LITNET teikiamų IT paslaugų plėtra

Tinklo atakų užkardinimo bei įsibrovimo prevencijos paslauga

PROJEKTO Nr. 09.3.3- ESFA-V-711-01-0003

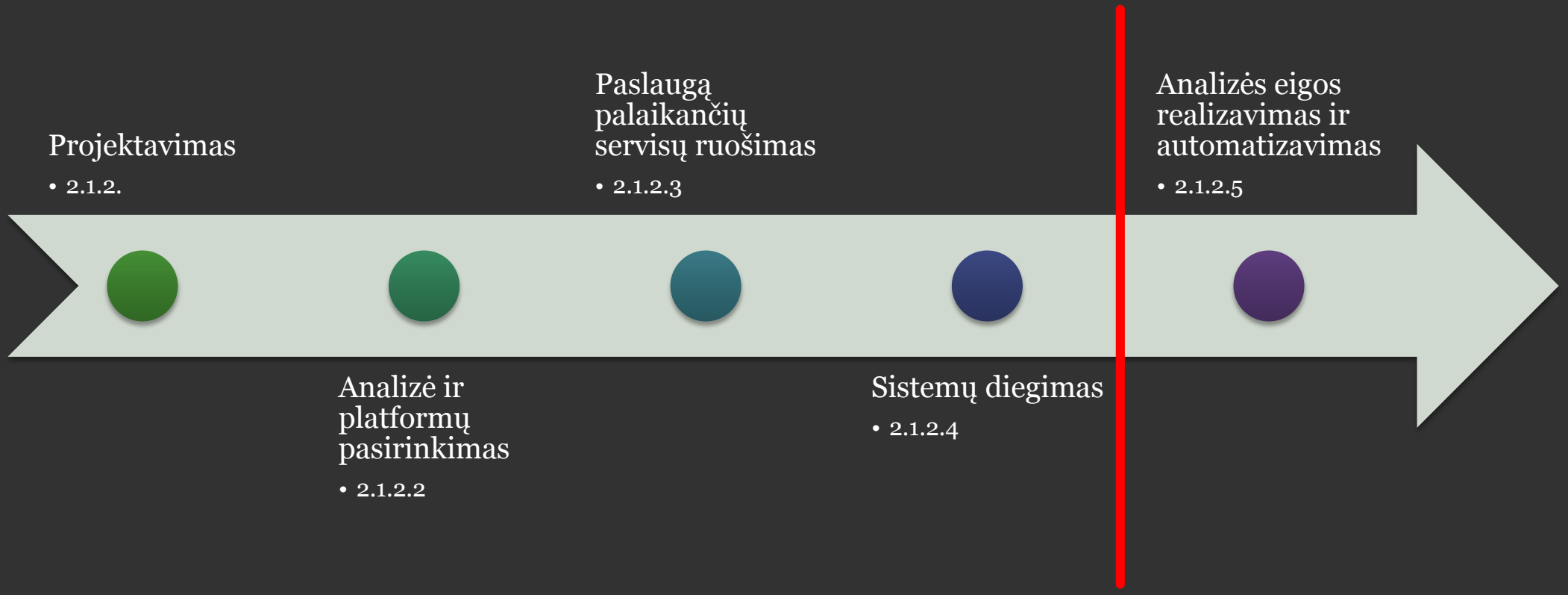
DARBŲ EIGA

KTU ITD: Š. Grigaliūnas

Pagrindinius iššūkius, su kuriais šiandien susiduria LITNET CERT

- Efektyvumas – iš IT funkcijos reikalaujama geresnės paslaugų kokybės ir kaštų mažinimo;
- Inovacijos, kai rinka ir naujų technologijų atsiradimas reikalauja keisti ne tik IT, kad išlikti konkurencingu;
- Plėtra ir dėl to augantis IT projektų portfelis turi būti nuolat peržiūrimas, suteikiant prioritetą didžiausią vertę nešančioms veikloms;
- Teisinės atitikties užtikrinimas verčia papildomai investuoti į IT;
- Procesai, kurie nuolat kinta įtakojami ir įtakodami IT, reikalaudami esminio IT funkcijos pokyčio;
- Reorganizacija – verslams plečiantis ar jungiantis, IT turi ne trukdyti, o padėti procesui.

TINKLO ATAKŲ UŽKARDINIMO BEI ĮSIBROVIMO PREVENCIJOS PASLAUGA



Projektavimas

- Analizės dalyje išnagrinėtos tinklo atakų užkardinimo bei įsibrovimo prevencijos platforma (programinė) įrangos charakteristikos.
- Sudarytas veiklos modelis: buvo išanalizuoti veiklos dalyviai ir vykstantys procesai, sudaryti panaudojimo atvejų modeliai.
- Panaudojus sudarytus modelius apibrėžti ryšiai tarp dalyvių ir veiklos procesų.
- Išnagrinėjus panašias, jau veikiančias sistemas, galime teigti, kad nei viena sistema neatitinka keliamų reikalavimų, turi ne visas reikiamas funkcijas. Todėl nuspręsta ieškoti kompleksinio sistemų apjungimo, kuris turėtų visas reikiamas savybes.

Analizės ir platformų pasirinkimo veiklos rezultatas

- Šiame projekto etape buvo analizuojama ir kuriama virtualių paslaugų platforma, t .y. atliekamas funkcinių ir nefunkcinių reikalavimų surinkimas, analizė bei specifikavimas; sistemos prototipo kūrimas. Vėliau vyko parengiamieji darbai - diegimo aplinkos (serverio) analizė, projektavimas bei paruošimas; panaudos atvejų sudarymas ir specifikavimas; komponentų tarpusavio sąveikos analizė; testavimo plano sudarymas; sistemos prototipo kūrimas. Šios veiklos metu buvo parengta funkcinių ir nefunkcinių reikalavimų projektinė specifikacija, sukurtas sistemos grafinis prototipas; parengta diegimo aplinkos specifikacija; sukurta diegimo aplinka; parengta platformos panaudos atvejų specifikacija.
- Projektui buvo pasirinktas bei įsigyta **Dell PowerEdge R630**. Pagrindinis keliamas kriterijus buvo *našumas*. Ateityje pritrukus vietos bus svarstoma apie dalies duomenų (pvz. Žalingo kodo pavyzdžių) iškėlimą į *išorinę duomenų saugyklas*.

Paslaugą palaikančių servisų ruošimas

Testuotas įrangos apkrovimas

- Pasiekiamas maksimalus įrangos apkrovimas su mažesniu fizinės įrangos kiekiu. Esant vienų resursų didelei apkrovai, papildomi resursai perkeliami iš mažiau apkrautų serverių.

Testuotas greitumas ir paprastumas

- Greitesnis ir paprastesnis aplikacijų diegimas, reikalingų resursų išskyrimas. Virtualios mašinos gali būti klonuojamos taip greitai ir paprastai kaip mums visiems žinoma „copy-paste“ operacija. Virtuali mašina gali būti lengvai perkeliama iš vieno fizinio serverio į kitą nenutraukiant jos darbo.

Išplėstos paslaugų teikimo galimybės

- Galimybė valdyti visus resursus nuotoliniu būdu, stebėti ir analizuoti resursų panaudojimo tendencijas, ieškoti dar efektyvesnių sprendimų pasitelkiant specialią programinę įrangą, sukurti virtualias darbo vietas, kai vienu kompiuteriu naudojasi keli darbuotojai netrukdydami vienas kitam.

Sistemų diegimas

- Kibernetinėje erdvėje plinta nauja atakų karta, kuri lengvai apeina tradicines saugos priemones, veikiančias statinės analizės pagrindu. Nuo šių atakų organizacijas gali apsaugoti smėliadėžės principu veikiantys įrenginiai. Jie simuliuoja įtartiną kodą bei failus skirtingose virtualiose aplinkose, tokiu būdu išanalizuodami jo veikimą ir pasekmes skirtingoms sistemoms.
- Įdiegta saugumo įranga padeda identifikuoti visus atakos lygius:
  - pažeidžiamumo išnaudojimo kodą;
  - kreipimąsi į CnC (Command & Control) centrą;
  - kenkėjiško kodo parsisiuntimą bei duomenų iš sistemų paėmimą.