HACKTIFY

KIBERBIZTONSÁGI TRENDEK 2023

MIRE SZÁMÍTHATUNK ÉS HOGYAN KÉSZÜLHETÜNK FEL?

Tartalom

2023-ban várható trendek a kiberbiztonságban

2023 a kiberbiztonság éve: Mire számíthatunk és hogyan készüljünk fel?

Mi a kiberbiztonság jelenlegi helyzete és mi várható 2023-ban?

Fejlődő trendek: A kiberbiztonság új és várható trendjei 2023-ban

Proaktív lépések: Hogyan tudnak a vállalkozások és az informatikai szakemberek a legjobban felkészülni a lehetséges fenyegetésekre 2023-ban?

Legjobb gyakorlatok: Iparági, technológiai legjobb gyakorlatok implementálása, hogy 2023-ban is biztonságban legyünk a lehetséges fenyegetésekkel szemben

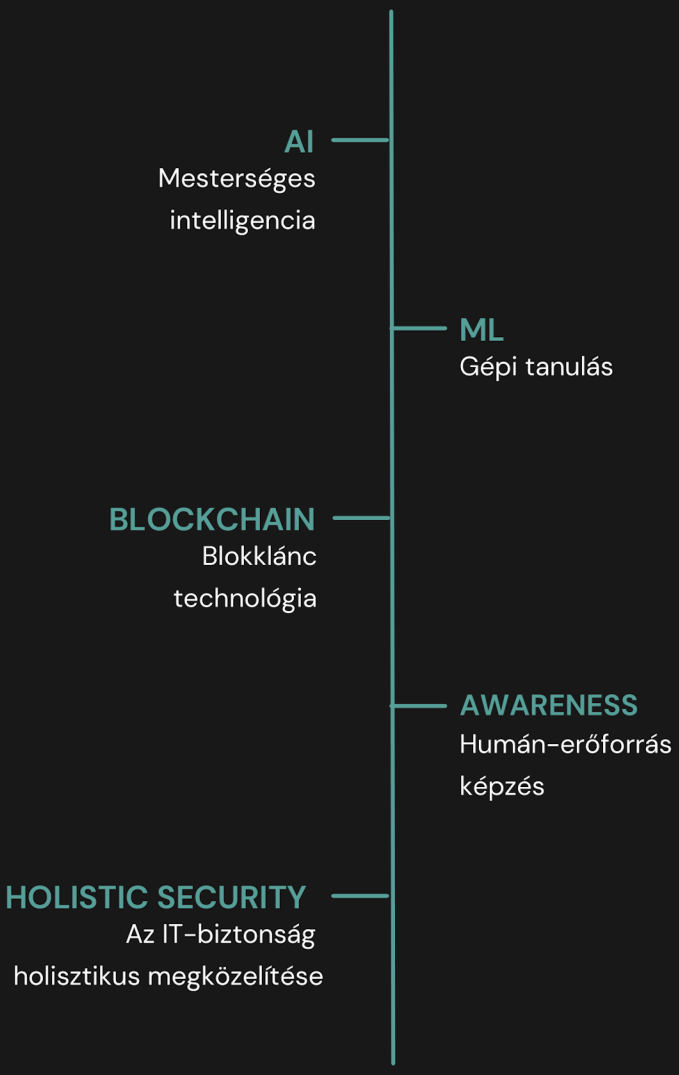
Bevezetés

Ebben az összefoglalóban áttekintést nyújtunk a kiberbiztonság várható új trendjeiről a 2023-as évben. Kitérünk arra, hogy a mesterséges intelligencia (AI), a gépi tanulás (ML) és a blokklánc technológia hogyan használható fel az IT-biztonság növelésére; tanácsot adunk arra vonatkozóan, hogy a szervezeteknek hogyan kellene befektetniük a humánerőforrás-képzésbe; és elmagyarázzuk, hogy a vállalatoknak miért kell holisztikus megközelítést alkalmazniuk rendszereik biztonságának megőrzése érdekében. Ezek az információk segítenek a vállalkozásoknak abban, hogy adataik és rendszereik védelmében lépést tarthassanak a támadókkal szemben.

HACKTIFY

2023-ban várható trendek a kiberbiztonságban

Mivel a kibertámadások száma folyamatosan növekszik, a vállalatoknak átfogó megközelítést kell alkalmazniuk rendszereik biztonsága érdekében - kívül és belül egyaránt. A biztonságos rendszerek fenntartásához minden lehetséges fenyegetésvektorral, minden szempontból foglalkozni kell - beleértve a fizikai biztonságot, a hozzáférés felügyeletet, a munkavállalók oktatási programjait és az olyan fejlett technológiákat, mint az AI, az ML és a blokklánc technológia-, hogy minden lehetséges kockázat csökkentésre kerüljön.



HACKTIFY

2023
a kiberbiztonság éve
Mire számíthatunk és hogyan készüljünk fel?

A kiberbiztonság jövője már itt kopogtat az ajtónkon. Mind a technológia, mind az életvitelünk sokat változott az elmúlt évtizedben, vele együtt az adatainkat érő potenciális fenyegetések is. 2023 a kiberbiztonság szempontjából sorsdöntő év lehet, mivel a vállalkozások minden iparágban egyre nagyobb mértékben támaszkodnak a digitális megoldásokra, felhős infrastruktúrára és online térben történő adatkezelésekre. Itt az ideje, hogy proaktív lépéseket tegyünk a lehetséges - ismert és ismeretlen - fenyegetésekkel szembeni felkészülés érdekében, mielőtt még túl késő lenne! Informatikai szakemberként a feltörekvő trendek előtt kell járnunk, meg kell ismernünk az új kockázatokat, el kell fogadnunk a legjobb gyakorlatokat, biztonságosabb rendszereket kell kiépítenünk, és meg kell értenünk, hogy mi vár ránk a kiberbiztonság arénájában.

A kiberbiztonsági fenyegetések az elmúlt években exponenciálisan nőttek, és jelentős kockázatot jelentenek a piaci szereplők, kormányok, de az egyén számára is. A technológia folyamatos fejlődése mellett a támadók által alkalmazott technikák, módszerek is fejlődnek, hogy még kifinomultabb eszközökkel szerezhessék meg bizalmas információinkat. Ahhoz, hogy e fenyegetések előtt járjunk, és megvédjük adatainkat, naprakésznek kell maradnunk az aktuális kiberbiztonsági trendekkel, eseményekkel kapcsolatban.

HACKTIFY

Mesterséges intelligencia

Artificial intelligence (AI)

A kiberbiztonság egyik legfontosabb trendjeként a mesterséges intelligencia (AI) és a gépi tanulási (ML) technológiák kihasználásának fontossága rajzolódik ki a kibertámadások felderítése és megelőzése érdekében. Az AI és a gépi tanulás felhasználható a rosszindulatú programok automatikus észlelésére, e-mail-szűrésre, felhasználói hitelesítésre és jelszókezelésre - ezek mind kritikus eszközök a rendszerek biztonságának megőrzéséhez. A mesterséges intelligencia prediktív elemzésekhez is használható, amelyekkel a potenciális fenyegetések még azok bekövetkezése előtt azonosíthatók, valamint automatizálhatók támadás esetén az elhárítással kapcsolatos teendők és incidenskezelési folyamatok.

Egy másik fontos trend a felhőalapú megoldások használata a szervezet biztonsági intézkedéseinek részeként. A felhőalapú számítástechnika alacsonyabb költségek mellett nagyobb skálázhatóságot kínál a szervezeteknek, miközben a hagyományos IT-infrastruktúrákhoz képest gyorsabb biztonsági frissítéseket tesz lehetővé.
Emellett számos felhőszolgáltatás fejlett titkosítási protokollokat és többszintű hozzáférés vezérlést kínál, amelyek segítik az adatok megfelelő védelmét.

Továbbá jelentős elmozdulás látszik a kiber-kockázatok kezelésének megelőző módszerei felé, szemben az olyan reaktív intézkedésekkel, mint a sérülékenységek kihasználását követő javítások. A szervezeteknek mérlegelniük kell, hogy külön biztonsági szakember(eke)t foglalkoztatnak vagy tanácsadó cégektől vesznek igénybe segítséget, hogy a vállalkozáshoz mért legjobb támogatást kaphassák meg adataik biztonságának garantálása érdekében. Ez magában foglalja a kockázatértékelési és -kezelési keretrendszer kidolgozását, amely azonosítja a potenciális fenyegetéseket, és meghatározza, hogyan lehet azokat a legjobban csökkenteni, kezelni, mielőtt valós problémává válnának. Emellett a szervezeteknek rendszeresen felül kell vizsgálniuk az incidensekre való reagálási terveiket, hogy felkészültek legyenek a rendszereiket vagy jogsértéssel, vagy más rosszindulatú tevékenységgel szemben.

Összességében a szervezeteknek tisztában kell lenniük a kiberbiztonsági technológia legújabb vívmányaival, ha a mai digitális világban biztonságban akarnak maradni a folyamatosan fejlődő kiberfenyegetésekkel szemben. Az AI és ML technológiák kihasználásával, a felhőalapú megoldások biztonsági keretrendszerükbe való beépítésével, a kockázatok kezelésének proaktív megközelítésével és az incidensekre adott válaszadási tervek folyamatos felülvizsgálatával a vállalatok naprakészek maradhatnak az aktuális kiberbiztonsági trendekkel kapcsolatban, és hatékonyan csökkenthetik a kiberbűncselekményekből eredő kockázatokat.

Mi a kiberbiztonság jelenlegi helyzete

és mi várható 2023-ban?

A kiberbiztonság helyzete drasztikusan más lesz, mint az elmúlt években. A kiberfenyegetések egyre kifinomultabbá válnak, így a vállalkozások és a magánszemélyek kiszolgáltatottá válnak az adathalász kísérletek, a kémprogramok, a zsarolóvírus-támadások és más rosszindulatú tevékenységeknek. Ez azt eredményezi, hogy a szervezeteknek át kellett fordulnia a reaktív intézkedésekről a megelőző tevékenységekre, hogy megvédjék rendszereiket és adataikat a lehetséges fenyegetésektől.

A kiberbiztonság nem csak a hackerek elleni védelméről szól; a szervezeteknek figyelembe kell venniük a felhőszolgáltatások, a mobilalkalmazások, az IoT-eszközök, a big data és más eszközök, szolgáltatások biztonságát is. Ahogy a világ egyre inkább összekapcsolódik a technológia révén, a kiberbiztonság még kritikusabbá válik. Már nem elég csupán egy tűzfal vagy vírusirtó megoldás; a szervezeteknek átfogó tervekkel is rendelkezniük kell, amelyek a digitális biztonság minden aspektusával foglalkozik.

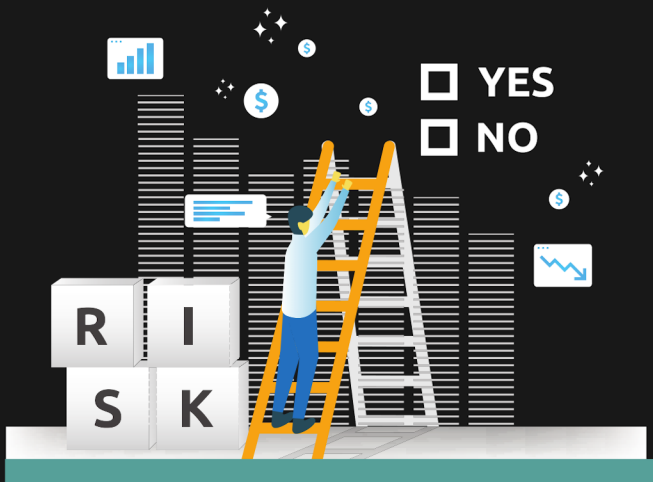
A szervezeteknek figyelembe kell venniük a mesterséges intelligencia (AI) és a gépi tanulási (ML) technológiák egyre szélesebb körű alkalmazását a kiberbiztonságban. Ezeket a technológiákat a rosszindulatú kódok gyorsabb felismerésére és a hálózati tevékenység, gyanús viselkedési formák elemzésére használhatják. Ahogy az AI/ML idővel tovább fejlődik, a szervezetek számára még fontosabbá válik, hogy a kibertámadások elleni átfogó védelmi stratégiájuk részeként kihasználják ezeket a nagy teljesítményű megoldásokat.

Emellett az állami szervezetek világszerte kezdik felismerni a kiberfenyegetésekkel kapcsolatos információk megosztásának fontosságát a piaci szereplők és nemzetek között egyaránt, annak érdekében, hogy jobb védelmet nyújtsanak polgáraik számára. 2023-ban további fejlődésre számíthatunk ezen a területen, mivel a kormányok keresik a nemzeti ügynökségek és a magán szektor közötti együttműködés erősítésének lehetőségeit. Tekintettel arra, hogy a vállalkozások továbbra is nagymértékben támaszkodnak a távoli elérési megoldásokra, még nagyobb hangsúlyt kap e rendszerek védelme.

Összességében elmondható, hogy a kiberbiztonság egy örök fejlődő terület, mivel a technológiai vívmányok, az új fejlesztések, innovatív eszközök újabb és újabb lehetőséget teremtenek a sérülékenységek kihasználására, a támadások hatékonyabbá tételése, amivel szemben a védekezést is folyamatosan fejleszteni szükséges. A szervezeteknek az újonnan megjelenő fenyegetések előtt kell járniuk azáltal, hogy folyamatosan beruháznak a kiberbiztonsági eszközök frissítésébe, miközben folyamatosan tájékozódnak a legjobb gyakorlatokról, amelyekkel a modern fenyegetésekkel szemben biztonságban tarthatják rendszereiket. Így biztosíthatják, hogy egy lépéssel a támadók előtt járhassanak.

Fejlődő trendek

A kiberbiztonság új és várható trendjei 2023-ban



Mivel a kiberbiztonság folyamatosan fejlődik, fontos, hogy lépést tartsunk a terület új és feltörekvő trendjeivel. 2023-ban a szervezeteknek számos új fenyegetésre és sebezhetőségre kell felkészülniük.

A gépi tanuláson alapuló rosszindulatú programok felismerő rendszerektől kezdve a natív felhő biztonsági megoldásokig számos módja van annak, hogy a kiberbiztonság alkalmazkodjon és védelmet nyújtson a támadásokkal szemben.

Cloud

A világ vállalati adatainak 60%-át a felhőben tárolják

Adatközpontok

A felhőalapú adatközpontok a világ energiafogyasztásának 3%-át teszik ki.

A 2023-as év egyik legfontosabb kiberbiztonsági trendje a mesterséges intelligencia (AI) és a gépi tanulás (ML) alkalmazása. A mesterséges intelligenciát és az ML-t már eddig is használták kiberbiztonsági alkalmazásokban, például a rosszindulatú programok felderítésében, de most már szélesebb körben alkalmazzák őket az egész iparágban.

A gépi tanuláson alapuló alkalmazások lehetővé teszik a rendszerek számára, hogy gyorsan elemezzenek nagy adathalmazokat, hogy olyan mintákat is felismerjenek, amelyek a hagyományos vizsgálati technikákkal nem lennének könnyen felderíthetők. Ezek a mesterséges intelligencia alapú megoldások csökkenthetik a téves pozitív találatokat, és jelentősen csökkenthetik az elemzéshez szükséges időt.

A felhőalapú számítástechnika egy másik olyan trend, amely 2023-ban várhatóan uralni fogja a kiberbiztonságot. A felhőalapú biztonsági megoldások lehetővé teszik a szervezetek számára, hogy adataikat és alkalmazásaikat a helyben lévő szerverekről könnyedén áthelyezzék felhőkörnyezetekbe. A felhőalapú számítástechnika révén a vállalkozások a nagyobb skálázhatóság, a költséghatékonyság, a szabályozásoknak való jobb megfelelés és a különböző eszközökön vagy platformokon keresztül nyújtott nagyobb teljesítmény előnyeit élvezhetik. Emellett számos felhőszolgáltató olyan beépített funkciókat kínál, mint a titkosítás, a biztonságos hozzáférés-kezelési protokollok, a személyazonosság-kezelési eszközök, a sebezhetőségek automatikus javítása és a fejlett elemzési képességek, amelyek segítségével a szervezetek hatékonyabban tudják felmérni a kockázataikat.

HACKTIFY

Tudatosítás

Egyre fontosabbá válik az is, hogy a vállalatok a felhasználók oktatására összpontosítsanak a kiberbiztonsági tudatosság tekintetében. Mivel napról napra több felhasználó fér hozzá bizalmas információkhoz online vagy mobileszközökön keresztül, a vállalkozásoknak egyértelmű utasításokat kell adniuk a felhasználóknak arról, hogyan védjék meg magukat online - beleértve az adathalász e-mailek vagy gyanús weboldalak felismerését. Ha az alkalmazottaknak rendszeres képzéseket biztosítanak, hogyan ismerhetik fel a legjobban a fenyegetéseket, az nagymértékben csökkenteni fogja annak esélyét, hogy 2023-ban és azon túl is áldozatul esnek a támadók trükkjeinek.

OKTÓBER

Az Európai Kiberbiztonsági Hónap (ECSM) elnevezésű kampányt 2012 óta szervezik meg Európa-szerte a tagállamok. A Kiberhónap nemzetközi koordinálását az ENISA (Európai Uniós Kiberbiztonsági Ügynökség) végzi.

Proaktív lépések

Hogyan tudnak a vállalkozások és az informatikai szakemberek a legjobban felkészülni a lehetséges fenyegetésekre 2023-ban?

Ahogyan előre tekintünk 2023-ra, a vállalkozásoknak és az informatikai szakembereknek meg kell kezdeniük a megelőző lépések tervezését és végrehajtását a potenciális kiberbiztonsági fenyegetések elleni védelem érdekében. Ahhoz, hogy mindig az élen járjanak, a szervezetek számára elengedhetetlen, hogy tájékozottak maradjanak a kiberbiztonság jelenlegi és újonnan megjelenő trendjeiről.

A leggyakoribb fenyegetések, amelyekkel a vállalkozásoknak ma szembe kell nézniük, a rosszindulatú szoftverek támadásai, az adathalász rendszerek, az adatvédelmi incidensek és a zsarolóvírusok. A malware-támadások akkor következnek be, amikor egy támadó rosszindulatú szoftvert telepít egy rendszerre azzal a szándékkal, hogy bizalmas információkat kompromittáljon, vagy átvegye az irányítást az eszközök felett. Az adathalász rendszerek olyan e-maileket vagy más kommunikációs formákat használnak, amelyek megbízható forrásból származónak tűnnek, de valójában átverések, amelyek célja bizalmas információk vagy pénz megszerzése az áldozatoktól. Az adatvédelmi incidensek akkor következnek be, amikor a hackerek hozzáférést szereznek a vállalat által kezelt személyes adatokhoz, és ha nem foglalkoznak velük gyorsan, akkor bevételkiesést és hírnévkárosodást, hatósági bírságot eredményezhetnek. A zsarolóprogramok a rosszindulatú szoftverek egy olyan formája, amely az áldozat fájljait titkosítja, amíg az áldozat ki nem fizet egy összeget a feloldásukért.

Emellett a vállalkozásoknak tisztában kell lenniük az olyan újonnan megjelenő trendekkel is, mint a felhőalapú fenyegetések, a célzott támadások, a mesterséges intelligencia alapú rosszindulatú programok, a bennfentes fenyegetések, a kritobányászat (a számítási teljesítmény jogosulatlan felhasználása kriptovaluta keresésére), a DDoS-támadások (túlterheléses támadás) és az ellátási lánc elleni támadások ('supply chain attacks', olyan támadásfajta, amikor a támadó a szállítókon vagy beszállítókon keresztül hatol be egy vállalkozás rendszerébe). Ezek mindegyike egyedi kockázatokat jelent, amelyeket ennek megfelelően kell kezelni; a potenciális veszélyek minimalizálásához elengedhetetlen, hogy naprakészek maradjunk a kiberbiztonsági színtér legújabb fejleményeivel.

A vállalkozásoknak arról is gondoskodniuk kell, hogy informatikai területeik megfelelő erőforrásokkal rendelkezzenek és olyan szakemberekkel dolgozzanak együtt, akik értik a legújabb technológiákat, és akik képesek hatékony biztonsági intézkedéseket bevezetni. Ehhez rendszeres képzésekre van szükség olyan témákban, mint a fenyegetések felismerési módszerei, az új fenyegetések által jelentett kockázatok csökkentésére irányuló akciótervek, a biztonságos programozási technikák és a megfelelő hozzáférés-ellenőrzéseket biztosító folyamatok. Emellett a szervezeteknek átfogó irányelveket kell kialakítaniuk a technológiai erőforrások felhasználására, a céges eszközök vállalaton belüli elfogadható használatára vonatkozóan, továbbá olyan eljárásokat, amelyek kifejezetten részletezik, hogy a munkavállalóknak hogyan kell biztonságosan kezelniük az ügyfelek/partnerek adatait.

Legjobb gyakorlatok

Iparági, technológiai legjobb gyakorlatok implementálása, hogy 2023-ban is biztonságban legyünk a lehetséges fenyegetésekkel szemben

Nem lehet elégszer hangsúlyozni, hogy a kiberbiztonság világa folyamatosan fejlődik, és a szervezetek számára rendkívül fontos, hogy 2023-ban is biztonságban maradjanak a lehetséges fenyegetésekkel szemben. Elengedhetetlen, hogy a vállalatok naprakészek maradjanak a legújabb kiberbiztonsági trendekkel kapcsolatban, és elfogadják az iparági szintű legjobb gyakorlatokat. Azzal, hogy a vállalkozások aktív szerepet vállalnak saját biztonsági stratégiájuk kialakításában, biztosíthatják, hogy védve legyenek a rosszindulatú támadásoktól és az adatvédelmi incidensektől.

A potenciális fenyegetések elleni védelem egyik leghatékonyabb módja, ha jól meghatározott irányelvek és eljárások vannak érvényben, amelyeket minden alkalmazottnak követnie kell. Ez magában foglalja a biztonsági protokollokról szóló ismétlődő munkavállalói képzéseket, a rendszeres szoftverfrissítéseket, valamint annak biztosítását, hogy mindenki csak a munkaköréhez kapcsolódó feladatai ellátásához szükséges információkhoz férjen hozzá. Ezenkívül a munkavállalók által használt összes eszközt megfelelően kell védeni jelszavakkal, titkosítással és egyéb eszközökkel, hogy a véletlen és szándékos károkozást is megelőzzük.

A szervezeteknek ki kell használniuk az olyan modern eszközöket is, mint a mesterséges intelligencia (AI) és a gépi tanulás (ML) a szokatlan hálózati interaktivitás, gyanús tevékenységek vagy kihasználható sérülékenységek felderítésére. A mesterséges intelligencia gyorsan felismeri a hálózaton található anomáliákat vagy rosszindulatú fájlokat, így a fenyegetésekkel még azelőtt lehet foglalkozni, mielőtt azok komoly problémává válnának. Emellett az ML algoritmusok a hálózati forgalom nagy adathalmazainak elemzésére és a rosszindulatú viselkedésre utaló minták vagy jellemzők azonosítására is használhatók.

A szervezeteknek lehetőség szerint felhőalapú megoldásokat kell alkalmazniuk, mivel ez bizonyítottan növeli a skálázhatóságot, miközben csökkenti az IT-infrastruktúra fenntartásával kapcsolatos költségeket. A felhőszolgáltatók további biztonsági rétegeket kínálnak, például adattitkosítást, hozzáférés felügyeleti megoldásokat, többfaktoros hitelesítési megoldásokat, tűzfalvédelmi szolgáltatásokat és egyebeket, ezért fontos, hogy a vállalkozások erős biztonsági referenciákkal rendelkező felhőszolgáltatót válasszanak. A kiberbiztonság ezen legjobb gyakorlatainak betartásával 2023-ban a vállalkozások nagymértékben csökkenthetik a rosszindulatú támadások által jelentett kockázatokat.

Záró gondolatok

Foglaljuk össze mit tehetünk, hogy lépéselőnyben lehessünk a kiberbiztonságban 2023-ban is

A technológia folyamatos fejlődésével és bővülésével a kiberbiztonsági fenyegetések egyre kifinomultabbá válnak. Ahhoz, hogy 2023-ban is a lépéselőnyben legyünk ezekkel a kialakulóban lévő kiberbiztonsági trendekkel szemben, a szervezeteknek proaktív megközelítést kell alkalmazniuk adataik és hálózataik védelme érdekében. Ehhez a szervezetnek átfogó biztonsági tervet, stratégiát kell készítenie, amely minden releváns területre, folyamatra kitejed.

A szervezeteknek először is leltárt kell készíteniük az általuk használt összes hardverről és szoftverről, valamint a csatlakoztatott eszközökről és szolgáltatásokról. Ennek tartalmaznia kell a vállalaton belül használt operációs rendszereket, alkalmazásokat, hálózati berendezéseket és felhőszolgáltatásokat is. Ennek birtokában stratégiát dolgozhatnak ki a hálózat védelmére a potenciális fenyegetésekkel szemben. Emellett a szervezeteknek nyomon kell követniük minden olyan új szoftverfrissítést vagy támogatást, amely hatással lehet a biztonságra.

A szervezeteknek a meglévő szoftverek és alkalmazások frissítésében is szorgalmasnak kell lenniük, hogy a legújabb hibajavításokat és biztonsági frissítéseket telepíthessék. A nem támogatott vagy korábbi hibás programok sebezhetővé tehetik a rendszereket. A frissítések kezelésére a szervezeteknek egy rendszert kell kialakítaniuk az elérhető javítások rendszeres nyomon követésére, és azok megjelenésüket követő ellenőrzésére, telepítésére. A megfelelően beállított automatikus frissítés engedélyezése biztosíthatja, hogy minden rendszer naprakész maradjon a legújabb biztonsági kiadásokkal.

A szervezeteknek fontolóra kell venniük a bug bounty programokban való részvételt, hogy a sérülékenységeket felderíthessék. A bug bounty programok lehetővé teszik a vállalkozások számára, hogy etikus hackerek kutassanak sérülékenységek után, melynek megtalálásáért és bejelentéséért jutalmat kapnak. Ez segít a vállalkozásoknak abban, hogy adataik és rendszereik védelmében élen járjanak, mindent költséghatékony módon.

A belső intézkedések mellett a szervezeteknek ébernek kell maradniuk a külső fenyegetésekkel, például az adathalász-támadásokkal és a rosszindulatú szoftverekkel kapcsolatban is, amelyek 2023-ban is népszerű támadási vektorok maradnak. A szervezeteknek olyan e-mail-szűrő megoldásokat kell használniuk, amelyek felismerik a bejövő üzenetek eltérő mintázatait, például a gyanús linkeket vagy mellékleteket, mielőtt azok eljutnának a címzettekhez. Emellett a megfelelő felhasználói oktatás elengedhetetlen ahhoz, hogy a munkavállalók felismerjék ezeket az e-maileket, és ne essenek áldozatul adathalász csalásoknak vagy más, e-mail levelezésen keresztül végzett rosszindulatú támadásnak.

Végezetül a szervezeteknek a kiberbiztonsági trendekkel azáltal is lépést kell tartaniuk, hogy rendszeresen olvassák a szakértők, iparági szereplők, szakmai csoportok által írt blogokat vagy kiadványokat. Ezek közé tartozik a biztonságos kódolási gyakorlatok, a támadók által napjainkban használt rosszindulatú technikák vagy akár a világszerte bevezetésre kerülő adatvédelmi, információbiztonsági jogszabályok, szabályozások. Ezekkel a folyamatosan változó trendekkel való lépéstartás segíthet abban, hogy egy szervezet rendszere 2023-ban és azon túl is biztonságos maradjon.

A kiberbiztonság folyamatosan változó és összetett terület. Mivel a támadások egyre kifinomultabbá válnak, fontos, hogy a vállalkozások és az informatikai szakemberek proaktívak maradjanak a kiberbiztonsággal kapcsolatos megközelítésükben. A legújabb trendek megértésével és a potenciális fenyegetések mérséklésére irányuló lépések megtételével a vállalkozások a legjobban felkészülhetnek az előttük álló feladatokra. Az iparági, technológiai szintű gyakorlatok és nemzetközi szabványok implementálása az egyik módja annak, hogy a megelőzhessük a károkat, és biztosítsuk, hogy szervezetünk megfelelően védett legyen a felmerülő fenyegetésekkel szemben.

HACKTIFY

KAPCSOLAT

Minden évben több tízezer cég esik áldozatul a rosszat akaró hackereknek.
Ne hagyd, hogy a Te cégeddel is megtörténjen!

Hacktify International Kft.
+36 30 851 8205
info@hacktify.eu

WWW.HACKTIFY.EU

Bug Bounty

Új generációs IT biztonság, mely vállalkozásod kiberellenállóságát növeli egy közösség erejével

Tekints át bug bounty programlehetőségeinket, ha elakadtál keress bennünket bizalommal, s segítünk megtalálni a számodra legmegfelelőbb szolgáltatásunkat.


HACKTIFY