



TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

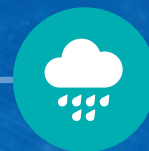
Juli 2019

Cybervädret juli 2019



Nätens funktion

- ▶ Tre betydande funktionsstörningar, vilket är färre än genomsnittet
- ▶ Satellitpositioneringssystemet Galileo avbröts för en vecka
- ▶ Överbelastningsangreppens verkningar kan avvärjas bättre än tidigare



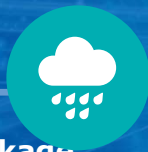
Spionage

- ▶ Nordkorea påstås ha stulit totalt 2 miljarder US dollar genom cyberangrepp för finansiering av landets kärnvapenprogram
- ▶ Den kinesiska hackergruppen Winnti har under flera år spionerat på många tyska hightech-företag



Skadeprogram och sårbarheter

- ▶ Många allvarliga sårbarheter i Apples iMessage-applikation
- ▶ I operativsystemet VxWorks hittades många allvarliga sårbarheter som kan påverka kritiska applikationer
- ▶ Sårbarheten BlueKeep kan utsätta datorer för skadlig kod



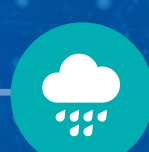
Dataintrång och dataläckage

- ▶ Staden Kokemäki drabbades av ett dataintrång och utpressningsprogram
- ▶ Dataintrång mot banken Capital One
- ▶ Organisationer som drabbats av dataintrång ska betala hundratals miljoner euro i ersättning till offren



Bluff och nätfiske

- ▶ VD-bedrägerier ökade igen under semesterperioden då skyldigheter överförs till ställföreträdare.
- ▶ O365-phishing fortsätter och medför lyckade dataintrång.



IoT och automation

- ▶ Europeisk reglering av IoT-säkerhet bereds
- ▶ Angripare utnyttjar IoT-apparater i organisationer genom växande skugg-IT

#cyberväder berättar om betydande säkerhetsincidenter och -fenomen under månaden. Läsaren får en snabb helhetsbild av vad som hänt på cybersäkerhetsfältet under perioden i fråga. Läget kan vara:



lugnt



oroande



allvarligt