AMIT EDDIG NEM TUDTÁL A BUG BOUNTY PROGRAMRÓL

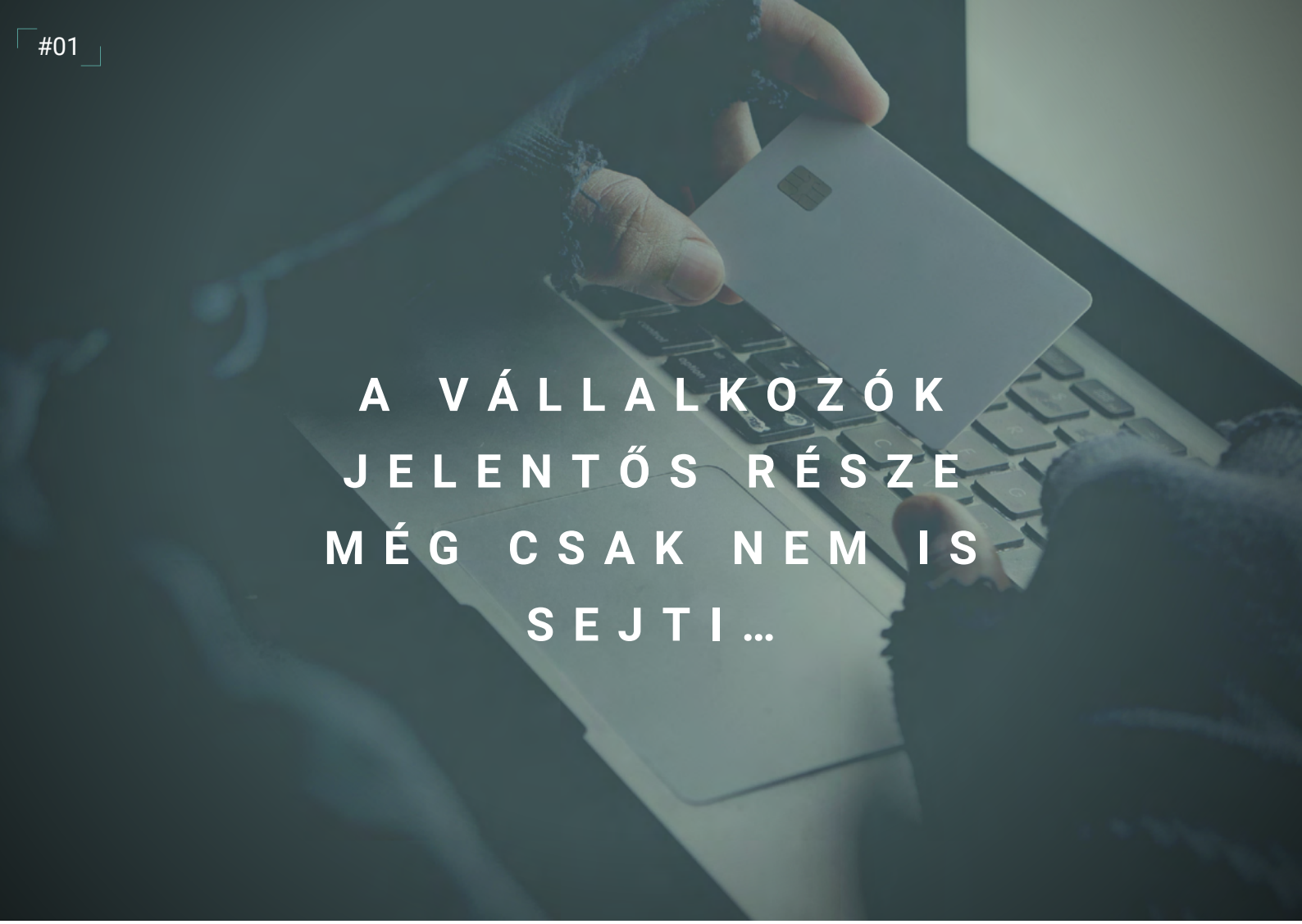
AVAGY A CÉGED IT OLDALRÓL MOST IS SEBEZHETŐ?

MÉG NEM TÖRTEK FEL, VAGY CSAK NEM TUDSZ RÓLA?

ÉLJ A BUG BOUNTY PROGRAMMAL, AMIKOR A JÓFIÚKKAL TÖRETED FEL A RENDSZEREIDET, HOGY MEGELŐZD A ROSSZFIÚK TÁMADÁSAIT!

HACKTIFY

#01



A VÁLLALKOZÓK JELENTŐS RÉSZE MÉG CSAK NEM IS SEJTI…

…HOGY NAP MINT NAP TÁMADÁSOKNAK VANNAK KITÉVE AZ ONLINE TÉRBEN.

Ha már feltűnt és nem tettél semmit, akkor baj van.

„De minket még nem törték fel!”. Az is lehet hogy csak nem tudsz róla.

Az sejthető, hogy szeretnéd hatékonyabbá és sikeresebbé tenni az üzleti folyamataidat, vállalkozásodat. Melyik piaci szereplő nem küzd azzal, hogy megtalálja a fejlődés leghatásosabb eszközeit?

Ha téged is bedobtak az online világ mély vizébe (web applikációk, webshop, azonnali fizetési megoldások, távmunka, VPN) akkor elkerülhetetlen, hogy a szakmai felkészültséged IT-biztonsági feladatokkal, egy „Informatikai Önvédelmi Rendszerrel” is párosítsd.
Erre nyilván felkapod a fejed, hiszen egy önvédelmi rendszer komoly védelmi vonal, ami lehetővé teszi, hogy megóvd magad nemcsak a jelenlegi, de jövőbeli események kedvezőtlen anyagi és presztizsvesztés hatásától is.

A Bug Bounty program megelőző megoldásokat kínál, hogy ne ússzanak el az üzleti partnerek, a jogszabályi előírásoknak naprakészen megfelelhess, elkerüld akár a több millió forintos bírságokat és megtartsd a verejtékkel megszerzett pozitív reputációd.
Ennek leghatékonyabb módja, ha nem egy ember, hanem egy közösség teszteli a RENDSZEREIDET.

Mit is jelent ez pontosan?

#02

HA ONLINE TÉRBEN MOZOGSZ, ERRE SZÜKSÉGED LESZ

Mert az értékteremtő vállalkozásodat fenyegető online kockázatok lesben állnak – előzd be őket! Most pedig eljött a pillanat, hogy feltedd a hibavadász program búvárszemüvegét és elmerülj a Bug Bounty óceánjában.

HACKTIFY CSAPATA

KEZDJÜK OTT: BIZTOS VAGY BENNE, HOGY TUDOD MI FOLYIK A CÉGEDBEN?

A tapasztalat az, hogy IGENT-t mondasz, holott a NEM a reális válasz.

Ezt nem mi mondjuk, a statisztikák.
Az egyre inkább digitális világban most minden eddiginél fontosabb vállalkozásod, ügyfeleid adatainak védelme.

Ráadásul létezik 3 olyan top informatikai biztonsági kihívás 2021-ben, amivel a legtöbb cég vérrel verejtékkel küzd. Pedig létezik hatékony eszköz, hogy megbizonyosodhass arról, hogy vállalkozásod biztonságban van-e az online térben.

» „Ohh, minket még sosem törtek fel!”
» „Mi évente átvizsgáltatjuk a rendszereinket.”
» „Ez az egész etikus hackerkedés túl kockázatos.”
» „Mi túl kicsik vagyunk ehhez, még nem állunk készen, épp új terméket fejlesztünk…túl drága.”
» „A menedzsment úgysem fogja jóváhagyni.”

Mindannyiunknak voltak-vannak ilyen és ehhez hasonló gondolatai. Ez persze nem meglepő: emberként a szokásaink és a kényelem rabjai vagyunk.

Egyszerűséget jelent, ha nem kell olyan dolgokkal foglalkozunk, ami még nem ég a körmünkre és nem ment kavicsként a cipőnkbe. Az online világ veszélyeire számos szakmai portál felhívja a figyelmet és sok-sok megelőző technikát közzétesz, mégis a magyar cégek tekintetében ugyanazok a hibák köszönnek vissza állandóan.
Gondoltad volna, hogy a cégek kb. fele még az alapvető biztonsági best practice-eket sem alkalmazza? Nincs lopásgátló, backup vagy titkosítás? Nem beszélve egyéb IT biztonsági kontrollokról. Nyugodtan lecserélhetnék négylevelű lóherére a logójukat.
Minden nap, minden órában, minden vállalkozás kicsit izzad azon 2021-ben, hogy:

01 A „BIZTONSÁGOT” BESZORÍTSA A BÜDZSÉBE.

A home office projektet száraz lábbal vezesse át a túlsó partra, biztosítsa a távoli hozzáférést, szerverkapacitást bővítésen, másodlagos hálózat bevezetést hozzon létre vagy éppen a 300-400 dolgozóját szolgálja ki IT szempontból.

Az online meetingek kihívásai között szerepel, hogy saját domainen vagy más szolgáltató által kivitelezve hozza létre őket és néhányan meg- megcsúsznak a chatalkalmazás biztonsági hibáinak imbolygó padlóján is. Miközben az emberi tényező veszélye mindig fennáll (jelszavak nem megfelelő tárolása, céges eszközökön magánjellegű ügyek intézése és „rossz kattintások” miatt, ezáltal a céges adatokhoz történő hozzáférés).

02 VÉDELMET BIZTOSÍTSON A SZOLGÁLTATÁSAI SZÁMÁRA A KÜLSŐ ROSSZINDULATÚ TÁMADÁSOKKAL SZEMBEN.

RDP, távmunka. Kéz a kézben jár.
Nincs merevlemez-titkosítás, azaz a munkat
árs a kocsiban hagyja a laptopot, amit feltörnek és viszik a laptopot és vele minden adatot is.

Ha kiírja az egyik program a frissítéseket, a hibaüzeneteket; fogalma sincs, hogy azzal mit csináljon. Tény, hogy a nagyobb cégek több sérülékenységnek vannak kitéve, míg egy 10 fős kisebb cég nincs annyira fókuszban célpontként a hackertámadások által (kisebb hasznot jelenthetnek), de ma egyetlen vállalkozás sem bújhat a nyugalom takarója alá.

Különösen, hogy a hackerek nem merülnek ki a fekete kapucnis srácokban, akik egy számítógép fölé roskadnak és dühösen írogatják a kódokat, hanem képzett szakemberek.

Megtalálják a rendszer gyengeségeit és rosszindulattal és anyagi haszonszerzéssel társulva ki is használják azokat; már nemcsak az adatok eltulajdonítása, hanem manapság leginkább az adatok hozzáférhetőségének megakadályozása a céljuk. A hozzáférhetetlen adatok szükségesek a cég működéséhez, a zsarolóvírusok ezért is népszerűek.

Korábban az adatok eltulajdonítása volt jellemző, míg manapság az adatok hozzáférhetőségének megakadályozása, hiszen azok az adatok minden bizonnyal a cégnek fontosak leginkább. (zsarolóvírusok elterjedése)

03 FRISSÍTSE A LEJÁRT TÁMOGATÁSSAL ÉLŐ FOLYAMATAIT, RENDSZEREIT.

Ismerős, amikor csak egy adott gépen fut egy munkatárs számlázóprogramja?
Az adatok biztonsága, ennek garantálásához szükséges lépések, eszközök, folyamatok, és szoftverek biztosítása is nagy falat.

Mert a mentés csak a jéghegy csúcsa.

HACKTIFY

TE MEGENGEDHETED MAGADNAK, HOGY MINDEN MARADJON A RÉGIBEN?

Kevesen tudják felmérni és számszerűsíteni, hogy egy biztonsági rés milyen méretű anyagi és reputációs veszteséget okozhat, illetve, hogy egyáltalán milyen lehetőségeik vannak a védekezésre.

Talán ismerősek az olyan kifejezések, mint VPN (virtuális magánhálózat, ami közvetlen internet kapcsolatunkat eltereli egy alternatív hálózatba, amelyen keresztül – jó esetben – titkosított formában közlekednek az adataink), a munkatársak IT biztonsági oktatása, az ellenőrzés, folyamatos monitoring, túlterheléses támadás elleni védelem, a gépek visszahívása és ellenőrzése, frissítések, vírusirtó használata, folyamatos mentés, mentés, mentés és végpontvédelem.

Igen, ezek azok kontrollok, amelyeket rengeteg cég elhanyagol.
Habár a jövőbe senki se lát, de a kockázatokat fel lehet térképezni.

Mi lenne a leghatékonyabb kivitelezés, hogy Fort Knox-á váljon a céged a gombamód szaporodó hacker hordák előtt?

AZÉRT, HOGY NE NÉZZENEK FERDE SZEMMEL A CÉGEDRE – EGY BUG BOUNTY PROGRAM ELŐNYEI, NEM A MISZTICIZMUS SZINTJÉN

Ha még nem hallottál a Bug Bountyról vagy hallottál, de bullshit szaga volt, akkor most egy csapásra képbe kerülhetsz vele.

A BUG BOUNTY OLYAN LEGÁLIS INFORMÁCIÓBIZTONSÁGI PROGRAM, AMELY ÁLTAL JUTALMAT KAPNAK A TESZTELŐK A SZOLGÁLTATÁSODBAN TALÁLT SÉRÜLÉKENYSÉGEKÉRT ÉS HIBÁKÉRT.

#1 FOLYAMATOS TESZTELÉS A HACKER KÖZÖSSÉG ÁLTAL

A cégedben esetlegesen elvégzett időszakonkénti penetration tesztek egy adott időpontban mutatják ki a rendszered gyengeségeit. Ezzel szemben egy bug bounty programban akár több száz szakember vizsgálhatja az applikációd folyamatosan!

Segítségével egy csapat állandó megbízása helyett az etikus hackertársadalom előnyeit használod ki, akik a sérülékenységet vizsgálják.

Megkéred, hogy törjék fel a rendszeredet. Fehér kalapos hacker az a kiemelt tudással rendelkező informatikai szakember; aki tudását arra használja fel, hogy megbízás alapján vagy állandó jelleggel biztonsági hibákra világítson rá. Ezáltal elkerülve és megelőzve a fekete kalapos hackerek, a rosszfiúk betörési kísérleteit.

Épp úgy működik, mint a közösségi autózás, a közösségi pizzaszállítás; ez egy közösségi kiberbiztonsági tesztelés.

Jobb ma egy Bug Bounty, mint holnap egy bírság. A veszély mindig abban áll, ha nem csinálsz semmit.

#2 HATÉKONYABB HIBAKERESÉS

Képzeld el, hogy minden évben egy ugyanazon ember kimegy „tesztelni a céged rendszereit”, majd kapsz egy riportot, mely egy pillanatnyi állapot alapján készült el. Ellenben nálunk a HACKTIFY oldalán a feladatra kihívásként tekintő etikus hackerek kezdik el tesztelni a szabályok betartásával a rendszereid hiányosságait, biztonsági kiskapuit. A hibát észlelve bejelentik azokat.

Nem 1-2 etikus hacker teszteli majd a céged szolgáltatásait, hanem akár több tíz is! Több szem többet lát!

A 60 emberből lehet 30 virtuóz és olyat is megtalál, ami felett más elsiklana. Ők nemcsak pénzt kereshetnek vele, de a r HACKTIFY-nál pontokat és jutalmakat kaphatnak. És referenciaként tekinthetnek a munkára.

Olyan jutalmazási eszközöket használunk, amiknek eredményessége bizonyított. A ranglisták funkciója az, hogy lássák a saját teljesítményüket a többiekéhez viszonyítva.
A magasabb helyezés elérésének reményében, ami által olyan információkhoz vagy szolgáltatásokhoz férhet hozzá, – mint a privát programok – , amihez mások nem, egy felhasználó gyakrabban látogat vissza a platformra és kutat hibák után.
Kézzel fogható eredményt jelent a számukra a jutalmazási rendszer, amelyeket különböző feladatok és küldetések teljesítéséért kaphatnak.

Tehát motiváció áll mögötte, valós kihívás.
Te viszont spórolsz a biztonsági büdzséden. Nálunk jutalék alapú fizetés van – csak akkor kell fizetned a jutalmat, ha sérülékenységet találtak az etikus hackerek a szolgáltatásodban.
Amíg egy standard vizsgálat során minden esetben kifizeted a cég szolgáltatását, akkor is, ha nem találnak semmit, addig a Bug Bounty esetében, ha nem találnak semmit, akkor nem fizetsz.

#3 BIZALOMÉPÍTÉS ÉS VERSENYELŐNY

Az emberek nem attól vásárolnak, akit kedvelnek.
Attól vásárolnak, akiben megbíznak.

A bizalomhoz pedig hozzátartozik a biztonságos üzleti viszony kiépítése is. Az adatvédelem. Folyamatosan hallani adatszivárgási botrányokról és cégekről, akiket megbüntettek. Holott a világ legnagyobb vállalatai is rendelkeznek bug bounty programmal.

A kockázatvállalás az üzleti sikerek fontos hajtóereje, egy bizonyos pontig. Onnantól kezelni kell a fennálló és várható kockázatokat.

Vajon kötsz-e Cascot a legújabb autódra? A pénzügyi védelmet életed számos területén alkalmazod. Mégis egy-egy elhanyagolt informatikai terület miatt akár 10 év munkája omolhat össze.

Viszik az adatbázisod, vele ügyfeleid adatait és bizalmát.
Legyen a legbiztonságosabb az oldalad és tűnj ki a versenytársaid közül. Legyél felkészülve az IT biztonsági auditokra! A Bug Bountyban való részvétel egy auditon evidenciaként is bemutatható.

#4 TE HATÁROZOD MEG A PROGRAM RÉSZLETEIT

Segítünk abban, hogy céged számára a legmegfelelőbb paramétereket határozd meg a teszteléshez.

A Bug Bounty sikerdíjas termék, te állítod be a hibavadász program szabályait, a jutalom nagyságát, minden díjazás és pénzügyi kiadás tőled függ. Mekkora pénzügyi jutalom jár a talált és elfogadott hibákra?

Te határozod meg, hogy mit akarsz átvizsgáltatni, megszabadhatod, hogy mire vagy kíváncsi és milyen metódus alapján teszteltetnél, milyen sérülékenységre vagy kíváncsi, melyik szolgáltatás kerüljön be a programba, van-e esetleg olyan része, ami out of scope. Azt is megszabhatod, hogy vannak-e tiltott módszerek, eszközök a tesztelés során.

Sérülékenységenként kézhez kapott riportokra vagy összesített jelentések kérésére – heti vagy havi – is adott a lehetőség.

Nemcsak a hibákat tárjuk fel, de javaslatokat is adunk az IT-szakembereidnek.

#5 A KÖNYVELÉSSEL MI FOGLALKOZUNK

Mi kezeljük a program teljes futását, beleértve a hackerek jutalmát, kapcsolódó adózási,könyvelési feladatokat is, így vállalkozásodnak csak a feltárt sérülékenységekkel kell foglalkoznia. A kiberbiztonsági tanácsadók jelentős része csupán sérülékenységi vizsgálatokat, behatolási teszteket végez.

Minden folyamatot kezelünk: neked nincs más dolgod, mint a riportokat kézhez venni. Ha módosítani szeretnél vagy netán költségkeretet állítani, akkor erre is van lehetőséged.
Amint elérted a projektre szánt költségkeretet, mi leállítjuk a folyamatodat.

A KIBERBIZTONSÁG OLYAN, MINT EGY AUTÓNÁL A FÉK: NÉLKÜLE LEHET GYORSABBAN MENNI, CSAK NEM ÉRDEMES

A kiberbiztonsági rizikók miatt kiemelkedő és elengedhetetlen a biztonsági kontrollok bevezetése a céged fejlődése szempontjából.

Olyan technikai intézkedésekkel támogatjuk a projektedet, mint felelősségbiztosítás, a folyamatosan bővülő szakmai tapasztalat, az egész folyamat kézben tartása.

Több mint 10 év szakmai hátterünk van IT biztonsági területen (Magyar Honvédség, pénzügyi szektor, kiberbiztonsági tanácsadó cégek, multinacionális pénzügyi vállalat, NATOnál információbiztonság); tapasztalatot szereztünk az adatvédelem, az ISO 27001 és GDPR projektek és antivírus szoftverek tanúsítása kapcsán. Jelen voltunk telekommunikációs nagyvállalatnál, mint sérülékenység menedzsment specialista. A HACKTIFY márkát 2020-ban álmodtuk meg.

CSEH PATRIK, MÉSZÁROS CSABA ÉS HIRLING PÉTER

A HACKTIFY MÁRKA, EGY BUG BOUNTY ÉS SÉRÜLÉKENYSÉG KÖZZÉTÉTELI PLATFORM MEGÁLMODÓI

A HACKTIFY egy új generációs IT biztonsági tesztelést kínál. A Bug Bounty megelőző megoldásközpontú programját biztosítva összeköti a cégeket az etikus hackerekkel, hogy kitűnhessenek biztonságukkal a versenytársak közül, a jogszabályi előírásoknak naprakészen megfelelhessenek és elkerülhessék akár a több millió forintos bírságokat.

A tapasztalatunk az, hogy a körülmények ugyan változnak, de a hackerek is fejlődnek. Tarts lépést velük! Velünk.

Agilis fejlesztés esetén a sok apró termékfejlesztés mellett a folyamatos tesztelés a „standard vizsgálatok által” követhetetlen, mert heti szinten kevesen fizetnének ki ekkora összeget egy klasszikus sérülékenységvizsgálatra.

Pedig a vizsgálatot meg kellene ismételni minden változtatás után a szolgáltatásban. Ennek hiányában a biztonsági sérülékenységekről nem szerzel tudomást. Erre a problémára nyújt megoldást a bug bounty program.
A komplex védelemben hiszünk. Adminisztráció, technika, humán interface folyamatos felügyeletében.

Egy hibavadász program futtatása előnyhöz juttat azáltal, hogy **proaktívan és prediktíven feltárja** a sérülékenységeidet. Külön humán erőforrás biztosítása nélkül, rögtön a sérülékenység kijavításával foglalkozhatsz!

HACKTIFY

A HACKTIFY EGY BUG BOUNTY ÉS SÉRÜLÉKENYSÉG KÖZZÉTÉTELI PLATFORM

Összekötjük a cégeket az etikus hackerekkel.

A szervezetek tesztelendő szolgáltatásainak részleteit és a tesztelési szabályokat feltöltjük az oldalunkra. A beregisztrált etikus hackerek láthatják ezeket és legális úton sérülékenységeket kereshetnek és jelenthetnek az oldalon keresztül.

A világ legnagyobb cégei rendelkeznek bug bounty programmal:
tartozz közéjük és tűnj ki a versenytársaid közül!

www.hacktify.eu

TALÁLJUK MEG A HIBÁKAT, MIELŐTT A ROSSZFIÚK TALÁLNÁK MEG ŐKET!

HACKTIFY BUG BOUNTY»

HACKTIFY