CSDM Views 38

Предизвикателства и рискове пред кибер сигурността в условията на пандемия от COVID-19

Станислав Атанасов

май 2020 г.

Станислав Атанасов, *Предизвикателства и рискове пред кибер сигурността в условията на пандемия от COVID-19*

Резюме: Пандемията от Ковид-19 предизвика криза в световен мащаб със здравни, социални, психологически, икономически и политически последици. Наложената социалната изолация доведе до изключително интензивна употреба на интернет и революционна дигитализация на човешкия живот, в неговия интерактивен, професионален, академичен и развлекателен аспект. Повишиха се и рисковете от кибер престъпления, което постави нови предизвикателства пред киберсигурността. Настоящият анализ разглежда типични рискове и вектори на кибератаки, в ситуация на нараснала дигитализация, както и основни мерки за справяне с тях. Обърнато е внимание на пропагандата и дезинформацията като вид кибер престъпления, критични за социалните системи.

Ключови думи: киберсигурност, кибер атака, Ковид-19, дезинформация, пропаганда, социална изолация, дистанционна работа

Stanislav Atanasov, *Cybersecurity Risks and Challenges in the Covid-19 Pandemic*

Abstract: The COVID-19 pandemic caused a worldwide crisis with health, social, psychological, economic and political consequences. The imposed social isolation has lea to an exceptionally intensive use of Internet and revolutionary digitalization of human life in its interactive professional, academic and entertainment aspects. The cybersecurity risks also increased, which made cyber risk reduction, protection and response more challenging. This analysis reviews the typical risks and vectors of cyberattacks in a situation of increased digitalisation, as well as main countermeasures. Special attention is paid to propaganda and disinformation as specific cybercrimes critical to the social systems.

Keywords: Cybersecurity, cyberattack, Covid-19, disinformation, propaganda, social isolation, distant work

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

ISSN 1314-5622

От началото на 2020г. човечеството е изправено пред сериозно предизвикателство в лицето на нов, застрашаващ живота вирус. Бързото разпространение на вируса в световен мащаб е само начален момент от развитието на глобална криза, засягаща здравето, социалната, психична, икономическа и политическа стабилност на обществата в цял свят. Необходимостта от социална дистанция и изолация доведе до изключителна по своя мащаб употреба на интернет и пренос на реалните физически операции в кибер среда. Нарасна ролята на дигитализацията за икономиката и образованието, а също така и за забавленията и социалните взаимодействия. Настоящата разработка проследява връзката между новата динамика в дигиталния живот и повишаването на риска от кибер престъпления, както и засилването на ролята на кибер сигурността в този контекст.

Covid-19 е напълно нов коронавирус, който не е срещан досега. Бързото му разпространение и малкото, което се знае за него създаде криза, каквато малко от живите хора по света са виждали. Магнитудът на промените няма да бъде сравним с нищо случило се от Втората световна война насам. Пандемията от Covid-19 доведе първо до здравна криза, която предизвиква след себе си икономическа и социална, което пък драстично увеличи вероятността за политическа криза. Тази вероятност за политическа криза е свързана с промените предизвикани от възникването на пандемията, довела до разширяване на локалните и дигитални измерения на живота за сметка на свиването на физическите и глобалните. Тази промяна ще създава и унищожава стойност. Като определящи ще бъдат създаването на психологическа и социална стойност, които стойности са пряко свързани и със създаването на икономическа и финансова стабилност, както и на национална стабилност и сигурност.

Механизмът, водещ до това са фактите и последиците свързани с новата пандемия, а именно, че тя доведе до блокиране на нормалното протичане на повечето социални и икономически дейности, като ги измести в сферата на кибер пространството - дистанционна работа от вкъщи, дистанционно образование, дистанционните социални контакти, социалният живот в кибер пространството на фона на една социална изолация.

Всичко това увеличи значението на кибер пространството, както и неговото използване, но също така увеличи и рисковете, свързани с него, както и значението на киберсигурността. Интернет винаги е привличал престъпници и престъпни групировки да се възползват от информационната и комуникационна инфраструктура, която той предоставя и която дава множество възможности за уязвимост както на бизнеса, така и на индивидуалния човек. [1] Не трябва да се забравя и че човешкият фактор много често се идентифицира като най-слабото звено във веригата на информационната сигурност и много често самото поведение на хората е това, което прави кибер престъпленията успешни.[2]

Основните кибер рискове и вектори на кибератака, според Боем и съавтори[3], свързани с интензивната онлайн дейност в резултат от пандемията и карантината са:

- Промяна в правата и правилата за достъп до информационните ресурси на компаниите.
- Масовото преминаване към договорености за работа от вкъщи усилва отдавна стоящите предизвикателства пред киберсигурността като: незащитено предаване на данни от хора, които не използват виртуални частни мрежи (VPN софтуер)

[1] Janine Kremling and Amanda M. Sharp Parker, *Cyber space, cyber security, and cyber crime*, SAGE Publications, Sep 5, 2017.

[2] John McAlaney, Lara A. Frumkin, Vladlena Benson, *Psychological and Behavioral Examinations in Cyber Securityp*, IGI Global, 2018.

[3] Jim Boehm, James Kaplan, and Nathan Sportsman, “Cybersecurity’s dual mission during the coronavirus crisis,” April 2020, https://www.mckinsey.com/business-functions/risk/our-insights/cybersecuritys-dual-mission-during-the-coronavirus-crisis.

слабо прилагане на правила за смекчаване на риска, така наречената „човешка защитна стена“ (human firewall), както и физически и психически стресогени, принуждаващи служителите да заобикалят контрола и процедурите за сигурност, за да свършат задачите си. Колкото повече служителите се затрудняват с достъпа до базата данни и фирмената система, толкова повече ще ползват рискови работни места. Екипите за киберсигурност ще трябва да осигурят системи за работа от дома и да тестват и мащабират VPN и други инструменти за реагиране на инциденти. В допълнение те могат да пожелаят да преразгледат политиките за управление на достъпа, така че служителите да могат да се свързват с критичната инфраструктура чрез лични устройства или отворени, насочени към интернет канали;

- Принудата да се премине от работа в офис към работа от вкъщи в рамките на броени дни завари много компании неподготвени да обезпечат ресурсно своите служители. Това наложи много от хората, които работят от вкъщи, да използват личните си компютри, таблети и смартфони, което доведе до повишаване на риска от заразяване със зловреден код. Тези персонални устройства не се обслужват централизирано и професионално, не винаги имат инсталиран лицензиран антивирусен софтуер с всички налични обновявания на базата данни с вируси, което ги прави уязвими на атаки.

- За да свършат своите задачи, много от служителите ползват инструменти, акаунти и устройства за широка употреба и това води до споделяне на сензитивни или критични за бизнеса данни през незащитени и неконтролирани канали;

- Отдалечената работа може да изисква от организациите да разширяват правата за достъп чрез активиране на достъп извън офисите и сградите на организацията до някои от най-критичните приложения, което увеличава киберриска.

- Някои потребители може да нямат силна многостепенна идентификация, защото обикновено техните права за достъп са ограничени. Промяната в правата за достъп, съчетана със слаба система за идентификация създава бъдещи заплахи;

- Възход на социално-инженерните тактики. В социално-инженерните гамбити атакуващите се опитват да получат информация, пари или достъп до защитени системи чрез проследяването на легитимни потребители.[4] Компаниите виждат все повече зловреден софтуер, свързан с и-мейл фишинг, вземащ самоличността на здравни, помощни и благотворителни организации. Повишават се случаите на измамници, представящи се за корпоративни екипи за помощ и поддръжка, които питат служителите за техните удостоверения за сигурност, използвайки текстови фишинг (“smishing”) и гласов фишинг (“vishing”). И-мейл измамниците се опитват да накарат ръководителите в организациите да преведат пари за доставчици, операции и свързани с вируса активности;

- Кибератаки, използващи уебсайтове със слаба защита за доставяне на зловреден софтуер. Със създаването на нови домейни и уебсайтове свързани с разпространението на коронавируса, информация за него и средства за борба с него, кибератакуващите използват слабите контроли за сигурност на много от тези уебсайтове за разпространение на зловреден софтуер чрез драйвери за изтегляне. Най-често се използва лесно наличен зловреден софтуер като AZORult вътре в сайтовете, показващи географски карти за разпространението на коронавируса или в приложенията за ранно предупреждение. Увеличава се и рискът от атаки за извличане на софтуер, блокиращ системата на потребителя, за чието отблокиране трябва да се плати („ransomware attack”);

[4] Shell&Wilmer, “Cybersecurity Risks Increasing During COVID-19 Pandemic,” April 2020, https://www.jdsupra.com/legalnews/cybersecurity-risks-increasing-during-38481/.

- Повишен риск за децата и непълнолетните ученици. Интернет пространството и използването на смарт технологии, особено при занижен родителски контрол, винаги са били предпоставка за кибер престъпления, свързани с експлоатирането или насилието над деца.[5] С прекъсването на нормалния учебен процес и налагането на дистанционната форма на обучение, се увеличава времето прекарано в киберпространството от страна на непълнолетните ученици, което води и до увеличаване на риска от посещение на неподходящи за тяхната възраст уебсайтове, както и от повишаване на риска от прояви на педофилия;

- Рискове на онлайн пазаруването и забавленията. Наложените карантини и престоят вкъщи увеличават времето на престой в киберпространството и от страна на пълнолетните потребители, което води до риск от появата и използването на сайтове за незаконни облози и залагания. Тези жизнени промени, както и страхът от заразяване, увеличават нивата на онлайн пазаруване, което от своя страна води до увеличаване на риска от интернет аукционни измами. Пример за това е, когато закупените стоки са фалшиви или откраднати или когато продавачът рекламира несъществуващи артикули за продажба, което означава, че стоките са платени, но никога не пристигат. Измамниците често използват услугите за превод на пари, тъй като чрез тях е по-лесно да получават пари, без да разкриват истинската си идентичност;

- Натиск от кибератаки и рискове свързани с киберсигурността за организациите от публичния сектор. Пример за това е голямата кибератака през март 2020 г. на болницата в Бърно, Чешка Република. Стейн и Джейкъбс[6] и Портър[7] описват как кибератаката принуди ръководството на болницата да изключи всички свои системи, да отложи всички операции и дейности и да насочи своите пациенти към отделения в други болници. Друг пример е уебсайтът на отдел на местната власт в САЩ, който е бил криптиран чрез атака на “ransomware”, лишила местната власт от възможността за публикуване на информация касаеща обществеността, както и е ограничила достъпа до определени файлове от страна на служителите. Агенцията за обществено здраве на САЩ пък пострада от атака за отказ на услуга („denial of service attack”), целяща да прекъсне услугите на агенцията и да предостави невярна информация (дезинформация) на населението на САЩ .

Именно този последен вид заплахи – дезинформацията и пропагандата и противодействието срещу тях са определящи за киберсигурността и националната сигурност в условията на пандемията с COVID-19, а и не само. Противодействието срещу този тип киберпрестъпления е определящо, защото пандемията от COVID-19, като частен пример за критична ситуация в значителни мащаби, прави най-несигурния фактор в киберсигурността (човешкият фактор, потребителите) все по-лабилен и податлив на дезинформация и пропаганда, поради допълнителния стрес от пандемията и изолацията, свързана с нея. Карантината доведе до все по-мащабна употреба на така или иначе все по-използваемото киберпространство от една страна и от друга страна на неговото въздействие върху информираността и оформянето на вземане на решения на фона на една социална изолация. Изглежда лесно за големите високоразвити технологични компании и среди да манипулират обществено и политически значимата информация

[5] United Nations Office on Drugs And Crime, “Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children,” Vienna, 2015.

[6] Shira Stein and Jennifer Jacobs, “Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak,” March 2020, https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack- during-covid-19-response.

[7] Sophie Porter, “Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak,” March, 2020, https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak.

(политически или икономически пи-ар, както правят Китай, САЩ и Русия в момента) за сметка на по-слабо развитите компании, страни и политически системи. Чрез публикуването на невярна здравна информация и средства за противодействие срещу коронавируса, се увеличава и рискът от публикуване на информация, която може да окаже негативно влияние върху общественото здраве, физическо и психическо благополучие на дадена страна или регион.

Всичко това превръща заплахите от тези два вида киберпрестъпления и средствата за противодействие срещу тях в критични за социалната и психологическа стойност, както и за свързаните с тях финансова и икономическа стойности и стабилност и национална стабилност и сигурност.

Дотук разгледахме основните предизвикателства в кибер сигурността в контекста на пандемията от COVID-19. Възниква въпросът как да се справим с всички тези предизвикателства. Огромният мащаб и непредсказуемата продължителност на пандемията COVID-19 са крайно необичайни, но въпреки всичко може да се използва опитът на специалисти в киберсигурността в минали кризи. Очевидно е, че няма книга с ясно написани правила за такива ситуации, поради естествената динамичност и непълна предсказуемост на киберпространството и на заплахите, свързани с него. Въпреки това могат да се използват препоръките на водещи главни офицери и мениджъри по киберсигурност, участвали в проучването на Боем и съавтори (Boehm, Kaplan &Sportsmen, 2020). Тези препоръки могат да се обобщят в няколко основни категории:

- **Фокус.** Екипите, свързани с риска и технологиите, трябва да се съсредоточат върху поддържането само на тези функции, възможности и услуги, които са критични за оперативната дейност. Примери за области на фокус включват поддържане на операции за сигурност, смекчаване на рисковете от отдалечен достъп до чувствителни данни и среда за разработка на софтуер и прилагане на многофакторна автентификация, за да се даде възможност на служителите да работят от дома. Организациите трябва също така да припомнят на служителите за своите протоколи за безопасна работа от разстояние и процедурите за идентифициране и ескалация на заплахи. Служителите на първа линия (пряко работещи с клиенти и доставчици) ще играят особено важна роля за поддържането на организацията в безопасност, тъй като нормалните мерки за сигурност в офисите стават по-малко уместни.

- **Тест.** Ако организациите имат планове за управление на риска или технология за риск от всякакъв вид - като планове за реакция на инциденти, непрекъснатост на бизнеса, възстановяване при бедствия, наследство на таланти и наследяване на доставчици, те следва да се тестват незабавно. Ако организациите нямат адекватни планове, те трябва да се създадат с приоритет и след това да се тестват. Трябва да се определи дали подходът на организацията за отговор на риска е ефективен и ефикасен. Пълното елиминиране на рисковите събития е невъзможно, но може да се минимизира рискът, свързан с лоша реакция.

- **Мониторинг.** Организациите следва да помислят за събирането на всички налични ресурси в помощ на мониторинга, което дава възможност за реагиране на риска и възстановяване. Областите за засилен мониторинг могат да включват отдалечен мониторинг на инструментите за дистанционна комуникация, на мрежите за нови щамове от злонамерен софтуер, на служители и на крайните точки за улавяне на инциденти свързани с данни, преди те да доведат до операционен риск.

- **Баланс.** Екипите за киберсигурност вероятно ще получат наплив от спешни заявки за изключения от политиката за киберсигурност, които ще позволят на екипите на други места в организацията да свършат работа (например, да одобрят инсталирането на нови приложения и да позволят използването на USB

устройства). Въпреки, че мениджмънтът по сигурността може да отказва подобни искания с цел предотвратяване на ненужен риск, той също трябва да има предвид важността бизнесът да се поддържа непрекъсваем дори в трудни времена. За да подкрепя продължаването на операциите може да се наложи мениджмънтът по сигурността да допусне малко по-висок риск в краткосрочен план, като предостави откази или временно отпаднат някои контроли. Демонстрираното разбиране към приоритетите на другите ще насърчи колегите да предприемат интелигентни рискове. Въпреки това, мениджмънтът по сигурността не трябва да позволяват тези изключения да отслабят рисковата позиция на организацията за постоянно. Ако се предоставят освобождаване или облекчаване на контрола, трябва да се установят официални процедури и срокове за налагане на периодична преоценка или ограничаване на изключенията за определени групи потребители.

Настоящата разработка имаше за цел да проследи как интензивният кибер-живот възникнал в резултат на пандемията, засили и рисковете, свързани с киберсигурността. Бяха изброени основните рискове и бяха предложени базисни мерки за тяхното минимизиране. По-сериозно внимание беше обърнато на ролята на кибер сигурността при случаи на дезинформация или блокиране на дейността на правителствени и обществени органи, което накърнява интересите на цялото население. Мащабът на този тип киберпрестъпления води до извода, че е наложително да се приеме международна политика за противодействие на кибератаките и престъпленията тип дезинформация и пропаганда независимо от разбираемата трудност, произтичаща от наличието на национални и регионални интереси, защото глобалната сигурност и интереси са от по-голямо значение. Това ще има не само благотворно влияние върху работата на обществените системи, но и ще минимизира негативните социални и психологически ефекти.

ЛИТЕРАТУРА

Jim Boehm, James Kaplan, and Nathan Sportsman, “Cybersecurity’s dual mission during the coronavirus crisis,” April 2020, https://www.mckinsey.com/business-functions/risk/our-insights/cybersecuritys-dual-mission-during-the-coronavirus-crisis.

Janine Kremling and Amanda M. Sharp Parker, *Cyber space, cyber security, and cyber crime*, SAGE Publications, Sep 5, 2017.

John McAlaney, Lara A. Frumkin, Vladlena Benson, *Psychological and Behavioral Examinations in Cyber Securityp*, IGI Global, 2018.

Shell&Wilmer, “Cybersecurity Risks Increasing During COVID-19 Pandemic,” April 2020, https://www.jdsupra.com/legalnews/cybersecurity-risks-increasing-during-38481/.

Shira Stein and Jennifer Jacobs, “Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak,” March 2020, https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response.

Sophie Porter, “Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak,” March, 2020, https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak.