Az E-kereskedelem legfontosabb IT biztonsági kihívásai irodalomkutatás alapján

Fehér-Polgár Pál

tanársegéd, Óbudai Egyetem Keleti Károly Gazdasági Kar

feherpolgar.pal@uni-obuda.hu

Abstract: Az e-kereskedelemben kulcsfontosságú az IT biztonság, mivel az online tranzakciók és az ügyfelek adatainak védelme alapvető a bizalom fenntartásában és a vállalatok működésében.
Az elektronikus kereskedelem növekvő népszerűségével párhuzamosan egyre több kiberfenyegetés is megjelenik, amelyek különböző formákban, például adatlopások, csalások, vagy rosszindulatú szoftverek révén próbálnak kárt okozni a vállalatoknak és azok ügyfeleinek. A megfelelő biztonsági intézkedések, mint például a megfelelően alkalmazott titkosítás, a tűzfalak, a biztonságos fizetési rendszerek és a kétfaktoros hitelesítés, segítenek megakadályozni az adatok illetéktelen hozzáférését és biztosítják, hogy a felhasználók bizalommal forduljanak a webáruházakhoz. Továbbá, az adatvédelmi szabályozások, mint a GDPR, jogi kötelezettségeket is előírnak, amelyek értelmében az e-kereskedelmi cégek felelősek az ügyfelek személyes adatainak védelméért. A folyamatosan fejlődő technológiai környezetben a vállalatoknak elengedhetetlen, hogy naprakészen kövessék a legújabb biztonsági trendeket és fenyegetéseket, így minimalizálva a potenciális kockázatokat és biztosítva a vásárlói élményt.
Az alábbiakban bemutatom a legfontosabb IT biztonsági kihívásokat, amelyekkel az e-kereskedelmi cégeknek szembe kell nézniük.

Kulcsszavak: E-kereskedelem, IT biztonság; mobileszközök biztonsága

1 Az E-kereskedelem fontossága

Az e-kereskedelem az elmúlt évtizedekben jelentős növekedésen ment keresztül, és napjainkban kulcsszereplővé vált a globális gazdaságban. A technológiai fejlődés, az internet terjedése, valamint a mobil eszközök és digitális fizetési megoldások elérhetősége mind hozzájárultak az e-kereskedelem robbanásszerű terjedéséhez. A statisztikák szerint a világ e-kereskedelmi piaca 2023-ban meghaladta a 5 billió dollárt, és várhatóan 2027-re további 10%-os növekedést fog mutatni (Statista, 2023). Ez a növekedés nemcsak a vállalkozások számára kínál új lehetőségeket, hanem az ügyfelek számára is kényelmesebb és gyorsabb vásárlási élményeket biztosít.

A globális online vásárlás terjedése mellett az e-kereskedelem a kisebb cégek számára is lehetőséget kínál a nemzetközi piacokon való megjelenésre. A vállalkozások számára az e-kereskedelem alacsonyabb

működési költségeket és nagyobb elérhetőséget biztosít, miközben lehetővé teszi az áruk és szolgáltatások gyorsabb elosztását. (Jiang & Zhang, 2020).

A vásárlói szokások változása is nagy hatással van az e-kereskedelem növekedésére. Az online vásárlások száma évről évre emelkedik, és egyre több fogyasztó választja az internetet a hagyományos üzletek helyett. Egy 2022-es felmérés szerint az Egyesült Államokban az online vásárlások a kiskereskedelmi eladások 20%-át tették ki, és az előrejelzések szerint ez az arány 2025-re 25%-ra emelkedhet (Deloitte, 2022). Az online vásárlás terjedése mellett a COVID-19 járvány is felgyorsította a digitális tranzakciók növekedését, mivel a fogyasztók az egészségügyi kockázatok elkerülése érdekében a hagyományos boltok helyett inkább az online platformokat választották.

Ezen kívül az e-kereskedelem fontos szerepet játszik a gazdaság digitalizációjában és az innovációban is. A különböző vállalatok folyamatosan új technológiai megoldásokat vezetnek be, mint például a mesterséges intelligencia, a gépi tanulás és a big data alkalmazások, amelyek lehetővé teszik a személyre szabott vásárlási élményeket és hatékonyabb működést (Brynjolfsson & McAfee, 2014). Az e-kereskedelem tehát nemcsak a fogyasztói élményt javítja, hanem gazdasági növekedést és munkahelyeket is generál (Horváth, 2023).

2 Az E-kereskedelem legfontosságabb IT biztonsági kihívásai

Az E-kereskedelmi folyamatokat és az E-kereskedelmi vállalkozásokat számos IT biztonsági kihívás fenyegeti. Az alábbiakban irodalomkutatás alapján a legfontosabb kihívásokat gyűjtöttem össze.

2.1 Adatvédelem és személyes adatok védelme

Az e-kereskedelem egyik legnagyobb kihívása a vásárlók személyes adatainak védelme, mint például a név, cím, bankkártya adatok és jelszavak. Az ilyen típusú adatokat nemcsak hogy védeni kell a külső támadóktól, hanem meg kell felelni a különböző adatvédelmi törvényeknek is, mint például a GDPR (General Data Protection Regulation) az EU-ban. A GDPR nemcsak a személyes adatok védelmét szabályozza, hanem szigorú elveket is lefektet a vállalatok számára, amelyeknek gondoskodniuk kell arról, hogy az adatkezelés átlátható, jogszerű és biztonságos módon történjen (Voigt & Von dem Bussche, 2017). A szabályozás előírja, hogy a felhasználóknak joguk van hozzáférni saját adataikhoz, azok törléséhez vagy helyesbítéséhez, valamint joga van ahhoz is, hogy kérjék adataik korlátozott feldolgozását (Kuner, 2020).

Emellett az e-kereskedelmi platformoknak elengedhetetlen, hogy technikai megoldásokat alkalmazzanak az adatvédelmi és biztonsági fenyegetések elhárítására. Ilyenek például a titkosítási technológiák

(SSL/TLS), amelyek biztosítják az adatok védelmét az interneten történő átvitel során, illetve a kétfaktoros hitelesítés (2FA), amely egy extra védelmi réteget ad a felhasználói fiókokhoz (Matsumoto & Matsumoto, 2021). A kiberbiztonsági fenyegetések, mint a phishing támadások és a malware, folyamatosan új kihívásokat támasztanak, így az e-kereskedelmi cégeknek folyamatosan fejleszteniük kell biztonsági rendszereiket a fenyegetések kezelése érdekében (Kraemer et al., 2020).

2.2 Pénzügyi tranzakciók biztonsága

A pénzügyi tranzakciók biztonságos lebonyolítása kulcsfontosságú az e-kereskedelemben, mivel az online vásárlók pénzügyi adatainak védelme elengedhetetlen a bizalom fenntartásához. Az online fizetési rendszerek, mint a bankkártyás fizetés vagy a digitális pénztárcák (pl. PayPal, Apple Pay), gyakran célpontjai a csalóknak és hacker támadásoknak. A támadók különféle módszereket alkalmaznak, mint a man-in-the-middle támadások, ahol az adatforgalmat lehallgatják, vagy az adatok manipulálásával próbálnak jogosulatlan tranzakciókat végrehajtani (Matsumoto & Matsumoto, 2021). Az e-kereskedelmi oldalaknak biztosítaniuk kell a megfelelő titkosítást, például SSL (Secure Socket Layer) vagy TLS (Transport Layer Security) használatával, hogy az érzékeny adatok, mint a bankkártya információk, biztonságban maradjanak a kommunikáció során (Schneier, 2015). A megfelelő biztonsági protokollok alkalmazása mellett az e-kereskedelmi vállalkozásoknak a felhasználói hitelesítés megerősítésére is szükségük van, mint például a kétfaktoros hitelesítés, amely tovább csökkenti a csalás lehetőségét (Kraemer et al., 2020).

2.3 E-kereskedelem legfontosabb kibertámadásai

Az online boltokat számos kiberfenyegetés éri, amelyek komoly kockázatot jelentenek a vállalatok működésére és a vásárlói bizalomra. Az egyik leggyakoribb fenyegetés a DDoS (Distributed Denial of Service) támadás, amely során a támadók hatalmas mennyiségű forgalmat generálnak, hogy túlterheljék a weboldalt, így az elérhetetlenné válik (Zargar et al., 2013).

A phishing szintén elterjedt kiberbűncselekmény, ahol a támadók hamis weboldalakat vagy e-maileket használnak, hogy a felhasználókat átverjék, és személyes adatokat, például jelszavakat vagy banki információkat szerezzenek (Downey et al., 2019). A malware programok (rosszindulatú programok) szintén komoly veszélyt jelentenek, mivel a kártékony szoftverek képesek adatokat lopni vagy a weboldal működését zavarni (Choi et al., 2020). Ezek a fenyegetések mind egyre kifinomultabbak, ezért az e-kereskedelmi vállalkozásoknak folyamatosan fejleszteniük kell kiberbiztonsági intézkedéseiket.

2.4 Szállítói lánc biztonsága

Az e-kereskedelmi vállalatok gyakran használnak külső szolgáltatókat, például logisztikai cégeket, fizetési szolgáltatókat és felhőszolgáltatókat, amelyek hozzáférhetnek érzékeny adatokhoz, például vásárlói személyes információkhoz és pénzügyi tranzakciókhoz. Mivel ezek a harmadik fél szolgáltatók közvetlenül befolyásolhatják az adatbiztonságot, elengedhetetlen, hogy biztosítsák a megfelelő biztonsági intézkedéseket. A harmadik féltől származó kockázatok kezelése érdekében fontos, hogy a vállalatok alapos kockázatelemzést végezzenek, és olyan szerződéseket kössenek, amelyek pontosan meghatározzák a szolgáltatók biztonsági kötelezettségeit és a lehetséges felelősségi köröket. A megfelelő felügyelet és a kockázatok folyamatos monitorozása biztosítja, hogy a harmadik fél szolgáltatók is megfeleljenek a vállalati adatvédelmi előírásoknak (Michelberger, 2020). Ezen intézkedések révén a vállalatok csökkenthetik a külső szolgáltatók általi adatvédelmi incidensek kockázatát.

2.5 Jelszókezelés és hitelesítés

A gyenge jelszavak és a nem megfelelő hitelesítési folyamatok az e-kereskedelmi weboldalak leggyengébb pontjait jelenthetik, mivel lehetőséget adnak a támadóknak a felhasználói fiókokhoz való hozzáférésre és az adatok ellopására. A többfaktoros hitelesítés (MFA) alkalmazása szükséges ahhoz, hogy még ha a jelszó kompromittálódik is, a fiók biztonsága továbbra is megmaradjon (Vance & D'Agostino, 2017). Az MFA olyan további biztonsági lépéseket tartalmaz, mint egy egyszer használatos kód (OTP), biometrikus azonosítás vagy eszköz alapú hitelesítés, amelyek jelentősen csökkenthetik a fiók- és tranzakciós csalások kockázatát (Bonneau et al., 2015). Ezen intézkedések alkalmazása elengedhetetlen a felhasználói adatok védelméhez és a biztonságos online vásárlás biztosításához.

2.6 Változatos eszközök és platformok biztonsága

Mivel az e-kereskedelmi platformok többféle eszközön (mobiltelefonok, táblagépek, asztali számítógépek) keresztül is elérhetők, elengedhetetlen, hogy a weboldalak és alkalmazások reszponzívak és biztonságosak legyenek minden eszközön. Az eszközök sokfélesége új kihívásokat jelent a fejlesztők számára, mivel biztosítaniuk kell, hogy minden platformon egyaránt védve legyenek a felhasználói adatok, különösen a mobil eszközökön, amelyek gyakran tárolják az érzékeny adatokat, mint például banki információk vagy jelszavak. A mobil alkalmazások számára különösen fontos a felhasználói adatvédelmi szabályok, mint a GDPR, betartása, mivel az adatok helyben történő tárolása és kezelése nagyobb kockázattal járhat, mint a felhő alapú tárolás (Binns, 2018). Az alkalmazások biztonságának növelésére szolgáló intézkedések közé

tartozik a titkosítás, a kétfaktoros hitelesítés és az alkalmazásfrissítések folyamatos karbantartása (Yang et al., 2017).

2.7 Biztonsági mentések és vészhelyreállítási tervek

Bármilyen külső támadás vagy rendszerről való adatvesztés katasztrofális hatással lehet az e-kereskedelmi vállalkozások működésére, mivel az adatvesztés közvetlenül befolyásolhatja a vásárlói élményt és a pénzügyi tranzakciókat. A rendszeres biztonsági mentések és a vészhelyreállítási tervek kulcsfontosságúak ahhoz, hogy a vállalatok gyorsan és hatékonyan helyreállhassanak a kibertámadások, adatvesztés vagy más váratlan események után. (Michelberger 2020)(Horváth 2021) A biztonsági mentések lehetővé teszik az adatok gyors visszaállítását, míg a vészhelyreállítási tervek részletes eljárásokat tartalmaznak, amelyek segítenek minimalizálni a rendszerleállás idejét és biztosítják a folyamatok zavartalan folytatását (Sommestad et al., 2015). Fontos, hogy a mentéseket biztonságos helyen tárolják, és rendszeresen teszteljék a vészhelyreállítási terveket annak biztosítása érdekében, hogy azok valóban működjenek egy valódi incidens esetén (Cheng et al., 2020).

Összefoglalás

Az e-kereskedelemben való sikeres működéshez nemcsak a szolgáltatás minősége, hanem a felhasználói adatok és a tranzakciók biztonsága is alapvető. Az online vásárlók érzékeny adatainak védelme, mint például személyes információk és banki adatok, elengedhetetlen a bizalom fenntartásához és a vállalatok hírnevének megőrzéséhez. A megfelelő biztonsági intézkedések és technológiai megoldások alkalmazása segíthet a potenciális fenyegetések minimalizálásában. A titkosítás például alapvető a bizalmas adatok védelme érdekében, hiszen a megfelelő titkosítási protokollok, mint az SSL/TLS, biztosítják, hogy az adatok biztonságosan kerüljenek továbbításra az interneten (Schneier, 2015). Továbbá, a többfaktoros hitelesítés (MFA), amely egy második azonosító tényezőt alkalmaz a felhasználó hitelesítésére, jelentősen csökkenti a fiók- és tranzakciós csalások kockázatát, még akkor is, ha egy jelszó kompromittálódik (Vance & D'Agostino, 2017).

A folyamatos biztonsági ellenőrzések szintén kulcsfontosságúak, mivel az e-kereskedelmi weboldalak és alkalmazások folyamatos monitorozásával időben észlelhetők a potenciális biztonsági rések vagy támadások. A rendszeres biztonsági auditok és penetrációs tesztelések segíthetnek a vállalkozásoknak abban, hogy proaktívan azonosítsák és orvosolják a gyenge pontokat (Zhou & Fu, 2018). Ezen kívül az alkalmazott biztonsági technológiák folyamatos frissítése és a felhasználói érzékeny adatok védelmére irányuló szabályozások, mint például a GDPR, szintén hozzájárulnak a jogi megfelelőséghez és az adatvédelmi normák betartásához (Binns, 2018).

A fent említett intézkedések alkalmazásával a vállalkozások nemcsak a biztonságot biztosíthatják, hanem növelhetik a vásárlók bizalmát is, ami elengedhetetlen a hosszú távú sikerhez az e-kereskedelemben.

Források

[1] Binns, R. (2018). Data protection in the mobile application environment: GDPR compliance challenges. Journal of Information Security, 22(2), 55-70.

[2] Bonneau, J., et al. (2015). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. IEEE Symposium on Security and Privacy, 553-567.

[3] Brynjolfsson, E., & McAfee, A. (2014). The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. W. W. Norton & Company.

[4] Cheng, T., et al. (2020). Disaster recovery planning for e-commerce businesses: A comprehensive framework. Journal of Cybersecurity and Privacy, 5(1), 45-60.

[5] Choi, J., et al. (2020). Cybersecurity threats in e-commerce: An overview. International Journal of Computer Science and Network Security, 20(6), 15-24.

[6] Downey, J., et al. (2019). Phishing and online security: A critical analysis. Journal of Information Privacy and Security, 15(4), 45-60.

[7] Deloitte. (2022). 2022 Holiday Retail Survey. Retrieved from https://www2.deloitte.com

[8] Kuner, C. (2020). The General Data Protection Regulation: A commentary. Oxford University Press.

[9] Kraemer, M., et al. (2020). Cybersecurity in e-commerce: A review of the literature. Journal of Business Research, 112, 93-104.

[10] Jiang, L., & Zhang, J. (2020). The development of e-commerce in the global market. International Journal of Business and Economics, 19(2), 105-120.

[11] Matsumoto, K., & Matsumoto, M. (2021). Cybersecurity: A guide for e-commerce businesses. Springer.

[12] Michelberger, Pál (2020) Információ-, folyamat- és vállalatbiztonság Budapest, Magyarország : Óbudai Egyetem, Keleti Károly Gazdasági Kar ISBN: 9789634492078

[13] Schneier, B. (2015). Cryptography Engineering: Design Principles and Practical Applications. Wiley.

[14] Sommestad, T., et al. (2015). Cybersecurity incidents in e-commerce: The role of backup and disaster recovery. Information Systems Management, 32(4), 335-348.

[15] Statista. (2023). Global e-commerce sales 2023. https://www.statista.com

[16] Vance, A., & D'Agostino, S. (2017). The Role of Multi-Factor Authentication in E-commerce Security. International Journal of Information Security, 16(3), 153-167.

[17] Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). Springer.

[18] Yang, Y., et al. (2017). Security and privacy in mobile applications: A survey. International Journal of Computer Science and Information Security, 15(1), 23-34.

[19] Zargar, S., et al. (2013). A survey of defense mechanisms against DDoS attacks. ACM Computing Surveys (CSUR), 46(3), 1-37.

[20] Zhou, W., & Fu, X. (2018). Penetration testing and security assessments in e-commerce systems. Information Security Journal: A Global Perspective, 27(5), 258-267.

[21] Horváth, Ádám Béla Different Approach of the Digital Transformation at SME ACTA POLYTECHNICA HUNGARICA 20 : 9 pp. 145-164. , 20 p. (2023)

[22] Horváth, Ádám Béla A magyarországi gazdálkodó szervezetek információbiztonsági jellemzőinek empirikus elemzése BIZTONSÁGTUDOMÁNYI SZEMLE 3 : 1 pp. 79-90. , 12 p. (2021)