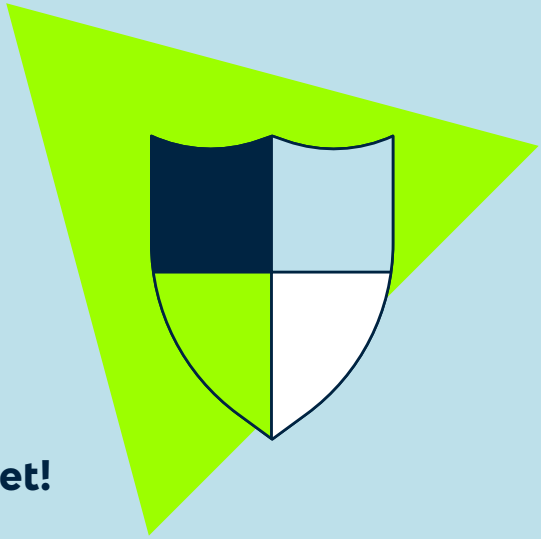
NetPajzs Szótár

Ismerd meg a kiberbiztonsági alapfogalmakat, a főbb veszélyeket és az ellenük bevethető védelmi eszközöket!



Tárgymutató

Adathalászat
Adathalászat elleni védelem
Adatlopás
Adatvédelmi incidens
Billentyűzetfigyelő
Biztonságszolgáltatás
Botnet
Botnet elleni védelem
CAPTCHA
Dark web
Fájl nélküli kártevő
Fehérlista, engedélyezési lista
Feketelista, tiltólista
Féreg
Hacker
Hátsóajtóprogram
Identitás- és hozzáférés-kezelés
Internetes megfélemlítés
IoT
Javítókészlet
Kártevő
Kártevőirtó
Kattintáseltérítés
Kémprogram
Kétfaktoros hitelesítés
Kétlépcsős hitelesítés
Kiberbiztonság
Közbeékelődéses támadás
Lehallgatás
Levélszemét
Pszichológiai manipuláció
Reklámprogramok elleni védelem
Robot
Rootkit
Sérülékenység
Személyazonosság-lopás
Szülői felügyelet
Szürkelista
Távoli asztali protokoll (Remote Desktop Protocol, RDP)
Titkosítás
Trójai program
Tűzfal
Végponti észlelés és reagálás
Végpontvédelem
Vírus
Vírusirtó
VPN
Zsarolóprogram

Yettel.

Fogalmak

Adathalászat

Az adathalászat az internetes csalás egyik formája, amely a felhasználó hitelesítő adatainak megtévesztés útján történő megszerzésére irányul. E körbe tartozik a jelszavak, a bankkártyaszámok, a bankszámlaadatok és más bizalmas információk eltulajdonítása. Az adathalász üzenetek rendszerint bankok, szolgáltatók, e-fizetési rendszerek és egyéb szervezetek hamis értesítéseiként érkeznek. Az adathalász kísérlet arra bátorítja a címzettet, hogy valamilyen okból adja meg vagy aktualizálja a személyes adatait. Gyakori indok lehet például „a fiókba való gyanús bejelentkezési kísérlet" vagy „jelszó lejárta".

Adathalászat elleni védelem

Az adathalászat elleni védelem a megtévesztő webhelyektől óvja a felhasználókat. Az ilyen webhelyek gyakran megbízható webhelyek tökéletes másolatai, amelyeknél ránézésre nem észlelhető különbség. A védelem a megtévesztő e-mailek észlelése és az adathalász webhelyek blokkolása révén érvényesül.

Adatlopás

Az adatlopás különleges adatok rosszindulatú személyek általi szándékos eltulajdonítása.

Adatvédelmi incidens

Adatvédelmi incidensnek nevezzük a biztonság olyan mértékű sérülését, amely a személyes adatok véletlen vagy jogosulatlan megsemmisítését, elvesztését, megváltoztatását, közlését, vagy az adatokhoz való jogosulatlan hozzáférést eredményezi.

Billentyűzetfigyelő

A billentyűzetfigyelő olyan kémszoftver, amely a számítógép billentyűzetén végrehajtott összes leütést rögzíti. A felhasználó által begépelt minden információt rögzít, így a csevegőüzeneteket, az e-maileket, a felhasználóneveket és a jelszavakat is.

Biztonságszolgáltatás

A biztonságszolgáltatás (Security as a Service, SECaaS) a felhőszolgáltatások egyik fajtája, amelynek keretében a szolgáltató a szolgáltatott biztonsági alkalmazás használatára nyújt lehetőséget az ügyfélnek. A SECaaS szolgáltatások körébe többek között olyan rendszerek tartoznak, amelyek az online e-mail- vagy dokumentumszerkesztők biztonsági szintjének emelését célozzák. A SECaaS-megoldás felhasználója használhatja a kínált alkalmazást, és módosíthat kisebb konfigurációs beállításokat annak érdekében, hogy a használt szolgáltatások biztonságosabbak legyenek. A SECaaS-szolgáltató feladata a biztonsági alkalmazás karbantartása. Az Allot Secure az első megoldás, amely széles körben kínál SECaaS szolgáltatásokat hálózati szolgáltatási előfizetőknek.

Botnet

A botnet kiberbűnöző által üzemeltetett C&C (command & control; parancs- és vezérlő) kiszolgálóval távolról vezérelt kártékony programokat futtató, feltört számítógépek együttese. A kiberbűnözők automatizált folyamatokon (robotokon) keresztül végeznek távvezérlést nyilvános IRC-csatornákon vagy webhelyeken. (Ilyen webhelyeket üzemeltethetnek közvetlenül a „botgazdák", illetve lehetnek megbízható webhelyek, amelyeket e célból eltérítettek.)

Botnet elleni védelem

A botnet elleni eszközök automatikusan végeznek botnetellenőrzéseket, amikor a felhasználó valamely webhelyen böngész. Kockázat észlelése esetén figyelmeztető üzenetet küldenek az eszköznek. A botnet elleni megoldások közül a leggyakoribb a CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart; teljesen automatizált, nyilvános Turing-teszt a számítógép és az ember megkülönböztetésére).

CAPTCHA

A CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart; teljesen automatizált, nyilvános Turing-teszt a számítógép és az ember megkülönböztetésére) feladat megoldásán alapuló teszt, amely webhelyeken gyakran használatos annak ellenőrzésére, hogy a felhasználó

valódi ember, nem pedig robot. Ilyen feladat lehet egyszerű számtani feladvány vagy képekkel kapcsolatos kérdés, amelynek megválaszolása nehézséget okoz a robotok számára.

Dark web

A dark web, azaz sötét web az internet titkosított részeinek összessége, amelyet nem indexelnek a keresőmotorok, és arról hírhedt, hogy különféle bűnözők, köztük pedofilok, emberkereskedők, csempészek és kiberbűnözők használják kommunikációra és információmegosztásra anélkül, hogy a bűnüldöző szervek észlelnék vagy azonosítanák őket. A sötét weben különféle kártevők is vásárolhatók. A mély web egyik részét képezi, amely a megfelelő URL-címen keresztül bárki számára hozzáférhető. A sötét web lapjai különleges szoftverrel (például Tor böngészővel) nyithatók meg a megfelelő visszafejtési kulcs és hozzáférési jogosultságok, valamint a tartalmak megtalálásához szükséges tudás birtokában. A sötét web felhasználói szinte teljesen névtelenek maradnak a P2P hálózati kapcsolatok miatt, amelyek nagyban megnehezítik a hálózati tevékenység nyomon követését.

Fájl nélküli kártevő

A fájl nélküli kártevő (Fileless Malware, FM) más néven „fájlmentes kártevő" vagy „fájl nélküli fertőzés" a kártékony számítógépes támadások egyik formája, amely kizárólag a felejtő adattárolási összetevőket, például a RAM-ot, továbbá a memóriafolyamatokat és a szolgáltatási területeket érinti. Ez különbözteti meg a kártevők e formáját a hagyományos rezidens vírusoktól, amelyeknek permanens adathordozóval, például merevlemezes meghajtóval vagy pendrive-val kell érintkezésbe lépnie. A rendszerint kártékony webhelyek felkeresése során bekerülő fájl nélküli kártevők nem léteznek a szokványos víruskereső programok által észlelhető fájlként. A számítógép munkamemóriájában rejtőzködnek, és rendkívül nehéz felismerni őket. A kártevők e típusa azonban ritkán marad a memóriában a számítógép újraindítása után is, amelyet követően a számítógépnek újra a fertőzés előtti módon kell működnie.

Fehérlista, engedélyezési lista

A fehérlista, engedélyezési lista vagy kivétellista a használatban lévő szűrőn, szabályrendszeren automatikusan átengedett elemek felsorolását tartalmazza.

Feketelista, tiltólista

A feketelista vagy tiltólista alapvető hozzáférés-vezérlési mechanizmus, amely bizonyos elemeket, például e-mail-címeket, felhasználókat, jelszavakat, URL-címeket, IP-címeket, tartományneveket, fájlkivonatokat stb. átenged a rendszeren, a kifejezetten megjelölteket viszont letiltja.

Féreg

A féreg olyan számítógépes program, amely az áldozat eszközére telepíti magát, majd módot keres arra, hogy más számítógépekre is átterjedjen, miközben kárt okoz a hálózat bizonyos részeinek leállításával.

Hacker

A hacker általában olyan személyre utal, aki megpróbál jogosulatlanul hozzáférni a hálózathoz, számítógéprendszerhez és/vagy adatokhoz.

Hátsóajtóprogram

A hátsóajtóprogramot arra használják a támadók, hogy hozzáférjenek a számítógéphez, a hálózathoz és/vagy adatokhoz. A számítógéprendszer vagy hálózatok ellen intézett támadás esetén egy programozó kiskapuk használatával kikerülheti a biztonsági lépéseket, és hozzáférhet a számítógéphez. A támadók emellett arra is használhatnak ilyen mechanizmusokat, hogy megfelelő engedély nélkül hatoljanak be számítógépekbe vagy hálózatokba.

Identitás- és hozzáférés-kezelés

Az identitás- és hozzáférés-kezelés (Identity and Access Management, IAM) az a folyamat, amellyel a szervezet engedélyezheti vagy megtagadhatja a hozzáférést a biztonságos rendszeréhez. Az IAM munkafolyamat-rendszereket integrál, aminek keretében aminek keretében a szervezet rendszerei alkalmazzák a szükséges biztonsági intézkedéseket, és hatékonyabbá teszik a működésüket.

Internetes megfélemlítés

Az internetes megfélemlítés elektronikus eszközök, elsősorban üzenetküldő és közösségimédia-platformok használata az áldozat

megfélemlítésére és zaklatására. Az internetes megfélemlítés különösen a fiatalok körében vált jelentős problémává, ugyanis felerősítheti a megfélemlítők agresszív viselkedését, valamint – a szülők és a tanárok számára nehezen észlelhető módon – lehetőséget ad az áldozatok széles körű, nyilvános kigúnyolására és káros tevékenységek folytatására.

IoT

A dolgok internete (Internet of Things, IoT) olyan hétköznapi használati tárgyakat foglal magában, amelyek az internethez kapcsolódnak, és képesek automatikusan, emberi közreműködés nélkül adatokat gyűjteni és továbbítani. A dolgok internete minden olyan létező tárgyat (tehát nem csak hagyományos számítógépeket) felölel, amelyhez IP-cím rendelhető, és amely képes adatokat továbbítani. E körbe tartoznak a háztartási készülékek, közüzemi mérőórák, gépjárművek, zárt láncú kamerarendszerek (CCTV) vagy akár az emberek által igénybevett egészségügyi eszközök is (például szívimplantátumok).

Javítókészlet

A javítókészlet kiegészítő, átdolgozott vagy frissített programkódot ad hozzá az operációs rendszerhez vagy valamely alkalmazáshoz. A nyílt forráskódú szoftverek kivételével a szoftvergyártók többsége nem hozza nyilvánosságra a forráskódot. A javítókészlet tehát rendszerint már meglévő program (telepítő használatával történő) javítására szolgáló bináris kódból áll.

Kártevő

A kártevő gyűjtőfogalom, amely a felhasználó számítógépébe rosszindulatúan behatoló szoftverek összes fajtáját magában foglalja.

Kártevőirtó

A kártevőirtó olyan program, amely a vírusokból, például reklámprogramból, kémprogramokból és más hasonló kártékony programokból fakadó veszélyforrásokkal és az általuk okozott támadásokkal szemben védi a számítógépeket és a hálózatokat.

Kattintáseltérítés

A kattintáseltérítés keretében csalárd módon rávesznek valakit, hogy kattintson a weblapon lévő egyik objektumra, miközben azt hiszi, hogy másvalamire (egy megbízható hovatkozásra vagy funkcióra) kattint. A támadó átlátszó oldalt tölt be a weblap tényleges tartalma fölé, így az áldozat azt hiszi, hogy megbízható elemre kattint, ám valójában a támadó láthatatlan lapján lévő objektumot nyitja meg. Így a támadó saját céljaira eltérítheti az áldozat kattintását. A kattintáseltérítés alkalmazható kártevő telepítésére, az áldozat egyik online fiókjához való hozzáférésre vagy az áldozat webkamerájának bekapcsolására.

Kémprogram

A kémprogram a felhasználó eszközére titokban, különleges adatok gyűjtése céljából telepített szoftver. A kémprogram észrevétlenül gyűjt és a harmadik félnek, rosszindulatú személyeknek küld különféle információkat, például hitelesítő adatokat. A kémprogramot gyakran ingyen letölthető fájl tartalmazza, és felhasználói hozzájárulással vagy anélkül, automatikusan települ.

Kétfaktoros hitelesítés

A kétfaktoros hitelesítés (2FA) egy állandó jelszó és külső hitelesítő eszköz, például véletlenszerűen generált, egyszeri jelszót generáló hardvertoken, intelligens kártya, SMS-üzenet (ahol a mobiltelefon a token) vagy egyedi testi jellemző, például ujjlenyomat együttese.

Kétlépcsős hitelesítés

A kétlépcsős hitelesítés webhelyek esetében elterjedt, és előrelépést jelent az egyfaktoros hitelesítéshez képest. A hitelesítés e formája felhasználónév (tehát identitásjogcím) és jelszó megadására (azaz egyfaktoros hitelesítésre), majd további lépés végrehajtására kötelezi a látogatót. A további lépés lehet kódot tartalmazó szöveges üzenet fogadása, majd a kód megadása a webhelyen megerősítés céljából. Egyéb alternatíva lehet e-mail fogadása és a kapott üzenetben szereplő hivatkozásra kattintás megerősítés céljából, illetve előre kiválasztott kép és állítás megtekintése, majd újabb jelszó vagy PIN-kód beírása.

Kiberbiztonság

A kiberbiztonság körébe a szervezet információit hordozó környezet, alkalmazás, eszköz

lopással vagy támadással szembeni védelmére szolgáló folyamatok tartoznak. A lehetséges veszélyforrások, például vírusok és más hasonló kártékony objektumok beható ismeretét igényli. Az identitáskezelés, a kockázatkezelés és az incidenskezelés képezi a szervezet kiberbiztonsági stratégiáinak magját.

Közbeékelődéses támadás

A közbeékelődéses támadás (Man-in-the-Middle Attack, MITM) olyan támadási forma, amelynél a támadó titokban késlelteti és adott esetben módosítja a kommunikációt két fél között, akik közben azt feltételezik, hogy közvetlenül kommunikálnak egymással. Például az áldozat azt feltételezi, hogy a bankja webhelyéhez kapcsolódik, a közte és a bankja valódi webhelye közötti adatforgalom pedig zavartalanul zajlik, így az áldozat nem fog gyanút. A támadó azonban átirányítja az adatforgalmat a saját webhelyére, ezáltal pedig összegyűjtheti az áldozat által megadott személyes adatokat (bejelentkezési név, jelszó, PIN-kód stb.).

Lehallgatás

Csomaglehallgatással a hálózaton keresztüli továbbítás közben rögzíthetők adatok. A csomaglehallgató programokat hálózati szakemberek használják hálózati problémák diagnosztizálására. Rosszindulatú személyek lehallgató használatával titkosítatlan adatokat, például jelszavakat és felhasználóneveket rögzíthetnek a hálózati forgalomban. Ezen információk rögzítése után a rosszindulatú személyek behatolhatnak a rendszerbe vagy a hálózatba.

Levélszemét

A levélszemét a kéretlen e-mailek általánosan használt megnevezése. Lényegét tekintve nemkívánatos reklám, a postai úton kézbesített, valódi levélszemét e-mailes megfelelője.

Pszichológiai manipuláció

A pszichológiai manipuláció egyre elterjedtebb módszer, amely betörés vagy hackelési technikák alkalmazása helyett az emberi lélektani jellegzetességek kihasználásával és a felhasználók manipulálásával teszi lehetővé az erőforrásokhoz való engedély nélküli hozzáférést. Ahelyett, hogy a vállalati rendszerben használt szoftverek sebezhető pontját próbálná megtalálni, a pszichológiai manipulátor magát az IT-részleg munkatársának kiadva e-mailt küldhet az egyik alkalmazottnak, hogy különleges információk felfedésére vegye rá. A pszichológiai manipuláció a célzott adathalász támadások alapja.

Reklámprogramok elleni védelem

A reklámprogramok vég nélküli reklámokkal és felugró ablakokkal ostromolják a felhasználókat, és rontják a felhasználói élményt. A reklámprogramok ráadásul valós veszélyt is jelenthetnek az eszközökre nézve, a nemkívánatos reklámok pedig kártevőket tartalmazhatnak, vagy a felhasználók személyes adatait gyűjtő, kártékony webhelyre irányíthatnak át. A reklámprogramok gyakran ingyenes vagy kipróbálható programokba épülnek be, amelyek révén a reklámprogram üzemeltetője közvetve szed be díjat a program használatáért. A reklámprogramok rendszerint semmilyen módon nem mutatják jelenlétüket a rendszerben. A reklámprogramok ritkán tartalmaznak eltávolítási eljárást, a manuális eltávolításukra tett kísérlet pedig működési zavart okozhat az eredeti hordozóprogramjukban.

Robot

A robot olyan program, amely műveleteket automatizál valamely fél nevében másik program vagy személy számára, és rutinfeladatok elvégzésére szolgál. Kártékony célra használható többek között levélszemét terjesztéséhez, hitelesítő adatok gyűjtéséhez és DDoS-támadások indításához.

Rootkit

A rootkit olyan szoftvereszköz-gyűjtemény vagy program, amellyel egy hacker távolról hozzáférhet a számítógéphez vagy hálózathoz, és vezérelheti azt. Maguk a rootkitek közvetlenül nem okoznak kárt, és az ilyen jellegű szoftverek jogszerű célra, például távoli végfelhasználói támogatás nyújtására is használhatók. Azonban a legtöbb rootkit hátsó ajtót nyit a célszámítógépen kártevők, vírusok és zsarolóprogramok telepítéséhez vagy a rendszer további hálózati biztonsági támadásokra való felhasználásához. A rootkitet jellemzően lopott jelszóval vagy a rendszer sebezhető pontjainak kihasználásával, az áldozat tudtán

kívül telepítik. A legtöbb esetben a rootkiteket más kártevővel együtt használják, hogy a végponti víruskereső ne észlelje őket.

Sérülékenység

A sérülékenység egy szoftver olyan gyengesége, amelyet kihasználva a hackerek behatolhatnak az eszközbe.

Személyazonosság-lopás

Személyazonosság-lopás akkor valósul meg, ha egy rosszindulatú személy elegendő személyes adatot (név, cím, születési idő stb.) gyűjt áldozatáról ahhoz, hogy személyazonossággal való visszaélést kövessen el, tehát a lopott hitelesítő adatokat arra használja, hogy megtévesztő módon termékeket vásároljon vagy szolgáltatásokat vegyen igénybe. A lopott adatok felhasználhatók az áldozat nevére szóló új fiók vagy számla (például bankszámla) létrehozására, az áldozat meglévő fiókja vagy számlája (például közösségimédia-fiókja) feletti irányítás átvételére vagy arra, hogy a támadó bűncselekmény elkövetése közben az áldozatnak adja ki magát.

Szülői felügyelet

A szülői felügyeleti beállítások körébe olyan, digitális televíziós szolgáltatásokban, számítógépes és videojátékokban, mobileszközökön és szoftverekben megtalálható funkciók tartoznak, amelyekkel a szülők korlátozhatják gyermekük hozzáférésének mértékét vagy idejét bizonyos tartalmakhoz. Ezek a beállítások arra szolgálnak, hogy a szülők könnyebben felügyelhessék, milyen jellegű tartalmakat, illetve mikor tekinthet meg a gyermekük.

Szürkelista

A szürkelista átmenetileg, további lépések végrehajtásáig letiltott (vagy átmenetileg engedélyezett) elemeket tartalmaz.

Távoli asztali protokoll (Remote Desktop Protocol, RDP)

Az RDP Windows operációs rendszerű számítógépekhez való távoli csatlakozásra szolgáló protokoll. Lehetővé teszi az asztali elemekkel való interakciót és más eszközerőforrásokhoz való hozzáférést. Az RDP eredeti rendeltetése szerint távfelügyeleti eszköz volt. Azonban a behatolók gyakran használják arra, hogy bejussanak a célszámítógépekbe. A kiberbűnözők a helytelenül konfigurált RDP-beállításokat vagy a rendszerszoftver sebezhetőségét kihasználva eltéríthetik az RDP-munkamenetet, és az áldozat engedélyeit használva bejelentkeznek a rendszerbe.

Titkosítás

A titkosítás az adatok bizalmasságának megőrzésére irányuló folyamat, amelynek keretében az egyszerű adatokat titkosítási algoritmus segítségével titkos kóddá alakítják. A felhasználók csak a megfelelő visszafejtési kulcs birtokában fejthetik vissza és ismerhetik meg a titkosított adatokat vagy rejtjelezett szöveget.

Trójai program

A trójai programok kártékony programok, amelyek a felhasználó által nem engedélyezett műveleteket hajtanak végre: adatokat törölnek, tiltanak le, módosítanak vagy másolnak, illetve zavarják a számítógépek vagy a számítógépes hálózatok működését. A vírusokkal és a férgekkel ellentétben a trójai programok nem tudnak másolatot készíteni önmagukról, azaz nem képesek önsokszorosításra.

Tűzfal

A tűzfal biztonsági rendszer, amely virtuális védelmi vonalat képez a munkaállomások hálózata körül, hogy megakadályozza a vírusok, férgek és hackerek bejutását.

Végponti észlelés és reagálás

A végponti észlelés és reagálás (Endpoint Detection and Response, EDR) körébe a számítógépes végpontok lehetséges veszélyforrásokkal szembeni védelmére szolgáló eszközök tartoznak. Az EDR-platformok olyan szoftver- és hálózati eszközöket foglalnak magukban, amelyekkel jellemzően folyamatos felügyelet útján észlelhetők a gyanús végponti tevékenységek.

Végpontvédelem

A végpontvédelem olyan hálózatbiztonság-kezelési rendszer, amely a hálózati végpontokat - vagyis a hálózathoz való hozzáférésre használt hardvereszközöket, például munkaállomásokat és mobileszközöket - felügyeli.

Vírus

A vírus kártékony számítógépes program, amely gyakran e-mail-mellékletként érkezik

vagy letöltéssel kerül az eszközre, hogy megfertőzze. Miután az eszköz megfertőződött, a vírus eltérítheti a webböngészőt, nemkívánatos hirdetéseket jeleníthet meg, levélszemetet küldhet, bűnözők számára hozzáférhetővé teheti az eszközt és a névjegyzéket, letilthat biztonsági beállításokat, átvizsgálhatja az eszközt, valamint személyes információkat, például jelszavakat tárhat fel.

Vírusirtó

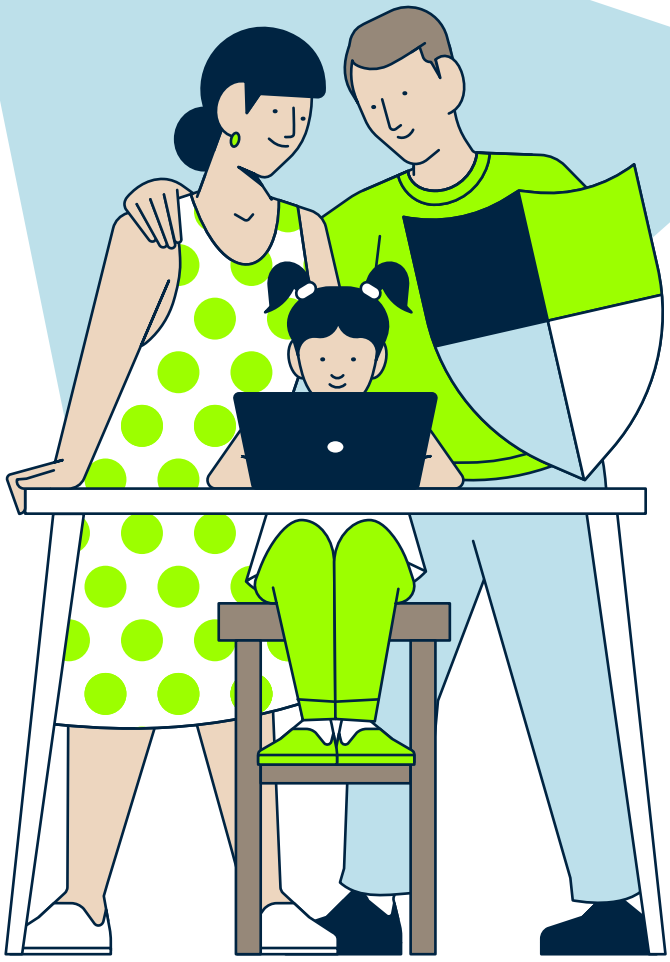
A vírusirtó megoldások a legújabb generációs víruskeresési technológiát tartalmazzák, hogy védelmet nyújtsanak a felhasználóknak olyan vírusokkal, kémprogramokkal, trójai programokkal és férgekkel szemben, amelyek e-mailen keresztül vagy internetezés közben fertőzhetik meg az eszközüket.

VPN

A virtuális magánhálózat (Virtual Private Network, VPN) nyilvános hálózaton keresztül terjeszt ki magánhálózatot, és lehetővé teszi, hogy a felhasználók úgy küldjenek és fogadjanak adatokat titkosítva megosztott vagy nyilvános hálózaton keresztül, mintha a számítástechnikai eszköz közvetlenül a magánhálózathoz kapcsolódna. Lényegét tekintve virtuális, biztonságos folyosó.

Zsarolóprogram

A zsarolóprogramok közé olyan kártékony programok tartoznak, amelyek célja pénz kizsarolása az áldozatoktól a számítógépükhöz való hozzáférés letiltása vagy a tárolt adataik titkosítása útján. A kártevő üzenetet jelenít meg, amely a rendszer vagy az adatok fizetés ellenében történő visszaállítását ajánlja. Az ilyen csalást elkövető kiberbűnözők néha bűnüldöző szerv tagjának adják ki magukat, hogy tevékenységük hitelességének látszatát keltsék. Zsarolóüzenetükben azt állítják, hogy azért zárolták a rendszert vagy titkosították az adatokat, mert az áldozat nem licencelt szoftvert futtat, vagy jogellenes tartalmakhoz jutott hozzá, emiatt pedig pénzbírságot kell fizetnie.



Yettel.