Centar Informacijske Sigurnosti

Nadzor korisnika s povećanim ovlastima

CIS-DOC-2011-01-002

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Svaka organizacija koja razvija svoju IT infrastrukturu ima potrebu za korisničkim računima s povećanim ovlastima. Pojam „korisnika s povećanom odgovornošću“ odnosi se na unaprijed ugrađene račune u gotovo svim operacijskim sustavima i aplikacijama. Takvi računi se od običnih korisničkih računa razlikuju po povećanim sigurnosnim administrativnim i/ili sustavskim ovlastima. Ti računi su svuda prisutni, a poznati su po svojim nazivima: root, Administrator, sa, sec_master, db2admin i drugi. Moguće im je pristupiti isključivo preko posebne lozinke koja je dodijeljena tom računu i gotovo ih je nemoguće onesposobiti. Korisnički računi s povećanim ovlastima uključuju sustavske račune, administratore, menadžere i izvršna tijela organizacije. Svim tim korisnicima dodjeljuju se posebne ovlasti kako bi mogli obavljati svoju ulogu u sustavu. Ovlasti uključuju upravljanje: resursima, operacijskim sustavom, bazom podataka, ERP sustavima (engl *Enterprise resource planning* – skup alata koji olakšavaju praćenje poslovanja organizacije) i mnogim drugim aplikacijama. Takvi povlašteni korisnički računi se obično dijele u organizaciji među određenim zaposlenicima, što može uzrokovati probleme kod nadzora korisnika zato što se ne može točno utvrditi koji korisnik (koja fizička osoba) se zaista u određeno vrijeme prijavio na sustav s povećanim ovlastima. Današnji trendovi sjedinjenja podatkovnih centara, računarstvo u oblacima (engl. *Cloud computing*) i virtualizacija povećavaju broj korisnika s povećanim ovlastima. Rastom broja korisnika s povećanim ovlastima povećava se i zona rizika za zlouporabu tih privilegiranih korisničkih računa. Iz tog razloga javlja se potreba za učinkovitijim, a posebice i sigurnijim načinom upravljanja i nadzora ovakvih korisnika. Zbog brojnih skandala uzrokovanih zlouporabom korisnika s povećanim ovlastima stvorene su brojne državne regulacije diljem svijeta koje ističu problem manjka odgovornosti i nadzora privilegiranih korisničkih računa. Budući da je nadzor korisnika s povećanim ovlastima izuzetno složen proces, stvoreni su posebni programski alati koji automatiziraju većinu posla. Neki od tih programskih alata biti će analizirani u 4. poglavlju.

2. Nadzor korisnika s povećanim ovlastima

Nadzor korisnika s povećanim ovlastima (engl. *PIM – Privileged Identity Management*) je područje nadzora korisnika usmjereno na posebne potrebe moćnih privilegiranih korisničkih računa koji se koriste za upravljanje i održavanje infrastrukture organizacije. Često je vezano sa posebnim stavkama informacijske sigurnosti kako bi se postigla suglasnost sa sigurnosnim regulacijama. Dodatno, koristi se u svrhu sprječavanja unutarnjih sigurnosni incidenata prilikom kojih se događa neovlašten pristup privatnim podacima korištenjem korisničkih računa s povećanim ovlastima.

2.1. Tipovi korisnika s povećanom ovlastima

Termin „korisnik s povećanim ovlastima“ odnosi se na bilo koji tip korisničkog računa koji posjeduje posebne ovlasti te mogućnosti pristupa i upravljanja ključnim sustavima u organizaciji. Korisničke račune s povećanim ovlastima je moguće kategorizirati u nekoliko tipova:

- **Opći/Dijeljeni administrativni računi** – ne-osobni (engl. *non-personal*) računi koji postoje u svakom uređaju i/ili programskom proizvodu. Ovi korisnički računi posjeduju super-korisničke[1] privilegije i često se dijele među zaposlenicima organizacije. Neki primjeri su: Windows Administrativni korisnik, UNIX *root* korisnik, Oracle *SYS* korisnik.
- **Privilegirani korisnički računi** – (engl. *Privileged Personal Accounts*) privilegirani računi koje koriste zaposlenici IT odjela i poslovni korisnici. Ovi korisnički računi posjeduju visok stupanj privilegija i njihovo korištenje ili zlouporaba može znatno utjecati na poslovanje organizacije. Primjeri takvih korisničkih računa su: korisnik direktora organizacije ili DBA korisnik baze podataka.
- **Aplikacijski računi** – (engl. *Application Accounts*) korisnički računi koje koriste aplikacije za pristup bazi podataka ili drugim aplikacijama. Ovi korisnički računi često imaju visoka prava pristupa poslovnim informacijama koje se nalaze u bazi podataka.
- **Računi za hitne intervencije** – (engl. *Emergency Accounts*) posebna vrsta općih korisničkih računa koja se koriste tokom uklanjanja hitnih problema koristeći povišenu razinu ovlasti. Primjer uporabe ovakvih korisničkih računa je prilikom oporavka od nepogoda ili u slučajevima narušavanja poslovnog kontinuiteta[2].

2.2. Posebne potrebe korisnika s povećanom ovlastima

Tehnologija za nadzor korisnika s povećanom ovlastima mora omogućiti zbrinjavanje posebnih potreba privilegiranih korisnika, što uključuje: dodjeljivanje korisnički računa i životni ciklus, ovjeru, autorizaciju, upravljanje lozinkama i nadzor.

- **Dodjeljivanje korisničkih računa i životni ciklus** – brine se za pristupna prava korisničkog računa, a zasniva se na ulogama i politikama.
- **Ovjera** – upravlja snažnim postupkom ovjere privilegiranih korisničkih računa. Točnije, pruža programsku potporu za sigurnu razmjenu podataka.
- **Autorizacija** – upravljanje velikim brojem prava pristupa korisnika s povećanim ovlastima.

[1] Superkorisnik – (engl. *superuser*) korisnik sa svim raspoloživim pravima ili dozvolama za korištenje računalnog sustava u svim mogućim modalitetima i situacijama. U mnogim informacijskim sustavima, superkorisnik je obično administrator sustava.

[2] Poslovni kontinuitet – (engl. *Business continuity*) je aktivnost koju provode tvrtke kako bi klijentima osigurali uporabu kritičnih poslovnih funkcija u svim situacijama.

- **Upravljanje lozinkama** – poštivanje pravila za lozinke korisnika s povećanim ovlastima prema sigurnosnoj politici organizacije. Za razliku od običnih korisničkih računa, korisničke račune s povećanim ovlastima može koristiti više ljudi.
- **Nadzor** – pruža potporu za nadzor akcija koje privilegirani korisnici rade. Ovo može uključivati praćenje i/ili snimanje korisničke sjednice kao i stvaranje korelacije između općeg/dijeljenog računa i fizičke osobe.

2.3. Razvoj

Nadzor korisnika je široko administrativno područje koje se bavi identifikacijom pojedinaca u sustavu (kao što su država, društvena mreža, organizacija) i kontrolom pristupa resursima koje se nalaze u sustavu. Pojam nadzora korisnika vezan je načinom kojim se identificiraju i autoriziraju korisnici kroz mrežu računala. Pokriva problematiku davanja identiteta korisnicima, zaštitu identiteta i tehnologiju koja podržava zaštitu identiteta (npr. mrežni protokoli, digitalni certifikati, lozinke). Pojam digitalnog identiteta (engl. *Digital identity*) može se interpretirati kao proces izdvajanja bitnih karakteristika promatrane fizičke instance na način koji olakšava obradu. Nadzor korisnika s povećanim ovlastima (engl. *PIM – Privileged Identity Management*) je posebno područje nadzora korisnika usmjereno na specifične potrebe moćnih privilegiranih korisničkih računa koji se koriste za upravljanje i održavanje infrastrukture organizacije. Ovo područje se počelo intenzivnije razvijati krajem 90-tih godina 20. stoljeća kao posljedica naglog razvoja Web 2.0[3] tehnologija. Pojavom sve većih zahtjeva za interaktivnim web aplikacijama, razvojem web servisa i usluga javio se i velik broj podsustava koje je trebalo održavati. Brzo se ustanovilo da održavanje tih novih podsustava treba odvojiti od običnih korisničkih računa, a to je izazvalo pojavu posebnih korisničkih računa sa dodatnim privilegijama ili ovlastima. Sve većim i bržim razvojem servisa i usluga dodavao se teret na postojeće korisničke račune s povećanim ovlastima. Dodavanjem sve većeg broja odgovornosti pojedinim privilegiranim korisničkim računima povećava se zona rizika u slučajevima krađe tih povlaštenih računa. Krađa korisničkih računa s povećanim ovlastima može nanijeti veliku materijalnu štetu organizacijama. Zato je upravljanje i nadzor korisnika s povećanim ovlastima vrlo važna stavka u sigurnosnoj politici organizacije.

[3] Web 2.0 – World Wide Web tehnologije bazirane na socijalizacijskoj noti koja korisnicima omogućava sudjelovanje u kreiranju sadržaja weba. Termin upućuje na novu (drugu) generaciju Weba i usluga koja, umjesto jednosmjernog protoka informacija, podrazumijeva interaktivnu dvosmjernu komunikaciju između korisnika i računala te korisnika i drugih korisnika, čime korisnik od pasivnog postaje aktivni sudionik.

3. Upravljanje lozinkama korisnika s povećanim ovlastima

Složen proces upravljanja lozinkama korisnika s povećanom ovlastima obavlja se putem posebnih programskih alata. Sigurnost lozinki korisnika s povećanim ovlastima se najčešće postiže periodičkim mijenjanjem stare lozinke sa novom lozinkom. Nove lozinke se proizvode na pseudoslučajan[4] način koristeći neki algoritam. Budući da je tim novim lozinkama potrebno pristupiti kako bi se korisnici ili procesi mogli prijaviti na sustav kao korisnici s povećanim ovlastima, programski alati moraju nove lozinke pohranjivati i pružati razne mehanizme za priopćenje tih lozinki na siguran i primjeren način. Postoji tri glavna tipa lozinki korisnika s povećanim ovlastima:

1. lozinke lokalnih administratora,
2. lozinke koje koriste servisi te
3. lozinke za aplikacije koje razmjenjuju podatke s drugim aplikacijama

3.1. Lozinke lokalnih administratora

Administratorski korisnički računi se često koriste u svim sustavima za održavanje. Na Unix i Linux sustavima postoji tzv. *root* korisnik koji predstavlja korisnika s povećanim ovlastima. Windows sustavi imaju ekvivalentan korisnički račun poznat kao *Administrator*. Na SQL bazama podataka postoji *sa* (engl. *System Administrator*) korisnički račun. Na većini operacijskih sustava, sustava za upravljanje bazama podataka, aplikacijama i mrežnim uređajima postoji administrativni korisnički račun koje se koristi za instalaciju novih programskih alata, konfiguraciju sustava, upravljanje korisnicima te ispravljanje grešaka u programskoj logici (engl. *Apply patches*). Na nekim sustavima postoje posebni administrativni računi koji mogu izvoditi samo neke administrativne funkcije, što znači da postoji više korisnika s povećanim ovlastima, ali svako od njih ima ograničen broj funkcija koje ima ovlasti raditi.

3.2. Lozinke koje koriste servisi

Na Windows operacijskim sustavima, servisi se pokreću ili pod ovlastima SYSTEM računa (koji posjeduje visok stupanj ovlasti ali nema lozinku) ili pod nekim korisničkim računom. Kada se servisi pokreću pod ovlastima korisnika koji nije SYSTEM, operacijski sustav zahtjeva korisničko ime i lozinku kako bi pokrenuo željeni servis. Na Unix i Linux sustavima, init[5] i inetd[6] procesi mogu pokretati servise kao ne privilegirani korisnici bez lozinke, odnosno operacijski sustav obično ne zahtjeva lozinku za pokretanje servisa.

3.3. Lozinke za aplikacije koje razmjenjuju podatke s drugim aplikacijama

Nekad aplikacija treba razmjenjivati poruke sa drugim aplikacijama kako bi izvela određen zadatak. Čest primjer takvih korisničkih računa je onaj koji se koristi kada aplikacija pristupa bazi podataka. Kako bi aplikacija mogla pristupiti bazi podataka mora predati valjano korisničko ime i lozinku, odnosno obaviti proces prijave (kao i bilo koji drugi fizički korisnik). Kako bi se jasno istaknule ovlasti koje aplikacija ima nad bazom podataka dodjeljuje joj se poseban korisnički račun sa odgovarajućim ovlastima. Iako aplikacija sama po sebi neće nikad izvesti niti jednu

[4] Pseudo-slučajnost – pojam slučajnih brojeva je u očitoj kontradikciji s pojmom računala kao determinističkih naprava, iz tog razloga uvodi se termin „pseudo-slučajnost“.

[5] Init – (engl. *Initialization*) je proces u Unix okruženjima koji je zadužen za stvaranje svih drugih procesa. Pokrenut je kao pozadinski proces (engl. *daemon*)

[6] inetd – je pozadinski proces na Unix okruženjima koji upravlja uslugama koje računalo nudi na globalnoj mreži Internet

naredbu koja joj nije izričito navedena u programskom kodu, ukoliko na aplikacijskom sloju postoji SQL injekcijska[7] ranjivost, napadač može pod ovlastima korisničkog računa koji je dodijeljen aplikaciji izvoditi proizvoljne naredbe. Na primjer, neka postoji aplikacija koja služi samo za pregledavanje stavki u nekoj tablici baze podataka (npr. prodane knjige u knjižari po mjesecima). Budući da aplikacija služi samo za pregledavanje podataka, a ne stvaranje i izmjenu podataka, dovoljno joj je dodijeliti korisnički račun koji ima ovlasti čitanja samo nad određenim tablicama u bazi podataka. Time se osigurava integritet baze podataka čak i u slučaju kada na aplikacijskom sloju postoji SQL injekcija.

3.4. Sigurnost lozinki korisnika s povećanim ovlastima

Alati za upravljanje lozinkama korisnika s povećanim ovlastima osiguravaju lozinke tako što:

- periodički mijenjaju svaku lozinku sa novom, pseudoslučajnom vrijednošću, pohranjuju te nove vrijednosti i
- štite pohranjene vrijednosti (npr. koristeći kriptografske algoritme i replikaciju podataka) pružajući mehanizme za priopćenje novih lozinki raznim sudionicima u sustavu kao što su: IT administratori, aplikacije koje pokreću servise, aplikacije koje razmjenjuju podatke s drugim aplikacijama i sl.

[7] SQL injekcija – je injekcijska ranjivost koja iskorištava ranjivost web aplikacije za izvršavanje vlastitih upita i naredbi nad pozadinskom bazom podataka

4. Sigurnosne prijetnje

Uz povlaštene korisnike s povećanim ovlastima postoji velika zona rizika. Kako fizički korisnik putem takvih računa može obavljati veliki broj funkcija, postoji opasnost da se napravi i nepoželjna akcija. Osim očitog problema da privilegirani korisnički račun iskoristi napadač (engl. *Hacker*), legitimni autorizirani korisnici također predstavljaju sigurnosnu prijetnju podatcima i IT infrastrukturi organizacije zato što imaju direktan (često i fizički) pristup unutarnjoj infrastrukturi. Često se autorizirani pristupi korisnika zanemaruju jer se pretpostavlja da samo vanjski napadači mogu nanijeti štetu, odnosno vjeruje se unutarnjim korisnicima. U 2007. godini organizacija *E-Crime Watch* je provela anketu kojom se ispitivao određen broj organizacija o njihovim sigurnosnim incidentima. Više od pola ispitanih organizacija imalo je barem jedan incident vezan uz unutarnju zlouporabu korisnika s povećanim ovlastima. Također, istaknuto je kako je svaka pojedina organizacija, kao posljedica zlouporabe, izgubila preko pola milijuna američkih dolara.

Primarna sigurnosna prijetnja kod korisnika s povećanim ovlastima je ta što organizacije često zanemaruju ili ne shvaćaju važnost procesa integracije i/ili implementacije programskih alata za upravljanje privilegiranim korisnicima. Često se taj zadatak delegira trećim stranama koje iskorištavaju smanjen interes organizacije kako bi površno izveli implementaciju programskog rješenja ili još gore, iskoristili povjerenje organizacije kako bi ukrali osjetljive podatke. Međutim, ako se integracija programskih alata provede korektno, ti alati mogu:

- olakšati zbrinjavanje kritičnih sigurnosnih propusta,
- olakšati preuzimanje odgovornosti za akcije koje utječu na IT usluge i sigurnost podataka te
- smanjiti troškove za postizanje usklađenosti sa sigurnosnim politikama i regulacijama organizacije.

Činjenica je da programski alati za upravljanje korisnicima s povećanim ovlastima nisu proizvodi koji bi se trebali kupovati na temelju generičkih ponuda koje jamče sigurnost u svim situacijama već bi se rješenje trebalo prilagoditi ovisno o stvarnim i jedinstvenim potrebama organizacije. Kada je riječ o upravljanju korisnika s povećanim ovlastima nisu sva rješenja jednako dobra u svim situacijama, a osnovni razlozi navedeni su u nastavku:

- Nizak stupanj sličnosti u računalima kojima je potrebno upravljati – počevši od operacijskog sustava koji se mogu bazirati na Linux ili Unix jezgrama, do Windows okruženja. Brojne razlike susrećemo se i u raznim mrežnim aplikacijama i platformama te središnjim jedinicama, infrastrukturom koja omogućuje izradu sigurnosnih kopija (engl. *Backup*) i drugim sklopovljem koje je potrebno uzeti u obzir.
- Velik broj ciljnih sustava koji se često mijenjaju, a koji mogu biti odvojeni sporim, nepouzdanim ili skupim WAN vezama.
- Značajan broj vlastitih i naslijeđenih aplikacija (engl. legacy applications) koje mogu biti loše dokumentirane i čije logičke greške i/ili propusti mogu predstavljati značajnu ranjivost cjelokupnom sustavu.
- Složene organizacijske strukture koje zahtijevaju prilagodljiva rješenja koja su sposobna obraditi preklapajuće linije delegacije i kontrole koje se često mijenjaju.

U slučaju poklapanja sa bilo kojim od prethodno navedenim scenarijima, trebalo bi se usredotočiti na :

- Probne implementacije koja obuhvaćaju testna okruženja s realnim uzorkom ciljnog sustava, njegovih aplikacija i korisničkih uloga.
- Stupanje u kontakt i dubinska analiza zahtjeva s referentnim korisnicima čiji su sustavi po raznolikosti i opsegu približno jednaki vlastitom sustavu, a čije aplikacije barem razumno odgovaraju vlastitim.
- Uzimati činjenice od drugih korisnika o stvarnim vremenskim rokovima isporuke i troškovima održavanja odabrane implementacije.

4.1. Loše zbrinjavanje korisnika s povećanim ovlastima

Sredinom listopada 2009. godine USCC (engl. *United States Congressional Committee*) kongresna komisija iznenadila je IT stručnjake izvješćem o novoj prijetnji na području kibernetičkog ratovanja (engl. *Cyber Warfare*). Izvješće koje je sastavila organizacija Northrop Grumman sadrži uznemirujuće detalje o napadima 2008. godine koji su omogućili inozemnim špijunima pristup osjetljivim podatcima američkih IT organizacija. Sljedeći isječak iz izvješća opisuje rezultate organizacije Northrop Grumman:

„*Nekoć nedodirljivim informacijama Američke vlade i organizacija u privatnom sektoru, sada je moguće pristupiti s relativnom lakoćom koristeći razne mrežne alate*."

U izvještaju je navedeno kako inozemni agenti koriste razne pristupe kako bi lansirali djelotvorne napade protiv sigurnosnih mjera ciljnog sustava. Primjer takvog napada je raspodijeljeni napad uskraćivanja usluga (engl. *DDoS – Distributed denial-of-service*) kojim je grupa kineskih hakera onesposobila web sjedište organizacije *CNN* (*Cable News Network*) 2008. godine. Prvo, koriste najnovije ranjivosti (engl. zero-day exploits) koje samostalno razvijaju, a maliciozan teret dostavljaju na ciljni sustav vještom uporabom društvenog inženjeringa (engl. *Social engineering*). Kada napadač kompromitira jedno računalo u sustavu, sa tog računala se kreće po drugim računalima u mreži. Kretajući se po internoj mreži, napadač kompromitira korisničke račune s povećanim ovlastima sve dok u potpunosti ne mapira cjelokupnu infrastrukturu organizacije. Ovim putem je moguće izlučiti razne osjetljive informacije organizacije brzinom koja onesposobljuje normalne sigurnosne mehanizme i IDS[8] sustave zaštite. U izvješću se to sažima na sljedeći način:

„*Napadači iskorištavaju ovaj reaktivan obrambeni model i imaju potrebne resurse koji im omogućavaju razvoj i iskorištavanje prethodno nepoznatih ranjivosti koje se često propuštaju korištenjem standardnih IDS/IPS sustava*."

Današnji sustavi za upravljanje korisnicima s povećanim ovlastima sposobni su u kratkom vremenskom periodu otkriti i katalogizirati privilegirane korisnike u cjelokupnom sustavu (u aplikacijama, web servisima, bazama podataka, operacijskim sustavima i drugdje). Zatim, sustav izolira međusobno zavisne servise kako bi se održao minimum zajedničkoga između više korisnika s povećanim ovlastima. Osim toga, sustav mora stalno (u pravilnim razmacima) mijenjati sve lozinke i omogućavati pristup privilegiranim korisničkim računima isključivo autoriziranom osoblju. Ovim putem jedan kompromitirani sustav ima kratkotrajno značenje i ne može predstavljati „odskočnu dasku" za narušavanje sigurnosti cjelokupne infrastrukture.

[8] IDS – (engl. Intrusion Detection System) sustavi za otkrivanje upada, koriste se za nadzor korisnika i sustava, nadgledanje ranjivosti sustava, procjena integriteta datoteka važnih za rad sustava i drugo.

4.2. Česti propusti

Rezultati istraživanja koje je provela organizacija *Cyber-Ark* otkrili su neke važne statističke podatke o lozinkama korisnika s povećanim ovlastima i prijetnje koje donose organizaciji.

Gdje lozinka perzistira	Primjer	Koliko ih postoji	Sigurnosni rizik
Osobna radna stanica ili računalo	Login: Administrator	**5000 ili više** 40% organizacija ima više od 5000 zaposlenika	**Visok** 21% administracijskih lozinki na pojedinim radnim stanicama se ne obnavljaju
Poslužitelji	UNIX (Root), LINUX(Root)	**5000 ili više** 44% organizacija ima više od 500 poslužitelja, svaka posjeduje 1 – 5 administrativnih lozinki	**Visok** 13% administratorskih lozinki na poslužiteljima nisu nikad obnovljene
Mrežni usmjernik (engl. *router*)	Cisco	**100 ili više** 41% organizacija ima više od 500 usmjernika, svaki od njih posjeduje 1 – 5 administrativnih računa	**Visok** 13% administratorskih lozinki na usmjernicima nisu nikad obnovljene
Baze podataka	Oracle (System, Sys), Microsoft SQL Server (SA)	**100 ili više** 66% organizacija ima više od 100 jedinstvenih aplikacija, uključujući bazu podataka	**Visok** 42% administratorskih lozinki na aplikacijama i bazama podataka se nikad ne obnovljaju
Skripte koje povezuju aplikacije	Praćenje prodaje neke aplikacije i evidentiranje u bazu podataka	**1000 ili više** Svaka organizacija ima preko 100 aplikacija, a 92% tih aplikacija stvara konekciju sa barem jednom aplikacijom. Svaka jedinstvena veza stvara jedinstveni incident sa lozinkama	**Visok** 42% administratorskih lozinki na aplikacijama i bazama podataka se nikad ne obnovljaju

Tablica 1. Statistika korištenja privilegiranih računa

Izvor: www.cyber-ark.com

Kako bi se spriječili navedeni propusti, organizacija Cyber-Ark preporuča korištenje PIM alata koji su posebno oblikovani za svaku organizaciju.

4.3. Identifikacija zlouporabe ovlasti

Problemi koji se očituju u organizaciji zbog zloupotrebe povlastica proizlaze iz: namjernih, slučajnih i neizravnih razloga. Broj sigurnosnih prijetnji koje su usmjerene na organizacije je porastao tolikom brzinom da ih sigurnosni profesionalci ne mogu učinkovito adresirati, otvarajući time prostor za nove sigurnosne prijetnje. U nastavku se opisuju tri tipa zlouporabe ovlasti.

4.3.1. Namjerna zlouporaba

Namjerna zloupotreba privilegija često proizlazi iz napada unutar organizacije. Napad koji potječe iznutra je definiran kao bilo koji zlonamjerni napad na korporativnom sustavu ili mreži, gdje je uljez netko tko posjeduje autoriziran pristup mreži ili čak dodatno znanje o mrežnoj arhitekturi organizacije (npr. fizički položaj poslužitelja, postojeće propuste u postavkama poslužitelja i aktivne sigurnosne ranjivosti i sl.). Organizacija *CSO Cyber Security Watch Survey* je 2010. godine objavila rezultate istraživanja koji su dobiveni ispitivanjem napada koji potječu iznutra. Naime, sada zločudni korisnici rade unutar sigurnosnih stijena i politika koji su osmišljeni kako bi se spriječio njihov ulazak u sustav s primjerice Interneta. Koriste razne tehnologije poput malih uređaja koji presreću promet, polimorfne malware[9] te razne *key logger*[10] alate za krađu povjerljivih informacija. Sve ovo izvode kao legitimni autorizirani zaposlenici organizacije i time izbjegavaju otkrivanje. Američka Bijela kuća je 2008. godine izdala članak poda nazivom *Cyber Security Policy*, koji profilira sustavske gubitke američke gospodarske vrijednosti intelektualnog vlasništva i krađe podataka na oko 1 trilijun dolara. Izvještaji instituta za računalnu sigurnost i američkog FBI-a govore da organizacije prosječno gube 2,7 milijuna američkih dolara po napadu. Magazin CSO[11] navodi sljedeće tvrdnje vezano uz ove prijetnje:

1. Organizacije imaju tendenciju upotrebljavati sigurnosnu metodu koja se temelji na *wall-and-fortress*[12] principu, što samo sprječava (ili otežava) upade izvana ali ne i napade iznutra.
2. Organizacije bi trebale više vremena uložiti u razumijevanje kako napadači gledaju organizaciju u smislu napadnih vektora, sustav interesa i obradu ranjivosti kako bi se učinkovitije zaštitili od napada.
3. Ekonomske poteškoće izazvane recesijom 2008. i 2009. godine mogu stvoriti ogorčenost i financijske motivacije koje će natjerati stranke ili bivše zaposlenike na kriminalne akcije.

Međunarodna agencija za savjetovanje *Deloitte*, je izjavila kako istraživanje provedeno od strane CSO magazina otkriva ozbiljan nedostatak svijesti i stupanj samozadovoljstva od strane IT organizacije, a možda i sigurnosnih inženjera. Organizacije se mogu usredotočiti na jednostavne napade koji potiču izvan ili unutar mreže, jer su najuočljivije i najlakše se otklanjanju. Ipak, ovim postupkom mogu se previdjeti napredniji napadi koji mogu proizvesti ozbiljne sustavske i monetarne učinke.

---

[9] Polimorfni malware – zločudni programi poput virusa, crva, trojanaca ili spyware-a koji mijenjaju svoje ponašanje i time otežavaju anti-virusnim programima detekciju.

[10] Key logger – je uređaj i program koji prati svaki pritisnuti gumb na tipkovnici računala na kojem je ugrađen ili pokrenut.

[11] CSO magazine – poznati časopis koji se bavi temom sigurnosti u informacijskim sustavima. Više na službenoj stranici: www.csoonline.com

[12] wall-and-fortress – metoda zaštite informacijskog sustava kojoj je glavni cilj spriječiti neovlašten pristup resursima. Ne razmatra prijetnje koje dolaze iznutra.

4.3.2. Slučajna zlouporaba

Iako je mnogima to teško priznati, ljudi su nesavršena bića. Ljudi nisu savršeno dosljedni svojim principima bilo u osobnom životu ili u poslovnom okruženju. Slučajna zloupotreba ovlasti na stolnim računalima i poslužiteljima se događa, a takvi napadi imaju mjerljivi utjecaj na organizaciju u cjelini. Prema IDC izvješću „The Relationship between IT Labor Costs and Best Practices for IAM“, konfiguracijske pogreške stolnih računala organizaciju koštaju u prosjeku 120 američkih dolara po računalu. U rujnu 2004. godine *HFC Bank*, jedna od najvećih banaka u Velikoj Britaniji, poslala je 2.600 e-mail poruka svojim klijentima koja je, zbog interne pogreške operatera, izložila primateljevu e-mail adresu svima na popisu. Problem je još složeniji kada se na poruke izvan ureda (koje sadrže kućnu adresu i brojeve mobitela) automatski javljaju prilikom primitka poruke. Jedan od poznatijih sigurnosnih inženjera, Kevin Mitnick, je rekao: "Najslabija karika u bilo kojoj mreži su ljudi." Koliko god se uloži u zaštitu, mreža je još uvijek ranjiva ako se korisnike može navesti da zanemare ili isključe sigurnosne postavke (npr. dajući lozinke ili druge povjerljive podatke preko telefona, obavljanje neke djelatnosti koja omogućuje malware programima preuzimanje administratorskih ovlasti nad računalima i sl.). Iz tog razloga, obrazovanje osoblja trebalo bi biti jedan kamen temeljac za korporativne sigurnosne politike. Zaposlenici bi morali biti svjesni o postojanju napada društvenog inženjeringa, rizicima koji su uključeni prilikom korištenja IT sustava te kako se boriti protiv njih. Također, potrebno je ugraditi svijest u sve korisnike računalnih sustava da prijave sumnjiva ponašanja čim ih uoče. U razdoblju gdje je krađa identiteta i povjerljivih podataka česta pojava, sigurnost je odgovornost koju svaki zaposlenik mora obavljati savjesno.

4.3.3. Neizravna zlouporaba

Neizravnom zlouporabom ovlasti smatra se situacija kada jedna ili više vrsta napada potiču od treće strane, odnosno od strane računala koje je preuzeo napadač (ili više napadača). *Georgia Tech Information Security Center* (GTISC) je 15. listopada 2010. godine objavila svoje godišnje izvješće u kojemu predviđaju razloge i tipove napada za iduću godinu. Prema njihovim istraživanjima, elektronske će domene doživjeti veće količine zlonamjernih napada i razne nove sigurnosne prijetnje u narednoj godini. Potvrdu tome daje i sigurnosni stručnjak Georgeu Heron u svojoj izjavi "Sve je vezano za podatke", misleći pri tome da će primarni motiv kibernetičkog kriminala ostati krađa podataka.

5. Sustavi za upravljanje korisnicima s povećanim ovlastima

Zbog činjenice da uobičajeni alati za održavanje korisničkih računa ne nude odgovarajuću podršku za upravljanje i/ili nadzor korisnika sa povećanim ovlastima, javila se potreba za specijaliziranim alatima. Programska potpora za upravljanje korisnicima s povećanim ovlastima počela se razvijati 2000. godine. Alati za nadzor i upravljanje korisnicima s povećanim ovlastima moraju zadovoljiti sve posebne potrebe (poglavlje 2.2):

- dodjeljivanje korisničkih računa i životni ciklus,
- ovjera, autorizacija i upravljanje lozinkama te
- nadzor.

Alati obično zahtijevaju da administratori prvo preuzmu lozinku za račun s povećanim ovlastima prije svake uporabe, a dodatno se zahtjeva i obrazloženje razloga za svaki pristup sustavu putem privilegiranog računa. Nakon uporabe privilegiranog računa postavlja se nova lozinka za taj privilegirani račun. Ovim postupkom alati za upravljanje korisnicima s povećanim ovlastima brane sustav od nedokumentiranih pristupa konfiguracijskim postavkama i privatnim podatcima, osiguravaju provođenje odredbi za upravljanje IT uslugama kao što su ITIL[13] i ostvarivanje papirnatih tragova za buduće revizije pomoću kojih se dokazuje usklađenosti (ili neusklađenost) sa standardima kao što su HIPAA[14] i PCI-DSS[15]. Dodatno, napredniji alati samostalno otkrivaju međuovisnosti između servisa te sinkroniziraju promjene lozinki među ovisnim računima kako bi se izbjegle smetnje u pružanju usluga.

5.1. Odabir sustava za upravljanje korisnicima s povećanom ovlastima

Odabir odgovarajućeg sustava za upravljanje privilegiranim korisnicima trebao bi započeti raspravom među svim dionicima procesa uključujući redatelja informacijske tehnologije (eng. *CIO*), glavnog sigurnosnog službenika (engl. *CSO*), IT administratore te sve druge osobe koji su uključene u proces upravljanja osjetljivim korisničkim računima (npr. administratori baza podataka). Ključni dionici bi trebali biti oni koji će najviše ispaštati od posljedica štete koju bi uzrokovao loše implementiran sustav. Potrebno je osvijestiti činjenicu da sustavi za upravljanje korisnicima s povećanim ovlastima ne zahtijevaju samo uvođenje dodatnih tehnologija, već i promjenu načina na koji se osjetljivi podatci (poput lozinke) prenose, mijenjaju, otkrivaju i dodjeljuju. Neovisno o tome koliko će novi sustav smanjiti količinu posla pojedinim članovima osoblja, neki pojedinci koji su prethodno uživali u potpunoj anonimnosti i velikom stupnju ovlasti u sustavu, odbijaju se prilagoditi novom sustavu. Iz tog razloga implementacija sustava za upravljanje korisnicima s povećanim ovlastima može uspjeti samo uz aktivnu podršku nadležnih tijela/institucija.

---

[13] ITIL – (engl. *Information Technology Infrastructure Library*) je skup koncepata i dobrih praksi za upravljanje uslugama i razvoj IT tehnologija i usluga.

[14] HIPAA – (engl. *Health Insurance Portability and Accountability Act*) je odredba Američkog kongresa kojom se štiti pokrivenost zdravstvenog osiguranja za radnike i njihove obitelji kada izgube ili mijenjaju svoja radna mjesta.

[15] PCI-DSS – (engl. *Payment Card Industry Security Standard)* je svjetski prihvaćen standard informacijske sigurnosti koje definira vijeće za standardizaciju sigurnosnih odredbi plaćanja putem kreditnih kartica (engl. *Payment Card Industry Security Standards Council*). Standard je nastao kako bi se spriječile prijevare vezane uz plaćanje putem kreditnih kartica, a odnosi se na sve organizacije koje drže, obrađuju ili mijenjaju podatke o vlasnicima kreditnih kartica. Članak 10.2. detaljno propisuje što se sve mora bilježiti prilikom svake interakcije sa sustavom.

5.2. Analiza Cyber-Ark sustava za upravljanje korisnicima s povećanim ovlastima

Organizacija *Cyber-Ark Software* je multinacionalna kompanija koja se bavi područjem informacijske sigurnosti, a specijalizira se na nadzoru i upravljanju korisnika s povećanim ovlastima. Sustav za nadzor korisnika s povećanim ovlastima koji je razvila organizacija *Cyber-Ark* trenutno je najraširenija sustav ove vrste. Skup alata koje je *Cyber-Ark* razvio, pomaže ujediniti sigurnosne politike koje se odnose na osiguravanje, upravljanje i nadziranje korisnika s povećanim ovlastima. Također, pomaže i u upravljanju podatkovnih centara neovisno o tome nalaze li se unutar organizacije ili u oblaku[16], a konkretno omogućuje sljedeće:

- kontrolu pristupa korisničkim računima s povećanim ovlastima,
- nadzor i bilježenje privilegiranih sjednica,
- upravljanje sjedničkim tokenima aplikacija i servisa,
- precizniji način kontrole naredbi koje administratori mogu pokretati,
- olakšano usklađivanje sa regulacijskim zahtjevima,
- pojednostavljeno upravljanje politikama vezanih za upravljanje privilegiranim računima te
- jednostavno integriranje s poslovnim sustavima

Alat za upravljanje privilegiranim korisnicima organizacije *Cyber-Ark* omogućuje implementacije efektivne politike „najmanje razine privilegija“. Dodatno, smanjuje prijetnje iskorištavanja privilegiranih računa unutar organizacije tako da administratorske ovlasti dodjeljuje po potrebi, za pojedinu razinu naredbi. Postupnim delegiranjem pristupa privilegiranim korisnicima, kao što su Unix/Linux administratori i *root* korisnici, organizacije mogu upravljati i osigurati pristup pojedinim privilegiranim računima ali i upravljati i nadzirati naredbe koje se izvode. Dodatno, sustav je moguće podesiti tako da bilježi svaku naredbu koja se izvodi pod računima s visokim privilegijama. Time se dobiva jasan forenzički trag u slučaju sigurnosnog incidenta. Sustav nudi i zamjenu za SUDO naredbu kojoj nedostaje mogućnost upravljanja, proizvodnja izvještaja i dodatne sigurnosne sposobnosti koje su potrebne kako bi se poštivali zahtjevi za revizije. *Cyber-Ark-ov PIM Suite v6*, koji uključuje *On-Demand Privileges Manager*, ostvaruje jednu pristupnu točku i jednostavno korisničko web sučelje koje omogućuje potpuni nadzor i upravljanje korisnika s povećanim ovlastima na svim razinama organizacije.

5.2.1. Potpun sigurnosni nadzor i upravljanje, prednosti automatskog otkrivanja

Cyber-Ark PIM Suite nudi alate koji podržavaju čitav životni ciklus za centralizirano upravljanje privilegiranih računa organizacije, korisnika i sjednice, kao i upravljanje ugrađenim lozinkama pronađenih u aplikacijama i skriptama. *PIM Suite* je alat koji funkcionira na razini organizacije, a temelji sigurnost sustava na unificiranju raznih sigurnosnih politika što uključuje: upravljanje i nadziranje svih korisnika s povećanim ovlastima i aktivnostima vezanih uz upravljanje podatkovnim centrima neovisno nalaze li se unutar organizacije ili u oblaku. Sa novom (šestom) inačicom svog alata Cyber-Ark podržava napredno automatsko otkrivanje rješenja za automatizaciju procesa otkrivanja svih oblika privilegiranih računa, uključujući i račune povezane sa Windows servisima koje je moguće naći na Windows poslužiteljima, radnim stanicama i osobnim računalima. Cyber-Ark proaktivno dodaje novo otkrivene korisničke račune u odgovarajuću rubriku, kao i sve nove uređaje i sustave koji se dodaju cjelokupnoj infrastrukturi. Pruža evidenciju i dodatne informacije za svaki prikupljeni račun neovisno o tome je li se korisnički račun nalazi u *Cyber-Ark PIM Suite* domeni nadzora. Organizacije koje koriste ovaj PIM Suite također će imati korist od novog i poboljšanog središnjeg sustava za izvještavanje koji podržava i isporuku zakazanih izvješća na temelju definiranih politika. Pružajući neprimjetno integriran

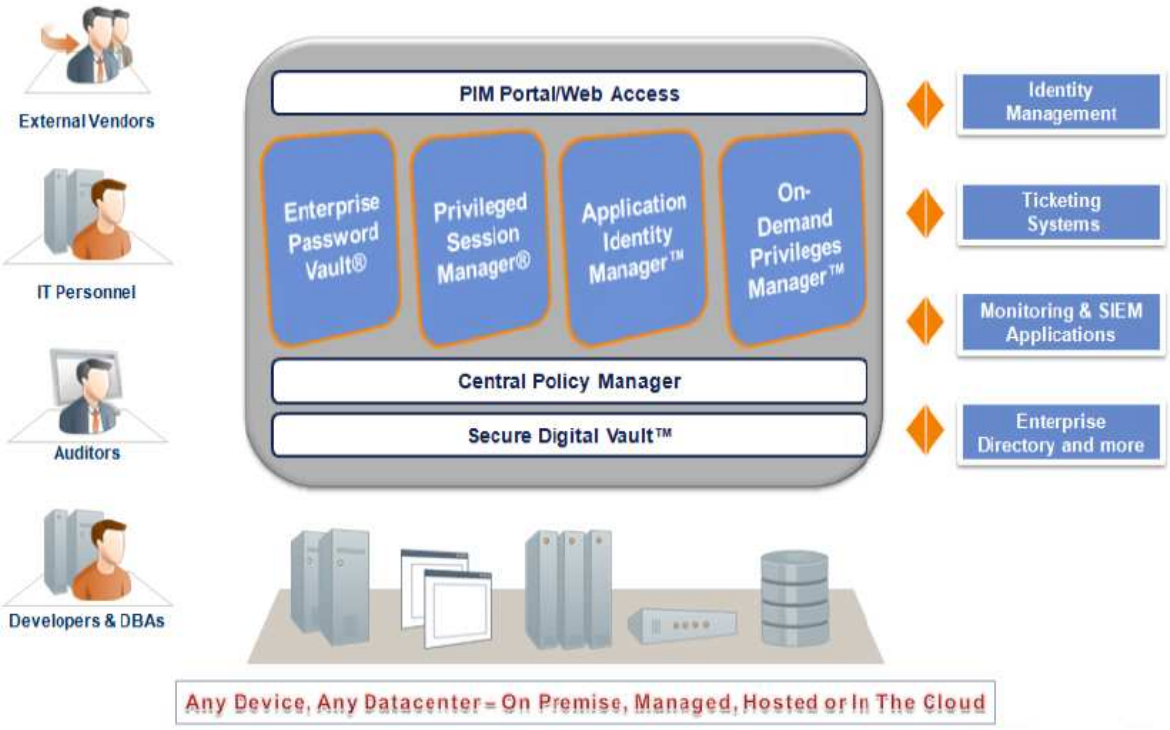
[16] Računalni oblak – (engl. Cloud Computing System) predstavlja novi oblik geografski neovisnog računarstva gdje korisnici na zahtjev mogu pristupati određenim informacijama i resursima.

skup rješenja za izazove upravljanja povlaštenih korisnika, Cyber-Ark omogućuje organizacijama upravljanje i reviziju privilegiranih korisnika, računa i korisničkih sjednica koristeći jedinstven alat. U konačnici, ovaj sustav donosi smanjenje ukupnih troškova uklanjanjem potrebe za investiranjem, u dva odvojena rješenja - jedan za superkorisnike i jedan za zajedničke račune uz jedinstveno rješenje i zajedničko korisničko sučelje za sve proizvode u *Cyber-Ark PIM Suite* alatu. Korisnici ovog sustava imaju pogodnost jednostavne implementacije, sustav se na jednostavan način usvaja, te je jednostavan za uporabu. Dodatno, Cyber-Ark posjeduje dodatnu *On-Demand Privileges Manager* komponentu koja spaja sigurnosnu tehnologiju sa alatima za napredno nadziranje, proizvodnju izvješća i upravljanje korisnicima s povećanim ovlastima, pružajući uvid u sve akcije koje se odvijaju unutar sustava organizacije. Dodatne pogodnosti uključuju:

- **Eliminacija unutarnjih sigurnosnih prijetnji granulacijom ovlasti** – korisnicima s povećanim ovlastima se dodjeljuju samo one ovlasti koje su im potrebne za obavljanje jedne jedinice posla. Time se smanjuju potencijalno štetne akcije koje jedan privilegirani korisni može napraviti.
- **Postizanje suglasnosti sa sigurnosnom politikom kroz vlastite revizije i zapisivanje tragova** – sposobnost povezivanja korisničkih računa s povećanim ovlastima sa fizičkom osobom je osnovni zahtjev za efektivno vođenje revizija. *On-Demand Privileges Manager* osigurava da će svaki korisnik biti odgovoran za svoje vlastite akcije. Tokom prijave na sustav sa privilegiranim računom pokreće se snimanje svih akcija, odnosno naredbi, koje se unose za vrijeme korištenja računa. Sve snimke se pohranjuju na sigurno mjesto zvano *Cyber-Ark's Digital Vault*.
- **Povećanje produktivnosti i učinkovitosti** – granulacijom ovlasti i snimanjem sjednice omogućuje se značajno smanjenje neispravnosti koje se redovito unose ljudskom greškom, povećanje radnog vremena i upravljanje kritičnih sustava, te efektivno rješavanje složenog problema višestrukih administratora.

Slika 1 prikazuje alate koji čine *Cyber-Ark PIM Suite*. To su alati :

- **Enterprise Password Vault** – ovaj alat automatski pronalazi privilegirane korisnike u sustavu, te omogućuje upravljanje i nadzor svakog privilegiranog korisnika u sustavu
- **Privileged Session Manager** – omogućuje nadziranje i upravlja pristupom osjetljivim informacijama, snima sjednicu i brine o tome da se samo jedan korisnik može prijaviti određenim korisničkim računom s povećanim ovlastima u jednom trenutku
- **Application Identity Manager** – eliminira ugrađene (engl. *hard-coded*) podatke o privilegiranim korisničkim računima koje se koriste u aplikacijama
- **On-Demand Privileges Manager** – jedinstveno rješenje za upravljanje i nadzor privilegiranih korisnika (i njihovih fizičkih korisnika) te provodi granulaciju ovlasti



Slika 1. Cyber-Ark PIM Suite alati

Izvor: www.cyber-ark.com

5.3. Analiza alata powerbroker

Organizacija *BeyondTrust* razvija alate koji pomažu IT stručnjacima ukloniti rizik namjernih, slučajnih i neizravnih zloupotreba ovlasti za stolna računala i poslužitelje. Svi alati su oblikovani u skladu sa dokazanim rješenjima koja povećavaju sigurnost i sukladnost sa sigurnosnim politikama bez utjecaja na produktivnost (npr. način upravljanja sjednicom je transparentan za krajnjeg korisnika, distribucija lozinki za korisnike s povećanim ovlastima obavlja se automatski). BeyondTrust je riješilo problem davanja prevelikih ovlasti pojedinim korisnicima transparentnim dodjeljivanjem ovlasti samo za one akcije koje pojedini korisnik treba kako bi obavio svoj posao. Svi povlašteni pristupi sustavu se snimaju i spremaju za kasniju reviziju. Organizacija je razvila sljedeće alate za nadzor korisnika s povećanim ovlastima: „Powerbroker desktops“, „Powerbroker servers“ te „Powerbraker password safe“. U nastavku je pregled tih alata.

5.3.1. Powerbroker desktops

BeyondTrust PowerBroker za stolna računala omogućuje organizacijama da uklone administratorska prava i da omogući krajnjim korisnicima pokretanje svih potrebnih Windows aplikacija, procesa i ActiveX kontrola. Eliminiranjem potrebe za dodjelom administratorskih prava krajnjim korisnicima, IT odjeli mogu stvoriti sigurniju okolinu za rad.

5.3.2. Powerbroker servers

PowerBroker za poslužitelje omogućuje administratorima sustava da delegiraju ovlasti i ovlaštenja bez otkrivanja *root* lozinke na Unix, Linux, Mac OS X poslužiteljima. Upravljanje je centralizirano putem jedinstvenog administrativnog web sučelja. Sučelje omogućuje izvođenje revizija, bilježenje događaja (kao pritisak svake tipki prilikom povlaštenog pristupa) te sadrži posebnu konzolu PSMC (*PowerSeries Management Console*). PSMC pruža platformu za automatizirano upravljanje povlaštenim pristupom, što uključuje bilježenje koja fizička osoba trenutno koristi privilegirani račun, koje akcije i koje naredbe je pokrenuo. Dodatno, omogućuje upravljanje korisničkom sjednicom za vrijeme cijelog životnog ciklusa (npr. mijenjanje lozinke nakon određenog broja korištenja) kroz razna heterogena okruženja (npr. aplikacija ili fizička osoba koja koristi privilegirani račun). PowerBroker alat moguće je integrirati sa postojećim poslužiteljima. Integracijom se omogućuje potpora za:

- izradu novih sigurnosnih politika i nadzor incidenata prilikom rada,
- centralizirano upravljanje, što omogućuje automatizirano stvaranje politika koje se odnose na ovlasti korisnika,
- reviziju podataka te
- propagaciju sigurnosnih politika u velikim implementacijama.

Ova integracija pomaže korisnicima da postignu visok stupanj sigurnosti i sukladnost sa sigurnosnim politikama, a uz to olakšava upravljanje velikim sustavima koji koriste korisničke račune sa povećanim ovlastima.

5.3.3. Powerbraker password safe

BeyondTrust PowerBroker Password Safe je alat za automatizirano upravljanje lozinkama, te kontrolu pristupa i izradu revizija svih vrsta privilegiranih računa (kao što su zajednički administrativni računi, računi koje koriste aplikacije i skripte, te lokalni administrativni računi). *BeyondTrust PowerBroker Password Safe* je dostupan kao fizički uređaj i kao virtualno računalo (koje se ostvaruje postojećim programskim rješenjima za virtualizaciju operacijskih sustava) kako bi se pokrile sve potrebe specifične za organizaciju. Omogućuje organizacijama da smanje rizik koji predstavljaju zajednički korisnički računi i umjesto toga nudi kontrolirani proces koji je moguće snimati i koji proizvodi lozinke za jednokratnu uporabu, rotira lozinke na bilo kojem sustavu kojim upravlja PowerBroker Password Safe te zapisuje korisničko ime i lozinku koja se aktivirala (kao i sve akcije koje korisnik izvodi). *PowerBroker Password Safe* je kritična komponenta proizvoda *BeyondTrust PowerSeries* koji automatizira upravljanje životnim ciklusom privilegiranih korisničkih računa. Osigurava pristup i postavlja temelj za „zrnato dodjeljivanje privilegija“ (stvaranje privilegiranih korisnički računa koji imaju ovlasti izvoditi samo mali skup operacija) i kontrolu pristupa iz drugih BeyondTrust alata.

5.4. Besplatna programska rješenja

Razvoj besplatnih programskih rješenja za nadzor korisnika s povećanim ovlastima je još u povoju. Postoje neki alati za općeniti nadzor korisnika sustava (npr. Central Authorization Service i Java Open Single Sign-On) ali ti sustavi ne pružaju funkcionalnost koja je potrebna za nadzor privilegiranih korisnika. Među korisnicima Unix/Linux operacijskih sustava često se susreću razna rješenja za problem nadzora korisnika s povećanim ovlastima. Neki korisnici koriste besplatna rješenja za nadzor korisnika s povećanim ovlastima (sudo[17]), neki pak komercijalna rješenja koja su jednostavnija za uporabu, ili pak ne koriste nikakav sustav za zaštitu privilegiranih računa. Todd Miller je 1994. godine objavio besplatno rješenje za nadzor korisnika s povećanim ovlastima pod nazivom *sudo*. sudo (engl. *superuser do*) omogućuje administratoru sustava da radi sa svojim korisničkim računom te da se prebaciti na administratorskog (*root*) korisnika (ili drugog korisnika) samo za naredbe kojima je potreban viši stupanj privilegija. *sudo* je također osmišljen radi poboljšanja postupka prijave kako bi se vidjele akcije koje su se obavljale u stanju povišenih ovlasti. Na ovaj način postiže se povezivanje fizičke osobe sa svim akcijama koje je izvršavao kao privilegirani korisnik. Ovo rješenje je vrlo jednostavno i automatski je podržano u svim novijim Unix/Linux operacijskim sustavima. U nastavku se obrađuju mane i prednosti korištenja sudo naredbe kao rješenja za nadzor korisnika s povećanim ovlastima.

5.4.1. Pozitivne strane

Jedan od najvažnijih čimbenika za ocjenjivanje *sudo* rješenja za nadzor korisnika s povećanim ovlastima je činjenica da je besplatan. Iako ne nudi niti približnu funkcionalnost kao komercijalni alati, često se nalazi u manjim organizacijama ili organizacijama koje se nalaze u prijelaznom stanju, odnosno nalaze se u procesu implementacije PIM rješenja te koriste sudo u prijelaznom razdoblju kako bi smanjili mogućnost napada. U nastavku su nabrojane i objašnjene dodatne pogodnosti korištenja sudo-a:

- **Pruža dodatan sloj zaštite prema *root* korisniku** – omogućuje korisnicima rad na sustavu, odnosno ne mijenja postojeći način pristupu sustava. Lozinka administrativnog korisnika (ili root korisnika) dodjeljuje se samo određenim osobama, a svaki puta kada korisnici izvedu privilegiran skup naredbi koristeći sudo te naredbe i korisnik se bilježe u posebne datoteke (npr. na RedHat/CentOS/Fedora sustavima ta datoteka se nalazi u */var/log/secure*, a na Debian/Ubuntu sustavima */var/log/auth.log*).
- **Pruža dodatan sloj zaštite protiv slučajnih zlouporaba** – prije korištenja sudo sustava, slučajne greške (male ili velike) je bilo mnogo teže odrediti, a pristup dijeljenim korisničkim računima bilo je nemoguće dovesti u vezu sa stvarnim korisnikom koji je unio promjenu u sustavu. Iako je ograničen u svojoj sposobnosti, sudo sprječava pogreške koje se mogu dogoditi kada administratori rade kao *root* korisnik i pokušavaju dovršiti poslove u žurbi.
- **Pojednostavljen proces za administratore** – sudo je moguće konfigurirati na način da se pripadnici određene grupe ne moraju autentificirati kako bi postali root korisnik, čime se postiže veća produktivnost. Ovo se često izbjegava u praksi jer predstavlja potencijalni sigurnosni rizik. Točnije, gubi se mogućnost bilježenja pojedinih akcija i time stvara propust u sustavu koji zločudni korisnici (npr. nezadovoljni zaposlenici) mogu iskoristiti za krađu podataka.
- **Dodaje mogućnost snimanja akcija u Unix sustavima** – snimanje u Unix/Linux sustavima nikad nije bio prioritet, a razlog tome je njegovo porijeklo (odnosno upotreba u naučno-istraživačkim programima i bazama podataka). Iako sudo ima znatne sigurnosne nedostatke u postupku prijave korisnika, definitivno predstavlja korak u pravom smjeru za snimanje akcija koje korisnik obavlja u stanju povišenih ovlasti.

[17] sudo – je program na Unix/Linux sustavima koji omogućava korisnicima izvođenje pojedinih naredbi sa ovlastima drugog korisnika.

- **Vremensko ograničenje** – kada korisnik poziva sudo i unosi svoju lozinku, sustav za tog korisnika proizvodi token[18] koji traje pet minuta (pretpostavljeno vrijeme, može se promijeniti). Ovaj sustav tokena daje sustavu jednu razinu zaštite u situacijama gdje postoji opasnost od napuštanja korisničke radne stanice pa drugi korisnici mogu koristiti tipkovnicu korisnika koji se prijavio kao korisnik s povećanim ovlastima.

5.4.2. Negativne strane

Glavni nedostatak sudo sustava kao PIM rješenja je to što se nemože koristiti u većim organizacijama. Sudo nije stvoren za implementacije velikih razmjera, tj. ne pruža dovoljnu razinu sigurnosti da bi bio efektivno PIM rješenja za kritične sustave. Sudo je „dobra odskočna daska“ za manja okruženja, ali nema arhitektonske vizije koje bi se mogle koristiti za zaštitu kritičnih sustava. Dok je sudo dobro primjenjivati u manjim organizacijama i okruženjima, u većim okruženjima sudo zahtjeva od organizacija da biraju između produktivnosti i sigurnosti. Točnije, sudo ne pruža transparentno korištenje već korisnici sami moraju inicirati njegovo pokretanje prilikom obavljanja akcija u stanju povišenih ovlasti. U nastavku su navedene još dva poprilično važna nedostatka korištenja sudo sustava.

1. **Nema službene podrške** – budući da je sudo proizvod napravljen pod *ISC*[19] licencom, nema izravnu podršku za korisnike/organizacije koji se susretnu sa tehničkim problemom. Međutim, postoji vrlo velika zajednica korisnika u kojoj je moguće potražiti odgovor na česta pitanja ili zatražiti savjet u rješavanju nekog novog problema u korištenju *sudo-baziranih* sustava. Ipak, ovakav pristup značajno smanjuje produktivnosti i povećava troškove za nadzor korisnika s povećanim ovlastima.
2. **Upitna sigurnost snimljenih podataka** – sudo snima i prati akcije koje pojedini korisnik izvodi, ali vrlo je teško osigurati sigurnost tih zapisa jer se nalaze na istom podatkovnom sustavu kao i računalo na kojem se pokreće sudo. Dodatno, ne nudi podršku za osiguravanje zapisa.

[18] Token – u području računarstva ima mnogo značenja. U ovom kontekstu tokeni označavaju objekte (najčešće pseudo-slučajan niz znakova) koji služe za jedinstvenu identifikaciju korisnika ili računala. Dodatna značenja za token su: uređaj za razmjenu lozinki između korisnika (elektroničko bankarstvo), virtualni objekt koji služi kao supstitut za određeni apoen novčane kovanice (u mikroplaćanju).

[19] ISC licenca –licenca za besplatan software koji je uvela organizacija ISC (*Internet Systems Consortium*). Funkcijski je ekvivalentna BSD liecnci i globalno je prihvaćena u zajednici slobodnog softwarea FSF (*Free Software Foundation*).

6. Budućnost

Vlada propisuje sve strože i strože industrijske standarde i zahtjeve kojima od organizacija traži da usvoje sigurnosne politike i dobru praksu upravljanja i nadzora korisnika s povećanim ovlastima. Tradicionalni pristupi za upravljanje korisnicima koji su u uporabi danas mogu uzrokovati sigurnosne prijetnje putem kojih organizacija može izgubiti značajne količine sredstava. Moderni PIM alati pomažu u nadzoru i upravljanju korisnika s povećanim ovlastima, ali ne nude jedinstvenu zaštitu. Svaka organizacija posjeduje infrastrukturu sa specifičnim svojstvima i samim time nije moguće jednim korakom pokriti sve sigurnosne propuste i nedostatke. Organizacije poput *Cyber-Ark Software*-a nude prilagodljiva rješenja koje se mogu prilagoditi većem broju infrastruktura, ali uz dodatnu konfiguraciju i integraciju. Ipak, niti jedno rješenje nije u stanju predvidjeti buduće sigurnosne prijetnje, a dolaskom novih tehnologija, aplikacija i okruženja dolaze i novi zahtjevi koji će se morati uzeti u obzir prilikom razvoja PIM sustava. Trenutna PIM rješenja pružaju dovoljan stupanj zaštite ali se i dalje rijetko kad nalaze u upotrebi u malim i srednje velikim organizacijama (prvenstveno zbog svoje visoke cijene). Neposredna budućnost PIM sustava značajno ovisi o javnom osvješćivanju organizacija o problemu nadzora korisnika s povećanim ovlastima. Obzirom na sve veći broj sigurnosnih propusta, stručnjaci vjeruju da će u narednih pet godina PIM sustavi postati sastavni dio svih IT odjela. Trenutno na tržištu dominiraju rješenja koja se integriraju kao dodatni servisi (npr. rješenja organizacije CyberArk) i ne postoji indikacija da će se raditi na razvoju tehnologija koje se ugrađuju u sigurnosni dio operacijskog sustava (npr. sudo). Razlog tome je prvenstveno portabilnost i transparentnost korištenja. Rješenja koja su usko vezana za pojedini operacijski sustav nisu pogodna za tržište koje se sastoji od velikog broja specijaliziranih operacijskih sustava. Također, rješenja koja su vezana uz operacijski sustav zasada nisu transparentna za krajnjeg korisnika, odnosno korisnik je svjestan da mora koristiti određeni alat za ostvarivanje povišenih ovlasti.

7. Zaključak

U današnja vremena vatrozid i IPS/IDS sustavi zaštite nisu dovoljni za zaštitu vitalnih informacija organizacije. Međutim, u procesu prilagođavanja na ovu novu suradnju putem virtualnog okruženja postoji ogroman izazov kako osigurati da se povlašteni pristup kritičnim informacijama ne zloupotrebljava. Novu sigurnosnu prijetnju predstavljaju unutarnji zlonamjerni korisnici, a posebice oni sa povećanim ovlastima. Kako bi se ograničila šteta koju takvi korisnici mogu nanijeti, organizacije uvode PIM (engl. *Privileged Identity Management*) rješenja. PIM rješenja, odnosno alati za nadzor korisnika s povećanim ovlastima, pomažu organizacijama u provođenju novih sigurnosnih politika koje su usmjerene na nadzor privilegiranih korisnika. Postoje brojna izvješća koja skreću pažnju na ovu novu vrstu sigurnosnog propusta, no većina organizacija i dalje ne shvaća njenu ozbiljnost. Primarna sigurnosna prijetnja kod korisnika s povećanim ovlastima je ta što organizacije često zanemaruju ili ne shvaćaju važnost procesa integracije i/ili implementacije programskih alata za upravljanje privilegiranim korisnicima. Najčešći razlog zbog kojeg organizacije koje imaju sustav za nadzor korisnika s povećanim ovlastima doživljavaju sigurnosne incidente je loša implementacija. Proizvođači nude generička rješenja koja nisu primjerena za sve organizacije. Većina organizacija se razlikuje po svojoj infrastrukturi i zato jedno rješenje nikako ne može pokriti sve potrebe. Alati poput Cyber-Ark PIM Suite-a se jednostavno implementiraju i prilagođavaju posebnim potrebama organizacija. No, njihova rješenja nisu pogodna svim organizacijama prvenstveno zbog visoke cijene, ali i zbog implicitne ovisnosti o Windows operacijskom sustavu. S druge strane, besplatna PIM rješenja su još uvijek u ranim fazama razvoja. Trenutno najpopularnije besplatno rješenje je *sudo*, no zbog velikih nedostataka u osiguravanju prikupljenih zapisa o korisničkoj sjednici i niskom razinom transparentnosti nisu pogodna za veće organizacije. Alati za upravljanje korisnicima s povećanim ovlastima trebali bi težiti platformskoj neovisnosti. Organizacije koriste razne kombinacije komercijalnih i besplatnih operacijskih sustava, a ako sustav za nadzor korisnika zahtjeva određenu platformu to dodatno otežava proces integracije i povećava troškove. Jedna od najbitnijih osobina sustava za nadzor korisnika s povećanim ovlastima je transparentnost za krajnjeg korisnika. Točnije, korisnik ne bi trebao promijeniti način rada (način na koji se prijavljivao na sustav) samo zato što se u pozadini pokreće snimanje svih privilegiranih akcija. Trenutno na tržištu ne postoje alati koji bi to omogućili, ali njihova pojava u skorijoj budućnosti je neupitna.

8. Reference

[1] Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

[2] How Secure is your sudo?, http://www.beyondtrust.com/WhitePapers/PDFS/wp002_How_Secure_Is_Your_sudo.pdf

[3] Privilege. Made Simple - Privilege Identity Management (PIM) demystified, http://www.beyondtrust.com/White-Papers-2.aspx?elq=3e3e705a76584ff8bb4483f7f60db795

[4] Compliance and Privileged Password Management, www.e-dmzsecurity.com/pdf/e-DMZ_Compliance_Passwords.pdf