Cyber Signals: egyre több kibertámadás éri a sportesemányeket és helyszíneiket

A sport– és szórakoztató rendezvények gördülékenyebb és kényelmesebb lebonyolításához egyre több digitális szolgáltatást vesznek igénybe a helyszínt biztosító intézmények és a szervezők. Emiatt megnőtt a háttérinfrastruktúrák sérülékenysége, kedvező célpontot kínálva a kiberbűnözőknek. A Cyber Signals ötödik kiadása arra hívja fel a figyelmet, hogy milyen sokrétű kiberbiztonsági előkészületekre van szükség ahhoz, hogy a rendezést vállaló intézmények infrastruktúrája mellett a sportolók, sportszövetségek és szponzorok, valamint a rendezvényeket látogató közönség adatai védve legyenek a kibertámadásoktól.

A Cyber Signals ötödik kiadása szerint – amelyet a Microsoft a közelmúltban hozott nyilvánosságra – a nagy rendezvényhelyszínek, a sport- és szórakoztató események sincsenek ma már biztonságban a kiberbűnözőktől. A Microsoft látta el a 2022-ben Katarban megrendezett FIFA futball világbajnokság kritikus létesítményeinek védelmét, amely közben több mint 100 000 végponti eszközt, 144 000 accountot, 14,6 millió emailt ellenőriztek, és mintegy 635 millió alkalommal hitelesítettek hálózatba történő belépést. A rendezvény biztosítása közben összegyűlt tapasztalataikat is összegezték a tanulmányban.

A sportrendezvényeket világszerte egyre több kibertámadás éri. Az Egyesült Királyság Nemzeti Kiberbiztonsági Központja (NCSC) által nemrégiben közzé tett felmérés szerint a sportszervezetek 70%-a tapasztal évente legalább egy támadást, ami jelentősen magasabb szám annál, mint amit a brit vállalkozásoknál általában regisztráltak. A Manchester United tavaly novemberben számolt be a rendszereiket ért súlyos támadásról, idén év elején pedig az amerikai NBA bajnokság szurkolóinak az adatai kerültek egy adathalász incidens utánilletéktelen kezekbe.

A nagyrendezvényeket és rendezvényhelyszíneket érő fenyegetések egyre sokrétűbbek és összetettebbek. A megelőzésükhöz, az esetleges károk mérsékléséhez a támadási kísérletek folyamatos nyomonkövetésére és az érintettekkel történő szoros együttműködésre van szükség. A világ sport-szórakoztatási piacának forgalmát ma több mint 600 milliárd dollárra becsülik; a csapatok, a jelentősebb bajnokságok szervezői, a nemzetközi sportszövetségek és a látogatók temérdek olyan információ birtokában vannak, amelyekre a kiberbűnözőkneknagyon fáj a foga.

Ez az információ sajnos egyre könnyebben hozzáférhető a bűnözők számára, hiszen egyre több helyszín, eszköz és hálózat kerül összeköttetésbe egymással. A helyszínt biztosító létesítmények IT-rendszerei, a stadionok és sportcsarnokok százszámra kínálnak ismert és kevésbé ismert biztonsági réseket. Ezek pedig módot adnak a támadóknak arra, hogy célba vegyék az üzleti szolgáltatásokat nyújtó infrastruktúrát – például az elárusító pontokat, az IT rendszereket – valamint a látogatók eszközeit. A csapatok, az edzők és maguk a sportolók iski vannak téve annak a veszélynek, hogy a teljesítményükről és a versenyben előnyt jelentő képességeikről szóló információkat, illetve a személyes adataikat illetéktelenek megszerzik. A látogatók személyes adatai is célkeresztbe kerülhetnek, miközben igénybe veszik az adott eseményhez kapcsolódó digitális szolgáltatásokat, például mobilalkalmazásokat, Wi-Fi hotspotokat használnak, vagy QR-kódokat olvasnak be, amelyek akár rosszindulatú URL-eketis tartalmazhatnak.

A Szlovák Labdarúgó Szövetség (SFZ) számára – amely rengeteg külső beszállítót foglalkoztat, akik általában a saját eszközeiket használják munkavégzésére – a biztonság valóban stratégiai kérdés. Ján Letko, az SFZ informatikai és technológiai igazgatójaelmondta: azért is fordítanak kiemelt figyelmet a megfelelő, központi engedélyezési és hitelesítési protokollok, valamint a Microsoft által biztosított kiberbiztonsági megoldásokalkalmazására, mert saját fejlesztésű rendszereket és nyilvánosan

elérhető szolgáltatásokat működtetnek, így képtelenek az összes végponti eszközt külön-külön megvédeni a támadásoktól.

A Microsoft Defender Experts for Hunting (DEX), a Microsoft kiberbiztonsági szolgáltatása komplex kibervédelmi megoldást nyújtott a katari létesítmények és szervezetek számára, így a futballvilágbajnokságot a szervezők zökkenőmentesen le tudták bonyolítani. A DEX szolgáltatáscsomag keretében a Microsoft szakértői előzetesen felmérték, milyen fenyegetésekre kell a szervezőknek felkészülniük. Számbavették a támadók sajátosságait, azt, hogy várhatóan milyen taktikát, módszereket, technikákat fognak alkalmazni, továbbá fontos következtetéseket tudtak levonni a Microsoft-rendszerek működtetése során kigyűjtött adatokból is. Összesen több mint 634,4 millió incidenst elemeztek ki a Microsoft szakembereia katari létesemények és szervezetek védelme során 2022 novemberében és decemberében.

A sport- és szórakoztató rendezvényekről általában elmondható, hogy kiberfenyegetettségükés sérülékenységük szintje magasabb az átlagosnál. Előfordul, hogy az ilyen rendezvényeket gyorsan kell tető alá hozni, gyakran új partnerek és beszállítók bevonásával, akik ideiglenesen hozzáférést kapnak a szervezést végző vállalat hálózatához is. Az is megesik, hogy ilyenkor elmarad a biztonsági átvilágítás, a biztonság feltételeit pedig menet közben alakítják ki.

Az adott biztonsági apparátus támogatásához szükséges előzetes tervezés mellett arendezvényhelyszíneknek figyelembe kell venniük az ideiglenes, ad-hoc és állandó számítógépes infrastruktúrával kapcsolatos adatvédelmi kockázatokat is. Ez gyakorlatilag azt jelenti, hogy tisztában kell lenniük és a tervezés során számolniuk kell azzal, hogy a digitális eszközök és szolgáltatások igénybevétele többlet kockázatokkal és a sérülékenység fokozódásával jár.

A kiberbiztonsági kockázatok mérséklése érdekében a kluboknak, a sportszövetségeknek, a csapatoknak és a helyszínt biztosító intézményeknek hatékony kiberbiztonsági intézkedéseket kell foganatosítaniuk. Az első és legfontosabb lépés egy komplex és többszintű védelmi rendszer kiépítése: tűzfalak, behatolásérzékelő és -megelőző rendszerek üzembehelyezése, hatékony titkosítási protokollok életbeléptetése annak érdekében, hogy a hálózatokhoz illetéktelenek ne tudjanak hozzáférni és onnan adatokat eltulajdonítani. Emellett rendszeresen felül kell vizsgálniuk a biztonsági rendszer állapotát, és fel kell deríteniük a biztonsági réseket, azonosítva és kiküszöbölve a hálózat sérülékenységeit.

Mindezeken túl elengedhetetlen a felhasználók felkészítése a várható veszélyekre, a munkatársak és az érintettek megismertetése a legjobb kiberbiztonsági gyakorlatokkal. Ide tartoznak azok a módszerek, amelyekkel az adathalász e-maileket fel lehet ismerni, a többtényezős hitelesítés vagy a jelszómentes védelem, valamint a gyanús linkek és letöltésre történő felhívások azonosítása és elkerülése. Fontos továbbá az együttműködés egymegbízható kiberbiztonsági céggel, amely képes folyamatosan ellenőrizni a hálózat forgalmát, valós időben észlelni a potenciális fenyegetéseket és gyors választ adni bármilyen incidensre. Ezekkel a megelőző intézkedésekkel a sportegyesületek és –csapatok, a rendezvények szervezői jelentős mértékben növelhetik a kibertámadásokkal szembeni ellenállóképességüket, megvédhetik a saját infrastruktúrájukat és a szponzoraik érzékeny adatait.

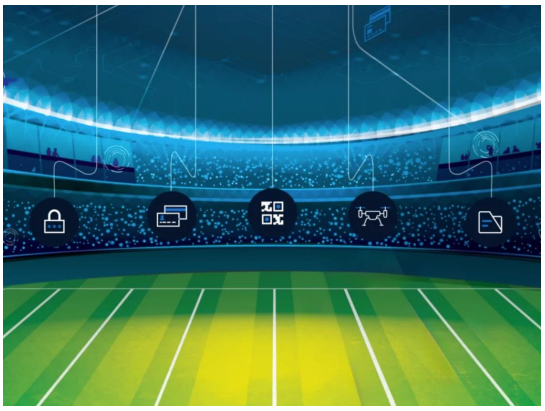
A Cyber Signals jelentés ötödik kiadását teljes terjedelmében a Microsoft weboldalán lehet elolvasni.

A Microsoft kifejezetten kiberbiztonságra fókuszáló blogján, LinkedIn és Twitter fiókján keresztül további kiberbiztonsági megoldásokról, a területet érintő újdonságokról és hírekről lehet tájékozódni.

Sajtókapcsolat:

- Kovács Ágnes Veronika, PR és vállalati kommunikációs vezető
- +36 1 267 4636

- sajto@microsoft.com



© Microsoft

Eredeti tartalom: Microsoft

Továbbította: Helló Sajtó! Üzleti Sajtószolgálat

Ez a sajtóközlemény a következő linken érhető el: https://hellosajto.hu/6426/cyber-signals-egyre-tobb-kibertamadas-eri-a-sportesemenyeket-es-helyszineiket/