

AMS (3/3)

Med intensjon eller feiltagelse blir en regel i brannmuroppsettet opprettet, med den konsekvensen at direkte aksess tillates fra et annet nettverk. Dette utnyttes av angripere og de klarer å komme seg inn i AMS-databasen der all informasjon om strømkundene og deres strømbruk ligger lagret.

AMS (3/3)

Spm 1:
Hvilke hensikter kan angriperen ha i dette tilfellet?

Spm 2:
Hvordan kan dette oppdages?

Spm 3:
Hvilke tiltak kan innføres for at dette ikke skjer?

AMS (2/2)

AMS-systemet gir varsel om at avlest/rapportert strømmengde fra sluttbrukere har for stort avvik i forhold til rapportert overført strøm gjennom en trafostasjon for et område. Det blir mistenkt at ryktet har gått i nabolaget, og vedkommende har delt sin kunnskap.

AMS (1/2)

Spm 1:
På hvilken måte forandrer dette situasjonen nå som feilmengden er betydelig stor?

Spm 2:
Hva kan bli worst-case i denne situasjonen?

AMS (1/2)

En sluttbruker med ønske om å spare inn noen kroner på strøm klarer å manipulere data i AMS -enheten ved å fysisk aksessere selve måleren, og deretter nedjustere forbruket sånn at måleren viser mye mindre strømbruk.

AMS (2/2)

Spm 1:
Hvordan kan dette oppdages når det skjer i såpass liten skala?

Spm 2:
Hva er eventuelle konsekvenser og hvordan kan det unngås?