PENSIONS MYNDIGHETEN

PENSIONS
MYNDIGHETEN

Hur vi arbetar med att skydda våra digitala tjänster mot bedrägerier

E-legitimationsdagen
1 februari

PENSIONS
MYNDIGHETEN

Agenda

- Kort om Pensionsmyndigheten och våra digitala tjänster
- Historik kring inloggningslösningar
- Vad hände?
- Vad gjorde vi?
- Lärdomar
- Framtid
- Frågor

PENSIONS
MYNDIGHETEN

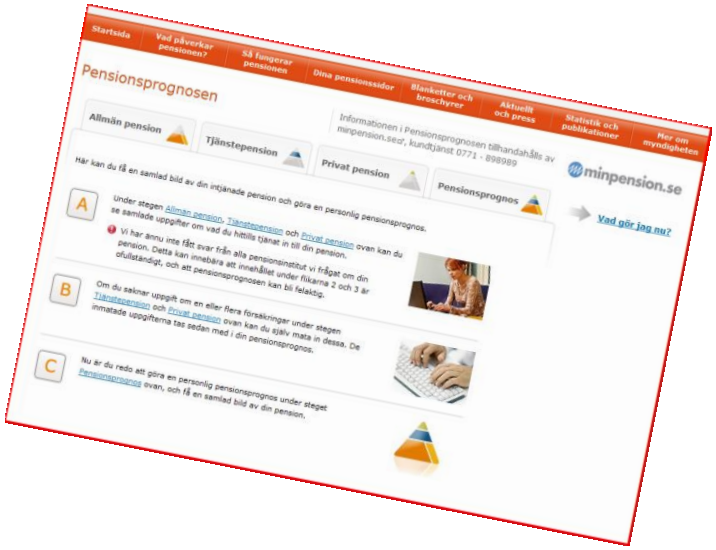
Pensionsmyndigheten

- Cirka 1 100 anställda på åtta orter runt om i landet:

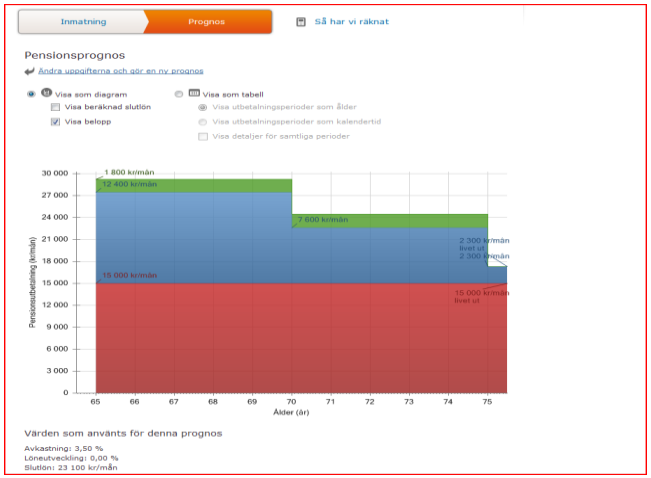
  Luleå, Söderhamn, Gävle, Stockholm, Karlstad, Växjö, Halmstad och Visby
- Pensionsmyndighetens uppdrag är att administrera och betala ut den allmänna pensionen. Vårt uppdrag är också att ge såväl generell som individuell information om pensionen
- 7,2 miljoner personer fick det orange kuvertet 2016
- Varje år betalar vi ut drygt 300 miljarder kr i pensioner till 2,1 miljoner pensionärer
- Det finns cirka 825 fonder inom premiepensionen
- Vi genomför cirka 800 000 fondbyten varje år
- Förvaltat kapital uppgår till cirka 1 000 Miljarder

PENSIONS
MYNDIGHETEN

Digitala tjänster, ett urval



- Gör din pensionsprognos
- Ansök om allmän pension
- Beställ pensionärsintyg
- Ändra bankkonto för din pension
- Ändra skatt på din pensionsutbetalning
- Byta fonder för premiepensionen
- Mobilappar:
  - Byta fonder
  - Pensionsprognos



PENSIONS
MYNDIGHETEN

Historik kring inloggningslösningar

- Personlig kod, distribuerats sedan september år 2000
- Införande av e-legitimation (BankID, Telia) år 2010
- Införande av Mobilt BankID april 2012
- Införande av SAML 2.0 enligt svensk e-legitimation under hösten 2016, mobilapp januari 2017. Samt även underskriftstjänst

PENSIONS
MYNDIGHETEN

Tillbakablick 2010 - 2014 Robot-tjänster byter fonder

PENSIONS
MYNDIGHETEN

Vad gjorde vi?

- Ledningsnivå
  - Skulle vi stödja denna typ av handel.
  - Gynnade den våra kunder
  - Debatt och dialog med aktörerna

- Juridiskt
  - Översyn av våra avtal och tittade på om detta var förenligt med rådande lagstiftning.

PENSIONS
MYNDIGHETEN

Vad gjorde vi?

- Tekniskt
  - Införande av robotfilter ”captcha-lösning”
  - Spärrade IP-nummer

PENSIONS
MYNDIGHETEN

Tillbakablick 2010 - 2014 Rådgivare använder personliga koder

PENSIONS
MYNDIGHETEN

Vad gjorde vi?

- Ledningsnivå
  - Gynnade den våra kunder
  - Resonemang med departementet
  - Debatt och dialog med aktörerna

- Juridiskt
  - Översyn av våra avtal och tittade på om detta var förenligt med rådande lagstiftning. Samverkade med finansinspektionen och ekobrottsmyndigheten.

PENSIONS
MYNDIGHETEN

Vad gjorde vi?

- Tekniskt
  - Möjligheten att använda pinkod för fondbyte togs bort för att försvåra för rådgivarna (säljbolagen) att byta fonder med användarnas uppgifter.

PENSIONS
MYNDIGHETEN

Tillbakablick 2015 – 2016 Mobilt BankID missbrukas

PENSIONS
MYNDIGHETEN

Vad gjorde vi?

- Ledningsnivå
  - Resonemang med departement och regering
  - Besluta att handelsstoppa vissa fonder
  - Debatt och dialog med olika aktörerna
  - Samverkan med utländska finansinspektioner

- Juridiskt
  - Polisanmälan
  - Uppdaterat samarbetsavtal som tydliggör god sed samt hårdare reglerar gällande marknadsföring samt ansvar för säljbolagens ageranden.

PENSIONS
MYNDIGHETEN

Vad gjorde vi?

- Tekniskt
  - Införande av signering vid byte av premiepensionsfonder
  - Tydliggjort vad som sker vid signeringen.
  - Inga samtidigt påbörjade inloggningar på pensionsmyndighetens websida, varning till användaren om detta pågår

PENSIONS
MYNDIGHETEN

SKP, Stärkt Konsumentskydd Premiepension

- Syftet är att genom tydligare och bättre anpassade lagar, författningar, regler och villkor uppnå stärkt konsumentskydd och säkra skyddet av pensionssystemets tillgångar.

- Nio separata förstudier ingår där varje förstudie drivs som sitt eget delprojekt. Skall vara genomfört tills 30 juni 2017.

Verkar inom E-Sam

- Medlemsdrivet program för samverkan mellan myndigheter och Sveriges Kommuner och Landsting (SKL) om digitaliseringen av det offentliga Sverige.

- Vi är med och tar fram ”Juridisk vägledning för införande av e-legitimering och e-underskrifter”.

- Vägledningen har till syfte att förklara
  - hur dessa funktioner är uppbyggda,
  - vilka rättsregler som aktualiseras och
  - vilka säkerhetsåtgärder som behöver vidtas.
  - Skapa samsyn bland samhällets aktörer rörande funktion, juridik och säkerhet.

Ser över våra tekniska tjänster

- Ser hela tiden över det tekniska skyddet för våra digitala tjänster i balans med kundnyttan och juridiken.

- Inför åtgärder för att göra det svårare för aktörer att ”lura” sparare.
  - Begränsningar av hur och varifrån man får logga in med Mobilt Bankid.
  - Utökade loggning och teknisk analys av mönster i fondbyten.
  - Tydligare upplysningar till användarna

Lärdomar

- Riskidentifiering
  - Svårt att identifiera denna typ av risker
- Erfarenhetsutbyte och samverkan med andra aktörer
  - Kan gälla andra BankID-tjänster, myndigheter samt funktioner internt
- Juridik viktigt
  - Kundinformation vid exempelvis signering skall både vara tydlig och skapa möjlighet till juridiska påföljder
- Kravställning
  - Vad är känsligt? – balansgång mellan kundvänlighet och säkerhet

Lärdomar

- Rätt uppföljning av loggar
  - Identifiera avvikande mönster

- Säkerhet måste ske i samverkan med kommunikation till kunder.
  - ”Personer ger ut sina inloggningsuppgifter”
  - Legitima bolag tänjer på gränserna

Slutsatser

- För att säkerställa vidareutveckling och innovation av digitaltjänster är det vikt att missbruk av e-legitimationer är stark skyddsvärda ur ett straffrättsligt perspektiv.

- Det är hela tiden en balans mellan kundnytta och säkerhet i de digitala-tjänsterna. För att komma framåt krävs ett samspel mellan ledning, juridik samt säkerhetsfunktioner.

- Det måste finnas ett stort förtroende vid nyttjande av digitala tjänster med e-legitimation. Av stor vikt att ställa krav på och samverkan med de olika aktörerna gällande vad man får och inte får göra med sin e-legitimation

PENSIONS
MYNDIGHETEN

Frågor?