ПРИНЦИП НУЛТОГ ПОВЕРЕЊА
У РАДУ СА ТАЈНИМ ПОДАЦИМА

Информациона безбедност у раду са тајним подацима представља један од кључних концепата заштите националних, корпоративних и институционалних вредности. Савремени информациони системи који управљају тајним подацима морају бити отпорни на потенцијалне претње и компромитацију. **Принцип нултог поверења је безбедносни приступ који елиминише подразумевано поверење и захтева континуирану верификацију идентитета и приступа. У раду са тајним подацима, овај модел осигурава да само овлашћени корисници могу приступити тајним подацима и информацијама.** Принцип нултог поверења се значајно разликује од традиционалних модела безбедности, посебно од **периметарског приступа** („castle and moat“), који претпоставља да су корисници унутар мреже поуздани.

ПРИНЦИП НУЛТОГ ПОВЕРЕЊА

1. **Никада не веруј, увек проверавај** – сваки захтев за приступ се верификује без обзира на локацију корисника.
2. **Минимални приступ** – корисници добијају само онолико привилегија колико им је неопходно.
3. **Континуирано праћење** – активности корисника се анализирају у реалном времену ради детекције потенцијалних претњи.
4. **Шифровање података** – тајни подаци се чувају и преносе у шифрованом облику.
5. **Сигурни комуникациони канали** – употреба VPN-а, шифрованих е-порука и безбедних платформи за размену тајних података и информација.

Принцип нултог поверења vs. Традиционални безбедносни модели у раду са тајним подацима

Карактеристика	Традиционални модел	Принцип нултог поверења
Приступ	Дозвољава приступ корисницима унутар мреже	Захтева верификацију за сваки приступ
Контрола приступа	Заснована на локацији корисника	Континуирана аутентификација и ауторизација
Сигурност података	Фокус на заштиту периметра	Шифровање и минимални приступ
Претпоставка о поверењу	Корисници унутар мреже се сматрају поузданим	Нико није поуздан по дефиницији
Мониторинг	Ограничен надзор активности	Континуирано праћење и анализа
Заштита комуникације	Стандардни канали комуникације	Шифровани и сигурни канали

ПРИНЦИП НУЛТОГ ПОВЕРЕЊА У РАДУ СА ТАЈНИМ ПОДАЦИМА

Need to Know и **Принцип нултог поверења** су два принципа безбедности који се примењују у раду са тајним подацима, али имају различите приступе и циљеве.

Сличности

- **Ограничен приступ** – Оба модела ограничавају приступ тајним подацима и информацијама само на овлашћене кориснике.
- **Минимални приступ** – Корисници добијају само онолико привилегија колико им је неопходно за обављање посла.
- **Заштита тајних података** – Оба модела имају за циљ спречавање неовлашћеног приступа и компромитације тајних података и информација.

Разлике

Карактеристика	**Need to Know**	**Принцип нултог поверења**
Фокус	Приступ подацима заснован на улози корисника	Континуирана верификација сваког приступа
Претпоставка о поверењу	Корисници који имају одобрење се сматрају поузданим	Нико није поуздан по дефиницији
Контрола приступа	Дефинисане листе приступа на основу пословних потреба	Динамичка аутентификација и ауторизација
Мониторинг	Периодичне провере приступа	Континуирано праћење и анализа активности
Заштита комуникације	Фокус на интерне процедуре и контролу приступа	Шифровани и сигурни комуникациони канали

Примена у информационим системима

- **Need to Know** се користи у **класичним безбедносним структурама**, као што су војне и државне институције, где се приступ подацима заснива на хијерархији и улогама.
- **Принцип нултог поверења** је погодан за **модерне ИКТ системе**, посебно у cloud окружењима, где се приступ подацима мора динамички контролисати и верификовати.

Принцип нултог поверења је еволуција безбедносног приступа, јер елиминише подразумевано поверење и примењује строге мере верификације. У комбинацији са **Need to Know**, може значајно унапредити заштиту тајних података у информационим системима од посебног значаја.

ПРИНЦИП НУЛТОГ ПОВЕРЕЊА У РАДУ СА ТАЈНИМ ПОДАЦИМА

Како имплементирати Принцип нултог поверења у раду са тајним подацима?

✓ **Строга контрола приступа** – дефинисање правила приступа и примена мултифакторске аутентификације.
✓ **Шифровање података** – коришћење криптографије за заштиту поверљивих информација.
✓ **Сигурни комуникациони канали** – избегавање јавних мрежа и коришћење VPN-а.
✓ **Континуирано праћење и анализа** – примена система детекције упада (IDS) и безбедносних информационих система (SIEM).
✓ **Едукација запослених** – обука за препознавање сајбер претњи и социјалног инжењеринга.

Принцип нултог поверења је идеалан модел за заштиту тајних података, јер елиминише ризик од неовлашћеног приступа и осигурава да се сваки захтев за приступ строго контролише.

КАНЦЕЛАРИЈА САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ И ЗАШТИТУ ТАЈНИХ ПОДАТАКА

e-mail: office@nsa.gov.rs, kontakt@nsa.gov.rs

web: www.nsa.gov.rs