TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädret

Juli 2023

#cyberväder

Cybervädret berättar om betydande säkerhetsincidenter och -fenomen under månaden.

Denna produkt är i första hand avsedd för dem som arbetar med informationssäkerhetsfrågor på olika nivåer i organisationer. Läsaren får en snabb helheltsbild av vad som har hänt och vad som kommer att hända på cybersäkerhetsfältet.

Cybervädret kan vara:

 lugnt

 oroande

 allvarligt

Cybervädret i juli 2023

Dataintrång och dataläckor

- I juli sjönk antalet anmälningar till samma nivå som i början av året.
- Nedgången var jämn både för inbrott i konton på sociala medier och inbrott i e-postkonton hos företag.

Bluff och nätfiske

- Bluffmeddelanden tar sig förbi e-postfiltren genom att dölja länkarna till nätfiskesidorna bakom en QR-kod.
- Under sommaren fiskades bankkoder genom att skrämma offren med bankers eller myndighetstjänsten Suomi.fi:s namn.

Skadeprogram och sårbarheter

- Under juli har flera kritiska sårbarheter offentliggjorts.
- I juli har Cybersäkerhetscentret gjort kartläggningar av kritiska programsårbarheter. Ingen organisation i Finland har hittills anmält bekräftade utnyttjanden.

Automation och IoT

- USA börjar använda ett nytt frivilligt program ”U.S. Cyber Trust Mark” för cybersäkerhetscertifiering och cybersäkerhetsmärkning av smarta enheter 2024.
- Behovet av att uppdatera enheter ska också följas upp under semestrarna genom att använda riskbaserad hantering av sårbarheter.

Nätens funktion

- I juli hade de allmänna kommunikationstjänsterna sex betydande funktionsstörningar.
- President Bidens besök orsakade inga funktionsstörningar på webbplatser.

Spionage

- Aktören Storm-0558, som är kopplad till Kina, trängde sig in i e-postkonton hos statliga organisationer i västländerna efter att ha fått tillgång till en krypteringsnyckel med vilken aktören kunde skapa falska inloggningsuppgifter för Microsoft-konton. I angreppet utnyttjades dessutom den brist som fanns i bekräftelsen av dessa uppgifter.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Vi har publicerat en ny anvisning där vi ger råd för att använda telefonen på ett informationssäkert sätt.

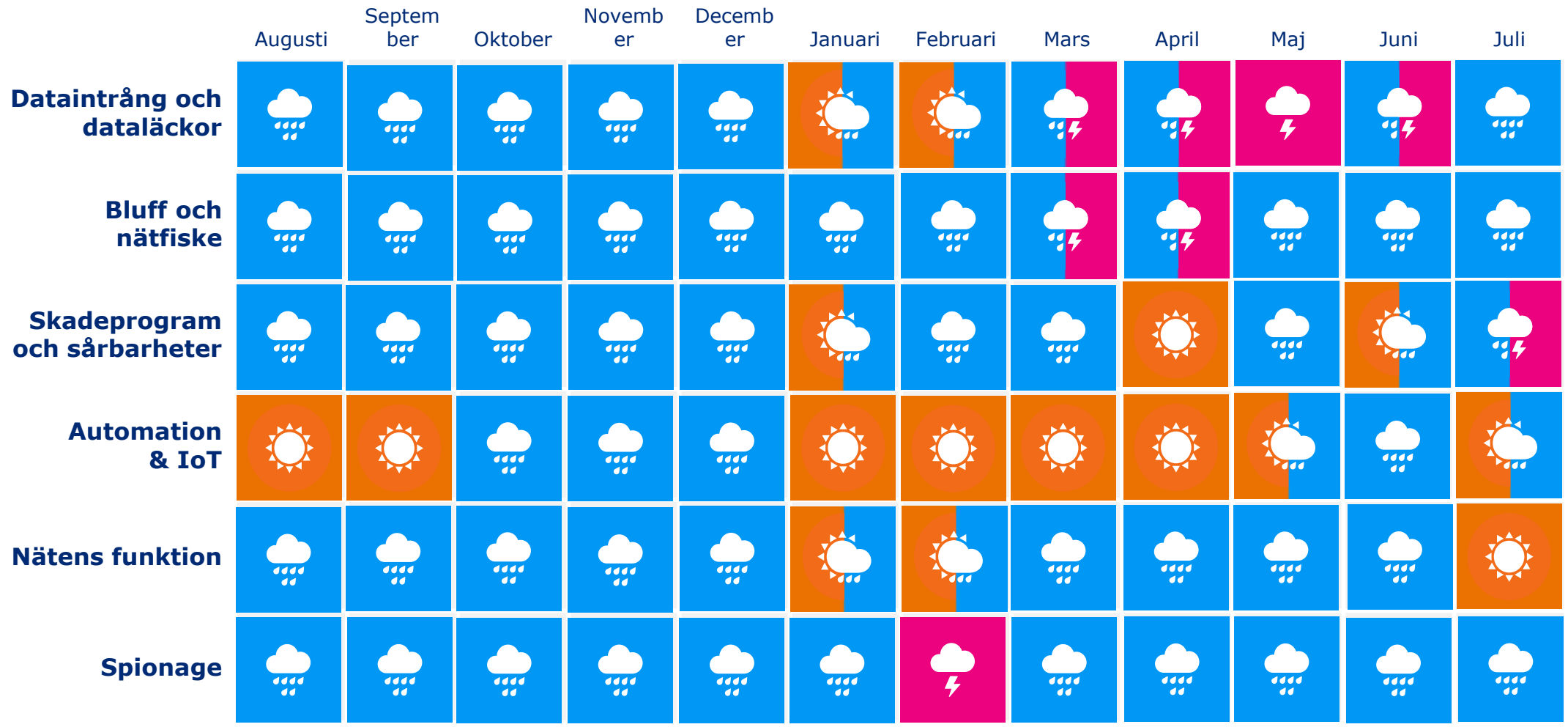
Vi delade våra tips för en informationssäker sommar.

I vår artikel Informationssäkerhet nu! gav vi anvisningar om hur du kan undvika och upptäcka eSIM-bedrägerier.

Allmän överskit över cybersäkerheten i juli

- Under juli publicerades flera uppdateringar av kritiska produkter som också används i stor utsträckning i Finland. Cybersäkerhetscentret kartlade situationen i Finland genast när sårbarheten avslöjades och kontaktade över hundra organisationer i anknytning till sårbarheterna.
  - Hittills har ingen organisation i Finland anmält utnyttjande av dessa sårbarheter.
- Vi rekommenderar att du tar hand om uppdateringar av enheter och system även under semestern.

Trenderna inom cybersäkerhet
de senaste 12 mån.



Top 5-cyberhot i den närmaste framtiden
(6 månader– 2 år)

1.

Hotnivån mot cybermiljön i Finland har förblivit förhöjd.

Antalet riktade angrepp har ökat. På grund av den förhöjda hotnivån betonas betydelsen av organisationernas beredskap.

2.

De politiska och ekonomiska fenomenen återspeglas också i cybersäkerheten.

Fenomenen kan synas snabbt i den digitala verksamhetsmiljön och orsaka svårförutsägbara händelser inom cybersäkerheten.

3.

Det är bra att förbereda sig för de utmaningar som artificiell intelligens medför i organisationer.

Det skulle vara bra för organisationer att identifiera de utmaningar som artificiell intelligens medför och förbereda sig på dem till exempel genom att utbilda sin personal.

Nytt

Uppdaterat

Symboler

4.

Informationssäkerheten och kontinuiteten i leverans- och servicekedjorna blir allt mer kritiska.

Förståelsen av underleverantörskedjan är central för organisationens egen cybersäkerhet. De flesta organisationer är mer eller mindre beroende av utkontrakterade digitala tjänster.

5.

Cybersäkerheten är beroende av experter och cybersäkerhetsfärdigheter omfattar alla!

Ny reglering och det faktum att cybersäkerhet smälter samman med företagens dagliga funktioner ökar allt mer behovet av olika experter. Även med tanke på riskhanteringen och kontinuiteten är det viktigt för organisationerna att säkerställa tillräcklig kompetens under alla årstider.