Vanlige hackerangrep i kraftsektoren

Alexander Meldal Andersen

Trondheim, 19.april 2018

Statnett

Da strømmen gikk i Ukraina

ANDY GREENBERG SECURITY 08.20.17 08:00 AM

HOW AN ENTIRE NATION BECAME RUSSIA'S TEST LAB FOR CYBERWAR

CURT MERLO

The clocks read zero when the lights went out.

It was a Saturday night last December, and Oleksii Yasinsky was sitting on the couch with his wife and teenage son in the living room of their Kiev apartment. The 40-year-old Ukrainian cybersecurity researcher and his family were an hour into Oliver Stone's film *Snowden* when their building abruptly lost power.

TECHNOLOGY NEWS JANUARY 18, 2017 / 12:06 PM / A YEAR AGO

Ukraine's power outage was a cyber attack: Ukrenergo

Pavel Polityuk, Oleg Vukmanovic, Stephen Jewkes 3 MIN READ

KIEV/MILAN (Reuters) - A power blackout in Ukraine's capital Kiev last month was caused by a cyber attack and investigators are trying to trace other potentially infected computers and establish the source of the breach, utility Ukrenergo told Reuters on Wednesday.

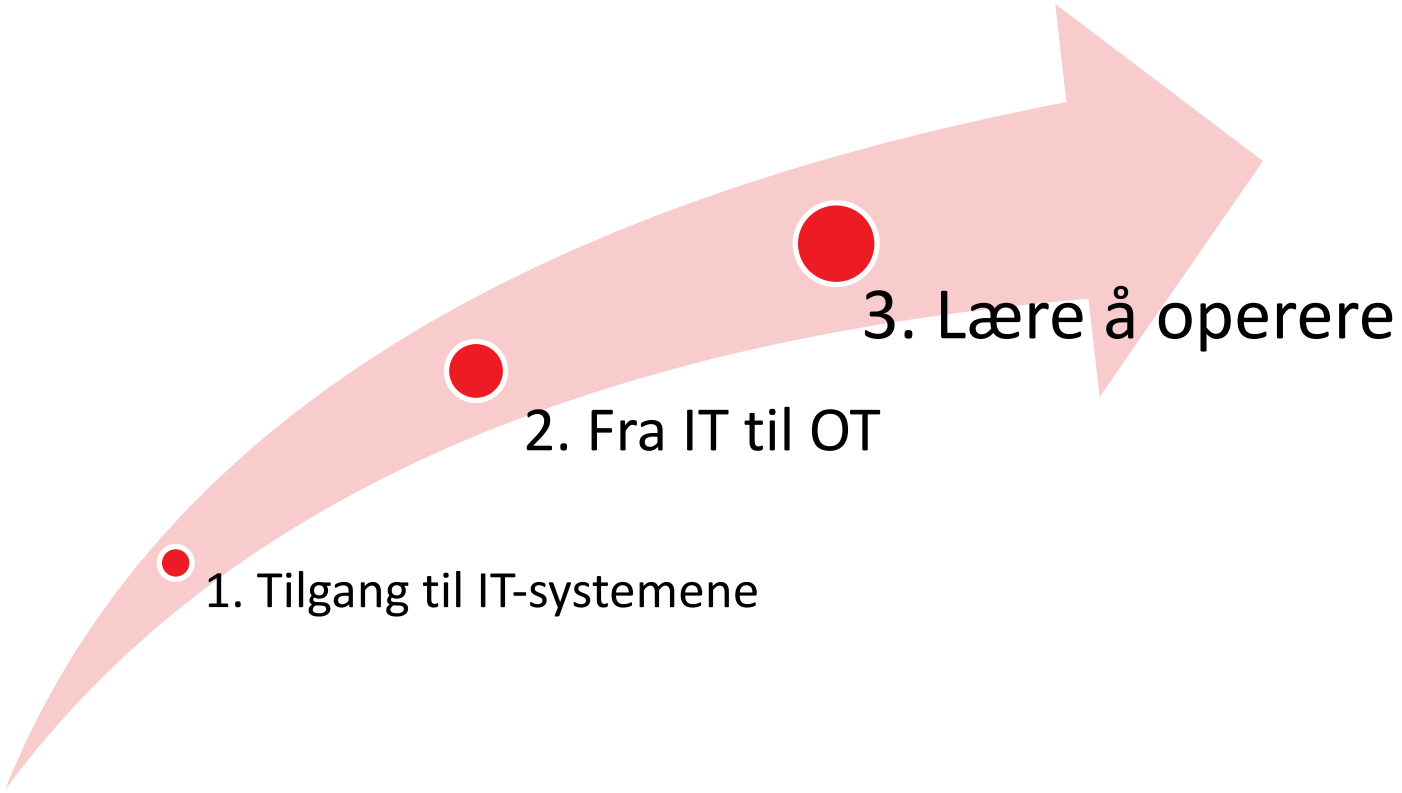
ANDY GREENBERG SECURITY 06.12.17 08:00 AM

'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID

GETTY IMAGES

AT MIDNIGHT, A week before last Christmas, hackers struck an electric transmission station north of the city of Kiev, blacking out a portion of the Ukrainian capital equivalent to

Hackerens tre steg



Steg 1: Tilgang til IT-systemene

- E-post
  - Vanligste kilden til angrep
  - Utgir seg for å være noen du stoler på
  - Kan inneholde «smittekilder»:
    - Filer som kan aktivere virus
    - Link til nettsider som ser pålitelige ut
- Fysisk tilgang
  - Mindre vanlig
  - Eks. ved tilgang til møterom, usikrede innganger, etc.
  - IoT-enheter med dårlig sikring

NTNU PÅ GJØVIK: Cybersikkerhet-senteret er drevet i samarbeid med privat næringsliv og sikkerhetsinstitusjoner.
Foto: Anders Gimmestad Gule / NTNU

Omfattende dataglipp fra sikkerhetsmiljø på NTNU

Tiltak mot steg 1

- E-post
  - «Utdanning» av de ansatte
  - Hold offentliggjøring begrenset
- Fysisk tilgang
  - Være strenge på hvem man slipper inn
  - Unngå at fysiske porter er tilgjengelige
- “An Interconnected system is only as strong as its weakest link”

Steg 2: Fra IT til OT

- IT-systemer har begrenset omfang
- Operasjonelle systemer (SCADA)
- Er sjelden helt isolerte fra hverandre

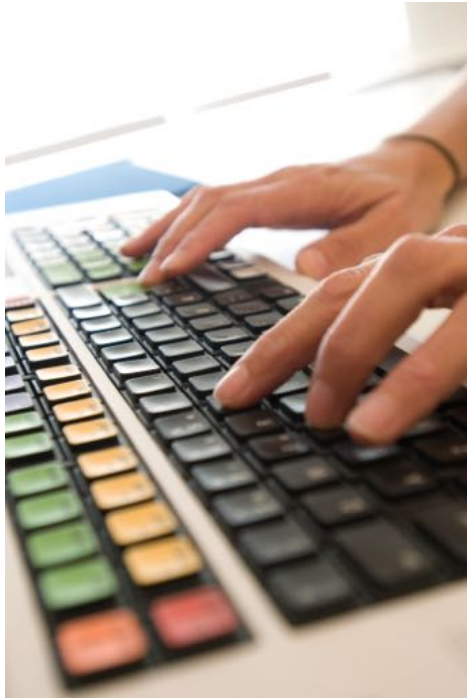


Tiltak mot steg 2

- Hold de ulike datasystemene strengt isolert
- Godt sikrede, oppdaterte operasjonelle systemer
- Hold tilgang begrenset

Steg 3: Lære å operere

- Tilgang betyr ikke forståelse
- Tar ofte lang tid å vite hvordan man bruker makten man har tatt til seg
- Kun 2 kjente tilfeller
  - Stuxnet
  - Industroyer (CRASHOVERRIDE)



Tiltak mot steg 3

- Finn og kast ut inntrengere ASAP
- Oppdaterte systemer (igjen)

Ha en backup-plan

- Kan ikke alltid være best
- Ingen systemer er ufeilbarlige
- Angriper trenger én seier

Spørsmål?