

Januari | 2019

# #CYBERVÄDER

**#cyberväder** berättar om betydande säkerhetsincidenter och -fenomen denna månad. Läsaren får en snabb helhetsbild av vad som hänt på cybersäkerhetsfältet under perioden i fråga.

Läget kan vara:



lugnt



oroande



allvarligt

# Cybervädret i januari 2019



## Nätens funktion

- Med tanke på överbelastningsangrepp var det lugnt i januari.
- Stormen Aapeli drabbade kommunikationsnät speciellt på Åland.
- Det fanns en omfattande störning i Microsoft Office 365 24-26.1.



## Spionage

- Ändring av uppgifter för domännamn möjliggjorde nätspionage då trafik styrdes till angriparens tjänst.
- Utvecklat spionage av smartmobiler väckte rubriker igen.



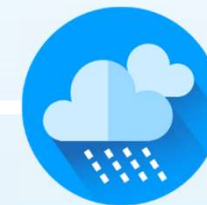
## Dataintrång & dataläckage

- Över en miljard användarnamn och lösenord publicerades på internet. Majoriteten av uppgifterna härstammar från gamla dataintrång.



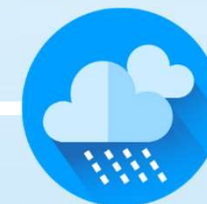
## Bluff och nätfiske

- Massiva samlingar av läckta lösenord väcker oro men de härstammar för det mesta från tidigare dataintrång.
- VD-bedrägerier ökar igen genom knäckta Office 365-e-postkonton.



## Skadeprogram & sårbarheter

- Sårbarhet i Microsoft Exchange möjliggör eskalering av rättigheter till Domain Admin.
- Via RDP-protokollet som är öppet mot internet är det möjligt att göra intrång och sprida t.ex. utpressningsprogram.



## IoT och automation

- I Japan bereds en lag som ger statsförvaltningen möjlighet att "hacka" medborgarnas IoT-apparater.
- Kritiska sårbarheter i kretsuppsättningar i trådlösa lokalnät.