Om IT-Säkerhet

SFK-årsmöte 2016-04-05

Frank Schliephacke
(mobil 070-4675434)

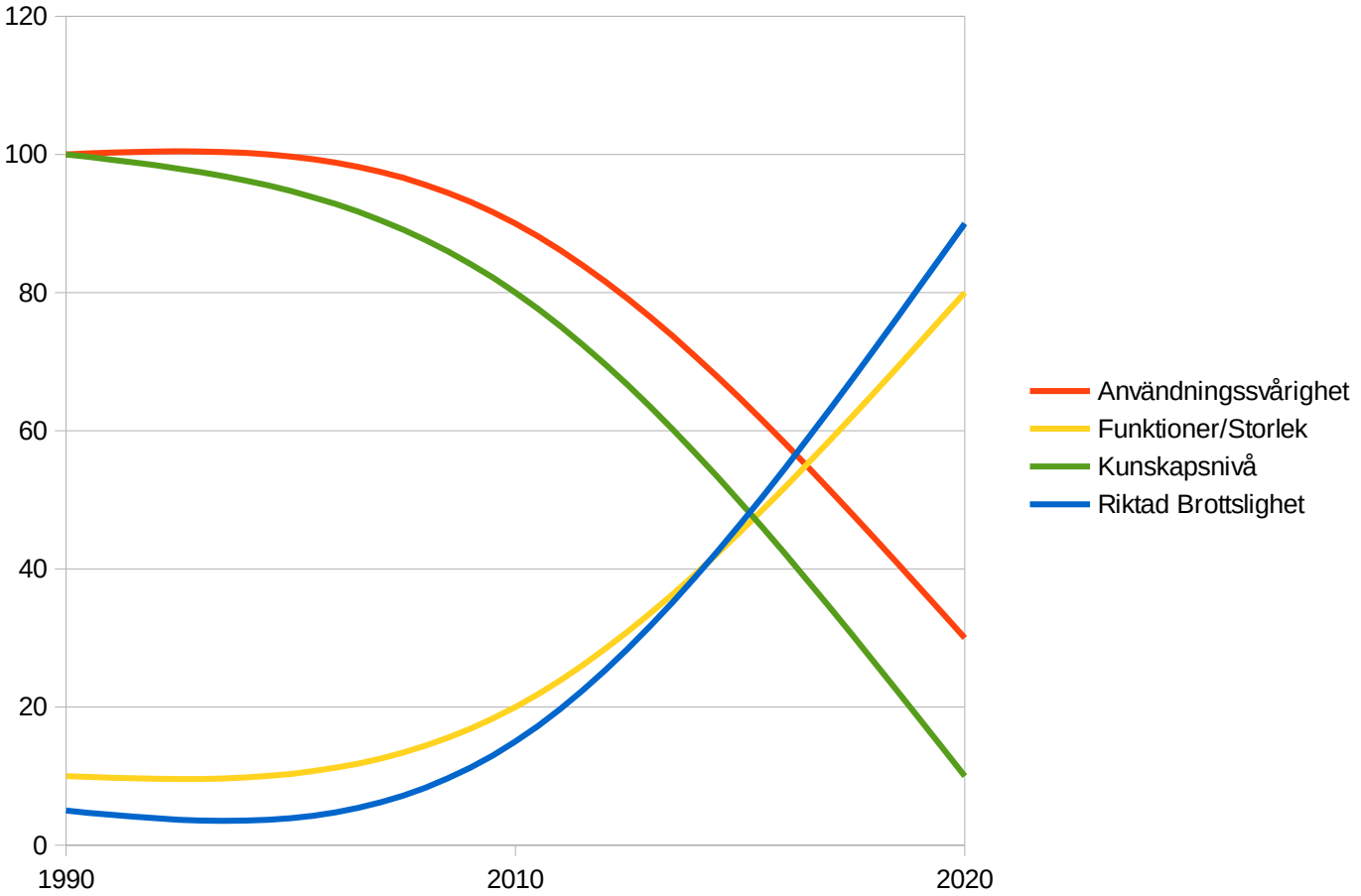
Ver. 3

Från Säkerhet till datorsäkerhet till informationssäkerhet

SÄKERHET baserad på Maslows behovstrappa

Maslow	**Säkerhet**	**IT-säkerhet**
Sälvförverkligande	Yrkesval-prova nytt	Bloggare, Youtubare
Uppskattning	Arbetskamerater	FB,Google+,Linkedin
Kärlek/Gemenskap	Familj,Förening	FB,Google+,Linkedin
Trygghet	Frihet, Rättsstat	BankID, Email
Mat, Kläder, Bostad	Öppet demokratiskt samhälle => transparent Socialt skyddsnät	Fri internet tillgång, EJ övervakad

Varför IT-Angreppen har ökad



Vad är vi rädd för ?

Hotbild - Risker

Vad är man rädd för ?
Data - Konfidentialitet, Riktighet och Tillgänglighet
Stöld
Förvanskning
Förstörelse

Hotbild
Anställda gör fel
Personliga intressen – hämnd, förtala en kollega
For Fun - slumpmässigt utvald inga djupa syften
Kommersiella intressen - data stöld, förstörelse, förvanskning.
Kriminella - hot, utpressning

Hot/risker hittas genom riskanalys

Företag	**Angreppspunkt**	**Teknik**
Anställda	Ekonomi	Utpressning,Stöld,Muta
Ekonomi	Ekonomisystem	Förvanskning,Radering,Stöld
Teknik	CAD	Förvanskning,Radering,Stöld
Tillverkning	Produktionsplanering	Förvanskning,Radering
Produktkvalitet	Tekniska underlag,CAE	Förvanskning
Produktfunktion	Tekniska underlag,CAE	Förvanskning
Knowhow	Tekniska underlag,CAE,CAD	Radering,Stöld
Goodwill	Kunder	Förtal/Sociala medier
Varumärke	Kunder	Förtal/Sociala medier
Lokaler	Dörrar,Fönster	Inbrott,Stöld

Angreppspunkter – Privat personer

Hemma	**Angreppspunkt**	**Teknik**
Bostad	Dörrar,Fönster	Inbrott,Stöld
Personer	Identitet	Lösenord stöld,Cracking
Ekonomi	Bank,Bil,Boendet	Pinkod,Koder,RiktadAvlysning
Bostad	Nätverk,Botnet,Malware	Avlysning,obehörig Användning
Individuell Egenskap	Mobiltelefon,Social a Medier,Email	Lösenord stöld,Cracking

Exempel - kända cyberangrepp

Stuxnet – riktad angrepp på iransk kärnanrikning
Bil – övertar styrning, bromsning i en bil
Elkraftnät – Dec2015, delar av ukrainsk elkraftnät stängs ned.
Ransomware – via email, krypterar hd, kräver betalning för avkryptering
Mobilt BankID – (obehörig) inloggning efter telefonsamtal, inloggningsförsök.

Data den nya hårdvalutan

Rörelsedata – geografisk, fysisk
=> IOS, WIN10
Sociala medier: interessen, åsikter, kunskaper
Webtjänster: personliga preferenser, intressen, läggning
=> YouTube, Facebook, etc.

DATA används för individanpassning av t.ex. erbjudanden, reklam, försäkringar, lån, etc.
=> data-innehållet som används kan inte påverkas av individen!
=> när övergår välmenande dataprocessering till besvärande för individen ? (Nätet glömmer ingenting !)

Riskanalys

Förstå hot och risker
Öka medvetande
Aktiva försvars åtgärder

Cyberangrepp – Var redo

Riskanalys - var är vi idag, var vill vi vara om 1 år.
=> Risk identifiering och värdering baserad på scenarier.
(Se även ISO 27001, 27002, ...)

Medvetande och beredskap

Vad gör vi om något händer ?
Drar ut elkontakten
Ta hjälp utifrån ?
Lider och ber
=>IRP (Incident respons plan - handlingsplan)

Ökad IT-säkerhet

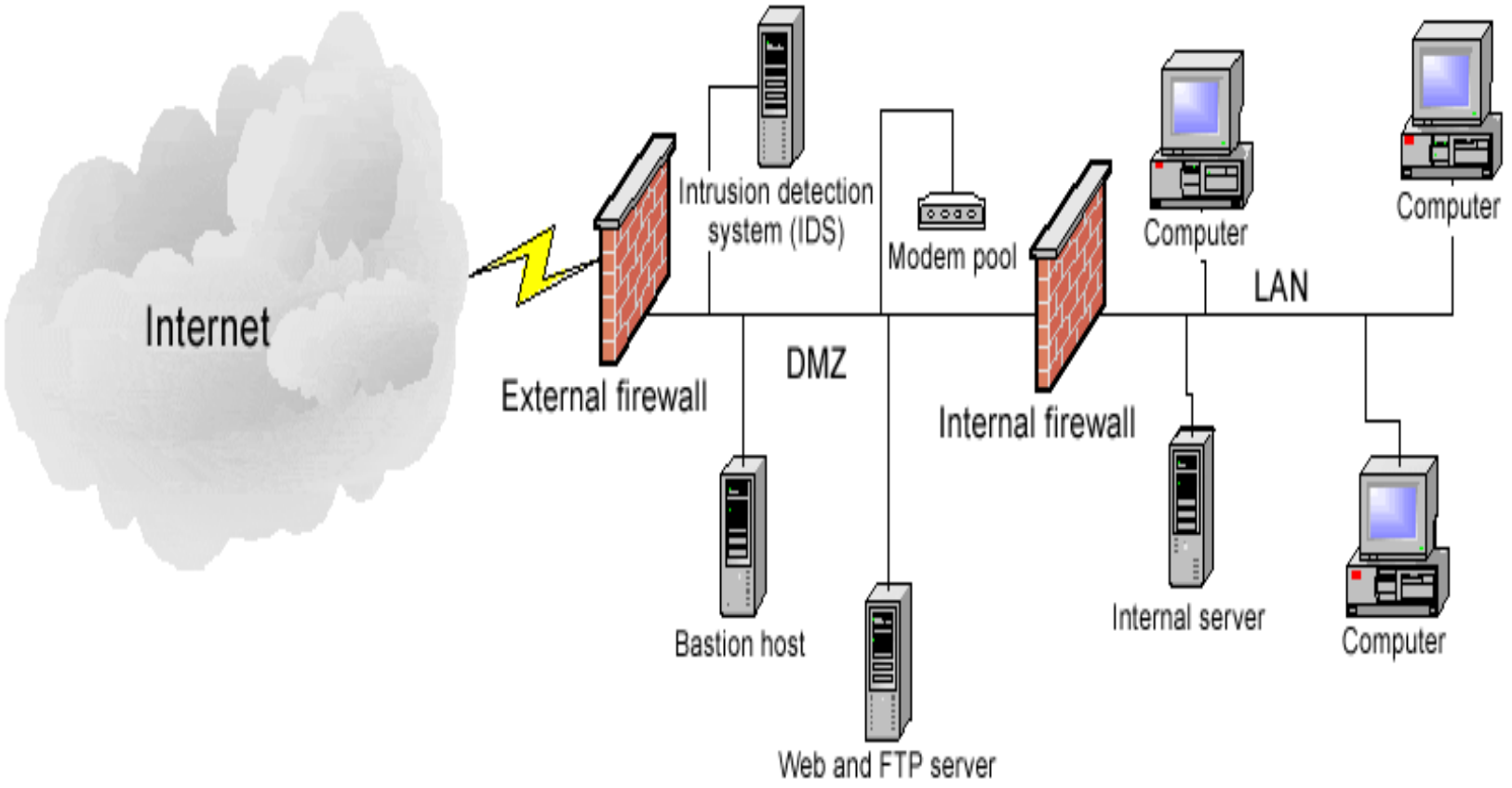
Medvetenhet
Segmenterade nätverk med flera skal, anpassad mot behovet av säkerhet.

Cyberangrepp - åtgärder

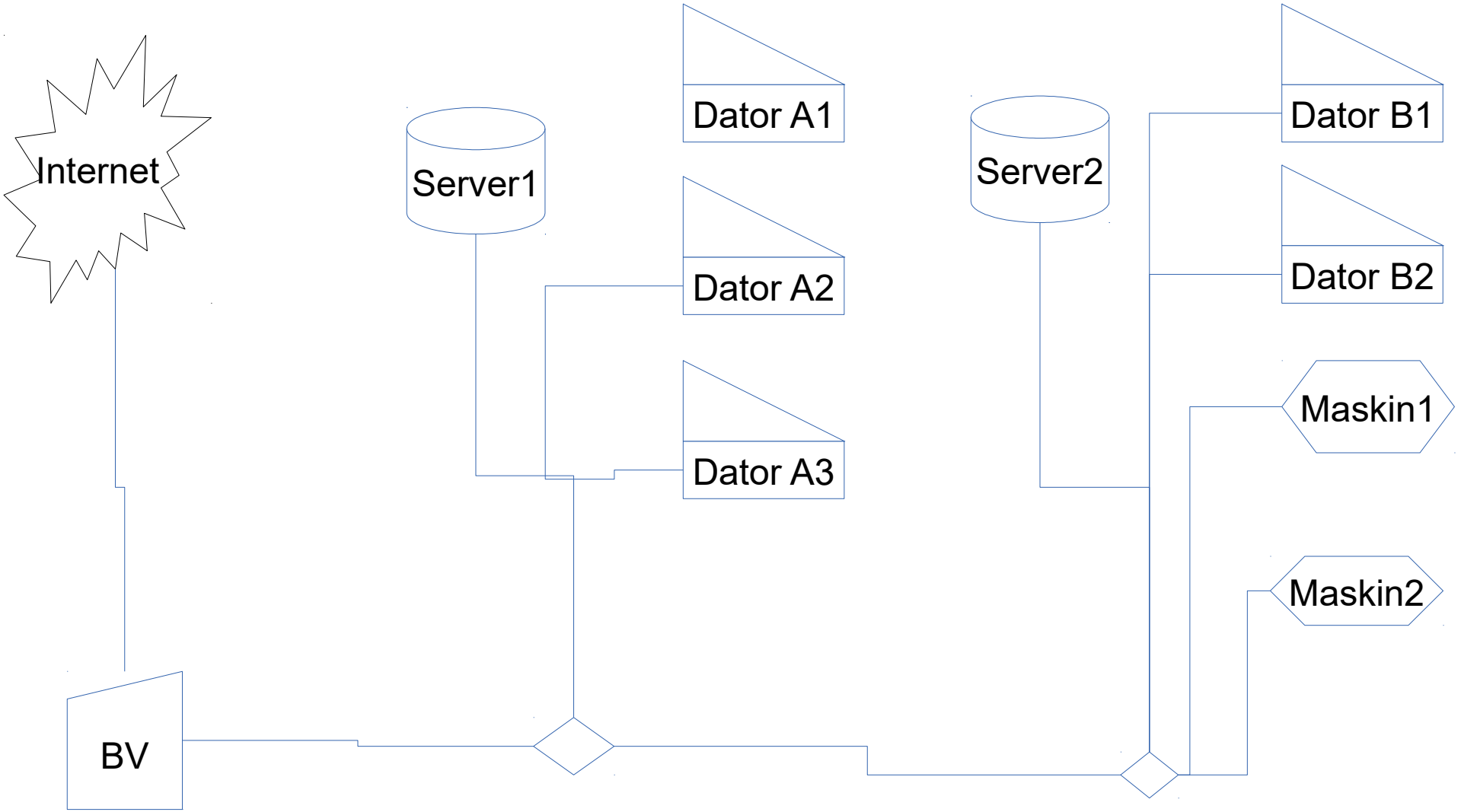
Var redo !(Antag intrång)
=> IRP – åtgärds/handlingsplan
Backup dag, vecka, månad
Backup i molnet - juridiska aspekter
Reservdatorer
Reservdelar & downtime
Testfall för viktiga applikationer

Moderna säkerhetslösningar
Brandvägg
AntiVirus/malware
White listing
Nätverk: skal indelad, segmenterad
Intrusion detection
Kryptera hd, filer
Password safe – krav på lösenord ?!
Skärmskydd mot insyn
Vattenmärkning
Kontrollsummor - checksum
Nätverkstrafikövervakning
Honeypot
Life beep
Applikationstatusövervakning => beteende mönster

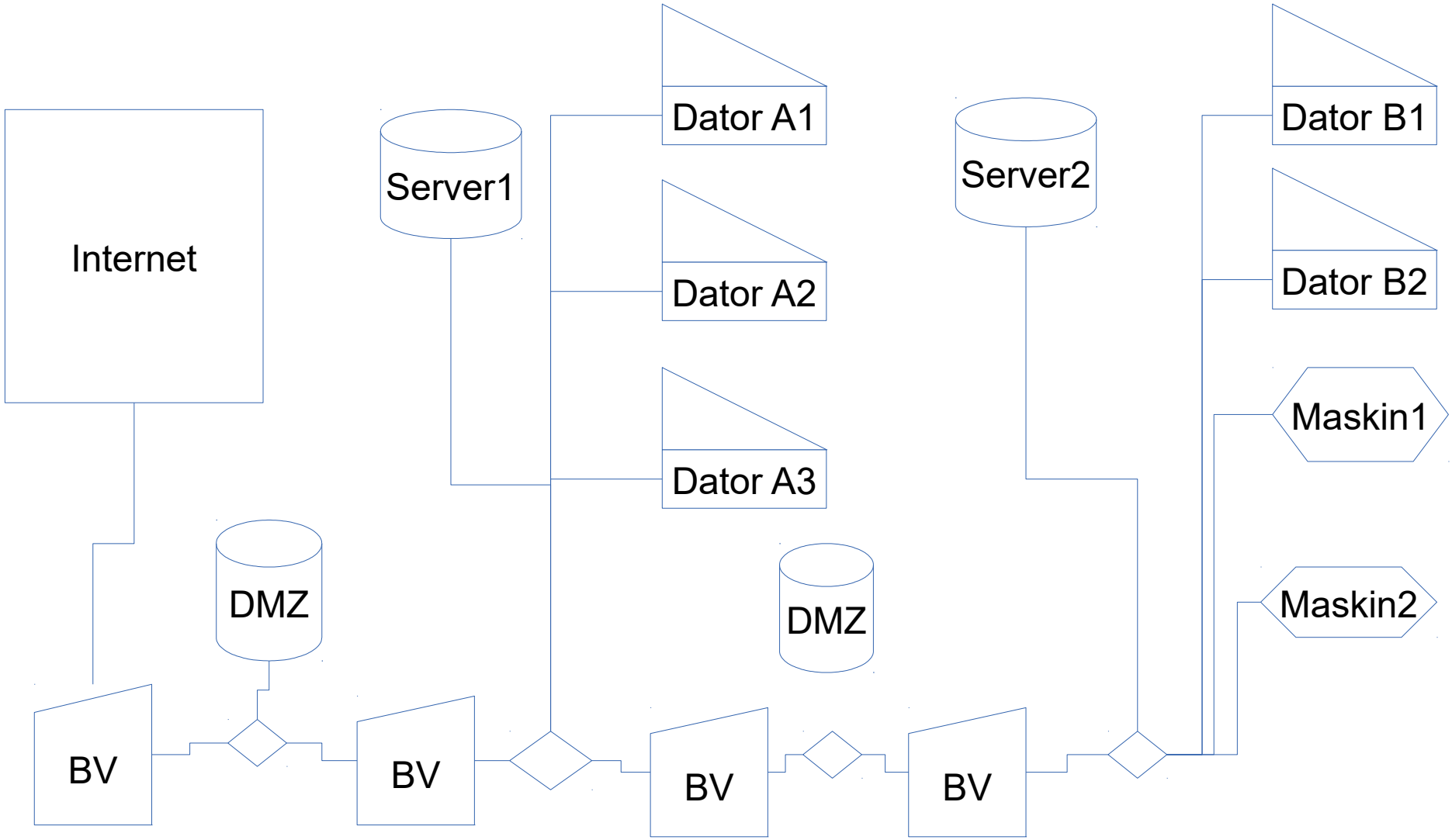
Nätverk - DMZ


Internet
External firewall
Intrusion detection system (IDS)
Modem pool
DMZ
Bastion host
Web and FTP server
Internal firewall
Computer
Computer
LAN
Internal server
Computer

Nätverk – Vanligt



Nätverk – nivåindelad / segmenterad



Finns mycket information på nätet
MSB publikationer
t.ex. ”Vägledning till ökad säkerhet i industriella informations och styrsystem”
Cyberangrepp status Nationellt, Internationellt
=> cert.se
Kommande krav på incendent rapportering !

IoT - Internet of Things

Små och stora datorenheter som styr och mäter
Visionen är att alla IoT-enheter skall prata med varandra
Idag VT2016 fortfarande mycket förändring i tekniken och hårdvaran

=>

A. IoT enheter för privatpersoner/individer – livslängd ca. 5 år.
B. IoT enheter i industriell användning – livslängd ca. 10-15 år

Individuell IoT

Mät och övervaka hur människor använder resp. IoT-enhet; Bil, Mobiltelefon, Joggingskor
Teknikdriven utveckling av hårdvara och mjukvara; nya behov skapas
Kräver oftast permanent uppkoppling mot internet och ett datamoln.
Stark teknikutveckling: många standarder kan tillämpas på t.ex. trådlös kommunikation
Teknisk funktionalitet framför IT-säkerhet – ändring pågår VT2016

Typisk enkelriktad dataflöde från sensor till molnet och applikationen.

Individuell IoT – problem områden

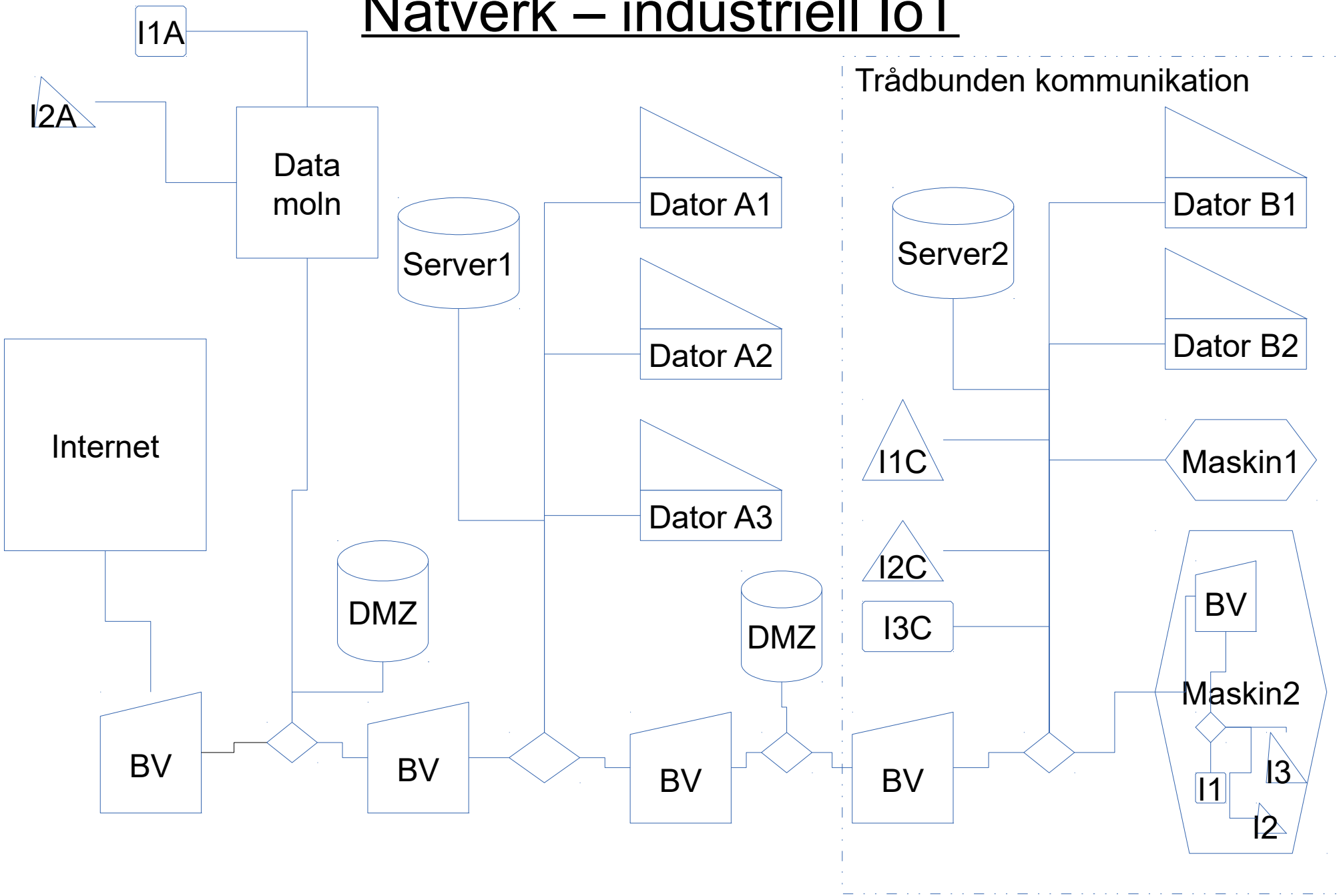
Vem äger data ?
Vems ansvar att håller data säker ?
Stark teknikutveckling – fokus på funktion framför säkerhet
IT-säkerhet beror på om och hur den har implementerats: kryptering, kommunikationssätt, hantering, lagring, etc. => IT-säkerhetsriskanalys skall ingå i leveransdokumentationen.
Hur kan förvanskad eller inget dataflöde påverka funktionen resp. användningen av IoT-enheten ?
Felsäkerhet ?

Industriell IoT

IoT-enheter d.v.s. styr och mätdatorer finns oftast på maskinutrustningsnivå t.ex. PLC, motorstyrning, rfid
IoT på sensor nivå håller på att komma till marknaden; ethernet, bluetooth
Oklart mervärde i att ”allt” är uppkopplad
=> produkt/tillverkningsberoende
Industri 4.0 – industrialiserad IoT: än så länge få bra affärstillämpningar som kan vinst räknas
Datasystemleverantörer t.ex. SAP, Microsoft jobbar hård på tillämpningar resp. tillämpningsstöd för industri4.0/IoT.

Typisk dubbelriktad dataflöde då man utför mätning och styrning

Nätverk – industriell IoT



Industriell IoT – problem områden

Livslängd min. 10 år, oftast längre

MS Windows centrerade utvecklingsverktyg
MS Windows baserade styr och kommunikations teknik t.ex. OPC
=> Versions låsning – Version Windows mot version-utvecklingsverktyg

Hur länge lever en utrustning hur länge finns Windows, drivrutiner

Kompetens för utveckling är inte samma som för underhåll/användning
=> Kunskapsgap utvecklare/underhålls personal => Konsultberoende

Dokumenterade arbetssätt, hur installerar man, hur ändra man Hw/sw?

Industriella MS Windows tillämpningar kan inte per automatik säkras på samma sätt som en kontors-PC, pga. Prestandard/realtidskrav.

Trådlösa IoT-enheter angrips - inträngningspunkt mot nätverk

Vad händer ifall kommunikationen fallera => stannar tillverkningen

=> Kompetens och kunkapsgap. Utvecklare förstår inte nödvändingtvis behovet.

Kravställning bör vara multi-disciplinär vilket inte är nödvändigtvis tillämpad arbetsmetodik i industrin idag.

Kunskaps och arbetsprocess problem; Ansvar, befogenheter, kompetens => dataavdelningen kontra maskinutrustningstillverkare / underhålls-automations kompetensen i en fabrik.

Utrustningar äldre än 5 år (tillverkad före 2010) har oftast ingen IT-säkerhet inbyggd

IOT cybersäkerhet - förbättringspotential

- Unik ID per IOT-enhet
- Endast krypterad kommunikation – två faktor

  => potential i t.ex. blockchain teknologi
- Skilj på enkel och dubbelriktade dataflöden och deras risker
- Specialiserade kommunikationssätt för högsta säkerhet (Ej Ethernet och TCP/IP) – Ej universellt utan specifikt för tillämpningen.
- Använd och släng bättre än uppdatera

  => modul byggda IOT-enheter
- Utveckling i multidisciplin team inkl. användare, underhållspersonal
- Självdiagnosticerande IOT-enheter

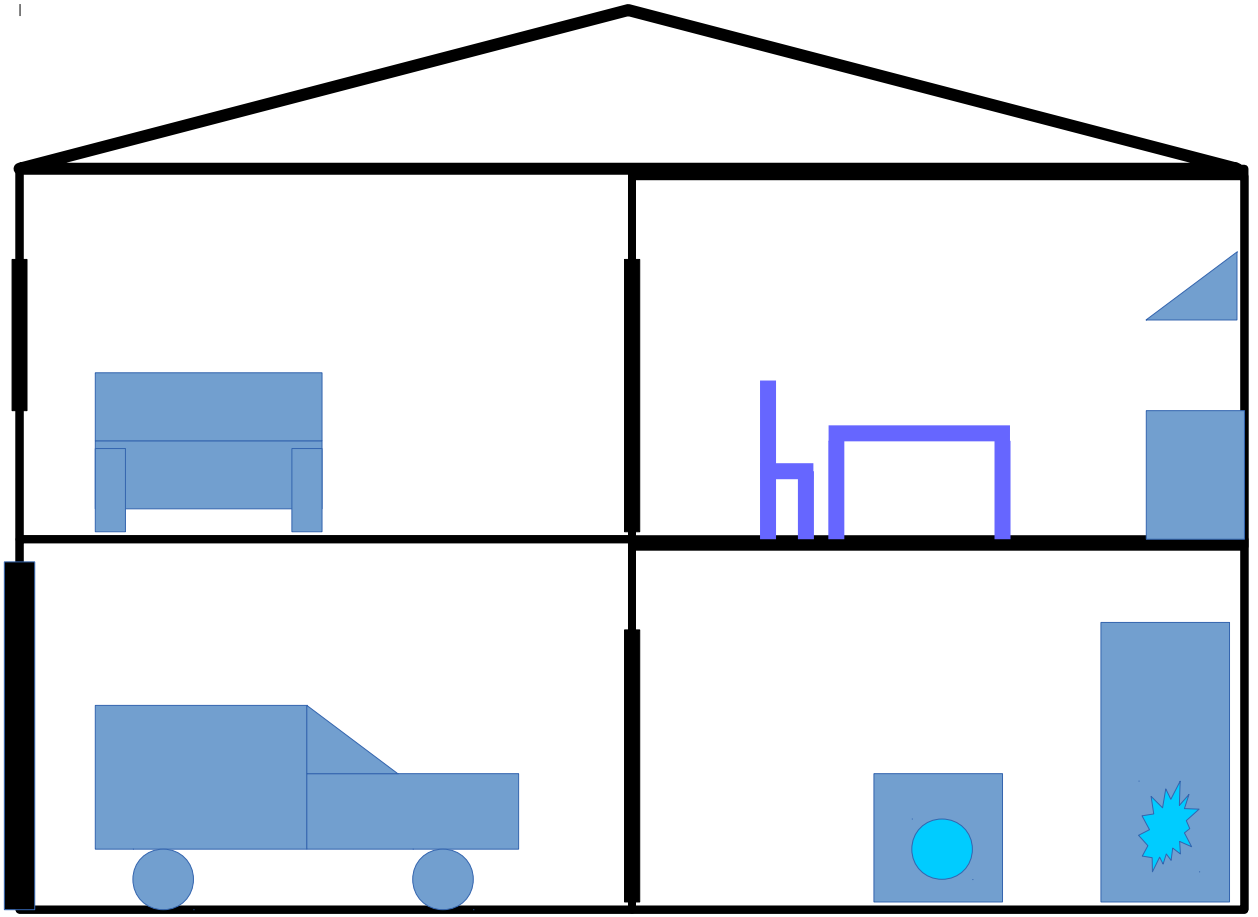
IoT referensmodel

- Enkelt att förstå
- Beskriver problem korrekt
- Flexibelt och expanderbart
- Alla tala samma ”språk” - enhetlig modelansats

=> Riskanalyser, Beräkningsmodeller, etc.

IoT referensmodel

- Du och ditt hem – Villa, lägenhet



Cyberangrepp – fiktiva exempel

1.Firmans tillverkningsbokning förvanskas vilket ger felaktiga produkter som inte lever upp till kundens förväntningar. Ändra 3% i data underlaget för tillverkning och produktionsplanering så att dålig fungerande produkter levereras vid felaktig tidpunkt.
=>Många klagomål, svårt att identifiera.
=>Dålig rykte, höga kostnader pga producentansvar.

Personalen är inhyrd
=>Man följer det som står i order/tillverkningssystemet, man kommer inte kunna se små orimliga förändringar i tillverkningsordern.

2.Angrepp på utrustning
I syfte att påverka tillverkningsutrustningarnas funktion för at kunna kräva pengar.
Överlasta frekvensstyrning så motorn påverkas negativt - går sönder snabbt.
=> tillverknings kapacitets bortfall, leveransförsening.

3.Identitetsstöld och kreditkorts scam – tjuven beställer div dyra verktyg per postorder som betalas via offrets kort. Offret märker först när räkningen kommer att något är konstigt, då beloppen är klart större än vanliga inköp.