Parengė IM Artūras Šakalys, 2024 m.

Konspektas

Kibernetinis saugumas

Kibernetinis saugumas yra technologijų, procesų ir praksių rinkinys, skirtas apsaugoti informacijos technologijų sistemų, tinklų ir duomenų nuo neteisėtų prieigų, nepageidaujamų įsibrovimų, duomenų vagysčių ir kitų kibernetinių grėsmių. Kibernetinis saugumas taip pat apima prevencinius metodus, kaip užkirsti kelią įsilaužimams, bei reakcines priemones, kaip greitai atkurti sistemos funkcionavimą po įvykio.

Kibernetinis saugumas yra itin svarbus šiuolaikiniam verslui, vyriausybėms ir privatiems asmenims, nes kibernetinės grėsmės nuolat tobulėja ir tampa vis sudėtingesnės. Todėl būtina nuolat tobulinti kibernetinį saugumą, naudojant naujausias technologijas, atnaujinant saugumo sistemas ir tinklų infrastruktūrą bei užtikrinant sąmoningumą ir apmokymus darbuotojams.

Kibernetinės atakos ir grėsmės

Kenkėjiška programinė įranga

Kenkėjiška programinė įranga yra programavimo kodas, kuris buvo sukurtas su blogais tikslais. Ši programinė įranga gali būti naudojama kenkėjiškai, kad būtų sukeltas žala kompiuteriams ar duomenims. Pavyzdžiui, kenkėjiška programa gali būti virusas, kuris įsiskverbia į kompiuterį ir pažeidžia failus, arba šnipinėjimo programa, kuri sekioja vartotojo veiklą be jo žinios.

Kenkėjiška programinė įranga gali būti paplitusi internete ir būti įrašyta į kompiuterį be vartotojo sutikimo. Todėl svarbu būti atsargiam, kai siunčiamos ar atsisiunčiamos programos iš nežinomų šaltinių ir visada naudoti patikimas antivirusines programas, kad būtų galima apsaugoti savo duomenis ir kompiuterį nuo kenkėjiškos programinės įrangos.

Phishing yra apgaulinga interneto sukčiavimo technika, kai bandymai įsilaužti į asmens duomenis, pvz., slaptažodžius, kreditinius kortelės duomenis arba kitus jautrius duomenis, yra vykdomi kenkėjišku būdu. Dažniausiai ši technika naudojama elektroninio pašto arba socialinių tinklų kanalais, siunčiant apgaulingus pranešimus, kuriuose įtikinami naudotojai pateikti savo jautrius duomenis. Tai pavojinga veikla, kurios metu asmenys gali patirti finansinių nuostolių ar padaryti žalą savo internetiniam saugumui.

Išpirkos reikalaujanti programinė įranga yra žalinga programinė įranga, kuri įsiskverbia į kompiuterį ar kitą elektroninį įrenginį, užšifruoja vartotojo failus ir reikalauja išpirkos sumokėjimo norint atšifruoti šiuos failus. Dažniausiai išpirkos reikalaujančios programos yra platinamos per kenksmingus el. laiškus, infekuotas interneto svetaines ar kitus šaltinius.

Kai įrenginys užkrėstas išpirkos reikalaujančią programine įranga, vartotojas praranda prieigą prie savo failų, o kenkėjai reikalauja išpirkos sumokėjimo (dažniausiai bitkoinais ar kitomis kriptovaliutomis) už atkūrimą raktą. Tačiau net ir sumokėjus išpirką, nėra garantijos, kad kenkėjai atšifruos failus ar palaikys savo žodį.

Dėl šios priežasties ekspertai rekomenduoja reguliariai atsarginės kopijos savo duomenims, naudotis patikima antivirusine programa ir atidžiai stebėti el. laiškus ir interneto naršymo veiklą, kad išvengti išpirkos reikalaujančių programų atakų.

Parengė IM Artūras Šakalys, 2024 m.

Atsisakymas teikti paslaugas (DOS) yra situacija, kai paslaugų teikėjas arba tiekėjas atsisako suteikti savo paslaugas vartotojui ar klientui. Tai gali būti padaryta dėl įvairių priežasčių, tokių kaip nepakankami ištekliai, nepasiekiamumas, arba tiesiog noras nesuteikti paslaugų tam tikrai asmeniui ar grupei žmonių. Atsitakymas gali būti ir dubijuojantis sąžiningais motyvais, tačiau dažniausiai tai kelia konfliktus tarp paslaugų teikėjo ir kliento. Šio teisės akto nustatyta tvarka klientui turi būti padedama rasti kitą paslaugų teikėją ar spręstas jo problemas.

1. Įsilaužimas į sistemos ar tinklą - galimas pasekmes gali būti duomenų vagystė ar sugadinimas, sistemų veikimo sutrikimai ar net išnaudojimas.

2. "Phishing" atakos - tai interneto sukčiavimo būdas, kai bandymas apgauti vartotojus ir gauti jų asmeninę informaciją, tokią kaip slaptažodžiai ar slapukai.

3. Malware įsijungimas - virusai, trojanai, kirminai ir kita kenksminga programinė įranga gali sugadinti duomenis, vartotojo įrenginį ar netgi palengvinti įsilaužėliams gauti prieigą prie sistemos.

4. DoS (Tarnybos atsisakymo) ataka - tai būdas perkrauti tinklą ar serverį didelėmis duomenų srautais, dėl kurių ši sistema nebegali tinkamai veikti ir laikinai atsiranda nepasiekiamumas.

5. "Man in the Middle" ataka - tai būdas, kai įsilaužėlis įsiterpia tarp komunikavimo tarp dviejų šalių ir gauna galimybę pasiekti ir modifikuoti duomenis.

6. Socialinis inžinierius - tai tipas atakos, kai įsilaužėlis naudoja manipuliacijas arba apgaulingus metodus, kad apgautų žmones ir gautų neleistą prieigą prie jų duomenų ar sistemos.

Įgyvendinant tinkamus saugumo priemones, tokius kaip stiprus slaptažodis, atnaujintos programinės įrangos naudojimas ir apsauginės programos, galite sumažinti atakų ir grėsmių riziką. Taip pat svarbu būti protingiems ir atsargiems, susiduriant su nežinomais ar įtartinais elgesiais arba pranešimais internete.

Pavieniai įsilauželiai yra asmenys, kurie netikėtai arba neleidžiantį patekia į uždarą ar saugomą vietą be leidimo ar pakvietimo. Jie gali bandyti įsibrauti į pastatus, svečių kambarius ar kitas teritorijas be leidimo arba įsilaužti į kompiuterinius tinklus. Šie individai dažniausiai ieško asmeninių ar finansinių duomenų, siekdami įsilaužti į sistemą ar gauti kitą naudą. Tai kriminalinis veiksmas, kuris gali turėti rimtų pasekmių tiek asmeniui, tiek organizacijai, į kurią buvo įsilaužta.

Smulkūs nusikaltėliai yra asmenys, kurie vykdo nedidelius nusikaltimus arba pažeidimus, tokius kaip vagystė, apgavystė, smurtas, narkotikų prekyba, vagystė iš maisto parduotuvės ir pan. Šie nusikaltėliai dažnai būna jauni ir nepatyrę, tačiau gali būti bet kurio amžiaus ar lyties. Smulkūs nusikaltėliai dažnai siekia lengvai gauti pinigus arba kitas materialines gėrybes, nesijaudindami dėl padaromų veiksmų padarinių ar netikėtų pasekmių. Tačiau reikia paminėti, kad smulkūs nusikaltėliai gali sukelti didelę žalą aukoms ir bendruomenei, todėl svarbu imtis veiksmų šiems nusikaltėliams sustabdyti bei užtikrinti teisingumą.

Tai asmenys, kurie vykdo organizuotą nusikalstamą veiklą, bendradarbiaudami ir struktūrizuotai planuodami nusikaltimus. Šios grupuotės dažnai turi lyderius, narių hierarchiją, atsakomybės dalijimąsi ir bendras taisykles bei procedūras veiklai vykdyti. Jų tikslas gali būti finansinis pelnas, kontrolės išlaikymas tam tikroje teritorijoje ar kitos neteisėtos priežastys.

Organizuotų nusikaltelinių grupuočių veikla gali apimti prekybą nelegaliais narkotikais, ginklais, žmonėmis, vagystes, pinigų plovimą, smurtinį išnaudojimą ir kitus nusikaltimus. Šios grupuotės dažnai veikia slaptai, stengdamiesi išlikti nepastebėti ir išvengti teisėsaugos institucijų įsikišimo.

Parengė IM Artūras Šakalys, 2024 m.

Organizuotos nusikalstamos grupuotės kelia rimtą grėsmę visuomenės saugumui ir teisėtvarkai, todėl joms skiriama daug dėmesio kovojant su organizuotu nusikalstamumu. Teisėsaugos institucijos stengiasi nustatyti ir neutralizuoti šias grupuotes, atpažindamos jų veikėjus, įrodymus ir bendradarbiavimo ryšius. Hacktyvistai yra žmonės, kurie naudoja savo technologinius gebėjimus ir kompiuterinių įgūdžių norėdami remti politinį ar socialinį judėjimą, arba siekiant kovoti su neteisingumu ir korupcija. Jie gali atlikti įsilaužimus į įmonių ar valdžios institucijų sistemas, kad atskleistų slaptą informaciją ar išreikštų savo politinius įsipareigojimus. Kartais jie gali naudoti savo galias internete siekiant išplatinti svarbias naujienas ar užkirsti kelią neteisingam elgesiui. Hacktyvistai gali būti pasaulinio masto veikėjai, atliekantys klaidingus veiksmus ar tiesiog atskleisdami svarbią informaciją, siekdami pakeisti visuomenės požiūrį. Tai yra sudėtingas ir kartais kontroversiškas veikėjų tipas, turintis tiek šalininkų, tiek priešininkų.

Valstybės remiami nusikalteliai yra asmenys ar organizacijos, kurie gauna finansinę ar kitokią paramą iš valstybės institucijų ar valdžios atstovų ir tuo pačiu metu dalyvauja nusikalstamoje veikloje. Tai gali būti tiek maži nusikaltimai, kaip pavogimas ar vagystė, tiek dideli nusikaltimai, kaip prekyba narkotikais ar net teroristiniai aktai.

Valstybės remiami nusikalteliai gali veikti įvairiose srityse, tokiomis kaip korupcija, nusikalstama veikla, terorizmas ar net valstybės finansų iššvaistymas. Šie asmenys dažnai naudojasi savo padėtimi valstybės institucijose ar politinėje erdvėje, kad galėtų veikti be pasekmių ar gauti palaikymą iš įtakingų asmenų.

Valstybės remiami nusikalteliai yra pavojingi visuomenei ir valstybei, nes jie gali kelti grėsmę teisinei valstybei, viešajai tvarkai ir žmonių saugumui. Todėl svarbu veiksmingai kovoti su jais ir užkirsti jiems kelią veikti nebaudžiamai.