Prilog 1. CARNET Oblak – Opis sustava i zahtjevi za Idejno rješenje

U svrhu realiziranja projekta CARNET Oblak, CARNET razvija Software-Defined Data Center - SDDC. Uz fizički (hardverski) dio infrastrukture, CARNET SDDC sastoji se od tri glavne komponente:

- Infrastructure as a Service – IaaS
- Platform as a Service – PaaS
- Software-Defined Storage – SDS

SDDC kao računalna infrastruktura mora biti sigurna od računalnih ugroza. Svaki dio SDDC platforme mora biti osiguran metodama primjenjivima za tehnologije koje se koriste. U takvim oblicima infrastrukture primjenjuje se defense-in-the-depth metoda zaštite. Takva metoda zaštite podrazumijeva nekoliko slojeva obrane cijelog sustava od računalnih ugroza, kako u slučaju kompromitacije određenog dijela infrastrukture, napadač ne može doći do njemu vrijednih informacija koje bi na neki način kompromitirale sustav ili njegove korisnike. **Potrebno je osigurati sigurnost cjelokupnog sustava implementacijom sigurnih postavki na već postojeće rješenje kao i dinamičkim provjerama sigurnosti kako bi se osiguralo kontinuirano praćenje razine sigurnosti cijelog SDDC sustava.**

Infrastructure as a Service

U projektu CARNET Oblak, kao IaaS platforma koristi se open-source rješenje OpenStack. OpenStack je platforma za upravljanje i održavanje velikog broja računalnih resursa (CPU i RAM), sustava za pohranu podataka (eng. storage) i mrežnih resursa u data centru. Resursima se upravlja kroz OpenStack API kroz standardne autentifikacijske mehanizme. OpenStack je multitenantna platforma gdje svaki korisnik ima pravo pristupa isključivo resursima svog tenanta te ne smije imati mogućnost pristupa resursima drugih tenanta.

Idejnim rješenjem potrebno je obuhvatiti:

- Snimku stanja i securty audit postojeće OpenStack infrastrukture te dodatnih komponenti koje koji čine cjelokupni IaaS ekosustav,
- Prijedlog sigurnosnih poboljšanja na temelju analiza postojećeg sustava,
- Prijedlog arhitekture i dizajna idealnog rješenja sa svim potrebnim sigurnosnim mehanizmima,
- Izradu procedura za sigurno održavanja postojećeg IaaS ekosustava,
- Isporuku prateće dokumentacije.

Platform as a Service

U projektu CARNET Oblak, kao PaaS platforma koristi se OKD (OpenShift Origin) što je open-source OpenShift distribucija čiji je glavni upravljački mehanizam Kubernetes. Kubernetes služi kao orkestrator kontejneriziranih aplikacija na OKD platformi. Orkestracija kontejnerima mora biti izvedena na siguran način uz dobre i valjane sigurnosne politike.

Idejnim rješenjem potrebno je obuhvatiti:

- Snimku stanja postojeće infrastrukture koju obuhvaća OKD,
- Definiranje i prijedlog sigurnog deploya kontejneriziranih aplikacija na OKD platformu,
- Prijedlog, dizajn i izrada CI/CD pipeline-a sa svim potrebnim security mehanizmima,
- Isporuku prateće dokumentacije.

Software-Defined Storage

U projektu CARNET Oblak, kao sustav za pohranu podataka, koristi se Ceph. Ceph je unificirani, distribuirani sustav za pohranu podataka dizajniran za izvrstan performanse, stabilnost i skalabilnost. Svaki klijent (*tenant*) koji ima rezerviran svoj dio SDDC dijela infrastrukture, smije koristi isključivo onaj dio sustava za pohranu podataka koji mu je dodijeljen, te ne smije imati mogućnost čitanja i pisanja podataka od drugih tenanta odnosno korisnika SDDC sustava.

Idejnim rješenjem potrebno je obuhvatiti:

- Snimku stanja postojeće Ceph infrastrukture te Ceph procesa,
- Prijedlog sigurnosnog jačanja (eng. hardening) Ceph infastrukture,
- Izradu procedura za sigurno održavanje Ceph infrastrukture,
- Isporuku prateće dokumentacije.

Sustav za evidenciju dodjeljivanja hardverskih i softverskih komponenti – inventory

Preduvjet bilo kakve sigurne kontrole resursa je korištenje sustava za evidenciju dodjeljivanja hardverskih i softverskih komponenti (*eng. hardware i software inventory*). U svakom trenutku se mora znati koje točno komponente su dodijeljene kojem korisniku, koliko resursa ima pravo koristiti i na koji vremenski period, uz sve potrebne informacije o pravnom subjektu koji je korisnik SDDC sustava.

U sklopu projekta e-Škole potrebno je izraditi softverski sustav kroz koji će se moći pratiti dodijeljeni hardverski i softverski resursi. Takav sustav služi za evidenciju dodijeljenih resursa te slanja zahtjeva za resursima, a ujedno i vrši provizioniranje resursa. Sustav mora imati sljedeće karakteristike:

- Inventory sustav mora biti multi-tenant - što znači da svaki korisnik može vidjeti isključivo podatke svog tenanta i ne smije imati mogućnost čitanja ili pisanja po podacima ostalih korisnika
- Sustav mora imati implementiranu AAI@EduHr autentifikaciju
- Sustav mora jedinstvenim identifikatorom vezati dodijeljene resurse korisnika za tog korisnika
- Sustav mora imati mogućnost komunikacije sa OpenStack API-em kako bi kroz inventory sustav korisnik mogao provisionati infrastrukturu, ovisno o resursima koji su mu dodijeljeni
- Sustav mora imati mogućnost slanja notifikacija, ovisno o definiranim scenarijima
- Sustav mora imati implementiran API, kako bi drugi sustavi upitom na taj API mogli dobiti određeni set informacija
- Baza podatka sustava, osim podataka o dodijeljenim hardverskim i softverskim resursima, mora sadržati sve podatke o ustanovi kojoj su dodijeljeni resursi, kao i kontakt podatke odgovornih osoba

Idejnim rješenjem potrebno je detaljno razraditi funkcionalnu i tehničku specifikaciju Inventory sustava.

Sigurnosni nadzor SDDC sustava

SDDC kao Software-Defined Data Center mora biti zaštićen kao i klasični data centri uz dodatne zaštite koje su primjenjive za ovakvu vrstu tehnologije. Na svakom dijelu infrastrukture moraju se nalaziti alati za analizu prometa te cijeli mrežni promet koji prolazi kroz SDDC sustav, mora biti monitoriran te se svaki sigurnosni incident mora biti proslijeđen u Security Information and Event Management – SIEM. Potrebno je implementirati pravila za detekciju sigurnosnih incidenata za svaki dio SDDC arhitekture, te svaki dio defense-in-the-depth modela obrane mora biti pokriven pravilima za detekciju sigurnosnih incidenata. Za uspješan nadzor cjelokupnog SDDC sustava potrebno je poštivati sljedeće smjernice:

- Pregled stanja postojećeg sustava za nadzor SDDC sustava,
- Prijedlog i izrada dizajna idealnog rješenja za sigurnosni nadzor SDDC sustava,
- Definiranje i izrada pravila na temelju kojih je moguće detektirati računalne ugroze prema ili unutar SDDC sustava,
- Isporučiti prateću dokumentaciju.

Idejnim rješenjem potrebno je detaljno opisati mogućnosti nadzora (pravila, metode, alate, scenarije) te ih opisati u obliku funkcionalne i tehničke specifikacije.