера на въздействие: Особено модерен подход е създаването на интерактивни географски карти, свързани с развитието на пандемията (най-често: броя заразени, починали, оздравели по региони), които всъщност са заредени със зловреден код и инфектират браузърите, а оттам и системите, на които се разглеждат.

3.7. Фалшиви приложения – новини и апликации, заредени с малуеър[5,9]

Фокус и сфера на въздействие: Огромна част от хората използват своите смартфони и таблети за да търсят актуална информация за COVID-19. При това се наблюдава лавинообразно увеличаване на броя на източници на фалшиви (подвеждащи) новини (най-често в социалните мрежи), както и злонамерени приложения за смартфони (най-вече за платформата Android, но не само). При това се претендира за предлагане на ранна или

---

[7] "COVID-19 Cyber Attacks," [Online]. Available: https://www.webarxsecurity.com/covid-19-cyber-attacks/ [Accessed 26 April 2020].

[8] N. Eddy, "Cyberattacks continue to mount during COVID-19 pandemic," [Online]. Available: https://www.healthcareitnews.com/news/cyberattacks-continue-mount-during-covid-19-pandemic [Accessed 26 April 2020].

[9] A. Hazelton, "How to read the news like a scientist and avoid the COVID-19 'infodemic'," [Online]. Available: https://www.weforum.org/agenda/2020/03/how-to-avoid-covid-19-fake-news-coronavirus/ [Accessed 26 April 2020].

скрита, но фалшива информация за пандемията. По отношение на апликациите, най-често се използват реплики на официалните решения, предоставени „усложливо“ за подпомагане на гражданите от правителствата или загрижени организации с неизвестен характер. Те позволяват на нападателите да манипулират, подвеждат и шпионират чрез техните устройства потребителите, като дори е възможно да ги криптират за откуп.

3.8. Уязвимости в популярни приложения по време на карантината, като Zoom и WebEx[7,10,11]

Фокус и сфера на въздействие: Широкото използване на популярни комуникационни приложения за видеоконферентна връзка, онлайн срещи и обучения, обуславя и експлоатирането на уязвимости в тях. Претоварването на сървърите, поддържащи тези приложения улесняват успеха на атаките, а драстичното нарастване на потребителите им увеличава и потенциалните жертви, чиито акаунти дори се продават в Dark Web, при тотално нарушаване на идеята за лично пространство в дигиталния свят.

3.9. Уязвимости в дистанционните услуги и BYOD, свързани с работата в режим Home Office[7,12]

Фокус и сфера на въздействие: Актуалния работен режим “Home Office” обуславя и по-широкото използване на дистанционни услуги и BYOD (Bring Your Own Device) устройства за достъп до служебна информация и ресурси. Този режим на работа води до изключителни затруднения на работата на екипите за ИТ сигурност и поддръжка на организациите и съответно – до увеличаването на пробивите и изтичанията на служебни и лични данни.

3.10. Robocall измамници и измами, прикриващи се зад техническа поддръжка[12]

Фокус и сфера на въздействие: Поради преминаването към гъвкави условия на работа от болшинството офис служители, все повече се разчита и на телефонни комуникации. От тази ситуация се възползват и кибер-престъпниците, опитвайки се да имитират официална бизнес комуникация, най-вече чрез Robocall, представляващ гласов фишинг или “vishing”. Това са автоматизирани телефонни обаждания, използващи предварително записани съобщения или синтез на говор, чрез които се примамва жертвата да сподели пароли, кодове или друга чувствителна информация. Особено са актуални и измамите с телефонни разговори с мнима техническа поддръжка на дадена услуги или организация.

4. МЕРКИ ЗА ЗАЩИТА

Осигуряването на защита от изброените рискове и заплахи от техно-социален тип, свързани с COVID-19 (вж. т. 2 и т. 3) е комплексна задача, която изисква динамично участие, както от страна на смарт технологии за кибер сигурност, така и от човешкия фактор (потребител и администратор). При това могат да се отбележат следните по-важни мерки за защита:

---

[10] L. Abrams, “Over 500,000 Zoom accounts sold on hacker forums, the dark web,” [Online]. Available: https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/ [Accessed 26 April 2020].

[11] I. Palli, “Cybercriminals Using Zoom, WebEx as Phishing Lures: Report,” [Online]. Available: https://www.bankinfosecurity.com/cybercriminals-using-zoom-webex-as-phishing-lures-report-a-14162 [Accessed 26 April 2020].

[12] A. Meyers, “Situational Awareness: Cyber Threats Heightened by COVID-19 and How to Protect Against Them,” [Online]. Available: https://www.crowdstrike.com/blog/covid-19-cyber-threats/ [Accessed 26 April 2020].

- Платформено или клауд ориентирани надеждни и актуализирани антивирусни и анти-малуер програми (вкл. и на мобилни устройства), добър анти-спам (системи срещу непоискани съобщения) и анти-фишинг филтър, системи за бекъп (системи за архивиране) в реално време, вкл. в клауд решение и на оптичен носител (при особена важност);

- Периодично обновяване на базовия и системния софтуер след предварително и надеждно архивиране на данните;

- Внедряване на Threat Intelligence системи, IDS (Intrusion Detection Systems), IPS (Intrusion Prevention Systems), DLP (Data Leak Prevention), Password Management, Firewalls, Business Continuity решения, Disaster Recovery системи и процедури;

- Въвеждане на политики за сигурност и правилна употреба на програмните продукти и услуги в мрежа, с използване на VPN (Virtual Private Network), особено при нужда от отдалечен достъп;

- Предварително обучение за security awareness, редовни инструктажи за кибер хигиена и спазване на добрите практики за потребителска безопасност, като: работа от акаунт с ограничени права (или такъв от виртуална работна конфигурация) за: отваряне на подозрителни и случайни писма. Тук са важни и следните прости правила: след предварителна проверка на адресата, да се проверява направлението на препратките в писмата, преди да се активират, да не се свалят прикачени файлове от непознати или подозрителни (по отношение на тяхната реална самоличност) податели, а когато това се налага да бъде извършено надеждно сканиране за зловреден код посредством антивирусен и антималуерен софтуер;

- Проверка на рейтинга, истинността и надеждността на приложения, технологии и новини, претендиращи че подпомагат вашата сигурност и информираност от утвърдени, официални новинарски сайтове, потребителски блогове, форуми и социални групи;

- Избягване предоставянето на информация, закупуването на стоки и решения със съмнителен произход, на нереално ниски цени и съмнителни източници без надлежна проверка за реалното качество, произход и себестойност от утвърдени до момента контакти и доставчици.

5. ДИСКУСИЯ

От направения кратък преглед и представените очаквания за динамиката на рисковете и заплахите, свързани с пандемията от COVID-19 става ясно че дигиталната реалност е също значително засегната от настоящата ситуация. Факт, който недвусмислено доказва, че дигиталната трансформация започва реално да променя едновременно, обществото, човешкия фактор и биотопа, предвид новата кибер-физическа вътрешна свързаност.

Установените тенденции, към момента демонстрират значими промени в обобщената картина на кибер рисковете и заплахите, които постоянно ще еволюират към техно-социален тип. Все пак е важно да се отбележи, че предвид високите нива на стрес за човешкия фактор (сериозно засегнат от пандемията), той става податлив на грешки и по-трудно се адаптира към новостите, защото начина и качеството на живот са променени.

Предвид този факт, е добре въвеждането на мерките за защита да става при максимално автоматизиране, като се разчита на интелигентни системни решения за сигурност и защита с многократно осигуряване.

Така от една страна ще се предотвратят загубите на данни, информация, технологични и икономически ресурси, а от друга – ще се улеснят ежедневните социални процеси (работа, обучение, пазаруване, информиране, общуване и др.), чрез интелигентна технологична подкрепа за ефективно трансформиране на обществото в новата дигитална реалност.