Kiber- és adatbiztonsági összehasonlítás

Bevezető

A mai digitális környezetben a kiber- és adatbiztonság kulcsfontosságú tényező minden szervezet számára. A Microsoft-termékek, mint a Windows és az Office, elterjedtségük miatt gyakran a támadók elsődleges célpontjai. Ezzel szemben a magyar blackPanther Projekt (asztali, office és szerver) rendszerei kisebb támadási felülettel rendelkeznek, gyorsabb hibajavítási ciklusokkal, és beépített speciális biztonsági funkciókkal, jogosultság kezeléssel. Ez az összehasonlítás kizárólag a kiber- és adatbiztonsági aspektusokra koncentrál, számszerű adatokkal és példákkal alátámasztva.

Összehasonlító táblázat – Kiber- és adatbiztonsági jellemzők

Biztonsági szempont	Microsoft (Windows, Office)	blackPanther OS + Server, Office	Megjegyzés
Támadási felület	Széles körben használt OS és alkalmazás, emiatt gyakori célpont. Havonta több tucat CVE-javítás.	Kisebb asztali piaci részesedés → kevesebb célzott támadás. Sérülékenységek gyors javítása.	A kisebb támadási felület nem jelenti, hogy támadhatatlan, de drasztikusan csökkenti a kockázatot.
Frissítési modell	Patch Tuesday (havonta egyszer főfrissítés), kritikus foltok akár napokig-hetekig, vagy akár évekig késhetnek.	Folyamatos (half-rolling release) vagy azonnali hibajavítási modell, rendszeres új és javított telepítővel	Gyorsabb reakció a 0-day sebezhetőségekre.
Vírusok és malware elleni védelem	Kiterjedt kártevő-ökoszisztéma. Alapértelmezett: Windows Defender, de sokszor kiegészítő antivírus kell.	Jóval kevesebb vírus készül, főként szerveroldali fenyegetések. Beépített védelem, opcionális AV	Windowsnál magasabb a folyamatos védelmi költség, és mégis súlyos problémák derülnek rendszeresen
Beépített tűzfal	Alapértelmezett Windows tűzfal (korlátozott, GUI-	IDS alapú védelem (iptables/nftables) , mély hálózati szintű	A tűzfal szabályrendszere finomhangolhatóbb

	orientált).	szabályozás, GUI, TUI vagy CLI vezérléssel.	blackPanther OS-ben.
IDS/IPS támogatás	Beépített nincs, harmadik féltől vagy felhőszolgáltatásból (pl. Microsoft Sentinel) érhető el.	Beépített IDS védelmen túl, Suricata, Snort, Zeek integrálható licencdíj nélkül.	Nyílt forráskódú IDS/IPS ingyenesen elérhető a blackPanther-ben
Adattitkosítás	BitLocker teljes lemezes titkosítás (Pro/Enterprise verzióban).	LUKS teljes lemezes titkosítás alapértelmezett opció.	Mindkettő erős titkosítás, de Linuxnál ingyenesen elérhető.
Hozzáférés-kezelés	Active Directory (AD), Azure AD integráció.	OpenLDAP, FreeIPA, AD kompatibilitás.	Mindkettő képes központi jogosultságkezelésre.
Adatvédelmi megfelelés (pl. GDPR)	Microsoft felhőszolgáltatásoknál adatrezidencia kérdéses lehet, adatküldés külföldi szerverekre.	Teljes adatkontroll lokális szerveren, nincs kényszerített felhőkapcsolat.	Közigazgatásnál ez kulcsfontosságú.
Nyílt forráskód átláthatósága	Zárt forráskód – auditálás csak gyártói engedéllyel.	Teljes forráskód nyíltan ellenőrizhető.	A nyílt kód előnye, hogy nincs rejtett adatgyűjtés.

Kiber- és adatbiztonsági mutatók (számszerű tényezők)

Kiemelném, hogy 2024-ben a Microsoft termékeket **1.43 milliárd** kártevő fenyegette! A legjobb vírusirtók esetében is, maximum 90%-os a találati arány, ami több mint 100 millió kártevőfenyegetettséget jelent, akár észrevétlenül.

A piacon elérhető vírusirtók hatékonyságáról az alábbi linken tettünk közzé mérési eredményekre alapozott tanulmányt: https://hu.blackpanther.hu/virusirtok-antivirus-szoftverek-melyiket-valasszam/

Az általános képzetlenségre, és emiatt téveszmékre támaszkodó rendszergazdákkal, illetve a valóságot feltárni hivatott tanulmányt tettünk közzé, ami ezen a linken érhető el: https://hu.blackpanther.hu/kiberbiztonsagi-teveszmek-veszelyei-windows-android-linux-mac/

Külön kiemelném, hogy a magyar blackPanther OS az elmúlt 10 évben feltárt 0-day sebezhetőségek egyikében sem volt érintett! Mindez az egyedi gyártásmodellnek köszönhető, pedig az összes nagy rendszergyártó, mint a Redhat, Suse, Debian, Ubuntu is érintettek voltak több súlyos és kritikus sebezhetőségben.

Mutató	Microsoft (érték / megjegyzés)	blackPanther / Linux (érték / megjegyzés)	Forrás / Megjegyzés
Új malware fenyegetés (2022)	59,6 millió új malware (a globális új malware-ek ≈95,6% célzott Windows ellen).	1,76 millió új malware (≈2,8% a 2022-es adatok szerint Linuxra).	Trend: Windows erősen célzott (összefoglaló iparági elemzések).
Felfedezett sérülékenységek (példa: 2024)	Például: több száz sebezhetőség Windows-összetevőkben; egyes források >500 CVE-t jeleznek, kritikus kategóriák többszörösen.	Linux kernel és disztribúciós komponensek sebezhetőségei kevesebb, javítási sebesség gyors.	Sok forrás, CVE-adattárak és biztonsági jelentések.
Aktív exploitok / példa	Példa: CVE-2025-24983 (példa a beszélgetésben említve) — aktív exploitok okozhatnak SYSTEM jogosultságot.	Linux-oldalon ritkábbak az ilyen széles körű, hosszú ideig aktív exploitok; gyorsabb közösségi patch-elés.	Aktív exploitok súlyossága függ a sebezhetőségtől és exploit készletétől.

Kritikus incidensek a közelmúltból (példák)

CrowdStrike frissítés okozta globális Windows leállás (2024. július 19.): Sérült CrowdStrike frissítés miatt több millió Windows eszköz leállt; becsült globális hatás nagy volumenű kiesés.

Microsoft SharePoint 0-day támadás (2025. július): Kiterjedt kampány, ~400 szervezet érintett, köztük állami és kritikus infrastruktúrák; ransomware és adatszivárgás veszély.

WinRAR nulladik napi sebezhetőség (CVE-2025-8088): Lehetővé tette rosszindulatú kód automatikus elhelyezését indító mappákban – Windows-specifikus célpont.

Akira ransomware – Defender megkerülése: Akira ransomware képes volt letiltani vagy megkerülni Windows Defender egyes védelmi mechanizmusait, lehetővé téve sikeres fertőzéseket.

Záró összegzés

A fenti összehasonlítás és számszerű adatok alapján a Microsoft-termékek esetében a kitettség a kiberfenyegetéseknek szignifikánsan magasabb, részben a nagy piaci részesedés **és a zárt fejlesztési modell miatt.**

A blackPanther Projekt rendszerei alacsonyabb fenyegetési lábnyommal, nagyobb átláthatósággal és rapidabb javítási ciklussal rendelkeznek, ami különösen előnyös közigazgatási és érzékeny adatokat kezelő környezetekben. Fontos megjegyezni, hogy a kockázatkezelés soha nem csupán a platform választásán múlik: a biztonságos konfiguráció, rendszeres frissítés, többrétegű védelem (végpontvédelem, tűzfalszabályok, IDS/IPS, SIEM) és a **képzett üzemeltető** csapat kritikus minden környezetben.

blackPanther Project

www.blackpanther.hu

info@blackpanther.hu