



TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

Juni 2019

Cybervädret juni 2019



Nätens funktion

- ▶ Sex funktionsstörningar orsakade av åskrelaterade störningar i eldistributionen samt apparatfel. Störningarna drabbade några tusen användare.
- ▶ Flera apparater belägna i Finland användes i ett överbelastningsangrepp.



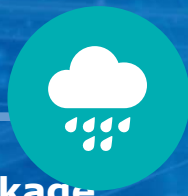
Spionage

- ▶ I juni rapporterade man om cyberoperationer med syfte att manipulera system i stället för att spionera.
- ▶ Man har också försökt spionera enstaka personers uppgifter bl.a. genom att göra intrång i teleoperatörernas system.



Skadeprogram och sårbarhet

- ▶ En sårbarhet i e-postservern Exim används aktivt för dataintrång.
- ▶ Sårbarheten BlueKeep kan utsätta datorer för skadlig kod som utbreder sig självständigt och snabbt.



Dataintrång och dataläckage

- ▶ Lahtis stad drabbades av ett omfattande dataintrång. Återhämtning efter händelsen och undersökning av den pågår fortfarande.
- ▶ Office 365-dataintrång görs så gott som varje dag.



Bluff och nätfiske

- ▶ Sommarperioden ökar igen hotet om VD-bedrägerier då skyldigheter överförs till ställföreträdare.
- ▶ I slutet av juni rapporterades många utpressningar genom porrbedrägeri.
- ▶ O365-nätfiske är fortfarande mycket vanligt.



IoT och automation

- ▶ Sårbarhet i DICOM-standarderna, som används i medicinsk hårdvara. Åtgärdande av sårbarheten förutsätter att standarderna ändras.

#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