Confidentiality in cyberspace and how it is violated

A. A. Ganiev [1]
K. F. Kerimov [1]
Z. I. Azizova, email: z.i.azizova@mail.ru [1]

[1] Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Аннотация. *Cyberspace is a new platform for social activities. Necessity to develop and improve legal restrictions on access to users' private information is as urgent as development and improvement of methods, mechanisms and software tools to protect personal data in cyberspace. This article discusses ways to breach privacy in cyberspace, as well as the application of personal data de-identification as a data privacy method.*

Ключевые слова: *personal data, cyberspace, privacy breach, data compromise, global network, de-identification.*

Introduction

Nowadays, there are a number of international and national legislations that limit the collection and use of personal data in cyberspace, ensuring the privacy of personal data of users, based on the idea of "fair information practices" as a necessity to develop the concept of multidimensional privacy on the Internet. Along with the protection of personal data, the process of de-identification of personal data becomes a necessary condition for the process of digitalization of society [1].

De-identification is a good strategy to preserve the usefulness of personal data and to reduce the risks of its compromise afterwards. When a dataset has undergone a de-identification process and it is not possible to determine whether the individual data belongs to a specific data subject, the data protection law becomes null and void. In this case, creating a true anonymised dataset from a huge set of personal data, with only the required information retained, becomes a difficult task.

Fields of attack targeting the dissemination of confidential information in cyberspace

Information processing and sharing are becoming a major revenue stream for many organizations. Improvements in Internet capabilities, such as increased speed and reduced costs of use, have given the global network a role to play. Focusing on key principles (obligations limiting the use of personal data; open and transparent data processing systems; limited procedural and substantive rights; timely external controls) "fair information practices" [2] provides the basis for modern international legislation on personal data protection and privacy. Consequently, each new improvement in the performance of the technical infrastructure and the connection of each new user to the global network has a positive effect on those who are already active users in cyberspace. Because cyberspace can be organized in any way, it is possible to create highly effective conditions for the security of privacy in cyberspace. This is facilitated by the various technical components and software tools that are used for the lawful use of personal data in cyberspace.

The use of one technology or another, including the development of data protection software, is an important element in structuring different types of access to personal data. Modern solutions increase the likelihood of the spread of confidential information in cyberspace, rather than reducing the quantity and quality of published personal data.

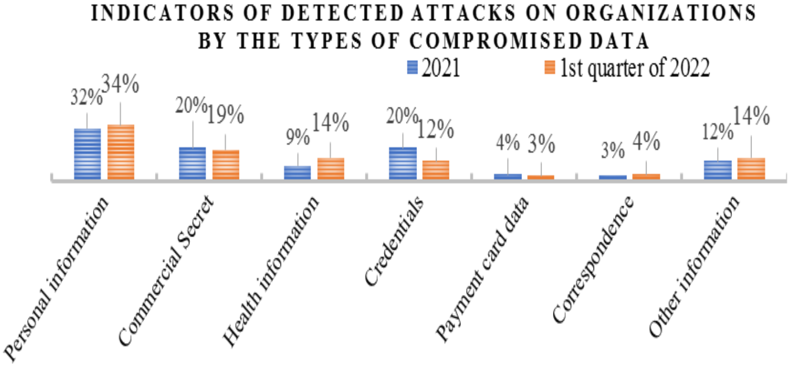

Рис. 1. Data theft rates in attacks on organisations

According to the Positive Technologies report "Topical Cyber Threats: Q1-2022" [3] in the first quarter of 2022, the number of detected attacks increased by 14.8% over the fourth quarter of 2021 to 714 detected attacks. At the same time, attacks against individuals accounted for 15% of the total number of detected attacks in Q1-2022. Thus, out of 107 detected attacks on individuals 49 attacks resulted in stealing user credentials, 22 attacks resulted in compromising payment card data, 20 attacks compromised personal data, 3 attacks resulted in providing correspondence data of individuals and 11 attacks resulted in compromising other information. Consequences of the attacks as compromise of confidential data made up 55%, direct financial losses - 25%, use of company or private person's resources for the attacks - 6%, damage to the state interests - 2%, violation of main activity - 1%, other information - 3% and 23% *- unknown from the total number of attacks detected. Attackers mostly targeted people (90%), followed by computers, servers and network equipment (32%), mobile devices (17%), web resources (2%) and other objects (1%). Attackers preferred social engineering methods, the use of malware, exploitation of vulnerabilities and compromising credentials to launch attacks on individuals.

It should be noted that cybercriminals predominantly targeted personal data belonging to employees of organizational structures. When comparing this indicator to the types of stolen data for 2021 [4], we can observe an upward trend of 2%. Fig. **Ошибка! Источник ссылки не найден.** illustrates this point.

Thus, we can conclude that the number of realized attacks on individuals is increasing, as well as the interest of attackers to sensitive user data, in particular personal data used by cybercriminals as a consequence of this, should be carried out to carefully select the tools and methods used to protect sensitive data.

The result of abusive information interactions in cyberspace arises from the creation, storage, transmission and processing of personal data in such areas as personal computers, Internet service providers and websites.

The compromise of personal data of personal computer owners can be accomplished in several ways. Primitive deletion of data from a personal computer carries some risk of recovering deleted information from a hard drive or other data storage location, except in cases of complete data destruction. Personal computers also allow confidentiality to be breached by storing information about users' online activities. Typically, web browsers contain software protocols that create files about websites visited. An outside user can access this data if he or she has physical access to this data, or if he or she accessed these files remotely by exploiting vulnerabilities in web browsers. In the process of information interaction in cyberspace, data is also written to the computer's cache files. And since cache files are stored on a computer's hard drive and in its RAM, it is not particularly difficult to gain remote access to these files. If you have access to a global network, personal computers can violate privacy through the use of cookies. When re-opening a particular website, the browser sends a copy of the cookie back to the website. On the one hand, cookies allow to identify the user. On the other hand, they can be seen as a source of detailed information about users' personal preferences on the global network, as they are used to provide information about users' accounts and for other administrative purposes. In terms of technical restrictions on reading cookies by the websites that set them - nothing prohibits the use of cookies to collect users' personal data.

Access to the global network requires the use of a service provider that provides Internet connectivity. Service providers may have access to confidential information about their customers' WAN activity. ISPs can aggregate this data together with information about the performance of the services provided. They have the ability to coordinate their customers' information. Internet service providers have detailed information (name, address, telephone number, residential address, credit card number, and so on) about each of their customers at the time that they create a customer account. In addition, they have detailed information about their online activity.

Websites can provide privacy risks and can be considered a third source of collection of personal information in cyberspace, as user data is collected, shared and commercialized through websites. Active user interaction on social networks has significant implications in terms of personal data protection. Users post personal messages in a database to which third parties also have access. There is no guarantee that messages, user data and email addresses are not archived without specific restrictions on further use.

There are quite a few sites on the Internet that collect and sell publicly available information about private persons. Organizations, individuals, media workers, and others can visit sites such as “DigDirt” or “WeSpy4U” and, for a fee, collect a dossier on almost anyone [5].

In each of the aforementioned areas a certain amount of detailed personal data emerges, and often cyberspace users falsely believe that they can control the process of personal information distribution - to limit this or that level of anonymity online, or to provide the data they publish with full disclosure of their identity and preferences. In reality, most users have no control over the complex processes of creating, integrating and publishing personal data, or no idea about the subsequent use of the data they publish online.

Conclusion

As a promising basis for the improvement of information technology, cyberspace forms new links for the interaction of society in any field of activity. The protection of personal data covers not only the definition of measures and means of personal data protection, but also the reduction of cost indicators allocated to data protection while complying with basic information protection requirements; training of personal data operators and compliance with the rights of subjects in the search, data collection and data processing of personal data in information systems. In this work, statistical indicators were analyzed in terms of the most relevant areas for data retrieval by attackers. Subsequent research activities will focus on algorithm development and software implementation of the personal data protection system, including re-identification plug-ins and evaluation of the effectiveness of the results.

References

1. Ganiev A.A.Ganiev, K.F.Kerimov and Z.I.Azizova, Understanding of Data De-identification: Issues of Relevance and Problems // 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-4, doi: 10.1109/ICISCT52966.2021.9670054. [Электронный ресурс] : база данных. – Режим доступа: https://ieeexplore.ieee.org/document/9670054
2. Flaherty, David H. Protecting privacy in surveillance societies : the Federal Republic of Germany, Sweden, France, Canada, and the United States / The University of North Carolina Press, 1989. – P.507. [Электронный ресурс] : база данных. – Режим доступа: https://flexpub.com/preview/protecting-privacy-in-surveillance-societies
3. Positive Technologies. Актуальные киберугрозы: I квартал 2022 года. [Электронный ресурс] : база данных. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1
4. Positive Technologies. Актуальные киберугрозы: итоги 2021 года. [Электронный ресурс] : база данных. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021
5. Rajiv M. Dewan, Bing Jing, Abraham Seidmann. One-to-one marketing on the internet // Proceedings of the Twentieth International Conference on Information Systems, (ICIS) 1999, Charlotte, North Carolina, USA, December 13-15, 1999 – P.93-102.