# Llojet e llogarive me të drejta të privilegjuara për të cilat duhet të jeni në dijeni

| | PËRDORIMI | VEKTORËT E SULMIT | SI TË MBROHENI |
|---|---|---|---|
| **LLOGARITË RRËNJË(ROOT) OSE TË SUPER PËRDORUESVE** | Ka nivelin më të lartë të aksesit dhe kontrollit mbi një sistem ose rrjet. Ato përdoren zakonisht për mirëmbajtjen e sistemit, konfigurimin dhe instalimin e softuerit ose përditësimeve | Sulmuesit shpesh synojnë këto llogari përmes vulnerabiliteteve në sistemet operative ose përmes inxhinierisë sociale për të marrë ose shfrytëzuar aksesin rrënjësor | Zbatoni autentifikim të fortë, përditësoni rregullisht sistemin operativ, kufizoni aksesin te administratorët e besuar |
| **LLOGARITË E ADMINIT** | Llogaritë e administratorit janë të përhapura në sistemet Windows dhe kanë privilegje të gjera aksesi për të menaxhuar llogaritë e përdoruesve, për të instaluar software dhe për të konfiguruar cilësimet e sistemit. | Sulmuesit mund të shfrytëzojnë vulnerabilitete, të përdorin sulme *brute force* ose të përfshihen në përshkallëzimin e privilegjeve për të kompromentuar llogaritë e administratorit. | Zbatoni politika të forta fjalëkalimi, zbatoni vërtetimin me dy faktorë, kufizoni aksesin administrativ për personelin e nevojshëm |
| **LLOGARITË E BAZËS SË TË DHËNAVE** | Menaxhon dhe mirëmban sistemin e bazës së të dhënave, kontrollon aksesin në bazat e të dhënave, ekzekutimin, kopjet rezervë dhe optimizimin e performancës. | Sulmuesit mund të shfrytëzojnë konfigurime të dobëta të bazës së të dhënave, dobësi të injektimit SQL ose të kenë akses nëpërmjet sulmeve phishing | Përdorni kontrolle të forta të hyrjes në bazën e të dhënave, përditësoni rregullisht softuerin e bazës së të dhënave, zbatoni parimet më të vogla të privilegjeve. |
| **LLOGARITË E SHËRBIMIT** | Përdoret nga aplikacionet ose serverët për të hyrë në bazat e të dhënave dhe burimet e tjera. Ato shpesh konfigurohen nëpërmjet privilegjeve të larta | Sulmuesit mund t'i komprometojnë këto llogari nëpërmjet vulnerabiliteteve në aplikacionet që ata shërbejnë, kredencialeve të dobëta ose përshkallëzimit të privilegjeve. | Mbroni aplikacionet, kufizoni privilegjin e llogarisë së shërbimit në atë që është e nevojshme, siguroni rregullisht fjalëkalimet e llogarisë së shërbimit, monitoroni aktivitetin e llogarisë së shërbimeve. |
| **LLOGARITË E APLIKACIONEVE** | Këto llogari përdoren për të ekzekutuar aplikacione ose shërbime specifike me leje të paracaktuara për të kryer detyra specifike. | Sulmuesit mund të synojnë vulnerabilitetet e aplikacionit, të shfrytëzojnë lejet e konfiguruara dobët ose të përdorin kredencialet e vjedhura , për të fituar akses të paautorizuar. | Siguroni aplikacionet, zbatoni parimin e privilegjit më të vogël për llogaritë e aplikacioneve, monitoroni dhe kontrolloni rregullisht aktivitetin e aplikacioneve |
| **LLOGARITË E SHITËSIT OSE PALËS SË TRETË** | Shitësit e palëve të treta mund të kërkojnë akses të privilegjuar për të ofruar mbështetje ose shërbime për organizatat. | Sulmuesit mund t'i komprometojnë këto llogari nëpërmjet sulmeve *"supply chain"*, inxhinierisë sociale ose shfrytëzimit të vulnerabiliteteve në praktikat e sigurisë së shitësit. | kontrolloni aktivitetin e palëve të treta, kufizoni aksesin e jashtëm, kërkoni vërtetim të fortë dhe kontrolle aksesi për llogaritë e palëve të treta |
| **LLOGARITË E PËRDORUESVE TË PRIVILEGJUAR** | Llogaritë e përdoruesve të privilegjuar përdoren nga punonjës ose administratorë që kanë nevojë për akses të lartë për detyra specifike, të tilla si konfigurimi i rrjetit, menaxhimi i serverit ose monitorimi i sigurisë. | Kërcënimet e brendshme, inxhinieria sociale ose sulmet phishing mund të përdoren për të kompromentuar llogaritë e përdoruesve të privilegjuar. | Edukoni punonjësit për praktikat më të mira të sigurisë, zbatoni politika të forta fjalëkalimi, monitoroni dhe kontrolloni rregullisht aktivitetin e llogarisë së përdoruesit të privilegjuar |
| **LLOGARITË E EMERGJENCËS** | Këto llogari zakonisht rezervohen për akses urgjent në sisteme ose të dhëna kur aksesi standard nuk është i disponueshëm. | Sulmuesit mund të synojnë këto llogari përmes menaxhimit të dobët të fjalëkalimit, aksesit të paautorizuar ose shfrytëzimit të procedurave të aksesit emergjent. | Enkriptoni dhe mbroni kredencialet e llogarisë së emergjencës, zbatoni vërtetim të fortë me shumë faktorë për akses emergjent |
| **LLOGARITË E PËRBASHKËTA** | Këto llogari përdoren zakonisht nga përdorues të shumtë për detyra specifike. | Ndarja e fjalëkalimit, kontrolli i dobët i aksesit, aksesi i paautorizuar dhe mungesa e përgjegjësisë individuale | Zbatoni kontrolle të forta aksesi, zbatoni përgjegjësinë individuale për përdorimin e llogarisë së përbashkët, ndryshoni rregullisht fjalëkalimin e llogarisë |