Säkerhet – utökat skydd

Projektplan

Innehåll

Innehållsförteckning

Innehåll **2**

Bakgrund och projektidé **3**
Projektdirektivet: Säkerhet – utökat skydd *3*
Bakgrund *3*
Direktiv *3*
Mål *4*
Organisation *4*

Avgränsningar **4**

Organisation **5**

Projektaktiviteter **6**
Huvudaktiviteter *6*
Delaktiviteterna *6*

Tidsplan **7**

Kommunikation och information **7**

Budget **8**

Bakgrund och projektidé

Projektdirektivet: Säkerhet – utökat skydd

Projekt utreder möjligheten till att öka skyddet på lärosäten genom att använda sig av *Nästa generations brandväggar (Next Generation FireWall)* och *System för intrångsskydd (Intrusion Prevention System).*

Bakgrund

Säkerhetsfrågor inom IT-området har blivit allt viktigare för svenska lärosäten då dataintrången ökar kraftigt. Idag ser vi betydligt mer av sofistikerade attacker och avancerade hot mot våra informationstillgångar vilket i sin tur gör det svårt eller omöjligt att hantera detta med traditionell teknik. Idag finns det ett starkt behov av sofistikerade och automatiserade tekniska lösningar för att möta hoten. Kostnaden för traditionella metoder att bemöta dessa hot är kraftigt ökande vilket är ett starkt incitament för att ett bättre stöd måste implementeras.

Direktiv

Projektet utreder två delar inom säkerhetsområdet d.v.s. *Nästa generations brandväggar* samt *System för intrångsskydd.*

Allmänna frågeställningar

- Vad sparar vi budgetmässigt på att införa ovanstående lösningar?
- Vilka aktuella produkter finns på marknaden som kan vara lämpliga att använda?
- Hur ser produkternas uppdateringar ut? Det krävs att produkterna får sin information om skadlig kod och säkerhetshot från de flesta tidszoner för att fungera tillfredställande.

Nästa generation brandväggar

- Vad ger *nästa generations brandväggar* för effektivitetsvinster?
- Att börja i liten skala och sedan expandera, vad ska man tänka på och ta i hänsyn vid ett sådant införande?
- Redundans?
- Kompabilitet mot nätinfrastruktur?
- Inom vilka områden ser man administrativa vinster?
- Ökning av administrativa/löpande kostnader?
- Administrationsgränssnitt och behörighetsnivåer (Nät, IRT, Support)

System för intrångsskydd

- Äldre IPS krävde mycket administration och underhåll, hur ser det ut idag?
- Hur kan man koppla ISP funktioner mot befintlig infrastruktur (övervakning, loggning mm.)
- Hur ser ett rekommenderat införande ut?
- Redundans?

Mål

Huvudmålet med projektet är att ta fram rekommendationer kring *Nästa generations brandväggar* samt *System för intrångsskydd*. Här är det viktigt att projektet kan visa på de vinster och extra kostnader det medför att implementera någon av dessa lösningar. Projektet skall även visa på skillnaden och likheter mellan dessa tekniska lösningar.

Projektet utvärderar olika produkter som implementerar de olika tekniska lösningarna och gör en jämförelse och rekommendation kopplat till dom olika produkterna.

Organisation

Projektledare utses som ansvarar för att ta fram en projektplan.
En referensgrupp skapas som kan ge input till projektet.

Avgränsningar

Projektet arbetar enbart med kvalificerade system för NGEN brandväggar och Intrusion Detection/Prevention systems. Andra typer av säkerhetssystem och verktyg t.ex. virusskydd för klienter eller krypteringsverktyg behandlas inte.

Organisation

Projektledare: Sören Berglund, UmU soren.berglund@umu.se

Projektresurs: NN

Utredningsstöd: NN

Uppdragsgivare: Per Hörnblad, projektkoordinator SUNET Inkubator, per.hornblad@umu.se

Projektet har en referensgrupp. Gruppen ska hjälpa till att leda projektet i rätt riktning.

Sören Berglund, PL	UmU	soren.berglund@umu.se
Maria Edblom-Tauson	UmU	maria.edblom-tauson@umu.se
Peter Hallin	LU	peter.hallin@ldc.lu.se
Jonatan Hazell	ORU	jonatan.hazell@oru.se
Pär Igsell	SLU	par.igsell@slu.se
Patrik Lidehäll	KTH	patrik@irt.kth.se
Björn Mattsson	BTH	bjorn.mattsson@bth.se
Håkan Pettersson	Konstfack	hakan.pettersson@konstfack.se
Mattias Pettersson	ORU	mattias.pettersson@oru.se
Fredrik Rönnvall	Chalmers	fredronn@chalmers.se

Projektet har ingen styrgrupp.

Projektaktiviteter

Eftersom detta projekt är av utredningskaraktär kommer det att vara ett iterativt arbete med att utreda och föreslå aktiviteter.

Huvudaktiviteter

Huvudaktiviteternas syfte är att beskriva och genomföra en övergripande plan.

A. Projektledning, projektstyrning och arbetssätt/metoder
B. Utredningsarbete inkl. dokumentation
C. Kommunikation och förankring
D. Projektavslut

Delaktiviteterna

Delaktiviteterna per område är följande:

A.
- Projektledning och projektstyrning
- Problem- och målbeskrivning

B.
- Marknadsanalys och marknadsvärdering
- Identifiering av tillämpliga arkitekturmönster
- Fastställande av omfattning av IPS- och NGEN-installation
- Fastställande av riskgrupper att monitorera (Intrång, DDOS etc.)
- Fastställande av strategi för IPS (övervägande enhet eller övervägande nätverksinstallation)
- Dimensionering av logg- och eventmottagare
- Framtagande av policy för IPS och NGEN
- Utredning hur och när forensik skall genomföras med avseende på information från IPS och NGEN
- Roller på lärosätet som krävs för att hantera IPS/NGEN.

C.
- Kommunikation, presentationer och högskoleinterna webinars

D.
- Slutrapport och förslag till fortsatta aktiviteter

Tidsplan

Tidplanen ger en vy över progressionen i utredningen och när milstolparna kan förväntas vara klara.

Milstolpar	2017	Jan	Feb	Mar	Apr	Maj	Juni	Aug	Sept	Okt	Nov	Dec
Skapa referensgrupp												
Skapa utkast till projektplan												
Fastställa projektplan												
Problem – och målbeskrivning												
Marknadsanalyser												
Kommunicera resultat												
Slutrapport												

Kommunikation och information

- Referensgruppen, e-möten via Adobe Connect på https://connect.sunet.se/inkubator
- Sunet-inkubator under Sunetdagarna vår och höst 2017. Presentation och deltagande.
- Aktivt använda webben för att sprida information. Wiki på portal.nordu.net
- Projektplace.se för planering, tidrapportering, projektdokument och kollaboration mellan projektmedlemmar.
- Aktivt använda Adobe Connect för webinars, erfarenhetsutbyte/resfria möten

Budget

Typ	Huvudaktiviteter	Resurs	Timmar	Budget 2017, SEK
A	Policys och roller		20	12000
B	Arkitektur		200	120000
C	Marknadsanalys		200	120000
D	Projektledning		80	48000
E	Konsulttid		40	48000
		Totalt		348000

Tillgänglig budget: 370.000 kr
Arbetskostnad/ersättning för personal från lärosäten: 600 kr/tim

Resor och omkostnader hanteras av projektets budget. Deltagande i Sunet Inkubatordagar bekostas av Inkubators aktivitet ”Samverkan”