IT4Sec Reports 136
http://dx.doi.org/10.11610/it4sec.0136

МОДИФИЦИРАНЕ НА КИБЕР ЗАПЛАХИТЕ ПО ВРЕМЕ НА ПАНДЕМИЯ ОТ COVID-19. КИБЕР ПАНДЕМИЯ

Габриела Бошнакова

Institute of Information and Communication Technologies
CSDM | Centre for Security and Defence Management
www.IT4Sec.org

Sofia, March 2020

Габриела Бошнакова, Модифициране на кибер заплахите по време на пандемия от COVID-19. Кибер пандемия**,** *IT4Sec Reports* 136 (March 2020), http://dx.doi.org/10.11610/it4sec.0136

IT4Sec Reports 136 „Модифициране на кибер заплахите по време на пандемия от COVID-19. Кибер пандемия“ Микроскопичен патоген, невидим, зловреден враг, който се разпространява бързо, неусетно и разрушително с различна форма, вид и предназначение, с различна цел – да навреди, наруши, повреди. SARS-CoV-2 или Малуер борба на хора и технологии срещу биологичната и технологичната зараза. В доклада се разглеждат предизвикателствата пред киберсигурността по време на пандемия, извънредно положение, социална изолация, страх и много въпросителни. Новият свят носи със себе си непознати предизвикателства и заплахи, преодоляването на които изисква повишена обща и техническа култура, компетентност, лична и онлайн хигиена.

Ключови думи: Киберсигурност, киберзаплахи, киберпрестъпност, пандемия, ефективност

IT4SecReports 136 „Cyber threats modification during the COVID-19. Cyber pandemia“ A microscopic pathogen, an invisible malicious enemy that spreads rapidly, imperceptibly, and destructively with different shapes, types and uses, for different purposes – to harm, disrupt, damage. SARS-CoV-2 or malware, the biological or the technological infection will more strongly affect our societies? This report presents the challenges of cybersecurity during a pandemic, the spread of fear in the increasing demand for information. The new world brings unfamiliar challenges and provocations. Overcoming them requires increased general and technical competences, culture, personal and online hygiene.

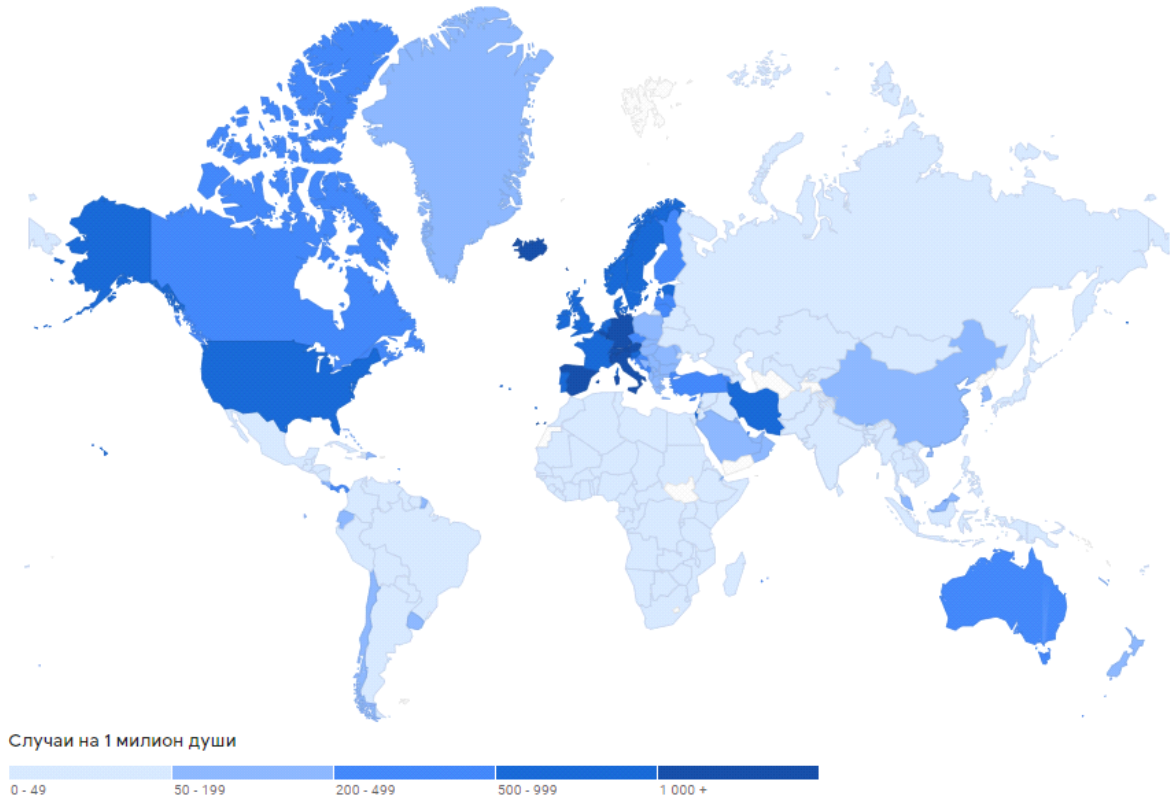
Keywords: Cybersecurity, cybercrime, cyber threats, pandemic, effectiveness

ISSN 1314-5614

ВЪВЕДЕНИЕ

Подемът на цифровата и информационната ера достига своя връх и постепенно го надгражда с все по-големи висини. Модерното общество уверено и интензивно насочва поглед върху новото безгранично, любопитно и предоставящо интересни предизвикателство „пето“ пространство, в което всички живеем и се адаптираме – кибер пространството. Интензивността и адаптивността се обръщат в друга насока, досегашният поглед, фокусиран върху научно-техническия прогрес трябва да се измести върху един от най-значимите морални аспекти за съществуване – човешкият живот и по-точно, здравето на хората.

Днес не е като вчера, а утре е неизвестно – пандемия, едно инфекциозно заболяване, което се разпространява по цялото земно кълбо, сякаш за миг, което заразява хората. COVID-19 или познат още като Коронавирус, невидимият враг срещу когото всички обединяват сили. Преди мащабното развитие на заразата, в хода на нейното разпространяване, в кулминацията и чак до пълното й отстраняване, хора и технологии се обединяват, за да се вземе надмощие и да се стигне до победа. (виж фиг.1).



Фиг. 1. Карта за разпространението на коронавирус COVID-19[1]

Новият свят носи със себе си уязвимости с непознат досега обхват и потенциална сила на въздействие, които изискват повишаване на общата култура и колективна сигурност на цялото общество. Дигиталната инфраструктура е свободна и достъпна за всеки. Тя е незаменим инструмент, който може както да бъде от полза, така и да навреди особено в момент на извънредна ситуация, когато масово обществото е обвзето от незнание, страх и

[1] На базата на статистически данни на Световната здравна организация към 03.04.2020 г. - 1 08 948 потвърдени случаи на заразени лица.

паника. Правителствата на много държави предприемат драстични превантивни мерки срещу разпространението на вируса, защото се осъзнава опасността, която той носи след себе си. Освен, че здравето на хората е в опасност, настъпва икономически дисбаланс, който най-вероятно ще доведе и до икономическа криза, рецесия, а защо не и депресия. COVID-19 променя ежедневният начин на живот, настъпват ограничения, които дори се доближават до границата с нарушаване на демократичните права. При тези условия най-правилното решение е хората и държавите да се обединят, за да бъде даден тласък на едно масово развитие и напредък, свързано с издигане на базовата информационна сигурност и кибер хигиена, способни да устоят на новите заплахи във всички области на социално-икономическия живот.

Във времена на повишена несигурност киберпрестъпниците имат по-голям шанс да използват общото объркване за да атакуват информационните системи. Бързото увеличаване на зависимостта от електронна комуникация значително нараства атакуващия потенциал за хакери, които търсят нови възможни вратички за проникване и въздействие.

Коронавирусът може би е първият биологичен вирус, който има отражение и влияние върху индустрията и сигурността в подобен мащаб. Пандемията и несигурността извеждат на преден план нови заплахи за киберсигурността, нови практики в киберпресъпленията, съответно и нови изисквания пред киберзащитата. Стресът предизвиква у много хора страх и дезориентираност, което довежда до по-голямата им уязвимост и техниките за манипулиране на хората и действията за неправомерен достъп стават по-успешни. Подобен тип атаки може би ще се увеличат през следващите месеци.

Въздействието на коронавируса променя моделите за работа и свободното движение. Препоръчителните стратегии включват предимно престой вкъщи, социална изолираност, работа от дома, дълъг период на карантина и големи ограничения в действията на хората, но в същото време онлайн пространството остава с неограничен достъп. Тези промени стават източник на нови заплахи за киберсигурността. Тъй като вирусът на практика „затваря“ физическия свят, киберпрестъпниците се възползват от възможността да използват интернет както за добре познати схеми за измами и изнудване на хора и компании, така и за атаки, който са особено удобни за тях в такъв момент.

РАБОТА И КИБЕРСИГУРНОСТ ПО ВРЕМЕ НА ПАНДЕМИЯ

Заплахите за киберпространството са също толкова разнообразни, колкото разнообразно е самото кибепространство. Поради тази причина е необходимо своевременно и актуално информиране на всички хора, работещи с Интернет за опасностите онлайн и как да се справяме с тях.

В неизмеримите мрежови системи организациите не могат да защитят поверителността, целостта и достъпността на данните без прилагане на ефективна и надеждна програма за обучение по сигурност. Security Awareness – Training, включва различни обучителни мерки за повишаване на чувствителността на служителите към въпроси, свързани със сигурността на информационните системи. Целта е да се сведат до приемливо ниво рисковете за информационната и кибер сигурност, причинени от служителя. Според доклад на лабораторията на Касперски над 46% от инцидентите в киберисгурността се дължат на човешка грешка и предприятията претърпяват огромни загуби, възстановявайки се от инциденти, предизвикани от персонала. Като пример, неинформирани служители могат да отговарят на фишинг имейли или да посетят уеб страници, заразени със зловреден софтуер или да съхраняват поверителна информация в несигурно място за запазване. Обучението за повишаване на сигурността може да включва много различни теми: базови знания за

сигурността на информацията и данните; безопасно боравене с имейли; опасност от зловреден софтуер; физическа сигурност на работното място; справяне с мобилно съхранение на лични данни; опасности от социалните мрежи; опасности чрез социално инженерство; фишинг атаки; сигурни пароли; сигурно използване не обществен достъп до Интернет и горещи точки; специфични указания за сигурността на фирмата; поведение при събития, свързани със сигурността; задължение за предоставяне на информация в случай на инцидент.

Операционни системи за компютри и лаптопи, медийни плейъри за възпроизвеждане на аудио и видео файлове, софтуер за мобилни телефони, дори програма за защита от вируси – всички те предлагат сигурна защита срещу компютърни вредители, ако са актуални. „Patch“ е вълшебната дума – пакети, с които производителите закриват пропуските в сигурността в своите програми или интегрират други подобрения. Пропуските в сигурността са софтуерни уязвимости, които позволяват на атакуващите например да инжектират злонамерена програма и да поемат контрол върху системата на трети страни. Вниманието следва да се насочи към използване на най-новите актуализации, които се предлагат от производителите на устройствата, които се ползват.

Информационни системи в сянка – в много компании служителите използват т.нар. сенчести ИТ системи, които се създават и администрират без официално одобрение или подкрепа от отдела за сигурност. Разширените операции като работа от вкъщи излагат на риск подобни системи, тъй като бизнес процесите, които зависят от информационните технологии в сянката в офиса ще се ограничат и дори разрушат след като служителите не могат да получат достъп до тези ресурси.

В условията на пандемия не малка част от служителите работят от вкъщи по т.нар. модел „Home Office“. Бързото преминаване към дистанционна работа създава заплахи, свързани с достъпа до мрежата. Очакват се широкомащабни внедрявания на дистанционна работа и отдалечена работна инфраструктура, без да се използва стабилна и защитена архитектурна сигурност. Създават се командни центрове в домашни условия с минимални защитни мерки. Това не застрашава само дейността и целта на фирмата, а и интегритета на информацията, с която тя работи и защитата на потребителските данни. В България случаите за подобен вид работа от вкъщи ще са многобройни, защото седмици след обявяването на извънредно положение, все още няма категорична информация за финансова помощ от държавата – нито за фирмите, нито за освободените от работа служители. Хората биват съкращавани от работа, а въпросът за финансовото им състояние остава неизяснен, при това без никой да може да предскаже продължителността на извънредното положение. Както показва практиката, човекът е най-слабото звено в системата за киберсигурност. На работотното място или вкъщи всички, които работят с Интернет поемат отговорност за информационна култура, защото всеки може да стане цел за атака. За да бъдат избегнати нежелани провали е необходима предварителна програма за обучение на служителите за подобни кризисни или извънредни ситуации. Също така спазване на процедурите по противодействие срещу киберзаплахите и добро управление на риска.

Използвайки инструмента, познат като „добри практики“, могат да бъдат отправени следните препоръки към работещите в режим Home Office[2]:

- корпоративното VPN решение трябва да поддържа и мащабира голям брой едновременни връзки;
- осигуряване на сигурна видеоконференция за корпоративни клиенти (аудио и видео възможност);

[2] От EU Agency for Cybersecurity, ENISA, 24.03.2020

- всички бизнес приложения трябва да са достъпни само чрез криптирани комуникационни канали (SSL VPN, IPSec VPN);
- достъпът до порталите за приложения трябва да бъде защитен чрез многофакторни механизми за идентификация и удостоверяване. Разширяването на този механизъм може да бъде предизвикателство, добавянето на тази защита изисква повишаване на скоростта в краткосрочен капацитет. В такъв случай може да се даде приоритет на потребителите, които имат повеишени привилегии (напр. администратори на домейни или разработчици на приложения) и работят с критични системи (напр. парични преводи);
- взаимното удостоверяване се предпочита при достъп до корпоративни системи (напр. клиент до сървър и сървър до клиент);
- корпоративните компютри на персонала трябва да имат актуален софтуер за сигурност - препоръчително е да има схема за подмяна на повредените устойства;
- BYOD (Bring your own device) трябва да бъдат проверени от гледна точна на сигурността (може да се използва NAC, NAP платформи);
- гарантиране на подходящи ИТ ресурси за подпомагане на персонала при нужда (пунктове за контакт);
- гарантиране на политики за реагиране при евентуален инцидент със сигурността или нарушение на личните данни и информиране на персонала за тези политики;
- всяка обработка на данните да е в съответствие с правната рамка на ЕС за защита на данните;
- Пачовете (Patches), които защитават отдалечената инфраструктура заслужават особено внимание.

В подкрепа на прилагането на горните добри практики може да бъде даден следния пример: 71% от ръководителите на бизнес решения, базирани в Обединеното кралство смятат, че преминаването към хоум офис на 100% по време на пандемията увеличава вероятността от нарушения в киберсигурността[3].

INTERNET OF THINGS ПО ВРЕМЕ НА ПАНДЕМИЯ

Вкъщи хората използват различни смарт уреди като умни високоговорители, телевизори, термостати, електрически крушки, прахосмукачки, перални, камери и др. Малко от тези устройства са създадени и инсталирани с достатъчно високо ниво на защита. Поставянето на корпоративните активи в същите мрежи създава нова входна точка на хакерите. Възможно е да се използват атаки, които осъществяват неправомерна връзка към видео чатове, конферентни разговори и други, които биха били неблагоприятни за организацията или атаки от вида DDoS. Не бива да се забравят и подценяват фишинг атаките и това, че домашната мрежа не забранява много от сайтовете, в които подобни атаки не се контролират.

Портфолиото от злонамерени софтуери, които се използват във връзка с пандемията включват фишинг, прикачени файлове със злонамерен софтуер, връзки към уебсайтове, които са заразени, компрометиране на бизнес имейли, фалшиви целеви страници и др. Свързан с Интернет на нещата е фактът, че някои правителства по света търсят варианти да използват обществени видеокамери за да откриват заразени лица, които игнорират карантината или за да оценят дали и доколко превантивните мерки за сигурност се спазват. Също така видеокамерите се ползват за да разпозават лица, които напускат жилищата си и с

[3] Проучване на Cyber security company Centrify a leading provider of identity-Centric Privileged Access Management solution.

тяхна помощ могат да се проследяват хора, които са влезли в контакт с лица, за които се подозира, че са заразени[4].

The Internet-of-Robotic-Things (IoRT) или нововъзникващата парадигма, която обединява автономни роботизирани системи с визията на Интернет на нещата (IoT) на свързани сензори и интелигентни обекти, вградени в ежедневната среда. Подобно сливане дава възможност за нови приложения в почти всички сектори, където може да се представи сътрудничество между роботи и IoT технология. Роботите изпълняват различни важни задачи, за да гарантират безопасността на човека.

В доклада „Пандемията на коронавирус се разпространява по целия свят“ президентът на Международната федерация на роботиката Милтън Гери, споделя че: „... представителите на индустрията за роботизация и автоматизация са най-подходящи да намерят решения, които подкрепят обществото и подпомагат неговото възстановяване. Фокусът на федерацията трябва да се насочи към усвояване на умения и знания, използването на това, което знаят най-добре, за да се справим с проблема и да станем по силни в свят без граници. Събират се идеи и добри практики за това, как тяхната технология да предостави полезни решения и роботиката да се използва за защита на местното производство и намаляване на зависимостта от световните вериги за доставки. Решенията за мобилна съвместна роботика облекчават недостига на ресурси, причинени от внезапни заболявания и карантинни мерки. Гъвкавите производствени технологии са успешни за управлението на стоки и ограничени доставки, докато мобилната роботика се използва за облекчаване на напрежението в болниците и логистичния сектор.“

Внедряваните подобни технологии в медицината прецизно, ясно и навременно подпомагат здравеопазването. Дезинфекция в болниците, разпространение на нужни клинични материали за пациентите, осведомяване с нужна информация без допълнителен човешки контакт и без риск за заразяване на технологиите с вируса, роботите играят важна роля, спасяват животи и са много полезни в борбата срещу COVID-19. „Ние сега помагаме за решаването на един от най-големите проблеми на нашето време, предотвратявайки разпространението на вируса и бактерии с робот, който спасява човешки животи“ казва Клаус Ризагер, изпълнителен директор на Blue Ocean Robotics.

Като примери за подобни решения могат да бъдат посочени:

Автономно движение. Датският робот от Blue Ocean се движи самостоятелно като има способността да обхване всички критични повърхности в стаите на пациентите и операционните зали с нужното количество ултра виолетова светлина, за да убие специфични вируси и бактерии. С колкото повече светлина се насища повърхността, толкова повече вредни микроорганизми се унищожават. В една типична болнична стая 99,99% от всички вируси и бактерии се убиват в рамките на 10 минути. По време на почистването помещението трябва да бъде празно. Маршрутът на робота може да бъде планиран от персонала с помощта на приложение. След пристигането си той предупреждава за почистване и приканва всички в стаята да напуснат и затворят вратата. Някои от тези роботи дори могат да работят с асансьори. Технологията работи и в среда на офис помещения, търговски центрове, училища, летища и производствени съоръжения.

Технологичната компания Robotise помага за облекчаване на сегашния недостиг на персонал в болници, лекарски кабинети и лечебни заведения. За тази цел компанията от Техническия университет в Мюнхен модифицира своя сервизен робот JEEVES, който след кратка фаза на инсталиране работи независимо в предварително определена среда. За целта той използва вътрешна карта, за да се ориентира например в конкретно отделение.

[4] Thomson Reuters Foundation news, Moscow deploys facial recognition technology for coronavirus quarantine, 21.02.2020.

Различните сензори му помагат да намери своя път наоколо, с който може да се ориентира в болничните коридори. JEEVES може да работи както самостоятелно, така и да следва лекари или медицински сестри и да подпомага с нужните материали и предмети като медикаменти, превръзки, маски и други.

В настоящата ситуация роботът може да улесни грижата за изолирани пациенти – да осигури напитки или храна. Докато медицинските лица се нуждаят от специално облекло, този робот не се нуждае от защитни мерки. По този начин рискът за клиничния персонал се свежда до минимум. JEEVES осигурява нужната подкрепа в трудните моменти, когато медицинският персонал достига своите граници – той може да работи денонощно, без да се уморява и да е склонен към допускане на грешки. Роботът има основа, която може да се индивидуализира и да бъде оборудвана с различни модули за съответното приложение. Като стандарт има три до четири чекмеджета, приема команди през специално програмно приложение или компютърен софтуер и разполага с 18,5 инчов дисплей, чрез който комуникира.

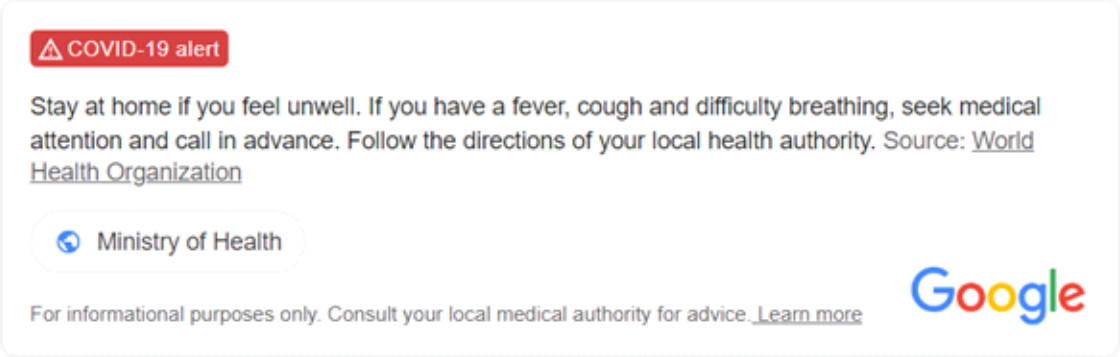
Телеприсъствие. В много страни една от превантивните мерки за ограничаване на разпространението на COVID-19 е насочена към намаляване на посещенията на членове от семейството, които не живеят под един покрив. По-възрастното население е помолено да си остане вкъщи и да няма лични контакти с членове на семейстовото и други лица за определен период от време. В този случай могат да се използват роботи за телеприсъствие за поддържане на конткат. Роботът, който е с изолирания човек предава изображение от местоположението си и на отдалечения потребител се показва екран с директна връзка. Роботът може да бъде направляван в стаята, за да предаде всичко около него. Може да бъде контролиран отвсякъде със смартфон или компютър с интернет връзка. Членове на семейството, приятели, лекари и медицински персонал могат да използват робота за телеприсъствие, до го контролират и да изследват средата с аудио и видео сигнал. Доставка на храна и медикаменти, приготвяне на храна, разпространяване на информация (на летища, места за хранене, магазини) до производство на медицинско оборудване и помощни средства правят битката срещу вируса с помощта на роботите да изглежда малко по-лека задача. „Роботите имат голям потенциал да ни подкрепят в настоящата тежка пандемия на короната“ заявява д-р Сюзън Билер, генерален секретар на Международната федерация по роботика.

Експертна система за онлайн тест за COVID-19. Представлява един от класовете системи с изкуствен интелект, които могат да получават, натрупват и коригират знания в определена предметна област. Не малък брой държави предоставят възможност на своите граждани да направят анонимен онлайн тест, чрез който може да се разбере дали човек попада в рисковата група за COVID-19 и съответно какви мерки трябва да предприеме, да свалят приложения, които показват актуалния брой инфектирани или болни, които са се идентифицирали като такива и се намират в близост до нас и др.

Центрове за контрол и профилактика на заболяванията, например Centers for Disease Control and Prevention (CDC) предоставят тази възможност[5] за самопроверка. Съществува и онлайн тест на български език, който съдържа 10 основни въпроса и отнема около 5 минути за отговор. https://covid.bg/

Друг пример, CovApp представлява софтуер, разработен от Charite в сътрудничество с Data4Life с помощта на който потребителите могат получат препоръки за действия само за няколко минути, да достигнат до правилните контакти по телефона, да предложи различни варианти за здравни грижи и ако е необходимо да покаже на потребителя най-прекия път към болницата (виж фиг. 2).

[5] Centers for Disease Control and Prevention (CDC).



Фиг. 2. Приложение COVID-19 alert

ЗДРАВЕОПАЗВАНЕ И КИБЕРСИГУРНОСТ ПО ВРЕМЕ НА ПАНДЕМИЯ

Съвременното ежедневие и начин на живот налагат преоценка на здравето като ценност за индивида и обществото, приоритетно развитие на първичното здравно обслужване, повишаване на удовлетвореността на пациентите и грижа за всеки човек.

Здравната индустрия в последните години се бори да осигури на всеки човек качествено и навременно лечение. Основно предизвикателство пред развитите страни е засилване участието и ролята на индивида в грижите по осигуряване на собственото си здраве, чрез повишаване на здравната грамотност, здравната отговорност и обществена солидарност – както всички сме свидетели, наистина факти, по който всички трябва да работим. Технологиите от години са част от медицината, поради тази причина съществуват познати атаки в здравеопазването, които за съжаление не са малко на брой.

При кражба на медицинска самоличност например, измамникът използва лични данни като име на жертвата, номера на здравни или социални осигуровки и други, за да получи "безплатни" медицински грижи, медикаменти или трудно достъпни рецепти. Тъй като здравната история на всеки пациент се пази в обща система, всяка фалшива информация в нея може да доведе до вземане на фатални решения, касаещи действителната личност. В тази връзка, атаките в условия на пандемията могат да бъдат изключително вредоносни. Пандемията отваря врати за фалшива медицинска информация свързана с медикаменти, тяхната продажба и действие.

На 13 март, на Университетската болница Бърно, която е един от най-големите центрове за борба с коронавируса в Чехия, се налага да спре операции след предполагаем ransomware инцидент. Зловредният софтуер забавя операции и тествания на десетки проби за коронавирус след като блокира цялостната система за работа в болницата. А в САЩ същата атака #Ransomware временно блокира актуализациите за Коронавируса на сайта на Urban Public Health[6].

ПРЕСТЪПНОСТ И КИБЕПРЕСТЪПНОСТ ПО ВРЕМЕ НА ПАНДЕМИЯ

За престъпност на Земята се говори от началото на човешкото съществуване. За киберпрестъпност обаче се говори от сравнително скоро. И двата термина продължават да са актуални по време на извънредното положение. Въпросът е колко време ще продължи

[6] Catalin Cimpanu, “Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak,” ZDNet, March 13, 2020, https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/

сегашната ситуация и какви мерки ще бъдат предприети за доброто на гражданите, защото ако е прекалено продължително и се сбъднат опасенията на хората, бедността и кризата, която ще настъпят в по-бедните държави определено биха повишили не само киберпрестъпността, но и битовата престъпност.

Относно киберсигурността и сигурността на работа и работното пространство, когато организацията се пренасочва от офис към домашен офис, не бива да се пренебрегва не само технологическата защита на мрежите и технологиите, а и физическата защита на обектите. Нормално е да възникне и въпросът кои са факторите, които правят специфична престъпността по време на пандемия (виж фиг. 3).

Фиг. 3. Фактори, които оказват влияние върху престъпността

Обръщайки поглед към престъпните действия в киберпространството специфични за условията на пандемия, като примери могат да бъдат посочени:

- *измама с доставки по време на пандемия и разпространение на фалшиви стоки, или стоки които не са по стандарт.* Като пример, разследване подкрепено от Европол се фокусира върху прехвърляне на 6,6 млн. евро от една компания на друга в Сингапур, с цел закупуване на алкохолни гелове, дезинфектанти и маски от типа FFP3/2. Платената стока така и не е получена от заявителя. Друг пример, компания опитва да закупи 3.85 млн. броя маски за сумата от 300 000 евро, но за съжаление доставката не се осъществява и фирмата губи цялата сума.

- *атаки със зловреден софтуер.* По-рано неизвестният зловреден софтуер, наречен Червена линия (Red Line)[7], се появява за първи път. Престъпниците се обръщат към желанието на хората да намерят лекарство за вируса. Друг вид атаки ползват имейлите, които са адресирани до „родители и настойници“ и съдържат зловреден софтуер – Malware Ursnif. В последствие този злонамерен софтуер краде информация като банкови данни. Фалшивите инструкции за защита на семейството и приятелите от вируса, в които потребителите са помолени да кликнат върху подготвена връзка, също се увеличават значително. Броят на имейлите, насочени към здравните организации предлагащи антидоти срещу коронавируса в замяна на биткойн или някакво друго заплащане също се увеличава. Престъпниците знаят, че хората търсят информация, която им осигурява сигурност. Затова са по-склонни да кликнат върху потенциално опасни връзки или да изтеглят прикачени файлове. Около 70% от имейлите, открити от Proofpoint, доставят злонамерен софтуер, а другите 30% имат за цел да откраднат данните за достъп на жертвата. Повечето от тези имейли се опитват да откраднат идентификационни данни с фалшиви целеви страници, които имитират Gmail или Office 365 и молят потребителите да въведат потребителско име или парола. Във връзка с решението на Народното събрание за обявяване на извънредно положение в страната и за ограничаване разпространението на коронавирус от МВР, ГДБОП уведомява, че сигналите за престъпления е препоръчително да се изпращат чрез формата за обратна връзка на адрес: https://gdbop.bg/bg/contacts

ДЕЗИНФОРМАЦИЯ ПО ВРЕМЕ НА ПАНДЕМИЯ. ИНФОДЕМИЯ

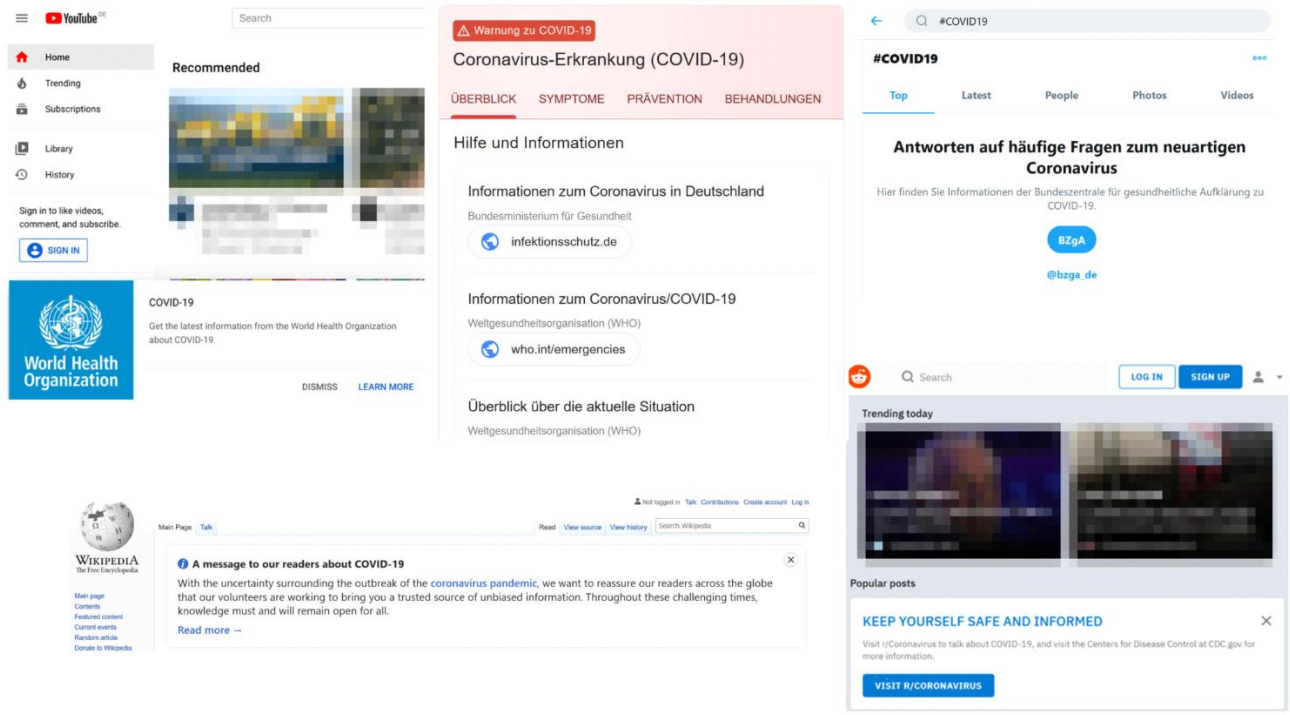
Дезинформацията представлява умишлено изкривена информация, разпространението на която преследва определена цел. В свои анализи Европейският съюз прави оценка, че се наблюдава изключителен бум в дезинформацията за коронавируса, с цел създаване на паника и всяване на страх у хората. Медийният и социален фокус около разпространението и развитието на коронавируса неминуемо предизвика създаване и разпространение на голямо количество заблуди и фалшиви новини. Дигиталните и интернет технологии позволяват много бързо информацията да достига до потребителите. Може да се каже, че дори широкото медийно отразяване подсилва паниката сред населението, още преди да се оцени реалната опасност от новата болест. Фалшивите новини се отличават със своята крайност и дори с конспиративен характер.

Инфодемията се разпространява със скоростта на пандемията, особено в социалните медии от декември 2019[8]. Това, което милиони хора четат, чуват и виждат за COVID-19 във Facebook, Twitter, YouTube, Instagram, новинарски сайтове и др, може да окаже влияние върху общественото здраве. Големите платформи имат известен опит в информирането на потребителите си с надеждна информация. Почти всички основни платформи са предприели мерки вследствие на пандемията:

- Филантропски мерки, главно под формата на дарения: Фейсбук например работи с ООН и Световната здравна организация. Добавя допълнително инсталиран панел в менюто на потребителя с „Информационен COVID-19 център“;
- YouTube вече показва връзка към Световната здравна организация на началната страница, която също сътрудничи с TickTok и Snapchat (фиг. 4).

[7] Peter Schmitz, „Cyberkriminelle nutzen Krise um Coronavirus aus,“ *SecurityInsider – web page,* March 19, 2020, https://www.security-insider.de/.
[8] Изследване на Wikipedia.

- Google имат ясно поставен информационен прозорец при търсене по темата. Не е ясно колко ефективни са мерките, но във всеки случай има смисъл да се даде възможност на потребителите поне да получат надеждни източници само с няколко кликвания.



Фиг. 4. Използване на платформи за споделяне на информация за коронавируса

Интерес представляват правените оценки, че доскоро представяните като особено значими киберзаплахи, на които трябваше да се противодейства категорично, днес се оказват едва ли не „детска игра“ в сравнение със заплахите от пандемията. Подобни оценки, особено когато са правени от хора на високо административно ниво, звучат не само некомпетентно, но и опасно предвид на възможността за загърбване на заплахите за информационните активи в усложнените условия на извънредното положение.

ЗАКЛЮЧЕНИЕ

Без съмнение, коронавирусът COVID-19 оказва огромно влияние върху киберсигурността по пътя на модифициране на съществуващите и появата на нови заплахи. Един от възможните начини да се намалят последствията за киберсигурността е да се ускорят вече съществуващи тенденции. „As a general matter, it would surprise me if the risk scenario is dramatically different from what we've seen before" казва Jamil Jaffer, който е старши президент в IronNet. Като се има предвид създалата се ситуация, организациите – особено тези които са принудени да се трансформират, бързо трябва да гарантират добро управление по време на криза и възможно най-стабилна киберсигурност.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

[1] Национална стратегия за киберсигурност „Киберустойчива България 2020,“ решение на МС от 18 юли 2016.

[2] ENISA, “Strategies for Incident Response and Cyber Crisis Cooperation,” August, 2020.

[3] Peter Schmitz, „Cyberkriminelle nutzen Krise um Coronavirus aus,“ *SecurityInsider – web page,* March 19, 2020, https://www.security-insider.de/.

[4] Brian Buntz, “Cybersecurity Crisis Management During the Coronavirus Pandemic,” *IoT World Today*, March 24, 2020, https://www.iotworldtoday.com/.

[5] Венелин Георгиев, *Противодействие срещу киберпрестъпността* (София, 2015)

[6] “Pandemic profiteering how criminals exploit the COVID-19 crisis,” *Europol* March 2020.

[7] МВР, ГДБОП – официална страница, [Accessed April 2020], https://www.gdbop.bg/.

[8] Карта на разпространение на коронавирус, *Google,* [Accessed April 2020], https://www.google.com/covid19-map/.

[9] Milton Guerry, “Coronavirus Pandemic is Spreading around the Globe,” *IFR*, April 02, 2020, https://ifr.org/ifr-press-releases/news/presidents-report-1-2020.

[10] Carsten Heer, “Robots help to fight coronavirus worldwide,” *IFR*, [Accessed April 2020], https://ifr.org/ifr-press-releases/news/robots-help-to-fight-corona-virus-sars-cov-2-%20worldwide.

[11] “Münchener Service-Roboter kann bei COVID-19-Pandemie unterstützen,“ *Robotis GmbH*, Aril 01, 2020, https://www.presseportal.de/pm/143245/4561663.

[12] “Praxisbeispiele: Roboter im Kampf gegen Covid-19,” IFR - International Federation of Robotics, *Konradin Mediengruppe* April 2, 2020, https://automationspraxis.industrie.de/news/ praxisbeispiele-roboter-im-kampf-gegen-covid-19/.

[13] Julian Jaursch, “Desinformation zu COVID-19: Wie die Platformen durchgreifen und welche Fragen das aufwirft,” *NetzPolitik.com*, March 24, 2020, https://netzpolitik.org/2020/wie-die-plattformen-durchgreifen-und-welche-fragen-das-aufwirft/.

[14] Stefan Luber, Peter Schmitz, “Was ist Security Awareness?” *Security Insider,* June 22, 18, https://www.security-insider.de/was-ist-security-awareness-a-727040/.

[15] Bundesamt für Sichereit in der Informationstechnik, “Update- und Patch- Management,” 2020.

[16] Jim Boehm, James Kaplan, Marc Sorel, Nathan Sportsman, and Trevor Steen “Cybersecurity tactics for coronavirus pandemic,” *McKinsey&Company*, March 2020, https://www.mckinsey.com/business-functions/risk/our-insights/cybersecurity-tactics-for-the-coronavirus-pandemic.