HÖGSKOLAN I SKÖVDE

HUR LÖSER VI ”CIRCLE OF TRUST”

Marcus Nohlberg, Ph.D/MBA
Högskolan i Skövde

IDAG BERÖR VI…

- Aktuellt inom informationssäkerhet + trender
- Praktiska erfarenheter från utveckling map säkerhetskrav + lagar
- Circle of trust – vad som kan göras

ÖKADE KRAV FRÅN SAMHÄLLET?

Digitaliserat samhälle

- Sverige ska vara världsledande i användningen av digitala tjänster (SOU 2016:89)
- Medborgaren
- Näringsliv
- Offentlig sektor

Ökat hot och bristande skydd

- Informationssäkerhetsutredningen (SOU 2015:23)
- Riksrevisionens rapport 2016:8

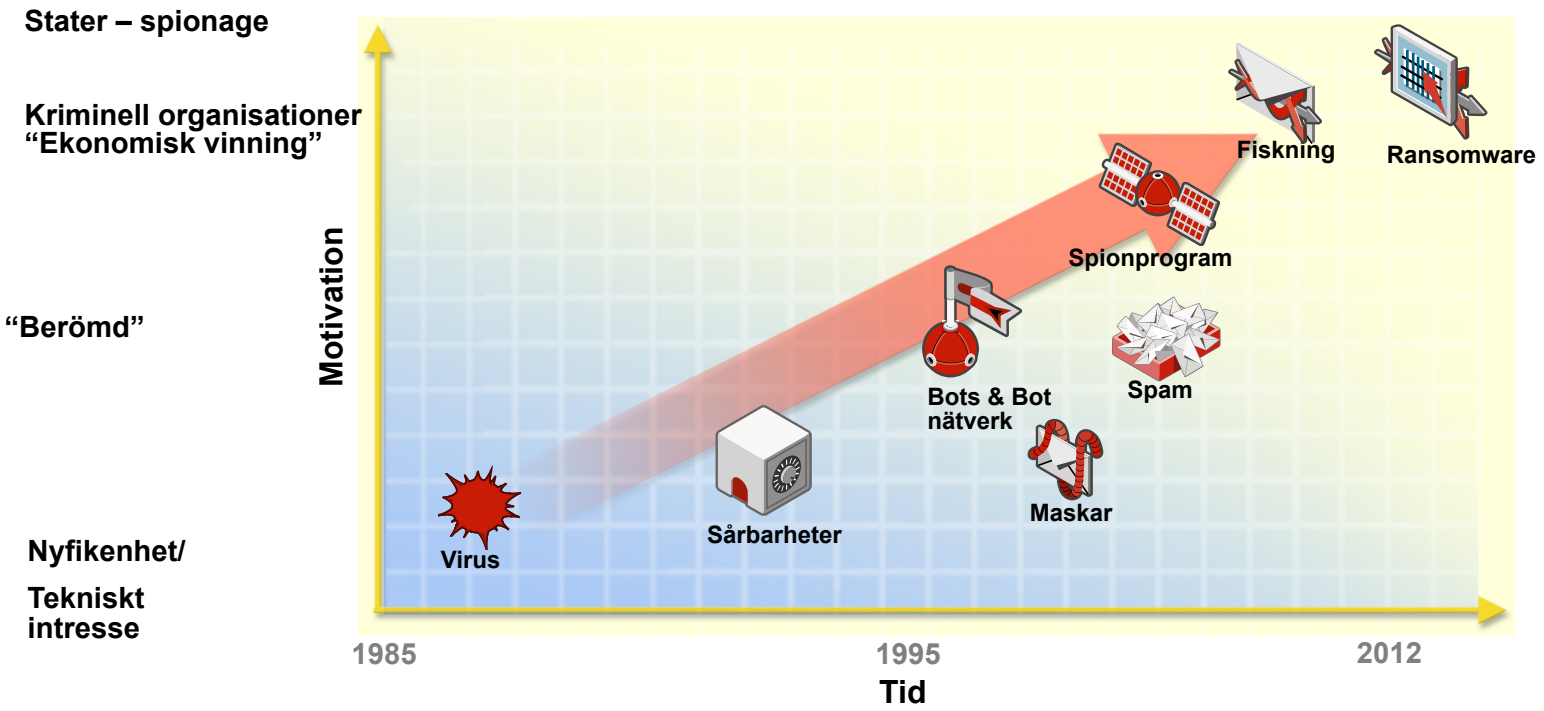
Nya lagar och regelverk

- Dataskyddsförordning GDPR (EU 2016/679)
- EU-direktiv om säkerhet i nätverk och informationssystem (EU 2016:29)

Behov av ökad samverkan kring utbildning och forskning

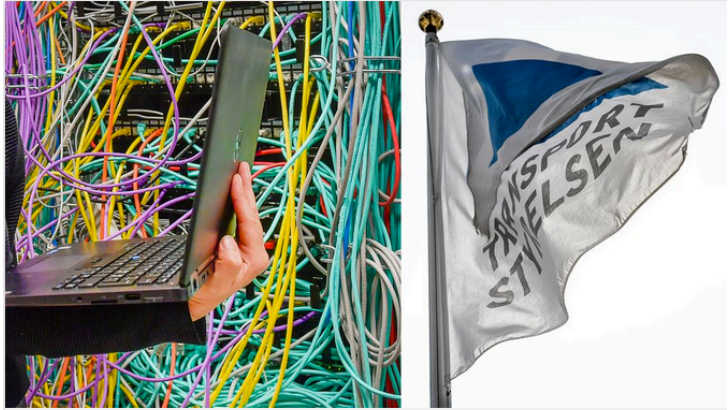
- Kompetensbrist
- Ny teknikutveckling ökar komplexiteten

HOTBILDEN FÖRÄNDRAS



2016

Swift-hacket mot centralbanken i Bangladesh, där förövaren kom över 81 miljoner dollar



Transportstyrelsen och IBM tvingades göra om hela upplägget så att IBM nu sköter IT-driften från Sverige i stället – och Transportstyrelsen tvingas betala kalaset. FOTO: TT

Transportstyrelsens IT-nota har ökat med 190 miljoner efter skandalen

Transportstyrelsen tvingas betala 190 miljoner kronor extra för IBM:s IT-drift nu när man uppfyller säkerhetskraven och använder IT-tekniker i Sverige i stället för i utlandet.

Det var för att spara pengar som Transportstyrelsen fattade beslut om att lägga ut IT-driften på ett externt företag. Man räknade med att sänka sina kostnader med 100 miljoner kronor om året.

I april 2015 gick uppdraget till IBM, som skulle ta 400 miljoner kronor för IT-driften under åren 2016 till 2020.

Ledde till hot mot rikets säkerhet

Avtalet byggde på att billiga IT-tekniker i bland annat Tjeckien och Serbien skulle sköta driften, men dessa gick inte att säkerhetspröva under den korta tid man hade på sig, visade det sig.

SVT 2017-04-05

Stor internationell cyberattack avslöjad – Sverige drabbat

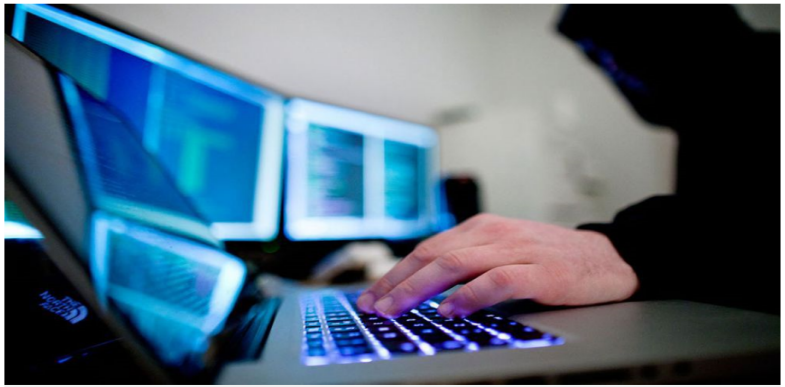


Foto: TT

Ett omfattande internationellt cyberangrepp som fått namnet ”Cloud Hopper” har avslöjats, uppger Myndigheten för Samhällsskydd och beredskap MSB i ett pressmeddelande. Enligt en källa till SVT Nyheter har flera svenska företag och organisationer hackats.

Angreppen ska i första hand ha riktats mot företag som sköter it-tjänster åt andra – men även mot deras kunder. Angreppet, som döpts till ”Cloud Hopper” men av

MSB:
Ett omfattande internationellt cyberangrepp har avslöjats. Cyberangreppet har fått beteckningen ”Cloud Hopper” och aktörens beteckning är ”APT10”.

Cyberangreppen har i ett första steg riktats mot företag som sköter it-tjänster åt andra, och därefter vidare mot deras kunder. Cyberangreppet har pågått sedan åtminstone 2016, men påbörjades troligen redan under 2014.

Så gick angreppen till

APT10 har inriktat sig på att infektera system genom att lura människor. De som ligger bakom angreppen har lagt stora resurser på att kartlägga sina mål, organisationer och deras anställda, för att kunna skicka riktade e-postmeddelanden med trovärdiga dokument (så kallat riktat nätfiske, spearphishing).

Metoden går ut på att förmå mottagaren att öppna dokument och därmed omedvetet starta skadlig programkod som ligger dold.

DAGENS NYHETER.

Ekonomi

Utredningens expert: Dataintrången skulle kunna ha förhindrats

Uppdaterad 2017-09-18 Publicerad 2017-09-18

Gekås i Ullared och Swedbank är två av de företag som drabbats. Foto: Foto: TT

Tiotals miljoner kronor tros ha stulits i en jättehärva av dataintrång och bedrägerier. Men mycket tyder på att attackerna hade kunnat stoppas – enkla medel hade räckt, enligt en av experterna i utredningen. Bland de drabbade finns bland annat Swedbank, Kriminalvården och Gekås i Ullared.

På måndagen väcktes åtal i en mångmiljonhärva med grova dataintrång. Med hjälp av virusliknande program och falska e-postadresser har en liga lyckats lura till sig stora belopp. Åtta personer står åtalade i vad som har beskrivits som ett av de största dataintrången i Sverige någonsin.

Sköterska polisanmäls

SKARABORG: Läste patientjournal utan att vara behörig

Inspektionen för vård och omsorg, vill att en sjuksköterska på Skaraborgs sjukhus ska åtalas för dataintrång. Hon läste en patientjournal utan att vara behörig.

Sjuksköterskan gick, tillsammans med en kollega, in och läste i en kvinnas patientjournal. Den drabbade kvinnan skrev i anmälan att dataintrånget bland annat gjordes av hennes makes exfru, vilket gjorde ärendet extra känsligt.

Ärendet anmäldes till Ivo. Myndigheten tog beslut om att granska hur Skas agerat. När intrånget utreddes fick den legitimerade sjuksköterskan en varning. Två andra medarbetare lämnade förklaringar om deras inblandning och ärendet avslutades för deras del. Ivo nöjer sig med hur Skas agerat, det finns tveksamheter men myndigheten avslutar ärendet.

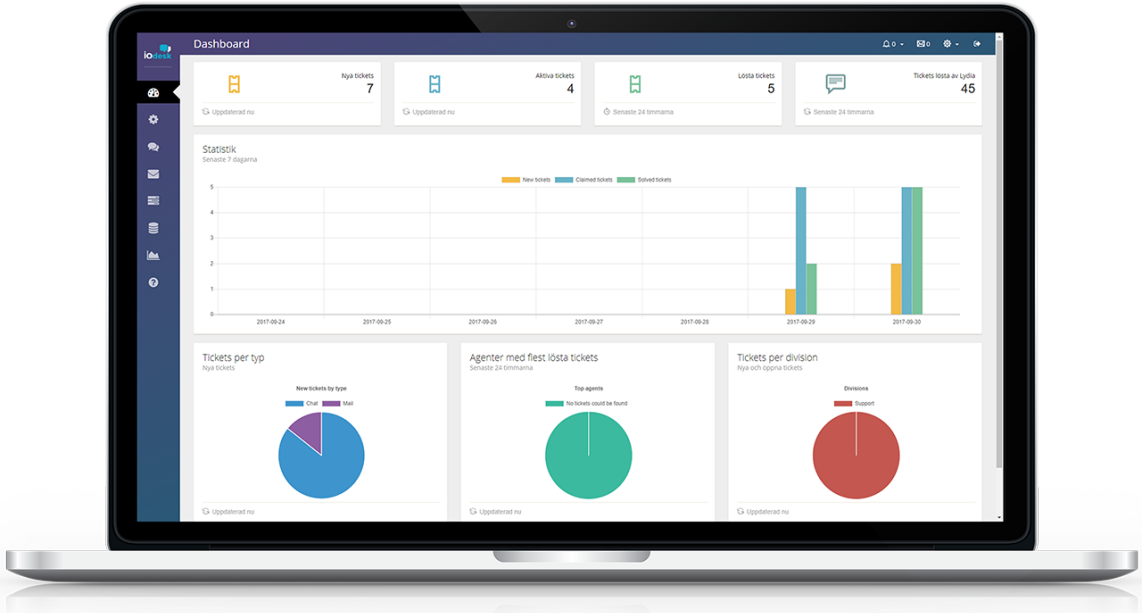
Ivo vill dock att sjuksköterskan ska åtalas för dataintrång och har lämnat in en åtalsanmälan.

LÄGESBESKRIVNING?

Så vad gör vi?

ERFARENHETER FRÅN PRAKTISKT KRAVSTÄLLDANDE OCH UTVECKLING

www.iodesk.net



UTMANINGAR VID MJUKVARUUTVECKLING

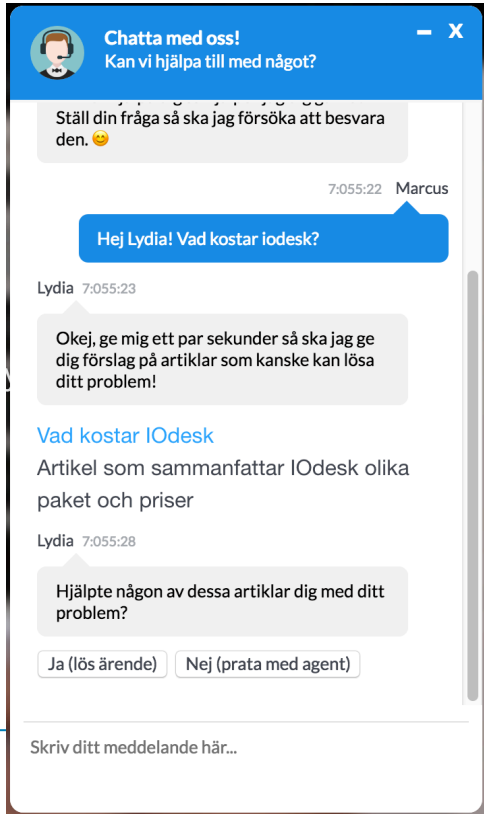
- Internationell mjukvara – vilka krav ska följas?
- Hur säker ska den vara?
- Vad innebär de lagar som finns i praktiken när mjukvara ska utvecklas?
- Vad kan vi ha för strategier – vad gör vi med information vi samlar in?
- …och hur tänka som informationssäkerhets-forskare när man ska delta i praktisk systemutveckling av kommersiell produkt?

VÅRA DESIGNVAL

- Bygg allt till max från början! (*Turn it up to eleven!*)
- Samla ingen ”nice to have” information alls (undvik facebooksjukan)
- Bygg framförallt kring att stödja **rätt att glömma** – ger struktur kring utvecklingen och gör det lätt att lätta på andra krav
- Använd standardiserad tekniska skydd och lagra data där den behövs (mellan länder)

OCH RESULTATET…

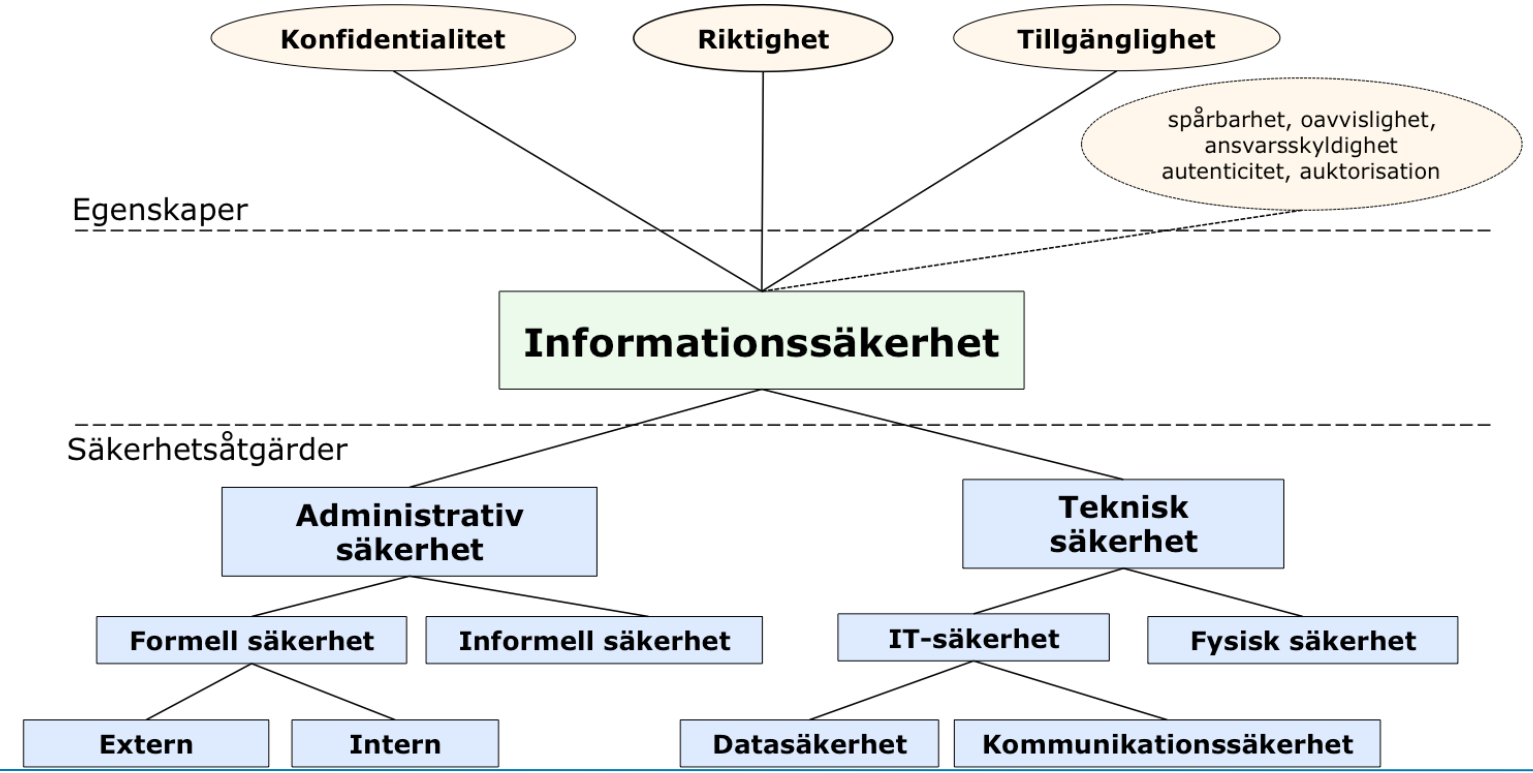
- Lagändringar påverkar marginellt
- Diverse nya hot påverkar egentligen inte kärnfunktioner, flera lager med skydd (KRACK)
- Enorm fördel att börja från början! Otroligt mycket svårare att ändra befintliga lösningar
- Också klar från början för nya domäner – oerhört svårt ändra lösningar till nya kunder längre fram
- ”Marknaden” marginellt intresserad av att mjukvaran följer lagar (det är intressant att se hur lite intresse laglydighet väcker)



Vilka verktyg finns?

INFORMATIONSSÄKERHETSMODELLEN

HÖGSKOLAN I SKÖVDE



VARFÖR ARBETA SYSTEMATISKT MED INFORMATIONSSÄKERHET?

HÖGSKOLAN I SKÖVDE

- Ger förutsättningar att öka kvaliteten i verksamheten - ordning och reda, ansvarsfördelning, förbättringsarbete
- Ledningen får ett verktyg för att följa och kontrollera nivån på informationssäkerhet i organisationen
- Verksamheten får riktlinjer och instruktioner som gör det lättare att bevara och höja säkerheten
- Underlättar utbytet av digital information och data mellan samhällsaktörer
- Säkerhetsmedveten ökar i hela organisationen
- Underlättar införande av nya digitala tjänster

INFORMATIONSSÄKERHETSPROGRAM 2020

HÖGSKOLAN I SKÖVDE

Mål och syfte:

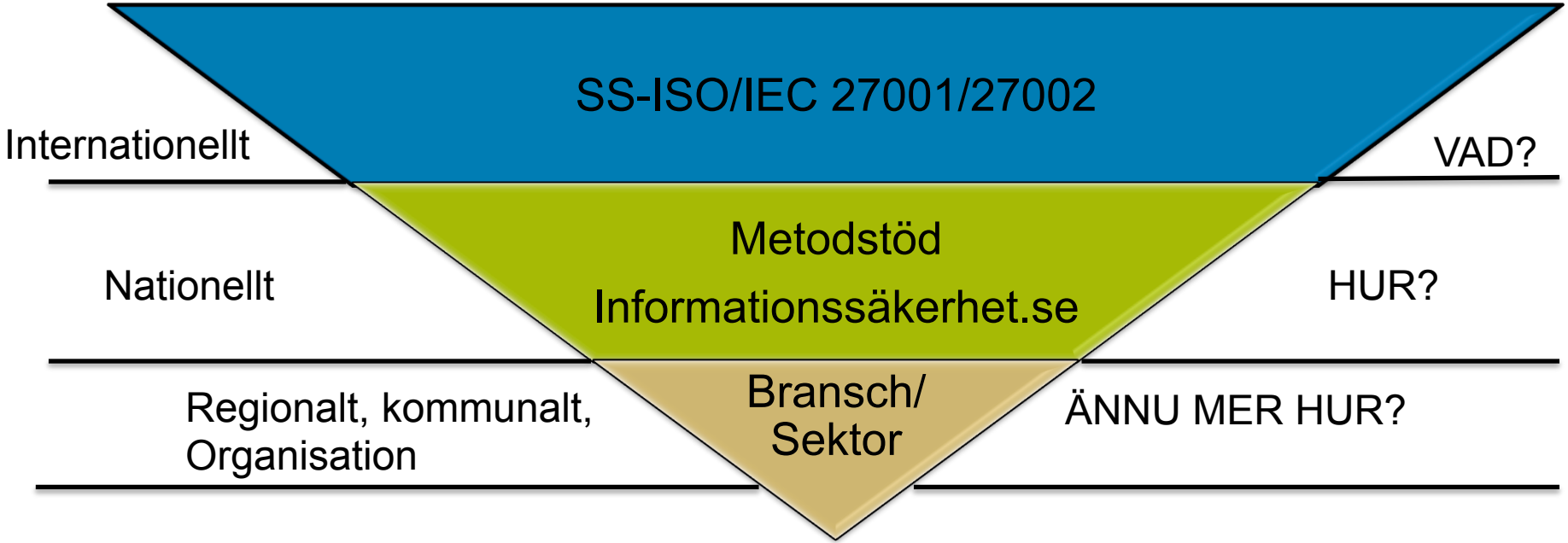
- **Införande av ledningssystem för informationssäkerhet i kommunen**
- **Öka förutsättningarna för digitalt samarbete i Västra Götaland**
- **Öka tilliten till offentlig sektor**

1. Informationsinsatser och förankring
2. Nuläge, risk- och Gapanalys
3. Utbildning av Informationssäkerhetssamordnare och personal
4. Informationsklassificering
5. Införande av ledningssystem för informationssäkerhet (LIS)
6. Tillgängliggöra öppna data

UPPDRAGSUTBILDNING

- Uppdragsutbildning i införande av ledningssystem för informationssäkerhet som ger högskolepoäng (7,5 hp)
- Samarbete mellan HiS, VGR (Digitaliseringsrådet)
- Ingår som en del i Informationssäkerhetsprogrammet 2020.
- Tilltänkt målgrupp: Informationssäkehetssamordnare i Västra Götalands kommuner

HUR IMPLEMENTERA?



CIRCLE OF TRUST

Säkerhet är ingen extra pålaga

Säkerhet är en normal del av verksamheten

HÖGSKOLAN I SKÖVDE

Frågor?

marcus@nohlberg.com
www.siguru.se