ÚTMUTATÓ

A KIBERBIZTONSÁGHOZ

yellowcube

frissítve: 07/01/23

ÉRTSÜK MEG

A KIBERBIZTONSÁGOT

yellowcube

A KIBERBIZTONSÁG ALKOTÓELEMEI

yellowcube

Üzemeltető, folyamat, technológia

Valódi kiberbiztonságot kizárólag egy olyan, üzletbe helyesen illeszkedő **folyamat** adhat, amelyet az optimális **technológiával** és a rendelkezésre álló **emberi erőforrással,** folyamatosan üzemeltet egy szervezet.

Például éppen ezért **nem beszélhetünk otthoni biztonságról**: egy családi wifi hálózaton a legjobb technológia és a legegyszerűbb működési folyamat ellenére sincsen üzemeltetőnk, aki a biztonsággal foglalkozik. Így az egyszerű, automatikusan védhető támadások elkerülésén kívül sajnos lehetetlen otthon valódi kiberbiztonságot fenntartani.

Önfejlesztő biztonsági folyamat

A kiberbiztonság alapvető működési folyamata egy állandóan megújuló, a technológia és a veszélyek fejlődését követő ciklus.

Első lépésként **felkészülünk**: a kockázatok és üzleti veszélyek alapján átgondoljuk a biztonságot. Kiépítjük a **preventív** védelmi rendszereinket, amelyek azonnal megállítják a számukra ismert támadásokat. Tudjuk, hogy a **prevenció nem lehet hibátlan**, ezért felkészülünk arra, hogy **detektáljuk** a védelmen átjutó támadót és időben **reagálva** megállítsuk a támadást. Az incidensekből tanulva módosítjuk a biztonsági modellünket, hogy a jövőben már elkerüljük a hasonló veszélyeket.

A kiberbiztonság több évtizedes fejlődése során három alapvető pillért hozott létre.

Először a **preventív** biztonsági rendszerek, mint a vírusirtók és tűzfalak jöttek létre, ahol a támadások automatikus, azonnali, emberi beavatkozás nélküli megállítás a cél.

Később a prevenció számára ismeretlen, a védelmi vonalakon átjutó fenyegetések leküzdésére kiépült a **detekció és reakció**.

Mindeközben a biztonságos felhasználói magatartást támogató rendszerek alapozzák meg a **kiberhigiéniát**, mint például a monitorra ragasztott jelszavakat kiváltó jelszókezelés vagy adatlopást megakadályozó DLP termékek.

A KIBERBIZTONSÁG 3 PILLÉRE

yellowcube

Mint az emberi szervezet

Jó hasonlat a kiberbiztonság megértéséhez az emberi egészséggel való összehasonlítás.

A **védőoltásokkal való prevenció** az ismert kórokozók ellen hatékony. Ha egy új vírusra viszont nincs még védőoltás, mint Covid-19 esetén is láttuk, akkor az egész világ hónapokra leáll.

A detekció és reakció hasonló a **folyamatos szűrésekhez**: MRI, mesterséges intelligencia és drága, komplex rendszerek keresik az ismeretlen veszélyeket. Ha jól működik, akkor azt sem tudjuk mit szűrtünk ki: nem várunk rá éveket, hogy megtudjuk, milyen betegség alakult volna ki.

Végül akinél a **személyes higiénia** is kihívást jelent, ott ezzel érdemes először továbblépnie, mielőtt a többi pilléren gondolkodna.

Prevenció

Folyamatosan frissülő veszélyadatbázisok alapján azonnal blokkolja az ismert támadásokat.

Detekció és reakció

Detektálja a prevención sikeresen átjutó támadókat és beavatkozási lehetőséget biztosít, mielőtt egy támadásból veszélyes biztonsági incidens és kár alakulhatna ki.

Kiberhigiénia

Megszünteti a biztonsági szempontból toxikus helyzeteket, kezeli a belső, a saját felhasználók figyelmetlenségéből vagy szándékos károkozásából származó veszélyeket.

OSZLASSUK EL

A TÉVHITEKET

yellowcube

KIBERBIZTONSÁGI TÉVHITEK

yellowcube

„A védelem hátrányban van”

Gyakori tévhit azt feltételezni, hogy a támadók több erőforrással rendelkeznek: bármilyen bűnözői csoport szinte biztosan **kevesebb pénzt és időt** tud fordítani egy támadásra, mint egy helyesen védekező, felkészült vállalat.

Míg egy hálózatba bejutáshoz elég egy védelmi hiba, de ott heteken át észrevétlenül bennmaradni és végig vinni egy támadási láncot szinte lehetetlen, ha a védők tudják a dolgukat.

Saját hálózatunk, mint ahogy saját telephelyünk védelme **sosem lehet hátrányban** a betörőkkel szemben, ha felelősen és átgondoltan építjük ki a szükséges védelmi vonalainkat.

„Felkészülés az ismeretlenre”

Visszatérő felelősséghárítás a folyamatos ismeretlenre való hivatkozás. Ugyanakkor **valódi ismeretlent még sosem láttunk**, ami ne lett volna a helyes átgondolással és a biztonság bővítésével megoldható.

Például egy **nulladik napi sebezhetőség** nem ismeretlen, hanem statisztika: ha tudjuk, hogy tízezer programsoronként vétünk egy biztonsági hibát, akkor egy százezer soros rendszer kb. tíz 0. napi sebezhetőséget tartalmazhat. Ezeknek a kezelésére pedig kötelességünk felkészülni.

Valódi ismeretlen ezzel szemben amikor például egy betörő a fal kibontásával jut be a lakásba: ez teljesen felborítja a biztonsági modellünket és alapjaiban kell újragondolni a biztonságot.

„A biztonságot termékek adják”

Utolsó tévhitünket már korábban is tisztáztuk: egyetlen vagy több terméktől, megfelelő üzleti folyamatok és helyes üzemeltetés hiányában nem számíthatunk valódi biztonságra.

Sőt, egy kutatás* szerint **a biztonsági rések egyharmada a biztonsági termékekben található**.

Vagyis hiába vásárolunk sok biztonsági terméket, a szakszerűtlen használattal valószínűleg csak sokkal lyukasabb és veszélyesebb hálózatot hozunk létre, mint ha egy kisebb, optimális, jól karbantartott biztonságot üzemeltetnénk.

* Forrás: Mudge/Google, 20 000+ vállalati hálózat átvizsgálása alapján, 2022-2023

A MINIMÁLIS

KIBERBIZTONSÁG

yellowcube

MINIMÁLIS KIBERBIZTONSÁG

yellowcube

2023-ban nem egyszerű feladat a kiberbiztonság világába belecsöppenni és **több évtizedes fejlődést bepótolni**. Ugyanakkor a mások által már elkövetett hibákból is tanulva meghatározhatunk egy minimális, hatékony, később tovább fejleszthető vállalati biztonságot.

Fontos megértenünk, hogy a **kiberbiztonság szerves része az üzletnek**, céljaik ezért közösek és együtt mérhetők. Nem lehet a biztonság túl korlátozó, nem akadályozhatja az üzleti célok hatékony elérését, ahogy az üzlet sem bírálhatja felül a kiberbiztonsági szempontokat.

Ha ezt nem tartjuk szem előtt, a biztonsági üzemeltetők gyorsan az üzlet ellenségeivé válhatnak, ami biztos recept a bajra.

A kiberbiztonság a **tudatosításnál kezdődik**. Minden döntéshozónak a maga szintjén látnia és értenie kell a fenyegető veszélyeket, különben biztosan nem lesz elkölthető keret a biztonság fejlesztésére.

Technikai szempontból a biztonság alapja a hozzáférés azonosítása: a **felhasználói címtár** és eszköz nyilvántartás, például Active Directory.

Az egyes eszközökön futó **végpontvédelem** és patch kezelés biztosítja az ismert támadások elhárítását, a **hálózati tűzfal** pedig biztonsági szegmensekre osztja szét a hálózatot.

A **detekció és reakció megvalósítása** felkészít egy jövőbeni incidensre, végül a reakcióterv elpróbálása adja meg a minimális biztonságot.

Minimális biztonság 2023-ban

0. Vezetői tudatosítás és veszély láthatóság a megfelelő büdzsé biztosításához

1. Azonosítás: címtár és eszköztár

2. Ismert sebezhetőségek befoltozása és ismert támadások elhárítása (patch, konfig és végpont)

3. Hálózat szegmentálása tűzfalakkal

4. Detekció és reakció valamilyen megvalósítása

5. Incidens reakció terv és elpróbálása

Majd következhet minden további, a hírekben is gyakran említett elem: többfaktoros beléptetés, fejlettebb phishing és email védelem, stb.

HOL TART JELENLEG

A KIBERBIZTONSÁGUNK?

yellowcube

MÉRJÜK MEG A BIZTONSÁGOT.

yellowcube

Kezdjük a **legegyszerűbb, papíron** is elvégezhető audittal, összegezzük erőforrás szerint a védelmi vonalakat: mennyibe kerül nekünk fenntartani, és mennyibe kerül a támadónak átjutni rajta.

Értelemszerűen ha egy védelem nekünk **olcsón fenntartható, de a támadónak nagy költséget jelent megkerülni**, akkor az jó irány. Ellenkező esetben viszont jobb leépíteni a drága védelmet és másra költeni a felszabaduló erőforrásokat.

Például egy hálózati detektáló rendszer, NDR üzemeltetése egyszerű és nagyon megnehezíti a támadó dolgát. Viszont egy végponti EDR legalább olyan komplex mint a támadónak átjutni rajta, így adott esetben jobban járunk, ha EDR helyett NDR mellett döntünk.

Folyamatos biztonsági validáció

Átfogóbb módszert adnak a folyamatos validációt végző offenzív biztonsági termékek, amelyek **valódi veszélyekkel és valódi támadásokkal**, objektívan mérik meg a kiberbiztonságot.

Az automatizált és folyamatos penetrációs tesztelést (CART) és betörés szimulációkat (BAS) viszont csak akkor lesz érdemes bevetnünk, ha erre már valóban felkészült a biztonságunk és **nincsenek hiányzó pillérek.**

Az így kapott **objektív mérőszámokkal** viszont jól követhető az egyes védelmi rendszerek teljesítménye és javíthatjuk valódi, bizonyított kiberbiztonsági ellenálló képességeinket.

Folyamatos biztonsági validáció **Cymulate** rendszerrel

KIBERBIZTONSÁGI BESOROLÁS

yellowcube

Védelmi vonalaink és üzleti kockázataink ismeretében, a kiberbiztonság pillérjei alapján meghatározhatjuk **saját fejlettségi szintünket**.

Logikusan egy **kezdeti** szinten indulhat el minden probléma és feladat, így a kiberbiztonság megvalósítása is.

Ahogyan elkezdjük jobban megérteni a problémát, először **ismétlődő**, kézi feladatokkal, tűzoltásszerűen próbáljuk kezelni.

Később ezek a feladatok egy **dokumentált** rendszert képeznek, majd a kialakított megoldásokat folyamatosan felügyelve már **menedzselt** biztonságról és kockázatkezelésről beszélhetünk.

Ha pedig folyamatosan javítunk a hatékonyságon, közelebb kerülhetünk az **optimális** megoldáshoz.

Kiberbiztonság szervezeti fejlettsége

kezdeti **Kiberbiztonságban tudatlan**	A szervezet nincsen kiberkockázatai tudatában. A kiber incidensekről vagy egyáltalán nem tud, vagy csak a kár után vesz tudomást.
ismétlődő **Ötletszerű biztonság**	Ötletszerűen bevezetett biztonsági termékek mellett egyenként, kézzel, tűzoltásszerűen történik a felismert incidensek elhárítása.
dokumentált **Vezetői elhatározás**	Felismerés vagy elszenvedett incidens miatt fontos vezetői döntés születik: kiberbiztonsági felelőst jelölnek ki és saját büdzsét kap a kiberbiztonság.
menedzselt **Menedzselt biztonság**	Kiépül a folyamatosan felügyelt biztonság, teljes szervezetet átfogó védelmi rendszerekkel, incidens kezeléssel és egyértelmű fejlesztési irányokkal.
optimális **Optimális biztonság**	Valódi támadásokkal folyamatosan ellenőrzött védelem, tudatosan fejlesztett kiber ellenálló képesség, közösséggel megosztott veszély-információk.

Kiberbiztonság fejlettsége a három pillér alapján

Kiberbiztonságunk a korábban említett három pillére épül: az ismert és megakadályozható támadások kivédését végző **preventív védelemre**, az ezen átjutó veszélyeket megállító **detekció és reakcióra**, illetve a felhasználók biztonságos viselkedését elősegítő, veszélyes helyzetek elkerülését biztosító **kiberhigiéniára**.

	1. pillér **Preventív védelem**	2. pillér **Detekció és reakció**	3. pillér **Kiberhigiénia**
Kezdeti	Beépített és ingyenes védelmi termékek.	Nincs.	Nincs.
Ismétlődő	Különálló, ötletszerűen telepített védelmi termékek.	Incidensek esetén tűzoltás, majd helyreállítás.	Felhasználói biztonsági oktatás.
Dokumentált	Üzleti kockázatok alapján kialakított védelem.	Incidenskezelő folyamat és elpróbált reakcióterv.	Felügyelet üzleti kockázatok alapján, beszállítók monitorozása.
Menedzselt	Változás menedzsment és céltudatos fejlesztés.	Átfogó veszély láthatóság, menedzselt incidenskezelés.	Incidens alapú beavatkozás veszélyes tevékenység esetén, automatikus tréningek.
Optimális	Objektíven mért hatékonyság és validált biztonság.	Folyamatosan validált biztonság és reakció automatizálás.	Felhasználók folyamatos veszélyességi besorolása, előrejelző felügyelet.

yellowcube

Fordítsuk le a kibervédelmi vonalakra!

A kiberbiztonsági pillérek fejlettségét a tipikus védelmi vonalakon keresztül is áttekinthetjük. A rétegek nem mindig épülnek egymásra, vagyis az egyes **védelmek átugorhatók**, ha a technológia fejlődésével már hatékonyabb megoldást tudunk az adott feladatra bevetni. A fejlettségi szintek az egyedi üzleti kockázatok szerint pontosíthatók, például a korábban említett költségmeghatározás módszerrel.

	1. pillér **Preventív védelem**	2. pillér **Detekció és reakció**	3. pillér **Kiberhigiénia**
0. szint	Beépített, ingyenes biztonsági termékek	Beavatkozás incidens által okozott kár után	Nincsen emberi kockázatkezelés
1. szint	Végpontvédelem (antivírus)	Naplógyűjtés (SIEM)	Többfaktoros beléptetés
2. szint	Patch és biztonságos konfiguráció menedzsment	Incidens kezelő rendszer	Közös jelszavak és API kulcsok felügyelete
3. szint	Hálózati szegmentálás tűzfalakkal	Anomália detekció, viselkedéselemzés (UEBA)	Rendszergazdák és beszállítók felügyelete (PAM)
4. szint	Átjáró biztonság, tartalomszűrés, webszűrés	XDR termékek és bizalom nélküli biztonság	Otthoni és távoli munkavégzés biztosítása
5. szint	DNS biztonság	Felhő és email detekció és reakció	Biztonságos belső kommunikáció
6. szint	Adatklasszifikáció és formális jogosultságkezelés	Adatközpontú detekció és reakció	Adatmozgások felügyelete
7. szint	Ipari (OT) hálózat biztonsága	Automatizálási forgatókönyvek (SOAR)	Felhasználói viselkedéselemzés (UEBA)
8. szint	Kiberbiztonsági validáció	Kiberbiztonsági validáció	Kiberbiztonsági validáció

yellowcube

MITŐL LESZ HATÉKONY

A KIBERBIZTONSÁG?

yellowcube

HATÉKONY KIBERBIZTONSÁG

yellowcube

Két évtized alatt, több ezer vállalati és intézményi ügyfele kiszolgálásán keresztül a Yellow Cube csapata pontosan megtanulta, hogy mitől válik a kibervédelem **hatékonnyá**, sőt, évtizedes távlatban is **fenntarthatóvá**.

Azonnal bevethető védelem

Legsikeresebb biztonsági termékeink **azonnal bekapcsolhatók**, így az eddig kezeletlen biztonsági kockázatok gyorsan láthatóvá válnak.

Így akár egy rövid tesztidőszak során is látványos, bizonyított **kiberbiztonsági fejlődést** tudunk felmutatni, amivel alátámasztjuk a bevezetéshez szükséges büdzsét.

Egyszerű termék, minimális karbantartási igénnyel

Alapelvünk, hogy inkább egy **egyszerű terméket használjunk 100 százalékig**, mint egy sokkal bonyolultabb megoldás töredékét.

Egy tízszer komplexebb rendszer valószínűleg 10x több biztonsági rést is tartalmaz. Mivel a hálózatunk biztonsági réseinek egyharmadát biztonsági termékek adják(!), így akár **rosszabb végeredményt** érhetünk el, mintha meg se vásároltuk volna a komplexebb megoldást.

Az egyszerű megoldás lehetőleg minimális karbantartás igénye pedig lehetővé teszi, hogy a kevés időnket a **biztonság fejlesztésével** töltsük.

Mesterséges intelligencia

A Yellow Cube már 2014 óta forgalmaz MI-alapú védelmi megoldásokat. A leküzdhetetlennek tűnő szakértőhiányban gyorsan felfedeztük, hogy kizárólag MI segítségével tudunk akár több évnyi **szakértelmet is „egy dobozban”** átadni.

Így rendszereink **szakértőtől függetlenül** működnek, nincsenek egyetlen emberhez kötve, az új kollégák számára rendkívül gyorsan tanulhatók.

A biztonsági elemzői feladatok MI-vel történő automatizálása óriási előnyt ad ügyfeleinknek, akik így **non-stop biztonsági felügyeletet** is megvalósíthatnak plusz emberek felvétele nélkül.

HATÉKONY KIBERBIZTONSÁG

yellowcube

Költséghatékony és hazai

Mivel régiónkban az anyagi szempontok mindig fontosak, ezért csak olyan gyártóval dolgozunk, aki megfelelő **árazási szabadságot és kedvezményeket** biztosít ügyfeleink sokszor szűkös költségvetése számára.

Közel két évtizedes működésünk során minden üzleti területen megfordultunk, így szívesen szállítunk azonos iparágú ügyfeleknél már bizonyított megoldásokat – előtérbe helyezve az ügyfeleink közötti **közös konzultációt**, egymás tapasztalataiból okulást az időigényes tesztelés és próbakörök helyett.

Ingyenes workshopjaink pedig mindenki számára elérhetővé teszik termékeinket.

RÖVIDEN

RÓLUNK

yellowcube

RÓLUNK

yellowcube

A Yellow Cube csoport

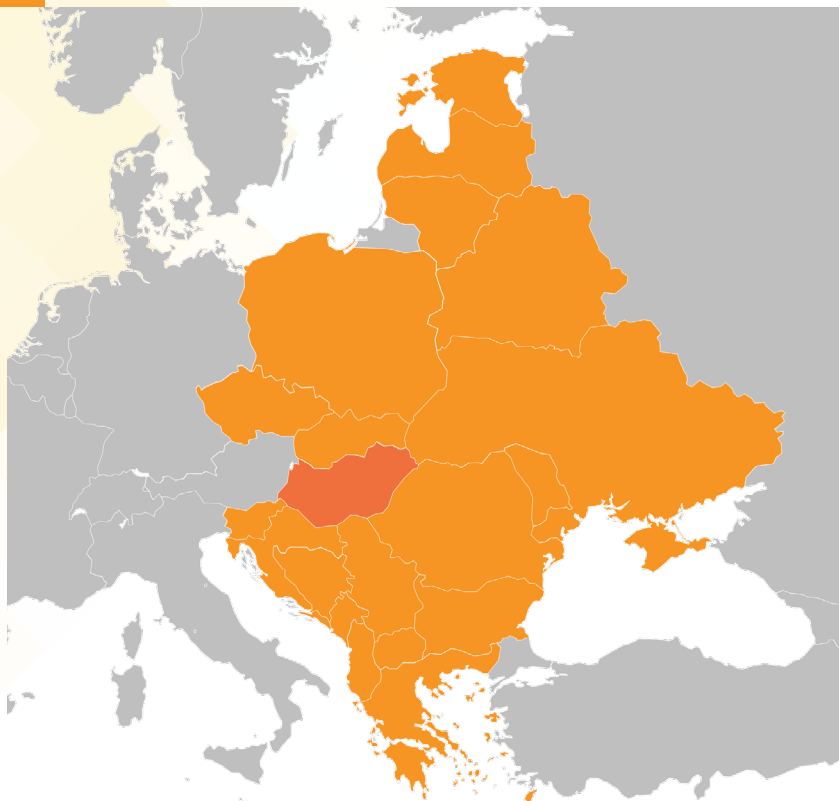
A magyar magántulajdonban álló Yellow Cube csoport Közép-Kelet-Európa országait szolgálja ki vezető kiberbiztonsági megoldásokkal.

Hiszünk benne, hogy mindenki jogosult saját **digitális szuverenitására**, az internet felől fenyegető egyre komplexebb támadások ellenére.

Ezért feladatunk olyan új biztonsági technológiák **meghonosítása, oktatása és szállítása**, amelyek képesek a régió vállalatai és kormányzati szervezetei digitális függetlenségének megvalósítására, akár sokkal **hatalmasabb és erősebb digitális ellenségek ellen**.

Yellow Cube számokban

- 2005-ben alapított vállalat
- 10 munkatárs (Magyarországon)
- 2 milliárd forint árbevétel (Magyarországon)
- 415 aktív integrátor partner
- 757 képzett kiberbiztonsági szakember
- **Prevenció:** 3992 tűzfal és 59.503 védett hoszt
- **Detekció és reakció:** 238.635 védett hoszt
- **Kiberhigiénia:** 15.681 felügyelt felhasználó



LÉPJÜNK KAPCSOLATBA

yellowcube

yellowcube.eu

hello@yellowcube.eu

Budapest, Nádorliget utca 7A

facebook.com/YellowCubeCyber

linkedin.com/company/YellowCube