Mi a KIBEV?

A KIBEV, az Önkéntes Kibervédelmi Összefogás egy magánszemélyek általi létrehozott kezdeményezés, amelynek célja fejleszteni Magyarország kritikus informatikai infrastruktúrájának védelmét. Tagjaink közé elsősorban azokat a szakembereket várjuk, akik az informatikai biztonság területén tevékenykednek és tenni kívánnak a hazai kritikus informatikai infrastruktúra-védelem előremozdításáért, illetve várjuk az ezen infrastruktúrákat üzemeltető szakembereket is.

Céljaink

- ⊕ Elérni, hogy az állam kijelölje a kritikus infrastruktúrák informatikai védelméért és az ország kiberterének védelméért felelős állami szervezetet, amellyel a KIBEV azonnal megkezdi a szakmai együttműködést.
- ⊕ Amennyiben Magyarország úgy dönt, hogy önkéntes vagy sorállományú alapon kiberhadsereget állít föl, úgy a KIBEV célja az ilyen szervezet hatékony támogatása.
- ⊕ A KIBEV nem titkolt célja, hogy az állam magáénak érezze az ország kiberterének védelmét, a KIBEV céljait és stratégiáját ehhez igazítja.
- ⊕ A KIBEV felajánlja az állam számára tagjainak szaktudását és tettrekészségét abból a célból, hogy a haza kiberterének védelmét szolgálja.
- ⊕ A KIBEV kiemelten fontosnak tartja közvetlenül és a magyar civil szervezetekkel való együttműködésen keresztül a magyar állampolgárok biztonságtudatosságának fejlesztését. Ilyen irányú kezdeményezéseket támogat, és erejéhez mérten közreműködik azok végrehajtásában.
- ⊕ A KIBEV függetlenségre törekszik, ezért tagjai között a biztonságért tenni akaró, megrendelő oldali rendszerüzemeltetőket és biztonsági szakembereket, auditorokat üdvözöl. A piaci szereplőkkel (gyártók, integrátorok, tanácsadók) közvetlen és folyamatos kapcsolatot tart fenn.
- ⊕ Cél, hogy a KIBEV elérje, hogy Magyarországon széleskörű egyetértés alakuljon ki a kritikus infrastruktúrák körének meghatározásában.
- ⊕ A KIBEV célja, hogy érdemben hívja fel a figyelmet a kibertér fenyegetettségeire, különös tekintettel azokra, amelyek az ország működésében bármilyen zavart vagy kárt okozhatnak.
- ⊕ A tagok közti kommunikációs hálózat megteremtése révén a KIBEV el szeretné érni, hogy a kritikus infrastruktúrák és a fontos informatikai rendszerek üzemeltetői folyamatos és hatékony kapcsolatban álljanak egymással.
- ⊕ A KIBEV célja, hogy Magyarország honvédségével, titkosszolgálataival és szakszolgálatával jó és hatékony kapcsolatot ápoljon, mivel a kibervédelem alapeszköze ezen szervezetek közti együttműködés és kommunikáció támogatása és előmozdítása.
- ⊕ A KIBEV feladatának érzi, hogy együttműködjön mindazon szervezetekkel és csoportokkal, amelyek a kritikus infrastruktúrák informatikai védelme érdekében már eddig is jelentős lépéseket tettek. Együtt szeretnénk működni a katasztrófavédelem szakembereivel, titkos és rejtjelzett kommunikáció szakértőivel és felügyeletével, a rádió felderítési és egyéb speciális szolgálatokkal, Magyarország képviseleteivel külföldi haderőknél (pl. NATO), az EBESZ képviseletével és további szervezetekkel, akik fontosnak tartják kezdeményezésünk ügyét.
- ⊕ A KIBEV fontosnak tartja a hatályos jogszabályokban, törvényben meghatározott állami szereplőkkel (pl. PTA-CERT), a piaci szereplőket (pl. IVSZ) illetve szakembereket képviselő (pl. ISACA) szervezetekkel való együttműködés folyamatos fenntartását és fejlesztését.
- ⊕ Cél, hogy a KIBEV a külföldi hasonló szervezetekkel, valamint más országok kibervédelmi kezdeményezéseivel aktív és jó viszonyt ápoljon, teret engedjen az információ és tudáscserének.
- ⊕ A KIBEV tagjai támogatni szeretnék a kibervédelemmel összefüggő kutatási projekteket, illetve együttműködnek a hazai tudásfejlesztő és képző intézményekkel, felsőoktatási intézményekkel.

További információkat a http://www.itbn.hu/kibev oldalon találhat. Kapcsolat: kibev@itbn.hu

kibev
önkéntes kibervédelmi összefogás
voluntary cyber defence collaboration

Célzott kiber támadások hatásainak hatékony csökkentése

A 2000-es évek végétől folyamatosan és egyre gyorsabban emelkedett azoknak a kiber támadásoknak a száma, amelyek már nem kizárólag magányos hacker-ek tevékenységére voltak visszavezethetők, hanem megjelentek a szervezett bűnözői csoportokhoz köthető informatikai támadások és a szervezett hacktivizmus is egyre nagyobb figyelmet követelt.

2010-ben az iráni atomprogramot megbénító, feltehetően az USA és Izrael által készített számítógépes vírus, a Stuxnet egy új fejezetet nyitott az informatikai- és szolgáltató rendszereket (pl. víz- és áramellátás, közlekedés, bankszektor) érintő fenyegetettségek történetében, amelyre a világ országai egyértelmű intézkedéseket hoztak. Irán és Kína hackerekből álló, elsősorban kémkedésre és szabotázsra kiképzett kiberhadsereget épített. Hasonló modellt követ Észak-Korea, amelyről 2011-ben szivárgott ki, hogy 3000 fős hacker-kommandót foglalkoztat, akik ipari és katonai titkok illegális megszerzésére és a célországok kritikus infrastruktúráinak számítógépes rendszereihez történő illetéktelen hozzáférésre kaptak kiképzést.

Ilyen körülmények között egyre fontosabbá válik, hogy az egyes szervezetek mennyire gyorsan és hatékonyan képesek alkalmazkodni az informatikai rendszerekre fenyegetést jelentő újabb és újabb kockázatokhoz.

Ez a kiadvány az ausztrál kormány által létrehozott Defense Signal Directorate (DSD) által publikált, Strategies to Mitigate Targeted Cyber Intrusions című kiadványa alapján az Önkéntes Kibervédelmi Összefogás (KIBEV) munkatársainak együttműködésében készült.

A DSD eredeti publikációja elérhető az alábbi weboldalon:

http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

Bár be kell látni, hogy semmilyen IT biztonsági stratégia nem képes teljesen megszüntetni az informatikai rendszereket fenyegető kockázatokat, azonban az itt felsorolt intézkedésekkel hatékonyan lehet csökkenteni a leggyakoribb támadások okozta negatív hatásokat.

A négy legfontosabb intézkedés bevezetésével jelentősen lehet csökkenteni a szervezetek informatikai rendszerei ellen indított támadások sikerességét, ezek implementálása után már ki lehet választani a többi intézkedés közül az adott informatikai rendszerben leginkább hatékony intézkedéseket.

Ez a kiadvány információt biztosít az egyes intézkedések költségeiről és felhasználói elfogadottságáról, ezáltal is megkönnyítve a leginkább hatékony intézkedések kiválasztását.

Hatás enyhítési stratégia - hatékonysági rangsor	Hatás enyhítési stratégia	Általános biztonsági hatékonyság	Felhasználói ellenállás	Felmerülő költségek (személyzet, felszerelés, technológiai összetettség)	Karbantartási költség (főképp személyzet)	Behatolás megelőzésére vagy észlelésére tervezve	Behatolások hatásának enyhítése - 1. lépés: Kód végrehajtás	Behatolások hatásának enyhítése - 2. lépés: Hálózati terjedés	Behatolások hatásának enyhítése - 3. lépés: Adat letöltés
1	Alkalmazások hibajavítása, pl. PDF-olvasó, Flash Player, Microsoft Office és Java. A magas kockázatú sérülékenységeknél két napon belül alkalmazni kell a javítást vagy egyéb módon csökkenteni a kockázat hatásait. Az egyes alkalmazások legutolsó verzióit kell használni.	Kiváló	Alacsony	Magas	Magas	Megelőző	Igen	Nem	Nem
2	Operációs rendszerek sérülékenységeinek javítása. A magas kockázatú sérülékenységeknél két napon belül alkalmazni kell a javítást vagy egyéb módon csökkenteni a kockázat hatásait. Az egyes operációs rendszereket naprakész állapotra frissítve kell használni.	Kiváló	Alacsony	Közepes	Közepes	Megelőző	Igen	Lehetséges	Lehetséges
3	Minimalizálni kell azoknak a felhasználóknak a számát, akik tartományi vagy helyi adminisztrátori jogosultságokkal rendelkeznek. Az ilyen felhasználóknak rendelkezniük kell egy második felhasználói fiókkal, amit e-mailezésre és web-böngészésre használnak.	Kiváló	Közepes	Közepes	Alacsony	Megelőző	Lehetséges	Igen	Lehetséges
4	Előzetesen engedélyezett alkalmazások használatával meg kell előzni kártékony szoftverek és egyéb, nem kívánatos alkalmazások futtatását. Ehhez használhatóak a Microsoft Software Restriction Policy-k, AppLocker, stb.	Kiváló	Közepes	Magas	Közepes	Mindkettő	Igen	Igen	Igen
Amikor a szervezetek alkalmazták az első 4 mérséklési stratégiát, elsőként a leginkább támadott felhasználói számítógépeken, majd ezt kiterjesztve minden felhasználóra, utána lehet választani a többi mérséklő stratégiából. Ennek hatására a rendszer biztonsági réseit lépésenként lehet foltozni, míg egy elfogadható biztonsági szintig nem jutunk, ahol a maradvány kockázatok szintje már elfogadható.									
5	Host-alapú IDS/IPS rendszerek használatával be kell azonosítani a rendellenes tevékenységeket, mint például a folyamat injektálás, a billentyűzet naplózás, a meghajtó programok betöltése vagy az alkalmazások indítás előtti megváltoztatása.	Kiváló	Alacsony	Közepes	Közepes	Mindkettő	Igen	Nem	Lehetséges
6	Engedélyezésen alapuló e-mail tartalomszűrés megvalósítása; csak az üzleti funkciókhoz kapcsolódó csatolmányok küldésének és fogadásának engedélyezése. PDF és Microsoft Office formátumú csatolmányok konvertálása más, kevésbé kockázatos formátumra vagy vírusmentesítése.	Kiváló	Magas	Magas	Közepes	Megelőző	Igen	Nem	Lehetséges
7	A Sender Policy Framework használatával blokkolni kell minden hamisított bejövő e-mailt és a szigorú SPF rekord ellenőrzés segít megelőzni a saját szervezet e-mail címének hamisítását.	Kiváló	Alacsony	Alacsony	Alacsony	Megelőző	Igen	Nem	Nem
8	Felhasználók oktatása, pl. Internetes fenyegetések, social engineering-el megvalósított, célzott adathalász e-mail. Kerülni kell a gyenge jelszavakat, egy jelszó több helyen történő használatát, e-mail címek publikálását, nem engedélyezett USB-eszközök használatát.	Kiváló	Közepes	Magas	Közepes	Mindkettő	Lehetséges	Nem	Nem
9	A bejövő és kimenő webes tartalom szűrése minták és értékelések, valamint más heurisztikák használatával és az engedélyezett weboldalak listájával történő összevetés után.	Kiváló	Közepes	Közepes	Közepes	Megelőző	Igen	Nem	Lehetséges
10	Engedélyezett webes domain-ek listázása; ez a megközelítés proaktívabb és hatékonyabb, mint a kártékony domian-ek kis százalékának tiltólistára vétele.	Kiváló	Magas	Magas	Közepes	Megelőző	Igen	Nem	Igen
11	Engedélyezett webes domain-ek listázása HTTPS/SSL domain-ek esetén; ez a megközelítés proaktívabb és hatékonyabb, mint a kártékony domian-ek kis százalékának tiltólistára vétele.	Kiváló	Közepes	Közepes	Közepes	Megelőző	Igen	Nem	Igen
12	Kliens oldali vizsgálat az Microsoft Office fájlok abnormalitásainak észlelésére, pl. a Microsoft Office File Validation szolgáltatással.	Kiváló	Alacsony	Alacsony	Alacsony	Megelőző	Igen	Nem	Nem
13	Alkalmazás-szintű tűzfalat kell használni a munkaállomásokon, úgy konfigurálva, hogy alapesetben tiltsa a hálózati forgalmat (és erre építeni az engedélyezetteket), így védve az ártó szándékú vagy nem engedélyezett bejövő csomagoktól.	Jó	Alacsony	Közepes	Közepes	Megelőző	Igen	Igen	Nem
14	Alkalmazás-tűzfal használata, mely alapból tilt minden forgalmat, és csak a fehérlistán lévő alkalmazásoknak engedi a kimenő forgalmat.	Jó	Közepes	Közepes	Közepes	Mindkettő	Nem	Igen	Igen
15	Hálózati szegmensek kialakítása és biztonsági zónákra történő felosztás az érzékeny információk és kritikus szolgáltatások (pl. felhasználói authentikáció és felhasználói információk) védelme érdekében.	Jó	Alacsony	Magas	Közepes	Megelőző	Lehetséges	Igen	Lehetséges
16	Több faktoros authentikációt kell megvalósítani, különösen, ha a felhasználó emelt szintű jogosultságot igénylő műveletet hajt végre, vagy hozzáfér egy adatbázishoz, illetve más, érzékeny adatokat tároló rendszerekhez.	Jó	Közepes	Magas	Közepes	Megelőző	Nem	Lehetséges	Nem
17	Véletlenszerű, egyedi és összetett lokális adminisztrátori jelszavakat kell használni minden számítógép esetén. A lokális adminisztrátori fiókok helyett tartományi csoportok számára osztott jogosultságokat kell használni.	Jó	Alacsony	Közepes	Alacsony	Megelőző	Nem	Igen	Nem
18	Erős jelszó-házirendet kell kötelezővé tenni, beleértve az összetettséget és a jelszóhosszt; kerülni kell a jelszavak ismételt felhasználását és a szótárbeli szavak használatát.	Jó	Közepes	Közepes	Alacsony	Megelőző	Nem	Igen	Nem
19	A hálózat külső átjáróinál IPv6-képes tűzfalak használatával meg kell előzni a számítógépek közvetlen Internet-hozzáférését, kivéve az osztott DNS-szervereket, levelező szervereket és a hitelesített webproxy-t.	Jó	Alacsony	Alacsony	Alacsony	Mindkettő	Lehetséges	Nem	Igen
20	Hardveres vagy szoftveres Adat Futtatás Megelőzés (DEP) minden olyan alkalmazás számára, mely támogatja a DEP-et.	Jó	Alacsony	Alacsony	Alacsony	Megelőző	Igen	Nem	Nem
21	Ismertségi besorolással és egyéb heurisztikus észlelőképességgel felszerelt naprakész tudásbázisú vírusvédelmi rendszer alkalmazása. A szerver és a kliens oldalon különböző vírusvédelmi termék alkalmazása.	Jó	Alacsony	Alacsony	Alacsony	Mindkettő	Igen	Nem	Nem
22	A kockázatos tevékenységekhez, mint az e-mail olvasás és a böngészés, ideiglenes, virtualizált, megbízható környezetet kell használni, korlátozott hozzáféréssel a hálózati fájlmegosztásokhoz.	Jó	Magas	Magas	Közepes	Megelőző	Nem	Igen	Lehetséges
23	Az engedélyezett és blokkolt hálózati aktivitások központosított és időszinkronizált naplózása, rendszeres naplóelemzéssel és a logok legalább 18 hónapig történő megőrzésével.	Jó	Alacsony	Magas	Magas	Észlelő	Lehetséges	Lehetséges	Lehetséges
24	Az engedélyezett és blokkolt számítógépes események központosított és időszinkronizált naplózása, rendszeres naplóelemzéssel és a logok legalább 18 hónapig történő megőrzése.	Jó	Alacsony	Magas	Magas	Észlelő	Lehetséges	Lehetséges	Lehetséges
25	Szabványos működési környezet alkalmazása a szükségtelen operációs rendszer szolgáltatások tiltásával, pl. IPv6, automatikus futtatás vagy távoli asztal. A fájl és rendszerleíró-adatbázis jogosultságokat is szigorúan kell kezelni (a szükséges és elégséges elv alapján).	Jó	Közepes	Közepes	Alacsony	Megelőző	Igen	Igen	Lehetséges
26	Munkaállomásokon futó alkalmazások biztonsági beállításainak szigorítása, pl. a szükségtelen szolgáltatások tiltása a PDF nézegetőkben, Irodai csomagokban és Web böngészőkben.	Jó	Közepes	Közepes	Közepes	Megelőző	Igen	Nem	Nem
27	Lehetőség szerint a NetBIOS szolgáltatásokhoz való hozzáféréseket a munkaállomásokon és szervereken korlátozni kell.	Jó	Alacsony	Közepes	Alacsony	Megelőző	Igen	Igen	Nem
28	Szervereken futó alkalmazások biztonsági beállításainak szigorítása, pl. adatbázisok, Web alkalmazások, ügyfélkezelő rendszerek (CRM) és egyéb adattároló rendszerek esetében.	Jó	Alacsony	Magas	Közepes	Megelőző	Igen	Nem	Igen
29	Az eltávolítható háttértárak (pl. USB) kezelése is részének kell legyen az Adatszivárgás elleni stratégiának, mely meghatározza az ilyen eszközök engedélyezését, kezelését, titkosítási követelményeit, tárolását és a megsemmisítést.	Jó	Magas	Közepes	Közepes	Megelőző	Igen	Lehetséges	Igen
30	TLS titkosítás az email-szerverek között, hogy az üzenetek illetéktelen kézbe jutása (és annak későbbi pl. social engineering-re történő felhasználása) megakadályozható legyen. Az átküldött tartalmat ki titkosítás után ellenőrizni kell.	Jó	Alacsony	Alacsony	Alacsony	Megelőző	Lehetséges	Nem	Nem
31	Le kell tiltani a LanMan jelszótámogatást és a hitelesítő adatok tárolását a munkaállomásokon és a szervereken, így nehezítve meg a támadók számára a jelszó-hash-ek törését.	Jó	Alacsony	Alacsony	Alacsony	Megelőző	Nem	Igen	Nem
32	Blokkolni kell azokat a kísérleteket, amikor egy weboldalt domain név helyett IP címmel próbálnak elérni.	Jó	Alacsony	Alacsony	Alacsony	Mindkettő	Igen	Nem	Igen
33	Hálózati behatolás-érzékelő/megelőző rendszer használata, ami mintaillesztéses és heurisztikus módszerekkel azonosítja a gyanús forgalmat úgy a belső hálózaton, mint a hálózati határokat átlépő forgalmak esetén.	Átlagos	Alacsony	Magas	Magas	Mindkettő	Lehetséges	Lehetséges	Lehetséges
34	A dinamikus, illetve a szabadon elérhető és használható domain nevek és IP címek használatának tiltása az átjárón.	Átlagos	Alacsony	Alacsony	Magas	Mindkettő	Igen	Nem	Igen
35	A teljes hálózati forgalom legalább 7 napra visszamenőleg történő tárolása a sikeres támadás utáni elemzésekhez.	Minimális	Alacsony	Magas	Alacsony	Észlelő	Nem	Nem	Nem