CTI elemzés

A deep web rejtelmei

1996

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERBIZTONSÁGI INTÉZET

Tartalomjegyzék

Bevezetés 4

Mi is az a deep web valójában? 5

Mi a különbség a deep web és a dark web között? 6

Példák a deep weben elérhető weboldalakra 7

A deep web legfőbb jellemzői 10

A deep web kiberbiztonsági kockázatai 12

Kártevők és kihasználhatósági rések 13

Adatvédelmi és kinyerési fenyegetések 14

Hálózati és belső fenyegetések felerősödése 15

Működési és megfelelési kockázatok 15

Esettanulmányok 16

Facebook API incidens 16

Jaguár Land Rover adatszivárgás 17

Ajánlások 18

Források 20

Bevezetés

Az internet felépítését általában 3 rétegre szokták bontani: az első réteg az úgynevezett „surface web”, azaz felszíni web, amely az internet nagyjából 5-10%-nak felel meg. Itt található minden olyan weboldal, amelyet hagyományos keresőmotorok segítségével meglátogathatunk. Ilyennek számíthatnak például a különböző online hírlapok vagy Wikipedia oldalak. A WorldWideWebSize adatai alapján 2025 januárjában nagyjából 3.98 milliárd volt az indexelt weboldalak száma.

Az internet százalékos felépítése
Kép forrása: AdobeStock

Léteznek azonban olyan oldalak is, amelyeket a sztenderd keresőmotorok nem érnek el, mégis szerves részét képezik a mindennapi online jelenlétünknek. Ezeken a rejtett oldalakon zajlik az internet adatforgalmának jelentős hányada: egyes számítások szerint nagyjából a 90%-a. Ide sorolhatók például a különböző

intézményi rendszerek, tudományos archívumok, streaming szolgáltatók és minden olyan weboldal, ahol bejelentkezés szükséges a további funkcionalitás eléréséhez. Ide tartoznak a gyakran sötét webként emlegetett oldalak is, bár fontos kiemelni, hogy a deep web és a dark web nem ugyanaz. A két terület között jelentős különbségek vannak. A dark webről készült jelentésünket az alábbi linken tekintheti meg.

Ezen jelentésünk célja betekintést nyerni ebbe a kevésbé ismert, gyakran félreértett világba azáltal, hogy bemutatjuk működésének alapelveit, kockázatait, és hogy miért fontos felelősségteljes felhasználóként használni.

Mi is az a deep web valójában?

A „deep web” elnevezést Michael K. Bergman alkotta meg a 2001-ben megjelenő *„The Deep Web: Surfacing the Hidden Value”* című tanulmányában. Jill Ellsworth 1994-ben az „invisible web” (azaz láthatatlan web) kifejezést használta azokra az információkra, amelyek láthatatlanok maradtak az akkoriban használt konvencionális keresőmotorok számára; Bergman alapvetően megtartotta ezt a meghatározást, de a láthatatlan jelzőt nem használta, mert célja sokkal inkább az ezen oldalak azonosításának és kereshetőségének javítása volt. Bergman tanulmánya vált végül a közismert, leginkább átfogó kutatássá a webkutatók közösségének keretein belül, ennek eredményeképpen pedig a deep web elnevezés vált végül a közismert, hivatalos elnevezéssé.

A mai hivatalos definíció alapján tehát a deep web az olyan tartalmak gyűjtőneveként szolgál, amelyeket a konvencionális

keresőmotorok (pl. Google vagy Yahoo) egyszerű keresés során nem indexelnek, más szóval nem fednek le, így célzott megközelítést igényelnek.

Mi a különbség a deep web és a dark web között?

Gyakori hibának mondható a deep- és dark web elnevezések felváltva történő használata. Ez a félreértés onnan eredeztethető, hogy a felhasználási alapelveik hasonlóak, az egyik a másik részhalmazának tekinthető. Mindkét esetben nem indexelhető webhelyekről beszélhetünk annyi különbséggel, hogy a dark web még csak hozzá sem férhető hagyományos keresőmotorok használatával, külön erre specializálódott böngészők használata szükséges a hozzáféréshez (pl. TOR).

A médiában gyakran minden olyan weboldalt, amely hagyományos böngészőkkel nem érhető el, automatikusan titkos vagy illegális piactérként ábrázolnak, aminek következtében a dark web ezeknek az oldalaknak a szinonimájaként rögzült a köztudatban. A technikai ismeretek hiánya tovább erősíti azt a tévképzetet, hogy a szaknyelvben „elérhetetlennek" nevezett tartalmak szükségszerűen különösen titkosak vagy rendkívüliek, holott ez a megjelölés jellemzően csupán a keresőmotorok által nem indexelt weboldalakra utal. A fogalmi zavarhoz hozzájárul az is, hogy a köznyelvben használt „láthatatlan web" kifejezés nem önálló technikai kategória, hanem elsősorban a deep web gyűjtőmegnevezéseként jelenik meg. Ennek következtében sokan nincsenek tisztában azzal, hogy a deep web valójában a mindennapok során rendszeresen használt, jellemzően legális és belépéshez kötött webes szolgáltatásokat foglalja magában, amelyek annyira szervesen beépültek a hétköznapi internethasználatba, hogy fel sem

merül a különbség az egyszerűen elérhető, felszíni weben található tartalmakkal szemben, miközben a dark web e körnek csupán egy szűk, technikailag elkülönülő részét képezi.

Példák a deep weben elérhető weboldalakra

Ahogy már korábban említésre került, a deep weben elérhető oldalak korlátozott hozzáférésre készültek, amelyeket például fizetési kötelezettség vagy regisztráció véd a nyilvánosságtól. Természetesen ez nem azt jelenti, hogy ezek az oldalak kivétel nélkül nehezen hozzáférhetők lennének; éppen ellenkezőleg, számos esetben nyilvános oldalakhoz köthetők, egyszerűen csak nem indexelődnek be például technikai beállítások, dinamikus tartalomgenerálás vagy jelszavas védelem miatt. Más szóval: a deep web nem feltétlenül egy „rejtett világ", hanem az internet azon rétegét jelenti, amelynek tartalmához a hozzáférés gyakran közvetlen, célzott kereséssel vagy jogosultsággal lehetséges, azaz nem nehezebb, mint más oldalak esetében, mindössze eltérő módon konfigurált vagy szervezett.

A nem indexelhető weboldalak rendezéséről átfogó tanulmány, vagy szakmabeli megállapodás még nem született, így az alábbiak szerint csoportosítottuk őket:

Fizetős szolgáltatások és prémium tartalmak

Ez a kategória olyan oldalakból áll, ahol a hozzáférés előfizetéshez vagy egyszeri fizetéshez kötött. Ide tartoznak például online folyóiratok, szakcikkek, kutatási adatbázisok (pl. tudományos publikációk), valamint digitális könyvtárak. Ezek az oldalak csak regisztrált vagy előfizető felhasználók számára elérhetők, és biztonsági mechanizmusok szükségesek hozzáférésükhöz. Ezen oldalak a tudományos kutatások és üzleti döntések alapjául szolgálnak, mivel naprakész, hiteles információkat kínálnak, amelyek nem találhatók meg a nyilvános keresőmotorokban.

Rejtett adatbázisok és információs rendszerek

A deep web egyik jelentős részét a strukturált adatbázisok teszik ki. Ezek az adatbázisok olyan információkat tárolnak, amelyeket nem lehet egyszerű link- vagy kulcsszókereséssel lekérdezni. Ide sorolhatók például kormányzati adatbázisok, egészségügyi nyilvántartások, bírósági ítéletek, jogi dokumentumok, hivatalos statisztikák vagy pénzügyi jelentések. Ezek a források rendszerint speciális keresőfelületeket vagy hitelesítést igényelnek, így az információkhoz csak a jogosult felhasználók férhetnek hozzá.

Céges és üzleti platformok

Ez a szegmens magában foglalja például azokat a vállalati intraneteket, B2B (business-to-business) rendszereket, belső

információs portálokat, valamint más üzleti célú platformokat, amelyek zárt környezetben működnek. Ezen oldalakat elzárják a nyilvánosság elől, mivel üzleti titkokat, ügyféladatokat vagy belső folyamatokat tartalmaznak. Ezek az oldalak rendszerint VPN segítségével férhetők hozzá, és általában erős jelszavas védelem és/vagy biztonsági protokollok kapcsolódnak hozzájuk, a hozzáférési jogosultságok pedig rendszerint szigorúan szabályozottak.

Dinamikusan generált oldalak

Ezek az oldalak nem statikus tartalmat kínálnak, hanem a felhasználói kérésnek megfelelően állítják elő a megjelenített információt, például keresési eredmények vagy lekérdezések alapján. A keresőrobotok számára technikai szempontból ezek az oldalak gyakran elérhetetlenek, mivel az URL-ek előre nem ismertek vagy csak interakció útján generálódnak. Ilyen típusú oldalak például a repülőjáratok státuszát mutató oldalak, a kérdőív-felvétel eredményeit bemutató oldalak vagy az online banki felületek.

Személyes profilok és közösségi média oldalainak részhalmazai

Számos közösségi média vagy webszolgáltatás tartalmaz mélyweb oldalakat, mint például privát profilok, beállítási oldalak, üzenetküldő rendszerek és egyéb, csak bejelentkezést követően elérhető tartalmak. Ezek az oldalak személyes vagy vállalati adatokkal dolgoznak, és hozzáférésük biztonsági szempontból kritikus lehet, így nem publikusak.

Speciális kutatási és tudományos erőforrások

A tudományos életben rengeteg adatbázis, mint például PubMed, JSTOR vagy egyetemek digitális archívuma is ebbe a körbe tartozik. Ezek a források szakmai és tudományos dolgozatokat, kutatói anyagokat, konferencia előadásokat vagy egyéb releváns dokumentumokat tartalmaznak, amelyekhez általában kizárólag regisztrált kutatók, hallgatók vagy egyetemi oktatók férnek hozzá.

A deep web legfőbb jellemzői

Felmerülhet a kérdés, hogy miért is van pontosan szükség a nem indexelhető weboldalakra? Képzeljük el, hogy a vállalati rendszerünk – ahol bizalmas ügyféladatokat kezelünk, és a privát levelezésünket intézzük – egy egyszerű hivatkozással bárki számára elérhetővé válna. Egy ilyen állapot teljes biztonsági káoszállapotot jelentene; és egyébként jelent is, ha a deep webre szánt oldalak nem rendelkeznek a megfelelő biztonsági előírásoknak megfelelő beállításoknak.

A mélyweb tartalmaihoz való hozzáférés nem igényel összetett eljárásokat, és kompatibilis a legtöbb telekommunikációs eszközzel anélkül, hogy speciális keresőmotorokat kellene telepíteni, szemben a dark web esetében szükséges hálózati kliensekkel. A kizárólagos akadályt gyakran a földrajzi korlátozások jelentik, amelyek egyes tartalmakat (pl. streaming platformok országonként eltérő kínálatát) elérhetetlenné tesznek. E korlátok áthidalására kiváló megoldás egy megbízható VPN-szolgáltatás alkalmazása, amely maszkolja a felhasználó IP-címét, így lehetővé téve a hazai tartalmak elérését külföldi tartózkodás során is.

A deep weben található tartalmak a felszíni webbel ellentétben rejtve

TUDTAD-E?

A mélyweb egyes részeihez feltehetőleg még soha nem fértek hozzá.

maradnak a keresések során, ennek oka pedig egyrészt az, hogy adatbázisokból szerzik információikat, másrészt az úgynevezett crawler programok működésében keresendő. A web crawlerek olyan automatizált szoftverek, amelyeket kifejezetten arra fejlesztettek, hogy az internet folyamatos bejárásával feltérképezzék és indexeljék a weboldalak tartalmát, valamint segítsék a keresőmotorokat az oldalak felfedezésében és ellenőrzésében. A legismertebb crawlerek közé tartozik például a Googlebot és a YandexBot. A deep weben található tartalmak abban különböznek, hogy a crawler programok nem képesek ezeket feltárni és a keresési eredmények között megjeleníteni. Ezek a tartalmak valamilyen módon elérési korláthoz kötődnek. Ilyen korlát lehet például a kötelező azonosítás, amikor e mail cím és jelszó páros szükséges a belépéshez, vagy egy adott szolgáltatás előfizetése. Ennek a fajta szűrőnek több előnye is van. Egyrészt lehetővé teszi, hogy a keresőmotorok ne zúdítsanak ránk kezelhetetlen mennyiségű találatot, ami megnehezítené a valóban releváns információk megtalálását. Másrészt fontos adatvédelmi funkciót lát el. Ennek köszönhetően személyes adatok, például egészségügyi információk vagy az egyének kórelőzményei nem jelennek meg akkor sem, amikor különböző betegségekre keresünk rá.

A deep web kiberbiztonsági kockázatai

A láthatatlan web alapvetően egy biztonságos rendszernek tűnhet anonimitása és „láthatatlansága" miatt, de ugyanezen jellemzők teszik rendkívül kitetté a kockázatokkal szemben. Ennek hatására

a rosszindulatú szereplők is képesek olyan ellenálló és rejtett infrastruktúrát kialakítani, amelyek képesek megkerülni a hagyományos biztonsági mechanizmusokat, vagy éppen olyan célokra tudják őket felhasználni, amelyek egy nyilvános internetes környezetben nehezen lennének megvalósíthatók. Ez magában foglalhatja botnetek működtetését, adatlopó kampányok és kémkedési műveletek elrejtését, valamint komplex kibertámadásokat, melyek ellen a hagyományos védekezési eszközök kevésbé hatékonyak. Mindez egy olyan komplex és dinamikus fenyegetési környezetet teremt, amely folyamatos kihívást jelent a kiberbiztonsági szakemberek számára.

Kártevők és kihasználhatósági rések

A mélyweb megfelelő környezetet biztosíthat a fejlett kártevők elterjedésének a felügyelet nélküli csatornákon - mint például privát fórumok és rejtett fizetési átjárók - keresztül. A kibertámadók kihasználják a dinamikus tartalom-generálást, hogy drive-by letöltéseket és exploit kit-eket juttassanak célba a böngésző sebezhetőségei ellen. Például a botnetek gyakran alkalmaznak olyan rejtőzködő infrastruktúrákat és technikákat, mint a fast flux DNS és a domain generation algoritmusok, valamint különféle mechanizmusokat építenek be a sinkholing és az infrastruktúra lefoglalása elleni ellenállás növelésére. Ezek célja, hogy a C2 szerverek ne legyenek könnyen azonosíthatók vagy felszámolhatók, ami jelentősen megnehezíti a hatósági beavatkozást. A felhasználók, akik fájlokat töltenek le látszólag legitim mélyweb-tárhelyekről, kockáztatják a ransomware-fertőzéseket, amelyek titkosíthatják a kritikus adatokat.

Adatvédelmi és kinyerési fenyegetések

Elsődleges kockázatot jelenthet az érzékeny információk kiszivárgása olyan hitelesítő adatok révén, amelyek vállalati rendszerekből vagy személyes fiókokból származó kompromittálódás után deep web környezetekben jelennek meg. A támadók, legyenek külső behatolók vagy kompromittált belső fiókokat kihasználó szereplők, gyakran deep web alapú infrastruktúrákat alkalmaznak ipari vagy üzleti adatok kinyerésére. Ennek során titkosított kommunikációs csatornákat és legitim protokollokra épülő adatátvitelt használnak, amelyek megnehezítik a hagyományos hálózati védelmi eszközök észlelését.

A credential stuffing támadások tovább növelik ezt a kockázatot, mivel korábbi adatvédelmi incidensekből származó bejelentkezési adatok automatizált módon kerülhetnek felhasználásra például banki

portálok vagy vállalati intranetek ellen. Ez személyazonosság lopáshoz, jogosulatlan hozzáféréshez és közvetlen anyagi veszteségekhez vezethet. A többfaktoros hitelesítés és fejlett végpontdetektálási megoldások hiányában az ilyen behatolások hosszú időn keresztül észrevétlenek maradhatnak.

Hálózati és belső fenyegetések felerősödése

A nem engedélyezett proxy vagy VPN használat megkerüli a standard vállalati biztonsági vezérléseket. Ez lehetővé teszi, hogy belső dolgozók a forgalmat olyan rejtett csatornákon továbbítsák, amelyeket a felügyeleti eszközök nem látnak. Az ilyen forgalom növelheti a hálózati terhelést és megnehezíti a támadások észlelését, noha valódi DDoS állapotot nem idéz elő. A munkavállalók által alkalmazott kontrollkerülési technikák, például geo blokkok megkerülése vagy anonim hozzáférési módszerek használata, ténylegesen bővítik a belső fenyegetési vektorokat és csökkentik a biztonsági láthatóságot. Az anonimizáló infrastruktúrák alkalmasak arra, hogy ellenállóbb botnet műveletek C2 csatornái legyenek, mivel a fertőzött eszközök ilyen rejtett hálózatokon keresztül kapcsolódhatnak egy nagyobb ökoszisztémához, különösen dark web alapú szolgáltatásokon. Ez tartós, nehezen felszámolható fenyegetések fennmaradását segítheti elő.

Működési és megfelelési kockázatok

A szervezetek megfelelési kockázatoknak vannak kitéve, amikor nem engedélyezett anonim hozzáférési eszközök vagy külső szolgáltatások használata sérti a szabályozási elvárásokat. Ilyen lehet például a GDPR megsértése nem megfelelően titkosított adatkezelési csatornák alkalmazása miatt. A rejtett vagy korlátozottan látható online tartalmak feldolgozása folyamatos alkalmazkodást igényel, mivel a

felügyeleti rendszerek gyakran nehezen kezelik az ilyen forrásokból származó nagy mennyiségű, heterogén adatot. Különösen nagy kihívást jelent a releváns fenyegetésjelzések azonosítása és elkülönítése a zajtól, vagyis az ismétlődő, irreleváns vagy félrevezető információktól. További kockázatot jelentenek a beszállítói lánc kompromittálódások, ahol harmadik féltől származó szolgáltatásokon keresztül kerülhetnek be sérülékenységek vagy zero-day exploitok, ami kiemeli a proaktív fenyegetés-hírszerzés szükségességét a hagyományos felszíni webes monitoringon túl.

Esettanulmányok

Facebook API incidens

2025 májusában egy masszív, összesen 1,2 milliárd felhasználói rekordot tartalmazó adatbázist loptak el a Facebookról az egyik API visszaélésszerű használatával. A Meta nyilatkozatában nem tagadta, hogy az adatlopás megtörtént. Kiberbiztonsági szakértők szerint az adathalmazban felhasználó azonosítók, nevek, e-mail címek, felhasználónevek, telefonszámok, helyszínek, születésnapok és az érintettek neme is feltüntetésre került; bár a szakértők szerint érdemes ezt az 1,2 milliárdos számot fenntartásokkal kezelni, az ismétlődő incidensek arra engednek következtetni, hogy a Meta biztonsági intézkedései inkább reaktívak, mintsem proaktívak.

Az API-k egyre inkább a modern digitális ökoszisztémák elengedhetetlen részévé válnak, mivel lehetővé teszik a felhőszolgáltatások, IoT-eszközök és szoftveralkalmazások közötti zökkenőmentes összeköttetést és integrációt. A vállalkozások

folyamatosan nagyobb hatékonyságra és interoperabilitásra törekszenek, mely láncolatban az API-k biztosítják azokat a nélkülözhetetlen kapcsolatokat, amelyek megkönnyítik a különböző rendszerek, alkalmazások és harmadik félhez köthető szolgáltatások közötti kommunikációt. Az API-k széles körű használata azonban komoly kockázatokat is rejthet magában: a hagyományos alkalmazásokkal ellentétben az API-k gyakran feltárják a belső üzleti működést és adatstruktúrákat, amelyek miatt jobban kitetté válnak a célzott támadásoknak. Mivel ezek az ökoszisztémák rendkívül összetett rendszert alkotnak, amelyek gyakran több végpontot, hitelesítési mechanizmust és harmadik feleket érintő integrációt tartalmaznak, így a potenciális támadási felület is megnő. Ezen felületek nem megfelelő biztosítása beláthatatlan és jelentős kockázatokat tarthat magában, mint ahogy a Facebook május adatszivárgási példáján is láthattuk.

Jaguár Land Rover adatszivárgás

2025 márciusában a Jaguar Land Rover egy kiberbiztonsági incidens áldozata lett, melyet a ShinyHunters nevű hekkercsoport vállalt magára. Ebben az esetben a támadók hozzáfértek a vállalat egy harmadik fél, a Cognizant SharePoint rendszeréhez, amelyen keresztül mintegy 50.000 volt és jelenlegi alkalmazott személyes adatait szerezték meg, beleértve neveket, telefonszámokat, e-maileket, fizetési információkat és lakcímeket. Az ellopott adatokat később mélywebes fórumokon értékesítették. A Jaguar Land Rover megerősítette az incidens tényét, értesítette az érintetteket, és hangsúlyozta, hogy ügyféladatok ellopására nincs bizonyíték. Az eset rávilágított a harmadik felek biztonsági kockázataira is, és felhívta a figyelmet a felhőalapú rendszerek védelmének fontosságára, különösen az MFA hiányára és a sebezhetőségek gyors kezelésének szükségességére.

Ajánlások

A deep web fiókok védelme során alapvető fontosságú a **többlépcsős hitelesítés (MFA) alkalmazása**, amellyel jelentősen csökkenthető az illetéktelen hozzáférés kockázata, még akkor is, ha valamilyen módon a jelszó kompromittálódna. A többlépcsős hitelesítés segít megakadályozni, hogy egyetlen lopott hitelesítési adat hozzáférést biztosítson a fiókhoz, így a támadók előretörését megállítja a második vagy harmadik hitelesítési tényező megléte. Továbbá alapvető a rendszeres szoftverfrissítés és a sérülékenységek mihamarabbi patchelése, ugyanis a folyamatos karbantartás révén megelőzhető, hogy ismert biztonsági rések kihasználásával behatoljanak a rendszerekbe.

Fontos szempont továbbá a **tűzfalak és behatolás-megelőző rendszerek (IDS/IPS) alkalmazása**, melyek képesek valós időben szűrni és blokkolni a gyanús hálózati forgalmat, ezáltal védelmet nyújtanak a céges fiókok és rendszerek számára. Ezek a rendszerek főleg a behatolási kísérletek, ismert exploitok és rosszindulatú forgalom ellen jelentenek első védelmi vonalat, így elengedhetetlen komponensei a deep webes fiókok védelmének. A vállalati webes környezetek üzemeltetése során kiemelt jelentősége van a **Zero Trust elv** következetes alkalmazásának, amely kizárólag ellenőrzött hozzáférést és a feladatellátáshoz feltétlenül szükséges minimális jogosultságokat biztosít a felhasználók és szolgáltatások számára, ezáltal csökkentve a jogosultságokkal való visszaélés kockázatát. Továbbá elengedhetetlen a **folyamatos szakmai tanulás és a tudatosság növelése**, hiszen az emberi tényező még mindig az egyik legnagyobb kockázat forrása. A dolgozók rendszeres képzése, az aktualizált biztonsági protokollok megismerése, és a social engineering támadások elleni

felkészülés mind hozzájárulnak a mélyebb védelmi szint kialakításához. Nem szabad megfeledkezni a **rendszeres biztonsági auditokról** sem, amelyek feltérképezik az esetleges gyenge pontokat és lehetőséget adnak ezek kijavítására.

A céges intranetek üzemeltetésénél az infrastruktúra szigorú biztonsági ellenőrzése, az adatmentési stratégiák felállítása, valamint hálózati szegmentáció megvalósítása alapvető követelmény. A hálózati szegmentáció csökkenti az esetleges betörések által elérhető károkat, mert elkülöníti az érzékeny és kevésbé kritikus infrastruktúrát. Ugyancsak javasolt a **fejlett viselkedéselemző rendszerek** (UEBA) és **automatizált javításkezelő megoldások** bevezetése, amelyek minimalizálják az emberi mulasztásból adódó kockázatokat és gyorsabb reagálást tesznek lehetővé a fenyegetések esetén.

Összegzésképp a deep web fiókok védelme egy **komplex, többrétegű megközelítést igényel**, melyben a többfaktoros hitelesítés, a sebezhetőségek folyamatos foltozása, a tűzfalak és behatolás-védelmi rendszerek állandó alkalmazása, valamint a folyamatos szakmai tudatosság is mind kulcsfontosságú elemek. A vállalati környezetben ezen felül hangsúlyosak a biztonsági auditok, a titkosítás, valamint a hozzáférési jogosultságok szigorú kontrollja és hálózati elkülönítése is a hatékony gyakorlatok között szerepelnek.

Források

SJOUWERMAN, STU. (2017) *Surface Web vs. Deep Web vs. Dark Web: Differences Explained.* https://blog.knowbe4.com/what-is-the-difference-between-the-surface-web-the-deep-web-and-the-dark-web (Letöltve: 2025. december 04.)

WORLDWIDEWEBSIZE. (2025) *The size of the World Wide Web (The Internet).* https://www.worldwidewebsize.com/ (Letöltve: 2025. december 04.)

PATRIZIO, ANDY. (2021) *Deep web definition.* https://www.techtarget.com/whatis/definition/deep-Web (Letöltve: 2025. december 08.)

RANKTRACKER. *Lánctalpas.* https://www.ranktracker.com/hu/seo/glossary/crawler/ (Letöltve: 2025. november 24.)

DR. SERBAKOV MÁRTON TIBOR. (2020) *Kriminalitás a dark weben: illegális piacok, pedofil oldalak, terroristák és az ellenük való küzdelem.* ORAC Kiadó, Budapest. Büntetőjogi Szemle. 2020/1. pp. 91-107.

PETER. (2024) *Hogyan férhet hozzá a Deep Webhez, és mit találhat ott.* https://eoldal.hu/hogyan-ferhet-hozza-a-deep-webhez-es-mit-talalhat-ott/ (Letöltve: 2025. november 27.)

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT NEMZETI KIBERBIZTONSÁGI INTÉZET. (2019) *Visszaélések a kibertérben.* https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/visszaelesek-a-kiberterben/ (Letöltve: 2025. november 27.)

EIMT. (2025) *Top 30 Best-Known Cybersecurity Case Studies 2025.* https://www.eimt.edu.eu/top-best-known-cybersecurity-case-studies (Letöltve: 2025. november 28.)

PETKAUSKAS, VILIUS. *Jaguar Land Rover's source code, tracking data leaked, attackers claim.* https://cybernews.com/security/jaguar-land-rover-data-breach-security-risks/ (Letöltve: 2025. november 28.)

PETKAUSKAS, VILIUS. (2025) *Major Facebook data leak reveals 1.2 billion user records, hacker claims.* https://cybernews.com/security/facebook-leak-exposes-users-hackers-claim/ (Letöltve: 2025. december 01.)

WNE SECURITY. (2025) *Why Hackers Are Targeting APIs: Emerging Threats in API Security.* https://wnesecurity.com/why-hackers-are-targeting-apis-emerging-threats-in-api-security/ (Letöltve: 2025. november 28.)

TUBAISHAT, ABDALLAH. (2023) *Security Issues in the Deep and Dark Web: What to know?* https://dl.acm.org/doi/fullHtml/10.1145/3634848.3634849 (Letöltve: 2025. december 01.)

NEMZETI
KIBERBIZTONSÁGI
INTÉZET

Kibertámadás!
podcast

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet

titkarsag@nki.gov.hu

nki.gov.hu

+36 (1) 325 7672

2026