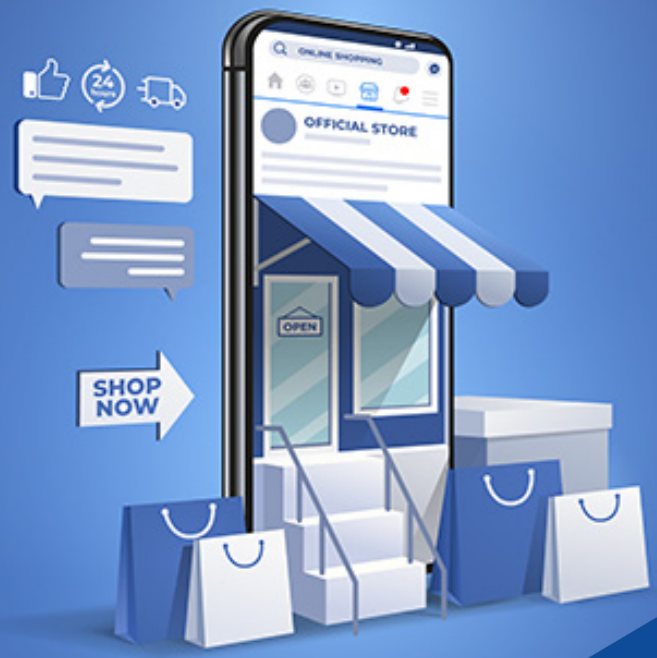


CTI Jelentés

Tudnivalók a biztonságos online vásárláshoz - II. rész

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET

Tartalomjegyzék

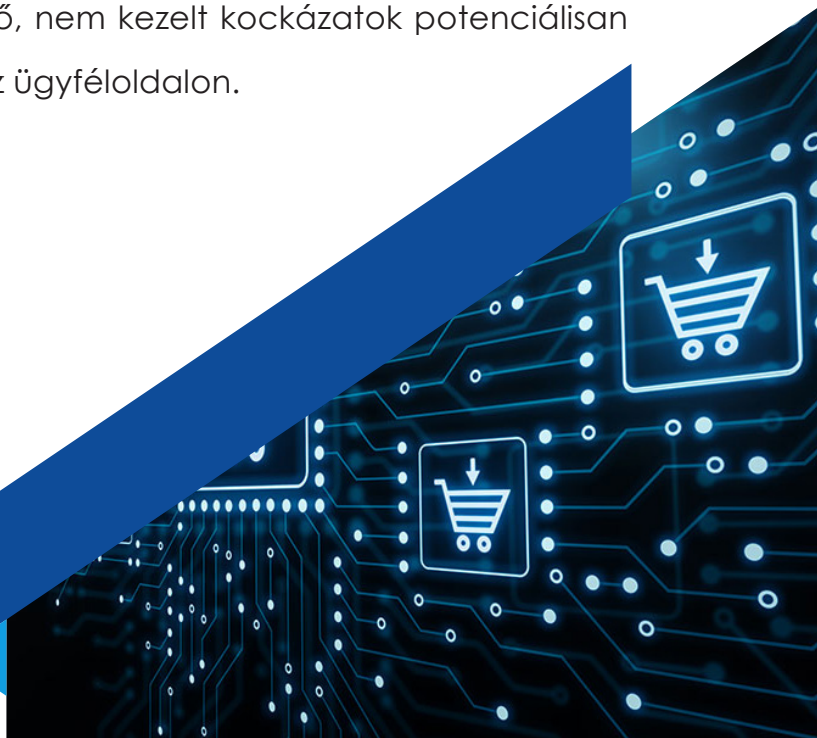
Bevezetés

A Tudnivalók a biztonságos online vásárlásokhoz - I. rész című tájékoztató dokumentumban bemutattuk a felhasználókat fenyegető leggyakoribb támadástípusokat, módszereket és számos javaslattal éltünk, amelyek betartásával nagy mértékben csökkenthető annak a kockázata, hogy személyes adataink és vagyonunk rossz kezekbe kerüljön. Az első részben a felhasználó oldaláról igyekeztünk bemutatni a legfőbb problémákat, jelen dokumentumban pedig mindezt az üzemeltetők, webshop tulajdonosok szemszögéből ismertetjük.

A legtöbb mai webes alkalmazás meglehetősen összetett, több komponensből épülhetnek fel, amelyek lehetnek meglévő szoftverek, nyílt forráskódú, harmadik féltől származó kódok, saját kódok és API-k. Míg a webalkalmazásokat egy szerveren tárolják és karbantartják, valójában a végfelhasználó böngészőjében futnak. Az alkalmazásokat futtató szkripteket ügyféloldali szkripteknek (client side scripts) nevezik. Ezek a szkriptek magas szintű funkcionalitást tesznek lehetővé, ugyanakkor nagy kockázatot is jelentenek, mivel a potenciálisan hibás vagy sebezhető rendszerek, szerverek, kódok és alkalmazások kombinációja tökéletes forgatókönyvet teremt a fenyegetési szereplők számára, amelyet az ügyféloldali támadások során kihasználhatnak. A „kliensoldali" kifejezés a végfelhasználói eszközökre utal, mint például az asztali számítógépek, laptopok, mobiltelefonok és táblagépek. Azokat a rendszereket, amelyekhez az eszközök csatlakoznak, „kiszolgálóknak" nevezzük.

Az ügyféloldali támadások akkor következnek be, amikor a felhasználó akaratlanul rosszindulatú vagy sebezhető tartalmat tölt le egy szerverről csupán egy kattintással vagy egy űrlap kitöltéssel.

A szervezeti rendszerekben jelen lévő, nem kezelt kockázatok potenciálisan súlyos támadásokhoz vezethetnek az ügyféloldalon.



A weboldalak elleni legyakoribb támadási technikák

Amikor valaki webáruház építésbe kezd, az első kötelező és rendkívül fontos lépések egyike, hogy megtervezze a webshopjának a biztonságát. Bár apró beállításokról, bizonyos modulok használatáról, egyes komponensek tiltásáról és alternatívák kereséséről szól az egész folyamat, azonban összeségében meglehetősen nehéz jól kivitelezni ezt, ha nem gyakorlott webfejlesztő vagy üzemeltető az ember. Biztosak vagyunk abba, hogy lesz olyan, akinek teljesen egyértelműek a lentebb leírtak, azonban a célunk az, hogy a kevésbé tapasztalt olvasóink olyan információhoz jussanak, amelyeknek nem voltak eddig birtokában. Fontos megjegyezni, hogy bár a főbb biztonsági kérdéseket érintjük, azonban az egyes témákban nem merülünk el részletesen, amiatt, hogy egy rövid, olvasható, hasznos tájékoztatót tudjunk olvasóink számára nyújtani.

Javasoljuk, hogy a tájékoztató elolvasása után keressenek rá egy-egy címszóra, és mélyüljenek el az adott témakörben, így tehetnek szert sokkal átfogóbb és szélesebb körű, gyakorlatias tudásra.

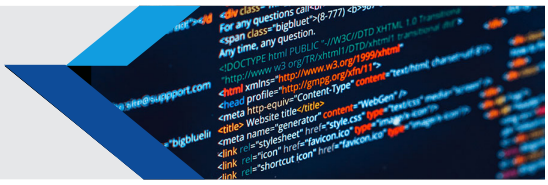
XSS (Cross-site Scripting)

Ez egy olyan sebezhetőség, amely lehetővé teszi a támadó számára, hogy saját rosszindulatú kódot juttasson be a felhasználók számára megjelenített HTML oldalakra. Ha a rosszindulatú kódot az áldozat böngészője végrehajtja, akkor a támadó hozzáférhet hitelkártyaadatokhoz, cookie-khoz (webes sütik), munkamenet tokenekhez és érzékeny hitelesítő adatokhoz. Védekezni ellene a felhasználói bemeneti adatok validálásával (user input validate) és adat-szanitációval lehetséges (data sanitize).

SQL Injection

Az SQL egy string alapú nyelv, és a fő probléma ebből adódik: azok a parancsok, amelyeket kiadunk egy-egy adatbázis lekérdezés során, egyszerű karakterláncok. Ha egy támadó egy input mezőbe beírja a megfelelő SQL parancsot, szerver oldalon lefuthat és válaszként minden személyes felhasználói adatot megszerezhet, ami az adatbázisban tárolva van. Ezenfelül adatbázis manipulációkat hajthat végre, ami akár a teljes adatbázis elvesztésével is járhat. A bemenetek validálásával és karakter escape-eléssel lehet védekezni ellene.

HTML Injection



Ez HTML kód bejuttatását jelenti a weboldal sebezhető részein keresztül, amely célja általában a weboldal dizájnjának vagy a weboldalon megjelenített információknak a megváltoztatása.

CSS Injection

A támadók olyan CSS kódot juttatnak be a weboldalra, amely megjelenik a felhasználó böngészőjében. Manapság ennek a védelmét már a webböngészők megoldják önmaguktól, de aki korábbi, elavult böngészőt használ, azokra ez veszélyt jelenthet. A CSP header használata (Content Security Policy) megakadályozza, hogy a böngészők rosszindulatú kódot hajtsanak végre a webhelyen.

Ügyféloldali URL átirányítás

A támadás ezen típusában a hackerek a felhasználó webböngészőjén keresztül a felhasználót rosszindulatú weboldalakra irányítják át. Ezt rendszerint adathalászatra és a felhasználói hitelesítő adatok ellopására használják a kiberbűnözők. A probléma kiküszöbölése érdekében javasolt az átirányítások tiltása, ne engedélyezzük, hogy a felhasználó URL-t adhasson meg inputként. Az injektálásoknál említett szanitáció és validálás használata jelen támadási felület ellen is megfelelő védelmet nyújt.

Cross-origin Resource Sharing (CORS)

A CORS egy HTTP fejlécen alapuló mechanizmus, ami megmondja (szerver oldalon), hogy milyen más eredettel rendelkező böngésző férhet hozzá egy erőforráshoz.

Clickjacking

A clickjacking során a felhasználó egy láthatatlan vagy más elemnek álcázott weblapelemre kattint. Ez rosszindulatú programok letöltéséhez, más, káros weboldalak megnyitásához, hitelesítő adatok és érzékeny információk ellopásához vezethet. A Frame Busting és az X-Frame-Options együttes használata ugyanakkor védelmet nyújthat a clickjacking ellen.

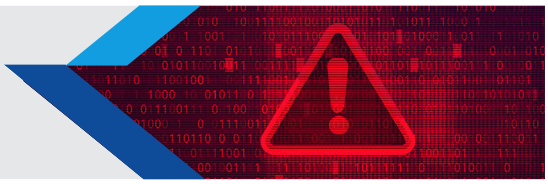
WebSockets

A WebSocket-ek nagy mértékben leegyszerűsítik az ügyfél és a kiszolgáló közötti kommunikációt. A protokoll az OSI modell alkalmazási rétegét használja a kétirányú kommunikációhoz, ami lehetővé teszi a dinamikus, valós idejű webalkalmazások létrehozását. Ha a kommunikáció nem a TLS protokoll használatával jön létre, akkor az hálózati szinten manipulálható lesz és olyan típusú támadásokhoz vezethet, mint a Sniffing, a Cross-Site WebSocket Hijacking (CSWSH), Cross-Site Request Forgery Vulnerability (CSRF), DoS támadások vagy tunneling. Az ilyen jellegű támadások kivédésére ajánlott ws:// helyett wss://-t, felhasználói input és szerveroldali adat validálást használni és mellőzni a tunnelinget.

Helyi tárolás

Ezek a sebezhetőségek akkor keletkeznek, amikor egy szkript a támadó által ellenőrzött adatokat tárol a webböngésző HTML5 tárolójában (sessionStorage, localStorage). A támadó ezt felhasználhatja arra, hogy olyan URL címet készítsen, amelyet, ha egy másik felhasználó meglátogat, akkor a felhasználó böngészője a támadó által ellenőrzött adatokat töltse be. Elkerüléséhez meg kell akadályozni, hogy bármilyen nem megbízható forrásból származó adat kerüljön be a HTML5 tárolóba.

Egyéb technikák



Számos egyéb technika létezik a támadók repertoárjában, amelyeket nem kizárólagosan e-commerce webáruház támadására használnak, azonban azok is áldozatul eshetnek. Ilyenek például a pénzügyi csalások, a pszichológiai manipuláció, az adathalászat, a rosszindulatú botok, a túlterheléses (DoS, DDoS) és Brute Force támadások a weboldal ellehetetlenítésére és teljes körű hozzáférés megszerzése érdekében, valamint zsarolóvírusok és malware-ek végtelen tárháza.

A korábban kiadott CMS rendszerek biztonsága című elemzésünkben kimondottan a CMS alapú rendszerekkel, azon belül is a WordPress biztonsági kihívásaival foglalkozunk.

További hasznos információkat olvashat a legkritikusabb biztonsági kockázatokról az OWASP oldalán.

Az NBSZ NKI javaslatai az online vásárlások során

- Használjunk HTTPS protokollt a webes felületeinken! A HTTP mára már elavultnak számít és nem biztosít biztonságos kommunikációt a kliens és a szerver között. Szükséges hozzá, hogy a tárhelyszolgáltató biztosítson SSL tanúsítványt. Habár nem ez a legfőbb érv a használata mellett, azonban üzleti szempontjából sem elhanyagolható, hogy a Google jobb helyre rangsorol egy olyan oldalt, amely HTTP helyett HTTPS-t használ.

- Rendkívül fontos a cégeknél valamilyen biztonságtudatossági képzés alkalmazása, ezzel naprakészen tartva a munkatársak tudását. Magánszemélyként fontos az önképzés, tájékozódjunk időnként a legújabb biztonsági kockázatokról és kampányokról, hogy ezzel is frissen tartsuk tudásunkat!

- Ha egy eddig ismeretlen személy keres meg bennünket egy már szerződött, ismert cégtől, győződjünk meg a megkereső hitelességéről egyéb kontakton keresztül! A pénzügyi csalások rendszerint úgy indulnak, hogy a csaló egy legitim személynek (cégnek) adja ki magát, és arra alapoz, hogy az áldozat figyelmetlen lesz.

- Soha ne tároljunk hitelkártya adatokat a szervereinken! Egy esetleges adatszivárgás után nem csak a cég hírneve mehet tönkre, azonban bírósági pereket követően hatalmas kártérítéseket is fizethetünk a károsultaknak.

- Opcionálisan használhatunk harmadik féltől származó fizetési rendszereket, mint például PayPal, Skrill vagy Stripe. Ez a vásárlóink számára is garanciát nyújt.
- Mobileszközeinkkel, laptopokkal mindig kerüljük el a nyilvános Wi-Fi hálózatokat, használjunk helyettük mobil internetet!
- Lehetőség szerint mindig használjunk VPN szolgáltatást!
- Mindig használjunk többfaktoros hitelesítést, ahol csak lehetőségünk van rá!
- Készítsünk rendszeresen biztonsági mentéseket az adatainkról! Alkalmazzunk automatikus biztonsági mentési szolgáltatást!
- Kísérjük figyelemmel a logfájlokat, tájékozódjon belőlük!
- Biztosítsunk minél hosszabb ideig tartó ügyfélszolgálatot, amivel a vásárlóink könnyedén a kapcsolatba tudnak lépni velünk technikai problémák esetén!
- Csökkentsük az ügyfelek által kitöltendő mezők számát! Ha a vásárlóknak nem kell megadniuk túl sok személyes adatot, úgy érezhetik, hogy kevesebb kockázatot vállalnak és ezzel a GDPR adattakarékossági elvének is eleget teszünk.
- Készítsünk DRP (Disaster Recovery Plan) stratégiát! A DRP dokumentáltan és strukturáltan leírja, hogy egy szervezet hogyan tudja a lehető leggyorsabban megoldani a váratlanul adódott problémákat. Előfordulhatnak alkalmazáshibák, kommunikációs hibák, kibertámadás áldozatává válhatunk, érhetnek minket különféle (építési, természeti, nemzeti,

regionális stb.) katasztrófák, amelyekre célszerű előzetesen felkészülni, hogy a szokványos munkamenetek mielőbb helyreálljanak.

- Választhatunk olyan menedzselt e-kereskedelmi webtárhelyszolgáltatást, amely automatikusan készít biztonsági mentéseket számunkra, mint például a Cloudways.

- A már nem szükséges papíralapú dokumentumokat, amelyek személyes és érzékeny adatokat tartalmaznak, ne dobjuk csak egyszerűen a szemétbe, hanem semmisítsük meg olyan módon, hogy azon ne maradjon visszanyerhető információ!

- Ha pénzügyi csalás áldozatává váltunk, azonnal jelentsük a bankunknál és az illetékes hatóságoknál!

Milyen szempontokat érdemes figyelembe venni jelszóválasztásnál?

- Ne legyen ránk jellemző, mert kevés információ birtokában is könnyen kitalálható (pl.: családtag neve + születési dátum egy rövid kereséssel a közösségi oldalakon kideríthető).
- Nem szerencsés, ha a jelszó csak egy szóból áll (például az „almafa" szó biztosan szerepel egy támadó által kipróbálandó jelszavak listájában).
- Jó, ha a jelszó hosszú és többféle karaktert (kisbetű, nagybetű, szám, írásjel) tartalmaz, mert ezzel megnehezíti a brute force technikával való feltörést.
- A legjobb, ha néhány szóból álló jelmondatot választunk, amelyben van kisbetű, nagybetű, szám és írásjel is. Ezt könnyű megjegyezni, azonban nehéz kitalálni, brute force technikával feltörni pedig szinte lehetetlen.

Hogyan kezeljük a jelszavainkat?

- Fontos, hogy ne adjuk „kölcsön" a jelszavunkat, hiszen nem tudhatjuk, hogy az adott személy körültekintően fogja-e kezelni.
- Ne írjuk fel a jelszavunkat, mert ez könnyen illetéktelen kezekbe kerülhet.
- Ne használjuk mindenhol ugyanazt a jelszót, ha a támadók egyet feltörnek, minden más rendszerünkhöz is hozzáférhetnek.
- Rendszeresen változtassuk meg a jelszavainkat, a támadónak minél több ideje van próbálkozni, annál nagyobb valószínűséggel tudja megszerezni a hozzáférésünket.
- Használjunk valamilyen jelszókezelő rendszert! Ezek olyan szoftverek, amelyek titkosított formában tárolják jelszavainkat, így azokhoz illetéktelenek (ideális esetben) nem – vagy csak irreálisan nagy erőforrás ráfordításával – férhetnek hozzá. A megoldás előnye, hogy ehhez csupán egyetlen, ún. mesterjelszót kell fejben tartanunk, azt, amellyel hozzáférhetünk az elmentett jelszavakhoz. A jelszókezelőkről bővebben az NBSZ NKI weboldalán itt írtunk.

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2022