Säkerhetsarbete

På

IT-avdelningen

Karlstads universitet

Vem är jag

Nicklas Lundqvist, 48 år, 2 barn (3 och 6 år) och sambo

Jobbar på IT-avdelningen som är indelad i följande 5 team:

Användarstöd, **Nätverk & säkerhet**, Systemapplikationer, Datacenter, AV(Audio Video)

Mina drygt 20 år på Karlstads universitet

- Läser till Systemvetare på Karlstads universitet 1995-1998
- 1998 projektassistent i Arkivet, fotodatabas och uppsatsdatabas och arkivering
- 1999-2006 IT-samordnare Institutionen för ekonomi, idag Handelshögskolan, allt utom nätverk
- 2006 IT-service alla tekniker dras in till en central enhet, Nätverk & säkerhet, IRT

- SUNET/TREFpunkt historien börjar i Kalmar 2006, var projektledare för införandet av eduroam inför förra sunetdagarna på KAU.
- IT-avdelningen, nytt namn ny chef, IRT
- Kuriosa: Är uppväxt i samma kvarter i Karlskoga som Gunnar Lindberg på Chalmers

Hösten 2017 mera fokus på säkerhetsarbetet då Göran Bolander går i pension

Fördelningen av min tid: 25% nätverk, **50% säkerhet, 25% Telefoni**

Vad skall säkras, hur gör man det på en halvtid med en begränsad budget?

- Ca 250 servrar av olika operativsystem windows, linux, MAC, backup mm.
- 350 accesspunkter med ca 11 000 unika enheter/vecka
- 132 switchar
- Klienter managerade PC: ca 1600
- Klienter managerade MAC: ca 420
- Klienter som sköter sin dator själv ?
- Mobiler: ca 300 IP-telefoner: 260
- Managerade printrar: 84 stora 25 små + egeninköpta
- AV utrustning, projektorer, digitala anslagstavlor osv.
- Internet Of Things som vi bara sett början på.

Hur gör vi för att maxa säkerheten? vi behöver ha...

- AI
- Next generation firewall
- Visibility
- Antimalware
- Tvåfaktor autenticering
- Skanna efter sårbarheter
- Separera dina roller
- Patcha automatiskt om möjligt
- Vitlista programvaror
- Mailkontroll, hur vet vi vem som loggar in och vartifrån

Grundsäkerhet/lägsta nivå

- Vi måste försöka förutse de mer generella behoven
- Anpassa behovet av säkerhet där det behövs, högsta säkerhet är kanske inte optimalt alltid.
- Hur gör vi med lånemaskiner osv. som ligger i förråd till någon behöver den? Hur får vi bort gamla maskiner som ingen ”äger”

Lagom med frihet

- Sen måste det så klart finnas en viss del av frihet, att göra lite ”hur man vill” inom ramen vi skapar, för hela iden med forskning och utveckling bygger ju på att man testar något som ingen annan gjort tidigare och att man vågar göra annorlunda. Då måste ju vi finnas där för verksamheten och ta fram dom bästa lösningarna för att på ett säkert sätt bidra till detta.
- Gör vi inte det så hittar man andra vägar att lösa detta då har vi ingen aning om vad dom gör.

Hur uppnår vi det här då?

- Samarbete över teamgränserna
- Snabba enkla kommunikationsvägar
- Utbilda all personal i vikten av säkerhet
- Mallar, klara ansvarsområden och inarbetade rutiner för IRT,

Hur uppnår vi det här då?

- Visibilitet
- Nätverka
- Tvåfaktors autenticering
- SUNET externskanning + andra
- Upphandling

På gång närmaste tiden

- Test av visibilitetsprogramvara, Netflow test klart innan sommaren, nästa på tur Stealthwatch?
- Utveckla IRT webben och utbilda personalen
- Next generation firewall, vad vill vi skydda vad skall vi ha, invänta SUNET?
- Arbetaklart IRT mallarna och bestämma arbetssätt för IRT
- Ny VPN
- IPV6
- Fortsatta tester av ny funktionalitet i Unomaly, frekvens osv.
- Tvåfaktorsautenticering