

Presentation Sunetdagarna i Gävle våren 2018

Säkerhet Utökat Skydd

En kort sammanfattning - presentation av våra slutsatser och en tidslinje för projektets avslut

Sunet Inkubator

Fredrik Rönnvall Chalmers Tekniska Högskola

Next-Generation Firewall

- Kallas numera *Enterprise Firewall*
-

Avgränsningar

Avgränsningar

Vi har haft som avsikt att enbart ha i åtanke fysiska "lådor" - dvs Enterprise Firewall in a box.

Det innebär att vi inte överväger andra metoder att åstadkomma samma funktioner med andra verktyg, utan enbart ett färdigt paket man kan beställa.

1- Policy

Generell Policy

- Lärosätet bestämmer
 - Etik / Moral
 - IT-Avdelningen skall inte skriva policy, men är policyn generell kan man snabbare anpassa sig till förändrad hotbild
 - Hänvisa till SUNET-regler i de fall de är tillgängliga
 - Risk att hindra forskare att forska med en för strikt policy
-

Personbundet

- Vem snarare än vilken enhet
 - Konsekvenser skall vara tydligt kommunicerade
 - Information om att loggning sker
-

2- Roller

Personal

- Dedikerat Team
- Svårt för mindre lärosäten
- Bemanningsfrågor
- Personal med flera roller
- Personal med mindre rättigheter för att kunna hantera larm

- Automatiserade hantering av *vardagliga* larm
-

Regeländringar

Avser ändringar av konfiguration i själva lådan

- Följer en tydlig process
 - Dokumenteras - centralt, loggas
 - Följs upp
-

3- Hotbild

Idag

- Ransomware
 - Cryptominers
 - Exploit kits
 - Phishing
 - "Bad actors" både externa och interna till lärosätet
-

Imorgon?

4- Arkitektur

Var

- Core
 - Potentiellt även datacenter
 - Molnlösningar
-

Hur

- Beror på lärosätet
 - Avgör vilka nät som behöver brandväggsskydd
 - Avgör vilka nät som *inte* behöver brandväggsskydd
 - Styr trafiken
-

Tekniska Krav

- Full routing
 - Länkaggregering
 - API tillgängligt
 - Larm skall kunna skickas till andra system
 - Möjlighet att använda flera olika, och "bespoke" källor för *vem* som använder en viss enhet
-

5- Produkter?

Vi har medvetet valt att inte överväga enskilda produkter, då vi tycker det viktigaste är att kunna ha ett underlag för att verkligen kunna utvärdera leverantörers produktförslag och hur de skall passa in nu och i framtiden.

Vad händer sen

Vad händer sen

- Har vi missat något?
- Inbjudan till marknaden att ge lösningsförslag baserat på slutrapporten
- Sammanfattning av leverantörsförslag i ett Appendix