НОВ
БЪЛГАРСКИ
УНИВЕРСИТЕТ

Магистърски факултет
Департамент „Национална и международна сигурност“

Цветомир Емилов Алексов

Киберпространството като пети домейн. Държавно подкрепяни и самостоятелни хакерски групи. Начини и методи за противодействие срещу кибератаки от различен произход.

АВТОРЕФЕРАТ

на дисертационен труд
за присъждане на научна степен „доктор“
в програма „Стратегии и политики за сигурност“
в област на висшето образование 9. Сигурност и отбрана,
професионално направление 9.1. Национална сигурност

София
2021

Дисертационният труд се състои от 218 страници.
Основен текст – 209 страници.
Брой на литературните източници – 111.
Брой на публикациите по дисертацията – 5.

Дисертантът е експерт по киберсигурност в Министерството на отбраната, има сертификати от различни курсове, както и участия в международни семинари и конференции в областта на киберзащитата.

Изследванията по дисертационния труд са извършени в НБУ и самостоятелно.

I. Обща характеристика на дисертационния труд

1. Обем и структура на труда

Дисертацията е в обем 218 страници. В структурно отношение трудът се състои от три глави, включително увод, заключение, използвана литература и списък на ключовите думи. Направени са 95 бележки под линия. Списъкът на използваната литература включва 111 източника, от които 6 на български език, и 105 електронни издания основно на английски език.

2. Актуалност на изследването

Разглежданата тема е свързана с въпроси, които са актуални, поради непрестанното развитие на новите технологии и приспособяването им в ежедневието на хората, което довежда до тяхното повсеместно използване. Интернет, като пети домейн, поставя нови предизвикателства пред системата за национална сигурност. Необходимо е да се състави пълна картина на взаимовръзките между технологиите, тяхната роля в архитектурата на системата за сигурност и въздействието им върху отделните й елементи. Технологичните иновации създават както преимущества, така предпоставки за нови проблеми в сигурността. По своята

същност схващането за информационна сигурност е от стратегическа важност за интересите на отделния индивид, обществото и държавата като цяло. В този контекст се анализират стратегическата среда, видовете и източниците на заплахи, състоянието, задачите и методите за гарантиране на сигурността, основните насоки на държавната политика и на системата за гарантиране на информационната сигурност. Всички технологии създават предпоставка за манипулации и използването им за дейност, нанасяща непоправими щети, финансови загуби и загуба на човешки живот. Това от своя страна налага създаването и прилагането на нормативна база в киберпространството за изграждане на определен тип рамка на поведение в информационната среда. ***Настоящото изследване е изключително перспективен продукт със стратегическа насоченост.***

Обект и предмет на изследването

Обект на изследването е съвременната киберсреда със своите предимства и недостатъци, но най-вече в перспективната светлина на използването на интернет пространството за злонамерени цели. Този обект е изключително динамично развиващ се, но неговите

възможности ще позволят обезпечаване на ново ниво на сигурност и безопасност в интернет.

Предмет на тази работа е да даде по-различен поглед върху киберпространството и да се осъзнае важността му във времето, в което живеем. Същевременно да се посочат разликите между различните типове атаки и по какво да ги разпознаваме в ежедневието. Разглеждането на подходите на различните хакерски групи ще допринесе за изграждане на реална оценка относно възможностите и опасностите, произхождащи от интернет, както и необходимостта от изграждане на адекватни и своевременни мерки за киберпротиводействие.

3. Цели и основни задачи на изследването

Тезата на дисертационния труд е, че ***навлизането на технологиите и постоянната свързаност на милиарди устройства в интернет дава възможност на различни хакери и хакерски групи да извършват действия, част от които са и престъпления и да получат различни облаги в полза на себе си или трети лица в това число правителства на различни държави.***

С оглед гореизложеното, целта на изследване-

то е да се идентифицират основните дефиниции и аспекти в киберпространството. Също така да се открояят опасностите и вредите за обществото. В тази връзка да се ***да се създаде визия за изграждането на киберсигурност***. За постигането на тази крайна цел дисертантът си поставя следните задачи:

1.1. Изясняване на основните понятия в киберпространството;

1.2. Яснота около основните нормативни документи регулиращи информационната среда с цел мониторинг на информационното пространство;

1.3. Анализиране на основните видове кибератаки и способите за осъществяване на неоторизиран достъп;

1.4. Запознаване с основните хакерски групи реализиращи мащабни киберпроекти, които засягат милиони граждани и евентуалната им връзка с правителствени структури.

1.5. Изграждане на примерна конфигурация на система за сигурност на корпоративна компютърна мрежи и даване да препоръки за киберзащита.

4. Методология

Дисертационният труд изследва една особена област, която до момента не е била обект на големи комплексни и задълбочени проучвания в нашата страна. В световен мащаб има редица компании, които правят анализи, проучвания на различни киберинциденти. При анализиране на проблемите на сигурността в светлината на съвременните, екстензивно развиващи се технологии, фокусът е насочен към приложението и ролята на технологиите.

Сигурността е свойство на една информационна система да противостои на външни или вътрешни дестабилизиращи фактори, които могат да доведат до нейното нежелателно състояние или поведение.

За прецизна оценка и защита на функционалността на системите за сигурност е важно да се изготви детайлна класификация на видовете заплахи. Тя може да бъде направена по различни критерии. Заплахите могат да бъдат външни и вътрешни, външни са дейността на разузнавателни и специални служби, дейността на разни политически, икономически и други структури, насочени срещу интересите на организацията, и престъпни действия на отделни групи и лица. Вътрешни заплахи са нарушаване на правилата за съ-

биране, обработка и предаване на информацията и нанасяне на вреди на интересите на физически и юридически лица на базата на тази информация.

5. Приноси

С нарастване на броя, видовете и сложността на информационни системи в световен мащаб нарастват и различните възможности за нерегламентиран и неоторизиран достъп до информационните ресурси на една компания. Определянето на систематизиран подход за защита на информационните системи е от основно значение за минимизирането на риска за различните видове информация, което от своя страна повишава способността на компанията да използва тази информация за формирането на оптимална и хомогенна във времето печалба.

Анализът на хакерските групи и методите им на действие биха допринесли за изграждане на по-ефективна киберзащита, както и ясен знак на къде да се насочат специалистите в изграждането и разработването на нови продукти за киберпротиводействие.

От друга странаq разглеждането на основните типове кибератаки и киберинструменти ще допринесат за усъвършенстване на лична защита и т.нар. кибер-

хигиена, която е доста занижена към момента.

6. Практическо значение на изследването

С оглед практическото изследване може да се добие реална представа за изграждане на ефективна защита на голяма компания от киберзаплахи. Ще се даде пример и яснота за едни от най-често използваните продукти и от какво могат да ни пазят те.

Ограничения

Ограниченията на анализа са свързани в най-висока степен с необятността и огромното количество информация и високотехнологични хардуерни и софтуерни решения. По време на изработване на настоящия труд към обема от данни е добавена нова информация. Но темповете на развитие и разпространение са на практика невъзможни за достигане и разглеждане в адекватен срок. Поради това стремежът на автора е да обхване процесите в дълбочина и по принцип, като дава частни примери само за по-добро разбиране и илюстрация на тезите си.

II. Основно съдържание на дисертационния труд

Въведение

Въведението има за цел да постави рамката на дисертационния труд. В него са обосновани актуалността, предметът и обектът на изследването, целите и задачите на работата, приложената методология. От поставените в него рамки логически следват следните няколко глави:

1. Глава първа. Рискове за информационната сигурност в компютърните мрежи

Тук са разгледани по-общи и базови понятия като нормативна уредба, определения, видове заплахи, атаки и т.н. Основната цел е да се добие ясна представа за киберпространството и неговите възможности.

Кибератаката е целенасочено действие на нарушител, състоящо се в търсене и използване на слаби страни с цел сриване сигурността на информационната система.

В резултат на успешна атака може да се постигне:

- Изтичане на информация;

➢ Отказ от обслужване (блокировка);

➢ Външна злоупотреба с ресурсите на фирмата, кражба на услуги;

➢ Записване и използване на мрежовия трафик на фирмата от външни лица;

➢ Разрушение на информация;

➢ Измама с данни;

➢ Инсталиране на вредни програми;

➢ Индиректна (непряка) злоупотреба (използване на други системи за създаване на вредни програми);

➢ Разбиване на пароли;

➢ Влошено администриране.

Формите на организиране на атаките са много разнообразни, те могат да бъдат различни, но като цяло те се включват в една от следните категории:

➢ Отдалечено проникване в компютърна система или мрежа чрез програми, които получават неоторизиран достъп до друг компютър през интернет;

➢ Отдалечено блокиране на компютърна система или мрежа чрез програми, които през интернет блокират работата на отдалечен компютър или на отделна негова програма;

➢ Локално проникване в компютър чрез програми, които получават неоторизиран достъп до компютъра, на който работят;

➢ Локално блокиране на компютър чрез програми, които блокират работата на компютъра, на който работят;

➢ Чрез мрежови скенери - програми, които събират информация за мрежата за да определят кои от компютрите и програмите работещи на тях, са потенциално уязвими за атаки;

➢ Чрез скенери за слабите страни - програми, които проверяват големи групи от компютри в търсене на слаби места към конкретен вид атаки;

➢ Чрез мрежови анализатори (снифери) - програми, прослушващи мрежовия трафик и с възможност за автоматично отделяне на имена на потребители, пароли и номера на кредитни карти от трафика;

➢ Модификация на предаваните данни или подмяна на информацията;

➢ Подмяна на доверения обект с лъжлив обект.

Голямо е разнообразието на мрежовите атаки, които могат да бъдат разделени на две големи групи:

➢ Пасивно подслушване на мрежата - наблюдение на потока от пакетен трафик, без намеса в него;

➢ Активно подслушване на мрежата - включва някои видове обработка на пакетният трафик, като например селективно промяна, изтриване, забавяне, промяна на реда, дублиране, повторно изпращане, вмъкване на фалшиво съобщение, IP измами и др.

Законови норми и стандарти за информационна сигурност:

- ISO/IEC 27001:2005 Система за управление на информационната сигурност
- ISO 27002:2005 Практически кодекс за управление на информационната сигурност
- ISO 31000:2009 Управление на риска
- Закон за киберсигурност
- Закон за електронно управление
- Постановление № 186 от 19 юли 2019 г. за приемане на Наредба за минималните изисквания за мрежова и информационна сигурност.
- Регламент 881-2019 на ЕС
- Стратегия за киберсигурност 2020

2. Глава втора. Видове хакерски групи. Проведени кибератаки. Способи при провеждането им

Тук се акцентира върху хакерските групи и в частност тези, които са подпомагани от различни правителства. Националните икономики и обектите от критичната инфраструктура са жизнено важни и това ги прави примамливи за кибердействия срещу тях. Разгледани са типовете кибероперации за шпионаж, нанасяне на щети, кражба на различни активи, видовете инструменти на групите и по какъв начин са обвързани с управляващите органи в редица страни като Русия, Китай, Иран, С. Корея и др. Внимателно са разгледани някои от най-известните киберкампании през последните години и последиците от тях. Също така и как киберпространството се променя след осъществяването на някои мащабни кибероперации.

Едни от най-известните хакерски групи като:

APT28 е може би най-опасната група, причислена към властите в Русия. Според различни източници тази група компрометира кампанията на Хилари Клинтън през 2016 г. в опит да се намеси в президентските избори в САЩ. APT28 е активна поне от

2004 г. и е взела участие в много киберкампании.

APT37 е севернокорейска група за кибершпионаж, която е активна поне от 2012 г. Насочена към Южна Корея, Япония, Виетнам, Русия, Непал, Китай, Индия, Кувейт и други части на Близкия изток. Известно е, че севернокорейската група има значително припокриване, с името Lazarus Group което обхваща широк спектър от кибердейности. Някои организации използват името Lazarus Group за обозначаване на всяка дейност приписвана на Северна Корея.

APT38 силно финансово мотивирана от севернокорейския режим. Групата е насочена главно към банки и финансови институции и е осъществила атаки срещу повече от 16 организации в поне 13 страни.

Katty kitten иранско подкрепяна група за кибершпионаж, която е активна от 2014 г. Фокусирана върху насочването на лица, представляващи интерес за Иран, които работят в академични изследвания, като повечето атакувани потребители са разположени в Иран, САЩ, Израел и Великобритания. Хакерите обикновено се опитват да получат достъп до лични имейли и Facebook акаунти. Често

се стремят да установяват достъп до личните компютри на жертвите. Прикриват следите си с друга група Magic Hound, което води до объркване на разследващите органи и анализаторите.

Turla е руска група провела операции в над 45 държави, обхващаща редица индустрии, включително правителства, посолства, военни, образователни, научноизследователски и фармацевтични компании.

3. Глава трета. Вариант за сигурност на корпоративна компютърна мрежа

В тази глава се разглежда примерен вариант за изграждане архитектурата на съвременна корпоративна компютърна мрежа, която да съответства на най-добрите практики и стандарти в международен мащаб. Реализиране на нейната защита от преднамерени и непреднамерени действия, позволяващи манипулация на информационните ресурси, които биха могли да доведат до директни или индиректни загуби за компанията. В тази глава се проектира мрежова сигурност и се разглеждат важни въпроси касаещи киберзащитата.

Описание на корпоративна компютърна мрежа.

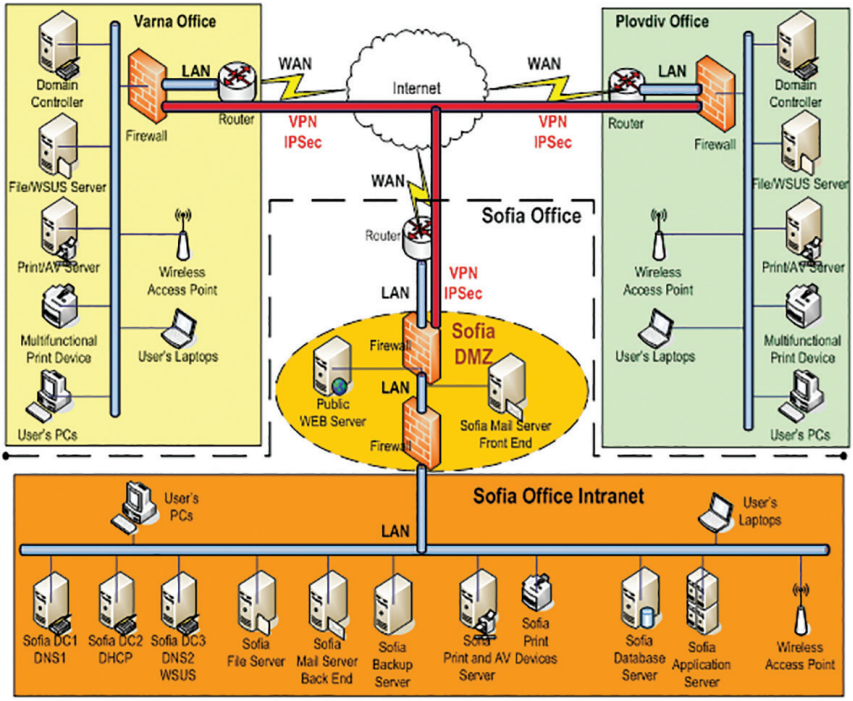

Схема 1. Корпоративна компютърна мрежа.

На схема 1 се вижда корпоративна компютърна мрежа изграждането и, свързаността на отделните офиси и използваните компоненти.

Предназначението на компютърна мрежа е за защитен обмен на информация между офисите, събиране на онлайн заявки от клиентите на фирмата вътрешна и външна комуникация (тук се включва комуникация между служителите на фирмата, както и между служителите и външни интернет потребители).

Заключение

Комуникационните мрежи и информационни системи станаха съществен фактор за икономическото и социално развитие. Използването на компютри за работа в мрежа вече става повсеместна комунална услуга, подобно на водопровода и електрозахранването. Ето защо сигурността на комуникационните мрежи и информационните системи, в частност тяхната наличност и работоспособност, става от все по-важно значение за обществото. Високо интелигентни хора си сътрудничат за създаването на нови вируси и други видове злонамерен код, споделянето на информация и големия брой талантливи хакери работещи заедно е винаги по-лошо от това да работят самостоятелно. За предпазване от тези намерения трябва защитните продукти винаги да вървят една крачка по-напред, но за съжаление обикновено е обратното. Коректността и лоялността на служителите също е много важна за опазването сигурността на една система.

Научни публикации по темата

1. Широката сигурност. Сборник с научни доклади от Международна научна конференция, 27 март 2020 г., Т. 1. Противодействие срещу престъпността и тероризма. Военна сигурност, София 2020 г. „Често срещани кибератаки и методи за осъществяването им“ ISBN 978-619-7383-19-5, стр.

2. Сборник с доклади от Международна научна конференция - втора част, Сигурност - образование, наука, индустрия - София, 2020 г. „Кибератаки през призмата на COVID-19“, ISBN 978-619-7478-58-7, 119-122 стр.

3. „Сигурността в условията на пандемична криза” - 15.01.2021 г., „APT групите и отпечатъка върху киберпространството през години до наши дни“ - под печат

4. Сборник с доклади от Международна научна конференция „Кризи и сигурност - корелации и предизвикателства - 14.05.2021 г., „Кибератаката срещу SolarWinds“ - под печат

5. Статията за списание „Език и публичност“: „Защо ни е необходима киберсигурност“ – под печат

6. Използвана литература за написване на автореферата

На кирилица

1. Семерджиев, Цветан. „Информационна сигурност“. 2004;
2. Каео Мерике. „Проектиране на мрежова сигурност“. 2006;
3. Цокев, А. „Етично хакерство“, 2017;
4. К. Калчев, „Организация и управление на КИС в операциите“, София, 2010
5. М. Михов, „Българската армия в информационното общество“.
6. А. С. Алпеев, „Терминология безопасности: кибербезопасность, информационная безопасность“, Вопросы кибербезопасности №5 (8), 2014 г.

На латиница

7. Cyber Operations: Building, Defending, and Attacking Modern Computer Networks – Mike O'Leary, 2019;
8. Cyber Security: Threats and Responses for Government and Business
Jack Caravelli, Nigel Jones, 2019;
9. The Innovators: How a Group of Hackers, Geniuses, and Geeks Created the Digital Revolution Walter Isaacson,

2015;
10. Open Source Intelligence Methods and Tools, A Practical Guide to Online Intelligence — Nihad A. Hassan, Rami Hijazi p. 22-30
11. CompTia Security + Get Certified Get Ahead SY0-401 Study Guide, Darril Gibson
12. Lallie, H., Shepherd, L., Nurse, J., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X. (2020) Cyber Security in the Age of COVID-19: ATimeline and Analysis of Cyber-Crime andCyber-Attacks during the Pandemic
13. J. Larry J. Hughes, Actually Useful Internet Security Techniques
14. D. E. Denning, „Information Warfare and Security", 2004 г.
15. Allied joint doctrine for information operations AJP-3.10, 2009 г.

Интернет източници

16. http://www.antivirus.trbk.net;
17. http://www.microsoft.com/;
18. http://cisco.com/;
19. http://www.symantec.com;
20. http://www.iso.org;

21. http://tuj.asenevtsi.com;

22. https://attack.mitre.org

23. https://cyberdefensemediagroup.com

24. https://thehackernews.com

25. https://medium.com

26. https://www.securityweek.com/

27. https://www.infosecurity-magazine.com/

28. https://www.kaspersky.com/blog/category/news/

29. https://threatpost.com/

30. https://www.enisa.europa.eu/

31. https://cyware.com/cyber-security-news-articles

32. https://www.govcert.bg/Pages/PageNotFoundError.aspx?requestUrl=https:

//www.govcert.bg/web/guest

33. https://www.bleepingcomputer.com/

34. https://www.hackread.com/

35. https://www.fireeye.com/company/newsroom.html

36. https://www.mcafee.com/enterprise/en-gb/about/newsroom.html

37. https://blog.360totalsecurity.com/en/

38. https://gbhackers.com/

39. https://www.sans.org/

40. https://hicomm.bg/

41. https://www.cyberark.com/newsroom/in-the-news/

42. http://securityaffairs.co/wordpress/

43. https://blog.malwarebytes.com/

44. https://www.malware-traffic-analysis.net/index.html

45. https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html

46.https://www.kaspersky.com/resource-center/definitions/vishing

47. https://ethicalhackersacademy.com/

48. https://owasp.org/www-community/attacks/Man-in-the-browser_attack

49. https://blog.malwarebytes.com/cybercrime/2013/03/hoaxes/

50. https://hackonology.com/

51. https://isc2central.blogspot.com/2019/12/difference-between-cyber-security-and.html?utm_source=dlvr.

it&utm_medium=facebook&m=1

52. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

53. https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/

54. https://itcsecure.com/covid-19-[4] related-cyber-attacks

55. https://www.dekra.com/en/cyber-attacks-due-to-covid-19

56. https://info.greathorn.com/report-2020-phishing-attack-landscape

57. https://www.securitymagazine.com/articles/92026-two-new-covid-19-related-phishing-scams

58. https://news.cision.com/f-secure/r/covid-19-spam--phishing-emails--plagued-users-in-first-half-of-2020,c3195746

59. https://www.cyfirma.com/covid-19-triggers-change-in-the-cyber-crime-world/ (Accessed 28 May 2020)

60. https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats

61. https://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf

62. http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/

100411CyberHearingRogers. pdf, accessed February 6, 2013.

63. https://www.washingtonpost.com/business/technology/chinese-hackers-suspected-in-attack-on-the-posts-computers/2013/02/01/d5a44fde-6cb1-11e2-bd36-c0fe61a205f6_story.html, accessed Feb. 1, 2013.

64. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

65. https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/

66. https://attack.mitre.org/groups/

67. https://blogvaronis2.wpengine.com/wp-content/uploads/2020/02/apt-groups-you-should-know-v3.png

68. https://postvai.com/cyber/tehnologichni-uiazvimosti.html

69. http://193.192.57.240/po/courses/problemni/mrezi/HTML/section5_theme2.html

70. http://pgds.org/books/km/19.htm

71. https://yurukov.net/blog/2012/linux-v-administraciqta/

72. https://slide-share.ru/sigurnost-i-zashchita-pri-rabota-v-lokalna-i-mrezhova-sreda-2-chast-doc-d-r-inzh-177330

73. https://drugi.dokumentite.com/download/zaplahi-i-ataki-kym-kompiutyrnite-sistemi-i-mreji/34615

74. http://www.edutechjournal.org/wp-content/uploads/2018/08/2_2018_377-382.pdf

75. https://www.netlaw.bg/bg/a/mezhdunarodna-konferentsiya-oblachnite-strukturi-i-zashchitata-na-informatsiyata-se-provezhda-v-shumen

76. https://lyuboblagoev.blog.bg/technology/2012/10/08/oblachnite-tehnologii-i-bylgarskoto-e-pravitelstvo.1007263?reply=3986302

77. D. C. Schleher, Electronic Warfare in the information Age

78. https://www.tuj.asenevtsi.com/Sec2009/Sec23.htm

79. http://www.dipku-sz.net/izdanie/240/izgrazhdane-na-info-struktura-za-upravlenie-na-znaniya-v-

organizaciyata

80. https://www.scribd.com/presentation/392315731/ZK-Mreji-pptx

81. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

82. https://www.idc.com/analysts

83. http://www.differencebetween.net/technology/difference-between-cyber-security-and-network-security/

84. https://www.geeksforgeeks.org/difference-between-network-security-and-cyber-security/

85. https://www.herzing.edu/blog/difference-between-cybersecurity-and-network-security

86. https://br.pinterest.com/pin/854206254304936579/

87. https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32016L1148

88. https://postvai.com/cyber/strategieski-komunikacii.html

89. http://www.washingtonpost.com/business/technology/chinese-hackers-suspected-in-attack-on-the-posts-computers/2013/02/01/d5a44fde-6cb1-11e2-bd36-c0fe61a205f6_story.html, accessed Feb. 1, 2013.

90. Mike Rogers, Statement to the U.S. House, Permanent Select Committee on Intelligence, Open Hearing: Cyber Threats and Ongoing Efforts to Protect the Nation, Hearing, October 4, 2011, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/100411CyberHearingRogers. pdf, accessed February 6, 2013.

91. https://www.fireeye.com/current-threats/apt-groups.html

92. https://blog.checkpoint.com/2020/03/19/covid-19-impact-as-retailers-close-their-doors-hackers-open-for-business/

93. https://www.hackmageddon.com/2020/01/23/2019-cyber-attacks-statistics/

94. https://www.hackmageddon.com/2020/03/03/january-2020-cyber-attacks-statistics/

95. https://help.eset.com/glossary/en-US/

96. https://medium.com/@heller_9/mitm-man-in-the-middle-attack-eavesdropping-at-its-best-685eb47acd32

97. https://doubleoctopus.com/security-wiki/threats-and-tools/man-in-the-browser-attack/

98. https://www.bleepingcomputer.com/news/security/

the-solarwinds-cyberattack-the-hack-the-victims-and-what-we-know/

99. https://twitter.com/RedDrip7/status/1339168187619790848

100. https://www.bleepingcomputer.com/news/security/the-solarwinds-cyberattack-the-hack-the-victims-and-what-we-know/

101. https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html

102. https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

103. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

104. https://www.channele2e.com/technology/security/solarwinds-orion-breach-hacking-incident-timeline-and-updated-details/3/

105. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-1

106. https://labs.sentinelone.com/solarwinds-sunburst-backdoor-inside-the-stealthy-apt-campaign/

107. Abi Tyas Tunggal, Upguard.com, Why is CyberSecurity Important in 2021, https://www.upguard.com/blog/cybersecurity-important#:~:text=Cybersecurity%20is%20important%20because%20it,governmental%20and%20industry%20information%20systems.

108. Annan Malla, DIGI Networking Solutions, Why do We need cyber security, https://diginetworks.co.in/why-do-we-need-cyber-security/.

109. Surfshark, DQL 2021 – Surfshark, https://surfshark.com/dql.

110. Visma.com, Why is cyber security important, https://www.visma.com/cyber-security/why-is-cyber-security-important/.

111. Sharon Shea, SearchSecurity What is Cybersecurity, https://searchsecurity.techtarget.com/definition/cybersecurity.