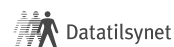




Tingenes Internett, hvilken info kan samles inn og hvordan skal disse dataene sikres?

Atle Årnes Fagdirektør teknologi

30. November 16



Personvernforordningen



- Nye EU personvernregler som tar sikte på å gi borgerne tilbake kontroll over deres personopplysninger og lage et høyt felles nivå for personvern i EU tilpasset den digitale tid, ble gitt den endelige godkjenning på torsdag 14. april 2016.
- Reformen setter også minimumsstandards på bruk av data for politiarbeid og juridiske formål.



Større sanksjoner



Ved brudd på reguleringen, så kan den aktuelle organisasjonen bli bøtlagt opp til 20 000 000 euro eller 4% av dens globale omsetning.



3

De nye reglene omfatter bestemmelser om:



- "Forskriften vil også skape klarhet for bedrifter ved å etablere en enkelt lov i EU. Den nye loven skaper tillit, rettssikkerhet og mer rettferdig konkurranse".
- "Tydelig og bekreftende samtykke» for å behandle personopplysninger fra vedkommende selv,
- rett til å vite når data har blitt hacket,
- sikre at personvernreglene er forklart i et klart og forståelig språk



4

IoT-utstyr kan være



- a) en avgrenset enhet, som kjører et tilpasset, eget sanntids operativsystem eller har ikke et operativsystem,
- b) mangler et brukergrensesnitt
- c) har begrenset funksjonalitet
- d) har lang levetid
- e) kan være gjenstand for begrenset tilgang når den er tatt i bruk (fysisk og logisk)
- f) ha evnen til å kommunisere direkte med hverandre eller til et nettverk (enten direkte eller via en eller annen form av gateway)

5

Firmware problem



- Software som ofte inneholder bugs som må bli rettet (patcher må lages og implementeres.
- Det kan være behov for rekonfigurasjon basert på bytte av internetprotokoller.
- Ny funksjonalitet trenger å bli lagt til
- Svak kryptografisk algoritme eller nøkler må byttes (alle kryptografiske algoritmer og nøkler har (eller bør ha) en utløpsdato.

6

Ytterligere risiko



- Kriminalitet, DDoS, SPAM e-mail sending
- Plattform for å skrive inn et hjemme- eller bedriftsnettverk som et forspill til et bredere angrep
- Angrep på selve enheten, webcamspionasje, termostatovertakelse, etc

7

IoT - Økosystem



- Utstysrprodusenter
- Firmware-utviklere
- System integratorer
- Sluttbrukere (offentlige, private, den enkelte eller andre)
- Nettverksleverandører (f.eks. ekomoperatører)

8

Problemer



- Noe IoT utstyr er ikke tilgjengelig hverken fysisk eller logisk. Noe som gjør firmware-oppdatering vanskelig eller umulig.
- Noe IoT-utstyr kan ikke oppdateres, og kan bare byttes.
- Man kan ha IoT-utstyr fra forskjellige produsenter.
- Firmware oppdatering kan endre utstyrets funksjonalitet på en uventet og uønsket måte.
- Hva skjer om bare deler av firmware trenger å bli endret.
- Feil i oppdateringen
- Manipulering av firmware oppdateringsprosess. Man in the middle angrep forutsetter integritet for prosess og kode.
- Kommer firmware oppdatering fra en autorisert kilde?

9

Problemer fortsetter



- Bør IoT-utstyr ha en begrenset levetid?
- Hvordan sikres support for IoT-utstyret i hele dets levetid?
- Bør oppdateringer være automatiske?
- Hvordan finner man ut om noe IoT-utstyr er kompromittert.
- Hvordan identifiseres kompromittert utstyr og hvordan slås det av.
- Hvordan håndtere bekymringer for personvernet? Hva slags meldinger bør sendes til eiere av kompromittert utstyr?

10

Hold kontroll



Nest Protect smøker 0 mg og holder deg opp på vakt.

Google kjøper selskapet bak superrøykvarsleren

Med kun tre år på baken går Nest Labs for nesten 20 milliarder kroner

OPPSATTET 14. DES. 2015 KL. 15:00. PUBLISERT 14. DES. 2015 KL. 15:00

VEIAR JENSEN, HÅRDRINGE.NO

Samsungs smarte hjem snart til Norge

SEEN AMUNDSEN

OPPSATTET 04. DES. 2015 KL. 15:00. PUBLISERT 04. DES. 2015 KL. 15:00



Hva skjer når tingene dine begynner å snakke sammen?
Se hvordan Samsung var for seg da teknologiske beretninger

Snart klare for Norges-lansering.



Har du lyst på smarthus? Svar i vår poll nederst i saken!

Klar for å styre huset med mobilen? På CES-messen i januar uttalte Samungs toppsjef at alle Samungs produkter skal være nettkoblete i 2020, og at [Tingenes internet \(IoT\)](#) er et satsingsområde for den koreanske teknologigiganten.

Herunder både smarte kiler, smart helse og

11

Åpenhet? Hva skjer?



12

Vanskelig å forstå



NETWORKWORLD

Home automation access: WeMo permissions explained



Credit: WeMo

App permissions and the access they allow are complicated and wildly misunderstood. For IoT home automation devices such as WeMo, owners can't pass on the app. For that reason, we're drilling down into WeMo app permissions, to find out what they really mean, as explained by Belkin engineers.

13

Viktige faktorer



- Tillit
- Personvern
- Sikkerhet
- Identitet

Hva skjer i hjemmet? Det er ikke bare søk på internett. Alt du gjør vil bli analysert og brukt.

1. Koble til
2. Lese
3. Sende
4. Behandle
5. Lagre
6. analysere

HP: 90% av tilkoblet utstyr samler personlig informasjon. 70% bruker kryptert informasjon.

14

Hva slags kommunikasjon



AMS

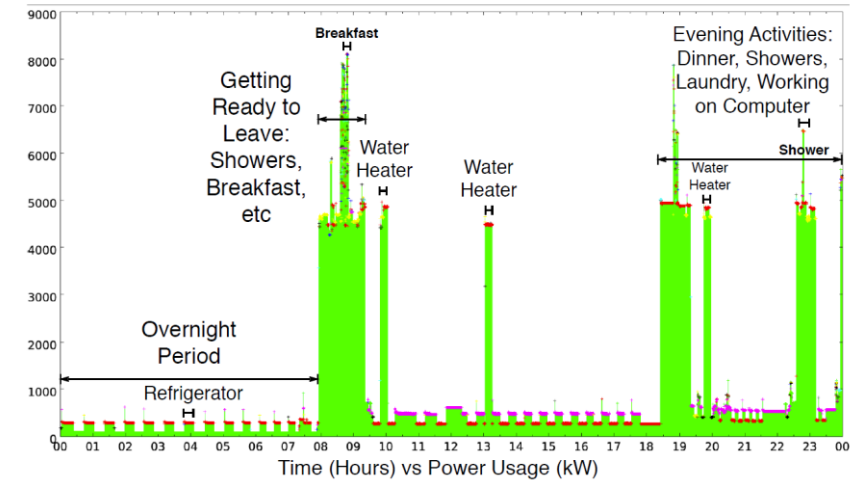


Typisk
Internet of things – utstyr.

Koblet til internet?



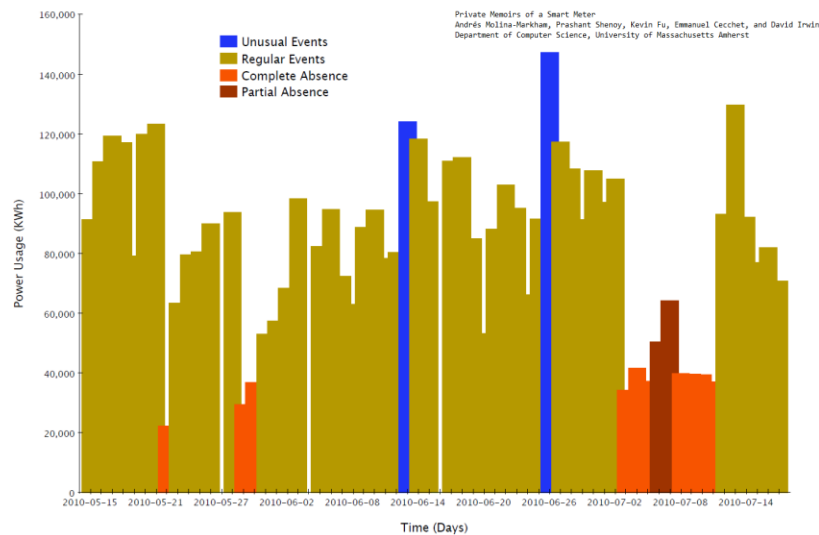
24 hours



Private Memoirs of a Smart Meter
Andrés Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, and David Irvin
Department of Computer Science, University of Massachusetts Amherst

17

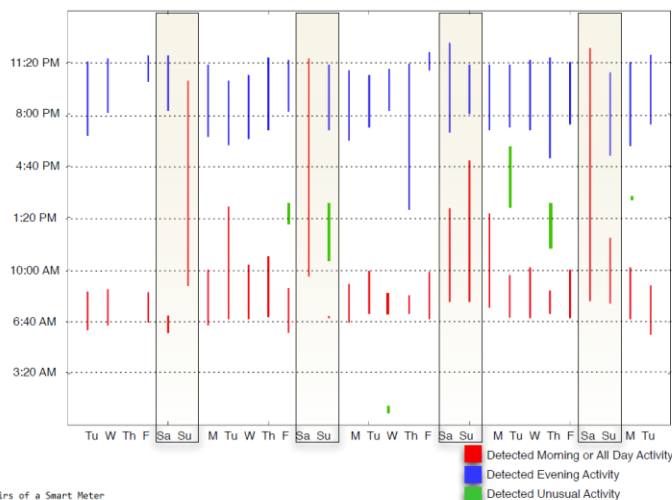
60 days



Private Memoirs of a Smart Meter
Andrés Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, and David Irvin
Department of Computer Science, University of Massachusetts Amherst

18

People present

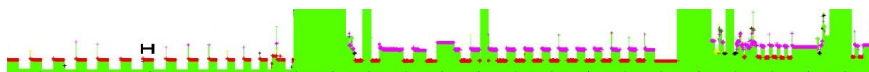


19

Personal data



- Fødselsnummer
- Kun rett til data for fakturering.
- Lagringstid på 3 år i Elhub for timemålte målepunkt.
- Sende melding til DT om det foretas lagring for andre formål.
- Tilrettelagt i Elhub for 15-minutters oppløsning.
- Sletting av opplysninger.
- Lagring opp til 10 år med sluttbrukers samtykke.
- Innsyn



20

Konsekvensanalyse, DPIA-Modellen



Databeskyttelse i forbindelse med intelligente nett og intelligente målesystemer

- Plattform for innovative energitjenester.
- Varsler en fremtid med tingenes internett.
- Den viktigste forutsetning er å beskytte privatlivets fred.
- Konsekvensanalyse blir i visse situasjoner obligatorisk.
- Innebygd personvern (Privacy by design).
- Personvern gjennom innstillinger (Privacy by default).
- Økt mengde og bruk av data er en utfordring.
- Det er forventet at Datatilsynene støtter konsekvensanalysemodellen og hjelpe virksomhetene.

21

Beskytte personopplysninger



- Beskytte personopplysninger hele vegen fra AMS til datahub.
- Konfidensialitet
- Integritet
- Oppdatering av software.



22

Eksempel på informasjon til kunde.



Kan informasjonen om strømforbruket bli misbrukt?

Personopplysningsloven stiller strenge krav til personvern, og XXX vil forholde seg til denne. Xxx har lang erfaring som bredbåndleverandør hvor kryptering av data er viktig. Gjennom kryptering vil ingen uvedkommende få tilgang til dine målerdata.

Xxx har valgt en løsning der software enkelt kan oppdateres slik at ny teknologi med tanke på for eksempel personvern kan benyttes.

23

Hvilken internettforbindelse?



Kundens nettverk, enten det er WIFI eller kabel, beskrives som en alternativ «gateway» for innhenting av måledata eller annen kommunikasjon med måleren.

Leverandørene er uklare her.

«Det er ønskelig å bruke internett, hvis du har det, for å sende inn måleravlesning. Montøren vil derfor spørre om du kan gi tilgang ved at du selv skriver inn passord til ditt trådløse nettverk. Ved å bruke internett blir det etter hvert mulig for deg å se hvor mye strøm du bruker til enhver tid.»

24

Mye nytt



- Du får altså mer detaljert data som kan brukes til for eksempel å tilpasse forbruket til tider av døgnet med lavere priser.
- En kommunikasjonsenhet (gateway), som også blir satt inn i sikringsskapet, er en liten men kraftig datamaskin. Den sørger for at dine målerdata kommer trygt fram til Xxx. Den samme enheten kan også være hjernen i et smarthus, der du kan styre lys, oppvarming, alarm, dør og andre funksjoner fra nettbrett eller mobiltelefon.

25

Samtykke



- Man trenger tillatelse til å behandle personopplysninger. Vanligvis er samtykke fra den registrerte det aktuelle behandlingsgrunnlag:
- Krav til samtykke:
 - Frivillig
 - Informert
 - Uttrykkelig



26

Hvordan sikre personvernet?



1. Velg den minst inngripende løsningen
2. Begrens mengden data som lagres
3. Velg sanntidsløsning hvis mulig
4. Lagre lokalt hvis mulig
5. La brukeren ha kontroll over løsningen
6. Slett data etter bruk
7. Begrens tilgangen til informasjon
8. Innsyn i egne data
9. Dataene bør krypteres
10. Anonymisering av data

27

Privacy by design



- Vær i forkant, forebygg fremfor å reparere
- Gjør personvern til standardinnstilling
- Bygg personvern inn i designet
- Skap full funksjonalitet: Både-og, ikke enten-eller
- Ivareta informasjonssikkerheten fra start til slutt
- Vis åpenhet
- Respekter brukerens personvern



28

Anonymisering



- Personvernlovgivningen gjelder ikke for anonyme data. Data er anonyme hvis det ikke lengre er mulig, selv ikke om man tar alle tenkelige midler i bruk, å identifisere enkeltpersoner i datasettet.
- Anonymisering av data gjør det mulig å utnytte verdien som ligger i dataanalyse på en personvernvennlig måte.



29

Personvern som norm



- I fremtiden vil selskapene måtte sette minstestandarder og produkter, slik at så lite personlige data som mulig er samlet inn og bearbeidet. "Privacy by design« (innebygd personvern) eller minstestandard bør bli et viktig prinsipp, og vil stimulere bedrifter til å skape noe nytt og utvikle nye ideer, metoder og teknologier for sikkerhet og beskyttelse av personopplysninger .



30

Atle Årnes er fagdirektør for teknologi i Datatilsynet.
Hans hovedarbeidsfelt er personvern innenfor
telekommunikasjons- og internettjenester, eID og biometri,
samt samferdsel og intelligente transportsystemer. Han
deltar i europeisk og internasjonal koordinering av
personvernarbeid.



postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no

@Datatilsynet
@AtleArnes