Revizija mreže

- Kako započeti?
- Što tražiti?
- Alati na raspolaganju
- Primjeri

Ciklus IR-a


Risk Assessment & Audit Plan Development
Information Gathering & Planning
Audit Program Development
Audit Program Execution & Documentation
Audit Report Development
Follow-Up Procedures
Audit Committee Board Reporting

PRIRODA REVIZIJE

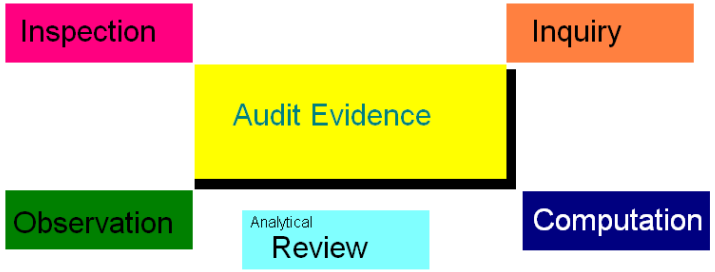
Planiranje revizije

- ✓ Utvrditi opseg rada i ciljeve
- ✓ Organizirati revizorski tim
- ✓ Poboljšati znanje o poslovanju
- ✓ Pregledati rezultate prethodnih revizija

  Identificirati faktore rizika
- ✓ Pripremiti program revizije

Prikupljanje revizorskih dokaza

- ✓ Promatranje poslovnih aktivnosti
- ✓ Pregled odgovarajuće dokumentacije
- ✓ Diskusije sa zaposlenicima
- ✓ Fizičko ispitivanje sredstava
- ✓ Potvrda putem trećih strana
- ✓ Ponovna provedba postupaka
- ✓ Analitički pregled Revizijsko uzorkovanje



PLANIRANJE, 1.

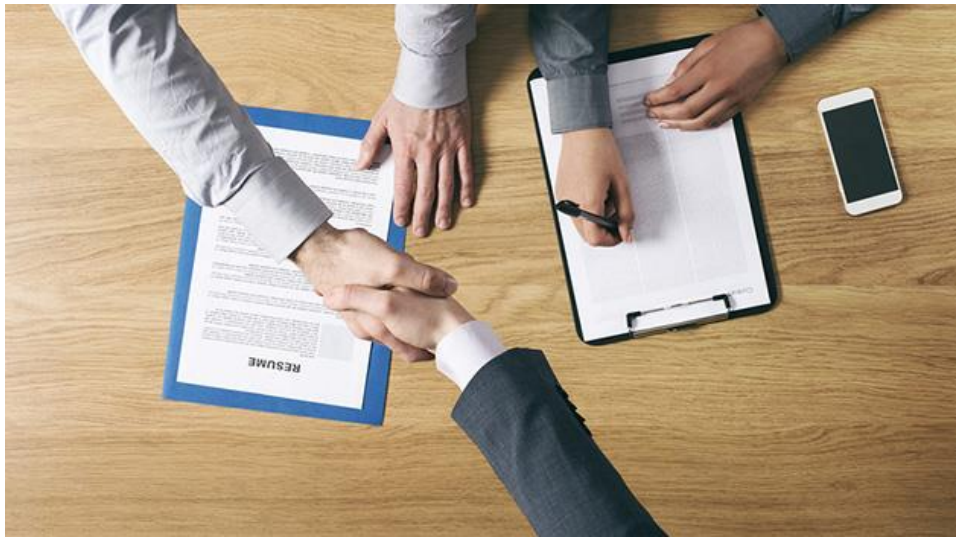
1. Razumijevanje svoje mreže na razini politike

- Shematski prikaz mreže *(fizički i logički)*
- Politika sigurnosti mreže
- Politika pristupa na daljinu
- Politika upravljanja konfiguracijama
- Politika upravljanja promjenama
- Politika upravljanja konfiguracijama
- Politika pristupa internetu
- Politika e-pošte i komunikacije
- Politika uporabe vlastite računalne opreme na poslu
- Politika sigurnosne kopije i vraćanja

2. Intervju s voditeljem Informacijskog odjela i voditeljem Odjela za informacijsku sigurnost

2.1. Intervju s višim administratorom mreže

2.2. Intervju s višim administratorom za sigurnost mreže



AKTIVNOSTI ZA PRELIMINARNI ANGAŽMAN

Odrediti zahtjeve tima za angažman u reviziji

Procijeniti postoje li dovoljne kompetencije

PLANIRANJE, 2.

3. Proučiti najnoviji izvještaj o procjeni i analizi rizika

3. Proučiti najnoviji izvještaj o pretraživanju mreže

Report Summary			
Scanner Name	Retina	Machines Scanned	1
Scanner Version	5.11.3.2156	Vulnerabilities Total	132
Scan Start Date	4/22/2010	High Risk Vulnerabilities	75
Scan Start Time	4:15:36 PM	Medium Risk Vulnerabilities	20
Scan Duration	0h 0m 57s	Low Risk Vulnerabilities	37
Scan Name	Untitled	Information Only Audits	18
Scan Status	Completed	Credential Used	56563119E37464C1B98CF5EB34680809
Vulnerable Machines	1		

CILJEVI I RIZICI KONTROLA

Uspostavljeni su mehanizmi za prepoznavanje rizika i reagiranje na njih, unutarnji i vanjski

Provedene su kontrole sigurnosti mreže za zaštitu IT sredstava i podataka poduzeća. Uređajima za mrežnu sigurnost odgovarajuće se upravlja

IT imovina odgovarajuće je zaštićena u mreži

Provedeno je odgovarajuće upravljanje promjenama

Odgovornosti IT-a odgovarajuće su definirane i o njima se odgovarajuće obavještava

Infrastruktura, kapacitet i sigurnost mreže podržavaju strateške planove IT-a koji su pomno usklađeni s poslovnim ciljevima.

Ovlasti za pristup korisnika su odobrene

Osmišljeni su i provedeni postupci za nepredviđene događaje.

Za pristup operativnim sustavima te značajnim aplikacijskim sustavima postoje kontrole odobrenja i autorizacije.

Nedefinirane uloge autorizacije i administratorskog pristupa

Nedostatan plan za oporavak podataka

Nedostaju kontrole za postavljanje novog korisnika i ukidanje računa

Strateški plan za IT je zastario ili ne postoji

Nedostaju administrativne politike, postupci i standardi konfiguracije lozinke IT-a

Potreba za formalnim upravljanjem promjenama

Nedovoljne kontrole prostorije s poslužiteljem

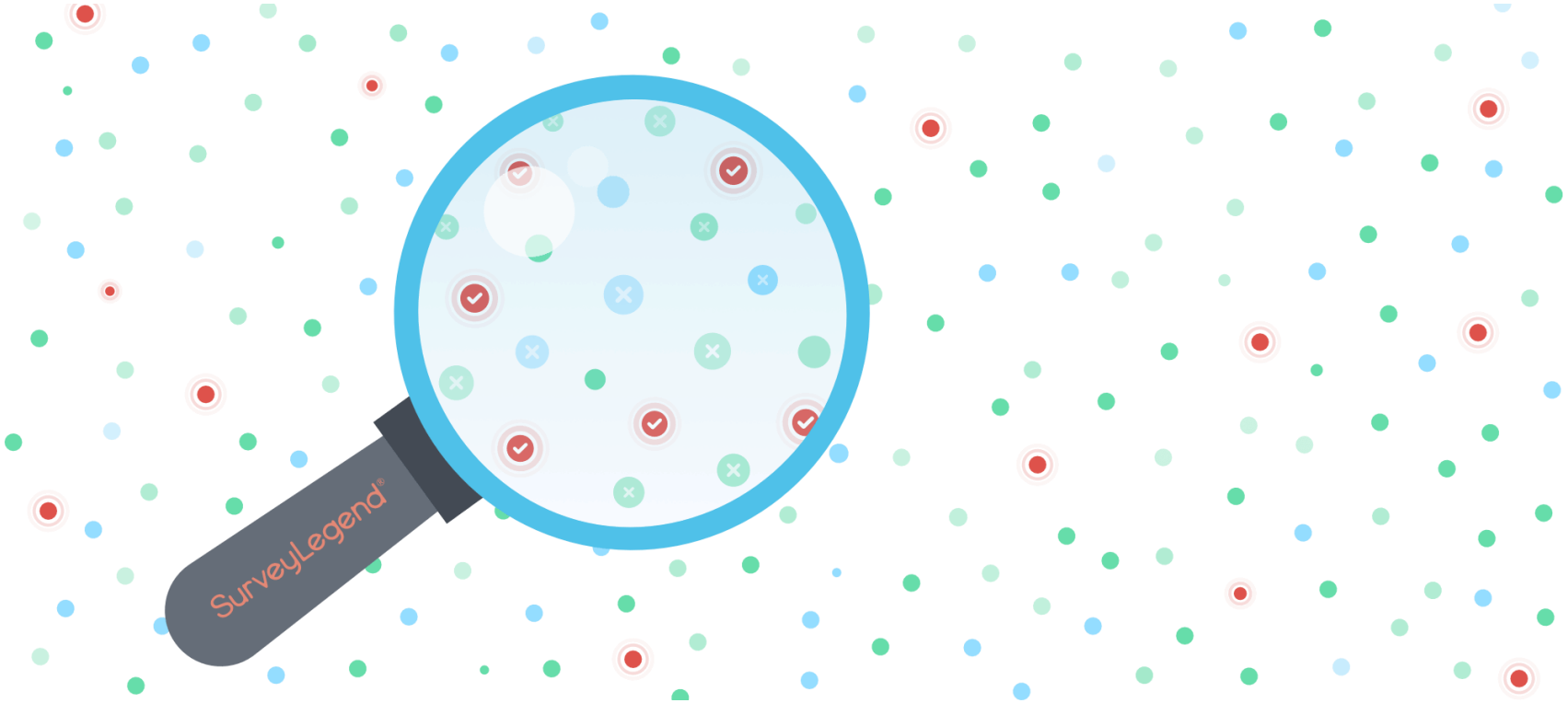
Nedostatan monitoring mreže

Nepostojanje procjene rizika u području IT-a

IZRADA MATRICE RIZIKA/KONTROLA

Rizik	Kontrola	Postupci testiranja
Procjena rizika u području IT-a ne postoji ili nije dovoljna	Utvrđivanje rizika *(unutarnjih i vanjskih)* dokumentira se u vodiču za upravljanje rizicima	Provjeriti i potvrditi jesu li uspostavljeni mehanizmi za prepoznavanje rizika i reagiranje na njih, unutarnji i vanjski ✓ Intervju s voditeljem informacijskog odjela i voditeljem odjela za informacijsku sigurnost ✓ Proučiti vodič za upravljanje rizicima ✓ Proučiti utvrđeni visoki rizik ✓ Proučiti provedene kontrole
Nedostatne kontrole za postavljanje novog korisnika i ukidanje računa	Postoji vodič za upravljanje korisnicima	✓ Intervju s ljudskim potencijalima ✓ Odabrati Ključno osoblje te provjeriti postavke i ukidanje njihovog računa
Nedostaju administrativne politike, postupci i standardi konfiguracije lozinke IT-a	Postoji politika za lozinke	✓ Intervju s administratorom mreže ✓ Provjeriti i potvrditi je li ispunjen zahtjev za složenost lozinke te poštuje li se za sve uređaje na mreži
Nedovoljan proces upravljanja promjenama	Proces upravljanja promjenama i relevantnim postupcima je uspostavljen	✓ Intervju s CISO-om, administratorom mreže ✓ Osigurati i potvrditi pridržavanje zahtjeva upravljanja promjenama za bilo kakvu promjenu na mreži, konfiguracije uređaja, pravila vatrozida, itd.
✓ Neovlašteni pristup prostoriji s poslužiteljem	✓ Pristup prostoriji s poslužiteljem odobren je samo odgovarajućem osoblju ✓ Uspostavljen je sustav kamera	✓ Proučiti snimke kako bi se osiguralo da nema neovlaštenog pristupa ✓ Proučiti zapise o pristupu

Uzorkovanje



PRIMJER

Opis kontrole: Samo viši administratori imaju puni pristup uređajima na mreži

Odgovorite na sljedeća pitanja o gore navedenom opisu kontrole:

1. Koji se dokazi moraju prikupiti?
2. Kako utvrditi veličinu uzorka?
3. Koji su potrebni koraci za testiranje ove kontrole?

PRIMJER, VELIČINA UZORKA

Veličina uzorka za puni*(administratorski)* pristup kontroli ovisi o kritičnosti sustava; broju korisničkih računa, broju uređaja na mreži itd.

Koraci testiranja:

1. Kako biste bolje razumjeli kako se konfigurira sigurnost, raspitajte se u informatičkoj službi
2. Promatrajte informacijsku službu pri generiranju upita sustava kako biste dobili popis korisnika s administratorskim dozvolama
3. Usporedite popis viših administratora s organigramom informacijske službe ili aktivnim popisom zaposlenika kako biste utvrdili je li pristup korisnika u skladu s odgovornostima posla
4. Raspitajte se kod rukovodstva IT-a kako biste utvrdili jesu li osobe s pristupom administratora odgovarajuće
5. Analizirajte zapisnike događaja kako biste vidjeli postoje li nepravilnosti

PRIMJER

Opis kontrole: Alati za automatizirano upravljanje konfiguracijama primijenjeni su za upravljanje sigurnosnom kopijom i zadržavanje svih uređaja na mreži. Zapisi o sigurnosnoj kopiji pregledavaju se nakon svake promjene konfiguracije te se dokumentiraju u obrascu za provjeru „Zapis o sigurnosnoj kopiji konfiguracije".

Odgovorite na sljedeća pitanja o gore navedenom opisu kontrole:

1. Koji se dokazi moraju prikupiti?
2. Kako utvrditi veličinu uzorka?
3. Koji su potrebni koraci za testiranje ove kontrole?

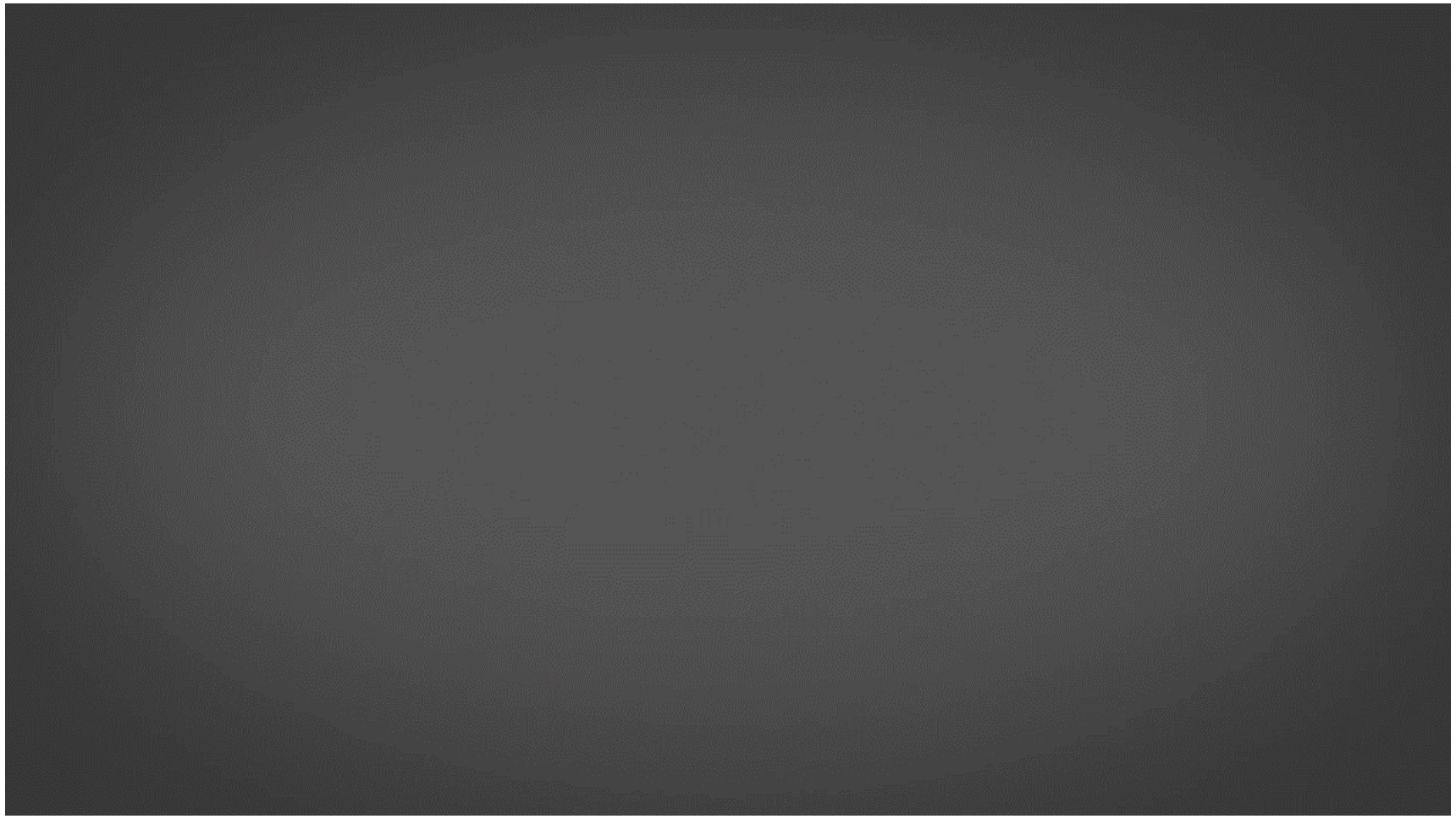
PRIMJER, VELIČINA UZORKA

Veličina uzorka za kontrolu upravljanja promjenama konfiguracije temelji se na cijeloj ukupnosti promjena, kritičnosti uređaja mreže itd.

Koraci testiranja:

1. Pribavite raspored sigurnosnih kopija *(za uređaje koji su obuhvaćeni)* iz automatiziranog alata administratora mreže.
2. Nasumično odaberite uzorak od nekoliko dana
3. Iz uzorka pribavite datoteku povijesti i utvrdite jesu li zadaci izvršeni prema politici
4. Pribavite obrazac za provjeru sa zapisom o sigurnosnoj kopiji konfiguracije i utvrdite jesu li zadaci izvršeni prema rasporedu sigurnosne kopije.
5. Ako zadaci nisu izvršeni prema politici, utvrdite jesu li istraženi i razriješeni.

ALATI ZA REVIZIJU MREŽE



ALATI ZA REVIZIJU MREŽE

1. **Spiceworks Inventory** - Alat za mrežni inventar koji automatski otkriva mrežne uređaje
2. **Nessus -** Besplatan alat za procjenu izloženosti s više od 450 predložaka konfiguracija i izvješćima koja je moguće prilagoditi
3. **Network Inventory Advisor** – Alat za skeniranje inventara koji je kompatibilan sa sustavima Windows, Mac OS i Linux
4. **ManageEngine Vulnerability Manager** *(dostupna je BESPLATNA PROBNA VERZIJA)* – Ovaj paket provjera sigurnosti sustava čisti vašu mrežu i provjerava postoje li sigurnosni nedostaci. Radi na sustavima Windows i Windows Server.
5. **Netwrix Auditor -** Softver za reviziju mrežne sigurnosti s upravljanjem konfiguracijama
6. **Nmap *(Zenmap GUI)*** - Alat otvorenog koda za pretraživanje portova i istraživanje mreže dostupan kao komandno-linijsko sučelje
7. **OpenVAS** - Alat za procjenu izloženosti za korisnike Linuxa s redovnim ažuriranjima
8. **Acunetix -** Mrežna aplikacija za provjeru mrežne sigurnosti koji može otkriti više od 50,000 mrežnih nedostataka kada se integrira s alatom OpenVAS
9. **Metasploit** - alat za testiranje prodornosti koji vam omogućava hakiranje zloupotreba u vašoj mreži

OSIGURANJE KVALITETE

Hvala!