КИБЕРСИГУРНОСТ КАТО ИНСТРУМЕНТ ЗА ЗАЩИТА НА ЦИФРОВИТЕ АКТИВИ

Cybersecurity as a tool for protecting digital assets

Андрей Вишневский[1]
e-mail: avishnevskiy_2520829@unwe.bg[1]

Резюме

В настоящия доклад ще бъде разгледана киберсигурността като инструмент за защита на цифровите активи. Каква е ролята за потребителя, която оказват съвременните технологии, какви цели се постигат, каква потенциална заплаха представляват за потребиля и как киберсигурността помага за съхраняването на ценни данни и ресурси. В допълнение към това ще се представят възможностите и предизвикателствата, срещани при киберсигурността в различни направления.

Ключови думи: киберсигурност, защита , изкуствен интелект , цифрови активи

JEL: L86,O33, D83,E42,G18

Abstract

This report will examine cybersecurity as a tool for protecting digital assets. What role does modern technology play for the user, what goals are achieved, what potential threats do they present to the user, and how cybersecurity helps to safeguard valuable data and resources. In addition, the opportunities and challenges encountered in cybersecurity in various areas will be presented.

Въведение

С напредването на технологиите, процесът на дигитализацията става все по-усилен и по-често потребителите използват своите “умни” устройства, такива като телефони, компютъри, часовници и други популярни устройства в своето всекидневие. Тези устройства се използват както за развлечения, така и с учебна или работна цел, в допълнение към това, те са много удобни за използване, имат голямо количество опции и възможности и могат значително да улеснят всекидневните задачи, с тях потребителят може да осъществява комуникация с други хора, да се разпорежда със своите финанси, да съхранява важна информация и т.н. Във всяко от устройствата по един или друг начин се съхраняват и създават различни данни, които могат да представляват ценност не само за потребителя или компанията която разполага с тях, но и за различни престъпници които могат да ги използват в личните си цели, обикновенно свързани с финансов интерес, такива престъпници извършват киберпрестъпления, а хората извършващи тях се наричат киберпрестъпници и често още ги наричат “хакери”. Практика създадена с цел на защита от такива престъпления се нарича “Киберсигурност” и тя ще стане предмет на обсъждане в този доклад.

Същност на киберсигурността

Киберсигурност представлява практика за защита на компютри, компютърни мрежи, приложения и различни видове софтуер от различни видове заплахи. Киберсигурността е набор от процеси, практики и технологични решения които имат цел да предпазят , данни и важни за работа и не само, системи и устройства, от злонаммерен софтуер и други видове дигитални или цифрови заплахи които са способни да донесат различни финансови, репутационни и други вреди. Киберсигуност включва, не само добри практики за защита на ценна информация, но и важен софтуер и други

[1] Студент-магистър, катедра “Информационни технологии и комуникации”, УНСС

технологични решения, които също оказват голямо влияние относно защита на потребителя от опасни действия с лоши последици.

Ролята на киберсигурността и задачи за които тя помага

Киберсигурността служи за защита на потребителите на смарт устройства от различни видове опасности, създавани от недобросъвестни специалисти с различни цели. Такива цели могат да бъдат кражба или неконтролиран достъп до ценна инфолмация, финансови активи, репутационни щети, които могат да бъдат нанесени върху дадена компания или частно лице, в допълнение към това различни киберпрестъпници могат временно или в някои случаи за постоянно да прекратят работа на дадена система,която те атакуват.

Задачи свързани с киберсигурност

- **Защита на конфиденциална информация:** (Лична информация, фирмени тайни, финансова информация)
  Такава информация могат да са данни на потребителите в една система, например в онлайн магазин може да има ценна информация свързана със служителите и с клиенти, тази информация могат да бъдат банкови данни, адреси, имена, телефонни номера и сведения за лични документи. Фирмени тайни могат да са свързани, не само с информация за клиенти и служители, но и свързани с фирмени стратегии, технологични патенти, производствени тайни и друга важна информация. Това което се касае финансова информация, обикновенно е свързана с ценни активи или сведения за тях, които също трябва да са строго пазени.

- **Предотвратяване на финансови загуби:** Кибератаки могат да доведат до значителни финансови загуби, особено ако това се случва в различни финансови организации, застрахователни дружества, банки и други организации работещи с големи парични суми.
- **Съхранение на репутация:** Загуба на данни или успешна кибератака може силно да навреди репутацията на компания. С това да понесе както и репутационни, така и финансови загуби по различни причини, тези причини могат да бъдат прекратяване на отношения с партньори, загуба на клиенти, съдебни разходи, ако се стига до такива и други видове загуби.
- **Спазване на законови норми:** Повечето държави имат определени норми свързани със съхраняването и обработването на лична информация, заради което за фирмата е важно да има начини как това да се реализира и да се предпази от злонамерени действия причинявани от киберпрестъпници.

Какво предпазва киберсигурността?

Практиките свързани с киберсигурност целят да предпазват от:

- **Fishing (Фишинг) атаки:** Това са подвеждащи фалшиви съобщения обикновенно по имейл с цел на получаване на конфиденциална информация. Съществуват още Smishing (Смишинг) и Vishing (Вишинг) това са подобни видове атаки само че, с помощта на съобщение и глас съответно, тоест по телефон и други гласови канали за комуникация.
- **Злонамерен софтуер:** Това е всякакъв софтуер нанасящ технически или финансови щети с някаква зла умисъл, такъв може да бъдат вируси, различен софтуер за кражба, изтриване или достъп до лична информация.

- **DDoS-атаки:** Атаки от много различни реални или виртуални устройства към един сървър в едновременно с цел частично или пълно изключване на даден сървър за неопределен срок от време.
- **Атаки с използване на уязвимости**: Такива могат да бъдат различни ситуации, в които атакуваното устройство е с острарял софтуер, когато то не е обезапасено според необходимите потребности или е открит някакъв труднозабележим проблем, в такъв момент се извършва атака с цел максимална резултативност.
- **Атаки на социална инженерия:** Това са атаки където се използват, не само технически средства, но и психологически техники и умения от престъпника с цел на получаване на ценна информация или финансови активи, като пари, акции, криптовалута и други.
- **Ransomware:** Това са програми криптиращи информация на устройствата на потребител или компания с цел изнудване за пари, унищожаване на информация или загуба на достъпа до нея.

- **Какви са практики за защита на данни и ценни финансови активи?**

Следните практики могат в значителна степен да предпазят потребителите и компаниите от злонамерени действия и сериозни проблеми.

- **Нулево доверие (Zero trust)**

- Нулево доверие- принцип на киберсигурността, в който се подразбира липса на доверие в такива случаи всеки отдел или служител има достъп само до тази част, до тези ресурси или данни, до които им е необходимо за изпълняваните им задачи, в случая те нямат достъп до други данни или ресурси за които отговарят други ресурси. Допълнително към това се използват средства за достъп и аутентификация с цел, за да се удостовери, че точно това е служител, който трябва да извърши някаква задача и че точно той има нужда от достъп до тези ценни ресурси, а не някой друг. В случай, ако служител си променя своята длъжност или напуска компанията, то и достъпите му се променят или прекратяват.

- **Поведенческа аналитичност**

- Поведенческа аналитика позволява да се следи предаването на данни и да следи за подозрителни достъпи, например ако извън работно време на компанията има опити за достъп до някакви фирмени системи или някакви лични данни, които не трябва да се разкриват, то това е подозрително поведение, за което може да бъде уведомено по различни начини. Също така при опит за достъп от място различно от обикновените, например извън сградата на компанията или за достъп до устройство от друг град или държава, това също е подозрително поведение, което ще бъде забелязано и ще бъдат взети мерки.

- **Система за откриване на проникване**

- Компании и организации използват системи за откриване на проникване, за да идентифицират кибератаки и да реагират бързо на тях. Съвременните решения за сигурност използват изкуствен интелект, машинно обучение и анализ на данни, за да идентифицират скрити заплахи в компютърните системи на компаниите и организациите.

  Използват се механизми за предотвратяване на проникване, които събират данни за инциденти, за достъп където се вижда време и място, от което е направен такъв опит, след което, екипите по сигурността могат да идентифицират източниците им.

- **Облачно шифроване (Криптиране).**

- Това е процес по криптиране на данни преди попадането им в облака, където те ще се съхраняват, в случая на непредвиден достъп от киберпрестъпници данните ще бъдат криптирани, в неизползваем вид, за тези които не трябва да имат достъп до тях и нямат специален ключ или алгоритъм с който да ги разшифроват. Това също е важно и полезно решение, в допълнение на това, фирмите обикновенно разполагат с копие на данните си и на други носители.

Принципите на работа на киберсигурността са следните:

- Удостоверяването и оторизацията проверяват самоличността на потребителите и контролират достъпа до ресурси.
- Криптирането на данните преобразува информацията в криптиран формат, което я прави недостъпна за престъпниците.
- Наблюдение и откриването на заплахи осигуряват непрекъснат контрол на мрежовата активност, за да се идентифицира подозрителна дейност.
- Обучението на служителите повишава осведомеността на потребителите за киберзаплахите и сигурното поведение.
- Копирането на данни позволява възстановяване в случай на атака и загубата им от основният носител.
- Управлението на събитията включва набор от процедури и инструменти за реагиране на кибератаки и намаляването на тяхното въздействие, разполагайки с данните от миналото е възможно да се предотвратят някои от сценариите.

Технологии помагащи за киберсигурност.

За защита се използват различни средства, те постоянно се подобряват спрямо нови потенциални проблеми, за такива средства могат да се представят следните съвременни технологии:

- Изкуствен интелект (AI), той се използва за анализ на поведението, препоръки към потребителите и намирането на аномалии.
- Машинно обучение помога да предсказва вероятните сценарии и да предотвратява заплахи.
- Блокчейн осигурява съхранение на данни, повишавайки тяхната сигурност.
- Многофакторното удостоверяване (MFA) използва множество методи за проверка на самоличността за достъп до системи.
- Платформите за управление на информацията за сигурност и събития (SIEM) събират, анализират и съпоставят данни за събития за сигурност.
- Криптографията използва методи за криптиране на данните, за да осигури максимално тяхната защитеност.

Заключение

Съвременният свят непрекъснато се развива и технологиите все повече са свързани със съвременният човек, всеки ден обработваме големи обеми от информация и работим с големи обеми от данни, също така все повече задачи се изпълняват от устройствата ни, различни покупко-продажби, поръчки, подписване на договори, работа с документи и други важни действия. Всяко едно от тези важни за нас действия може да бъде по някакъв начин атакувано от киберпрестъпници или така наречените “хакери”. Техните атаки могат да бъдат с различни цели и върху различни дейности извършвани от обикновен потребител или някаква компания

или организация, което поставя в опасност данни и финансови активи, които могат да бъдат засегнати. В резултат на такива кибератаки могат да бъдат откраднати, загубени и получени ценни данни, а също така и финансови активи от различни видове. За да се избегнат такива атаки и да се минимизират последствията от потенциални такива, съществува Киберсигурност, това е набор от практики и технологии създадени с цел на обезопасяване в технолгичните пространства и спазването на всички препоръки и използването на съществуващите средства за защита, значително помага за сигурността на един потребител или цяла компания.

Литература:

1. Microsoft, (н.д.). Какво представлява киберсигурността? Достъпно от: https://www.microsoft.com/bg-bg/security/business/security-101/what-is-cybersecurity
2. Microsoft, (н.д.). Какво е фишинг? Достъпно от:
3. https://www.microsoft.com/bg-bg/security/business/security-101/what-is-phishing
4. Amazon Web Services, (2025). What is Cybersecurity? Cybersecurity Explained. Достъпно от: https://aws.amazon.com/what-is/cybersecurity
5. Kaspersky, (н.д.). Cyber Security Solutions for Home & Business. Достъпно от: https://www.kaspersky.ca
6. Economic.bg, (2016). Yahoo призна за най-голямата кибератака в историята. Достъпно от: https://www.economic.bg/bg/a/view/yahoo-prizna-za-naj-golyamata-kiberataka-v-istoriyata-64311
7. РБК Тренды, (2021). 10 самых громких кибератак XXI века. Достъпно от:
8. https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e
9. bTV Новините, (н.д.). 5 кибератаки, по-страшни от тази срещу НАП. Достъпно от: https://btvnovinite.bg/svetut/5-kiberataki-po-loshi-ot-tazi-sreshtu-nap.html
10. BBC News, (2016). Petya ransomware encryption system cracked. Достъпно от: https://www.bbc.com/news/technology-36014810
11. BBC News, (2016). The ransomware that knows where you live. Достъпно от: https://www.bbc.com/news/technology-35996408
12. Goodreads, (н.д.). Quotes Library. Достъпно от: https://www.goodreads.com/quotes
13. CrowdStrike, (н.д.). What Is a Ransomware Attack? Достъпно от: https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware
14. Khan Academy, (н.д.). Phishing Attacks – Cyber Crime Section. Достъпно от: https://www.khanacademy.org/computing/.../phishing-attacks
15. PayPal, (н.д.). PayPal Bulgaria – Home. Достъпно от: https://www.paypal.com/bg/home
16. DTU.kz, (н.д.). Что такое кибербезопасность и ее основные характеристики. Достъпно от: https://www.dtu.kz/blog-post/chto-takoe-kiberbezopasnost-i-ee-osnovnye-harakteristiki