CSDM Views 31

Прогнозни заплахи и предизвикателства в киберпространството

Златогор Минчев

юли 2015 г.

Златогор Минчев, *Прогнозни заплахи и предизвикателства в киберпространството*

Резюме: Този доклад е разработен на основата на експертно проучване и данни от сходни изследвания за еволюцията на заплахите и предизвикателства в киберпространството в следващите пет години. Акцентът е върху технологичните и социални моменти от съвременните и бъдещи уеб решения и услуги за процесите на: комуникация, усъвършенстването на средата на живот и повишаване нейното качество в дигиталната ера. Прогнозните очаквания са за запазване ролята на човешкия фактор като генератор и потребител на технологичните новости и произтичащите от тях кибер заплахи в новата среда за сигурност. Очакваните заплахи в кибер пространството до 2020 година са свързани преди всичко с развитието на Уеб 3.0 технологиите и 4G/5G комуникациите, с акцент върху защитата и контрола на личното пространство и данни, облаковите услуги, мултимедийната комуникация в социалните мрежи, интернет на обектите, роботизираните системи с изкуствен интелект и ефекта от въвеждането на електронните пари. Докладът се представя в подкрепа на разработването и обсъждането на Национална стратегия за киберсигурност.

Ключови думи: Web 3.0, кибер заплахи, кибер пространство, киберсигурност

Zlatogor Minchev, *Future Threats and Challenges in Cyberspace*

Abstract: This report is based on an expert study and findings of related studies on the evolution of threats and challenges in cyberspace with a five-year outlook. The focus is technological and social aspect of current and future web solutions and services in the processes of communication and enhancing living environments in the digital age. We can forecast preservation of the role of the human factor as generator and user of technological innovation, with the consequent cyber threats in the new security environment. Anticipated threats in the 2020 horizon relate to the development of Web 3.0 technologies and 4G/5G communications, with emphasis on protection and control of personal space and data, cloud services, multimedia communication in social media, internet of things, robotic systems with artificial intelligence, and the effects of digital money. This report aims to support the development and the discussions of Bulgaria's national cybersecurity strategy.

Keywords: cyber threats, Cybersecurity, cyberspace, Web 3.0

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

ISSN 1314-5622

ВЪВЕДЕНИЕ

Съвременната дигитална среда е динамична, иновативна и крие множество явни и скрити заплахи с хибриден характер, породени от човеко-машинната интеракция в киберпространството. Това, от своя страна, е свързано с потребителските необходимости и икономически реалности в дигиталната ера, които постоянно прогресират.

Изследването на проблема е особено важно и когато говорим за изготвяне на адекватни политики, обобщени в единна стратегия за посрещане на новите кибер предизвикателства, и за изграждане на устойчиво общество в дигиталната ера[1].

Такава задача е и изготвянето на Национална стратегия по киберсигурност за България, която трябва да посрещне адекватно новите реалности до 2020 година.

Съществен момент в това изследване е използването на реални данни за вече осъществени кибер атаки от националния и регионалните Центрове за действия при инциденти в информационната сигурност, в съчетание с експертно прогнозиране на бъдещи атаки и очаквани нови кибер заплахи.

ЕКСПЕРТНО ИЗСЛЕДВАНЕ И АНАЛИЗ

С цел изследване на бъдещите заплахи и предизвикателства в киберпространството до 2020 бяха проведени консултации, дискусии и обсъждания с над 100 национални и международни представители и експерти от Балканите, Европа и НАТО по време на: NATO ATC 'Terrorist use of Cyber Space', м. декември 2014; NATO ARW 'Encouraging Cyber Defence Awareness in the Balkans', м. март 2015 и „Адекватността на НАТО в съвременната и бъдеща среда за сигурност: изводи за България", м. юни 2015. Използван бе и позитивния опит от Европейската мрежа по системна сигурност – SysSec за периода 2010 -2015 [2].

Обобщените резултати в таблична форма, с времеви хоризонт от пет години (до 2020 година) за осем области (по колони) и десет агрегирани заплахи (по редове) са показани на Фиг. 1.

Както става ясно от Фиг. 1, актуалните технологии днес и в близко бъдеще ще бъдат свързани с Уеб 3.0 решенията в процесите на комуникация чрез: уеб социалните мрежи, облаковото складиране, използване на данни и достъпа до изчислителни ресурси. От друга страна, средата на живот и вграждането на разпределените сензори (в т.ч. 4G/5G мобилни решения, вкл. и дрони), добавената смесена реалност (включваща смарт инфраструктура и безжични сензори), електронното управление, обучение, здравеопазване и икономика също са направления, представляващи интерес [3, 4, 5].

---

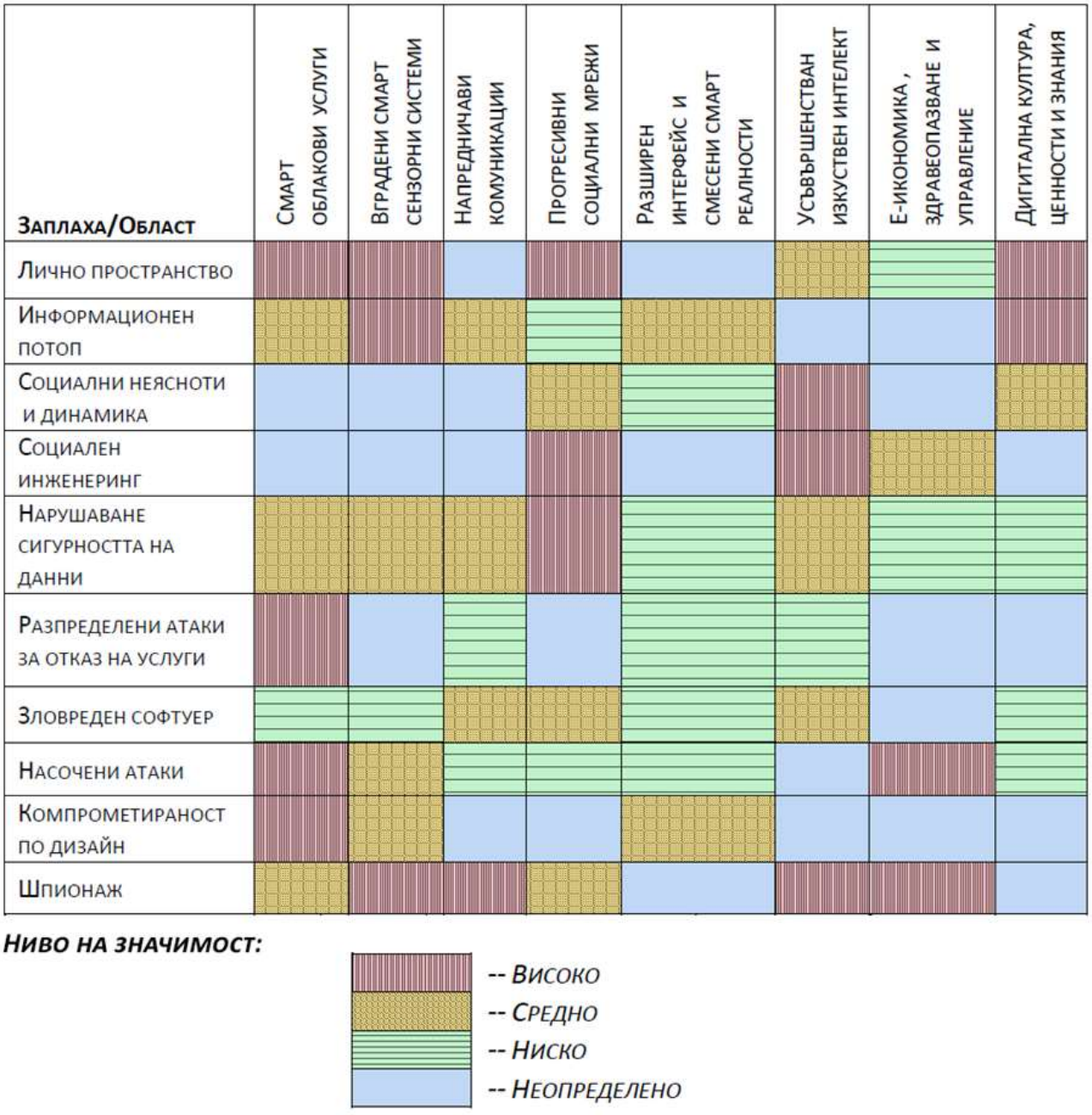
[1] Minchev, Z. Human Factor Role for Cyber Threats Resilience, In Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare, IGI Global, 2015

[2] SysSec Project Web Page, www.syssec-project.eu

[3] The Red Book. A Roadmap for Systems Security Research, SysSec Consortium, September, 2013, http://www.red-book.eu/ (link is external)

[4] Final Report on Threats on the Future Internet: A Research Outlook, SysSec Consortium, September 2014, http://www.syssec-project.eu/m/page-media/3/syssec-d4.4.pdf

[5] Cybersecurity in 2015: What to expect?, ZDNET, 2014, http://www.zdnet.com/article/cybersecurity-in-2015-what-to-expect/



Фиг.1. Експертно проучване за очакваните кибер заплахи по избрани области в дигиталното пространство до 2020 година.

Породените в тези области заплахи от технологиите за човешкия фактор са отнесени главно към: личното пространство, влиянието на голямата информационна и социална динамика и произтичащия от това потоп в информационното пространство. Те ще бъдат в пряка връзка с новоизграждащите се смарт инфраструктури (смесени реалности на градове, домове, производства и системи), посредством вградени и разпределени сензорни мрежи и предоставените чрез тях електронни услуги [6, 7, 8].

Практическото реализиране на тези заплахи се очаква да става по различни начини, като: разработка на зловреден софтуер, използване и дизайн на компрометираните технологии, разпределени и насочени кибер атаки, нарушаване сигурността (изтичане) на данни, социален инженеринг, шпионаж[9], [10].

Предвид общия прогнозен характер на получените резултати, тяхното практическо, по-задълбочено, изследване може да стане и експериментално, с участието на човешкия фактор [1], [11].

ДИСКУСИЯ

Представеният анализ дава някои приоритети за Уеб 3.0 технологиите и неопределеностите по отношение на техните очаквани развития и кибер заплахи. Тук ще отбележим и перспективите за следващите Уеб 4.0, които са също свързани с обичайните човешки дейности, като се очаква да се постави фокус върху: усъвършенстването и интеграцията на комуникациите, сензорните системи, изкуствения интелект и подобрения интелигентен интерфейс (вкл. и с използване на усъвършенствани аватари, с качества близки до тези на живите им първообрази), използвани в смесените (виртуални и добавени) смарт реалности за живот. Това генерира множество заплахи за човешкия фактор в технологичен и социален план.

Същевременно, проектирането на електронни услуги за подобряване качеството на живот, образование, здравеопазване, управление и използването на нови валути, като „електронните пари“ в е-икономиката, крият също множество неясноти за бъдещето на киберпространството. Акцентът тук ще бъде поставен върху комуникацията „машина-

---

6 Boyanov, L., & Minchev, Z. Cyber security Challenges in Smart Homes, In Proceedings of NATO ARW “Best Practices and Innovative Approaches to Develop Cyber Security and Resiliency Policy Framework”, Ohrid, Macedonia, June 10-12, 2013, Published by IOS Press, NATO Science for Peace and Security Series - D: Information and Communication Security, 38, 99-114, 2014

7 Boyanov, L. & Minchev, Z. Virtual Assisting Agents in Internet of Things, KSI Journal of Knowledge Society, no.1, pp.3-5, January, 2015

8 An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks , IOActive,2015, http://www.ioactive.com/pdfs/IOActive_HackingCitiesPaper_CesarCerrudo.pdf

9 Final Report on Cyberattacks, SysSec Consortium, September 2014, http://www.syssec-project.eu/m/page-media/3/syssec-d7.4-Cyberattacks.pdf

10 2015 Global Megatrends in Cybersecurity, Phonemon Institute, 2015, http://www.raytheon.com/news/rtnwcm/groups/gallery/documents/content/rtn_233811.pdf

11 Минчев, З. и к-в. Хибридни предизвикателства в киберпространството и ролята на човешкия фактор, сборник доклади от Международна научна конференция „Югоизточна Европа: новите заплахи за регионалната сигурност“, Нов български университет, юни, 2015, https://goo.gl/lXFeRz

машина“, автономността на роботизираните системи и предизвикателствата пред осигуряването и контрола в новата средата за сигурност. До 2020 се очаква човешкият фактор да остане генератор и потребител на технологичните новости и произтичащите от тях кибер заплахи.

БИБЛИОГРАФИЯ

2015 Global Megatrends in Cybersecurity, Phonemon Institute, 2015, http://www.raytheon.com/news/rtnwcm/groups/gallery/documents/content/rtn_233811.pdf

An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks , IOActive, 2015, http://www.ioactive.com/pdfs/IOActive_HackingCitiesPaper_CesarCerrudo.pdf

Boyanov, L. & Minchev, Z. Virtual Assisting Agents in Internet of Things, KSI Journal of Knowledge Society, no.1, pp.3-5, January, 2015

Boyanov, L., & Minchev, Z. Cyber security Challenges in Smart Homes, In Proceedings of NATO ARW “Best Practices and Innovative Approaches to Develop Cyber Security and Resiliency Policy Framework”, Ohrid, Macedonia, June 10-12, 2013, Published by IOS Press, NATO Science for Peace and Security Series - D: Information and Communication Security, 38, 99-114, 2014

Cybersecurity in 2015: What to expect?, ZDNET, 2014, http://www.zdnet.com/article/cybersecurity-in-2015-what-to-expect/

Final Report on Cyberattacks, SysSec Consortium, September 2014, http://www.syssec-project.eu/m/page-media/3/syssec-d7.4-Cyberattacks.pdf

Final Report on Threats on the Future Internet: A Research Outlook, SysSec Consortium, September 2014, http://www.syssec-project.eu/m/page-media/3/syssec-d4.4.pdf

Minchev, Z. Human Factor Role for Cyber Threats Resilience, In Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare, IGI Global, 2015

SysSec Project Web Page, www.syssec-project.eu

The Red Book. A Roadmap for Systems Security Research, SysSec Consortium, September, 2013, http://www.red-book.eu/ (link is external)

Минчев, З. и к-в. Хибридни предизвикателства в киберпространството и ролята на човешкия фактор, сборник доклади от Международна научна конференция „Югоизточна Европа: новите заплахи за регионалната сигурност“, Нов български университет, юни, 2015, https://goo.gl/lXFeRz