TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

# Cybervädret

April 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 april 2023

## Dataintrång och dataläckor

- April var som mars i fråga om dataintrång och dataläckor.
- De största fenomenen i Finland är fortfarande dataintrång i företagens e-postkonton (M365) och konton för sociala medier.

## Bluff och nätfiske

- Bedrägerisamtal som använder förfalskade nummer har orsakat mycket besvär för de verkliga innehavarna av numren. I bedrägerierna har man använt både företags och privatpersoners telefonnummer.
- I april har man igen sett nya aggressiva nätfiskekampanjer för att få bankkoder och betalkortsuppgifter. Temana gällde skatteåterbäringar och meddelanden som skickats i bankers och OmaPosti-tjänstens namn.

## Skadeprogram och sårbarheter

- Vi har igen påmint människor om hur viktiga uppdateringar är och uppmanat användarna att installera uppdateringar mot kritiska sårbarheter i Apples enheter.
- I april var antalet rapporterade skadliga program och sårbarheter lägre än i mars.

## Automation och IoT

- Ibland får vi anmälningar om digitala tjänster och enheter som marknadsförs medarbetare i organisationer. Dessa produkter är ofta molnbaserade och kunde väl tas i bruk utan stöd från organisa-tionens egen IT-avdelning.
- Idrifttagningen av digitala tjänster och apparater ska dock alltid vara kontrollerad.

## Nätens funktion

- I april förekom det sju betydande störningar i allmänna kommunikationstjänster.
- Tre av dem var orsakade av problem med elförsörjning.
- Finland blev medlem i NATO den 4 april 2023. Den dagen förekom det också överbelastningsangrepp, det totala antalet var 7.

## Spionage

- Polska myndigheter publicerade en rapport om en omfattande spionagekampanj som är länkad till cyberhotsaktören APT29.
- Enligt rapporten är syftet med kampanjen att samla in uppgifter bland annat från NATOs och EU:s diplomatiska enheter med hjälp av riktat nätfiske.

# **Cybersäkerhetscentrets**
# åtgärder och tips för förberedelser

Cybersäkerhetscentret undersöker läget för programsäkerheten i Finland. Utöver undersökningen av nuläget önskar vi kunna samla in information om smärtpunkter och bra praxis som kunde hjälpa oss att stöda företag och andra organisationer. Svara på enkäten!

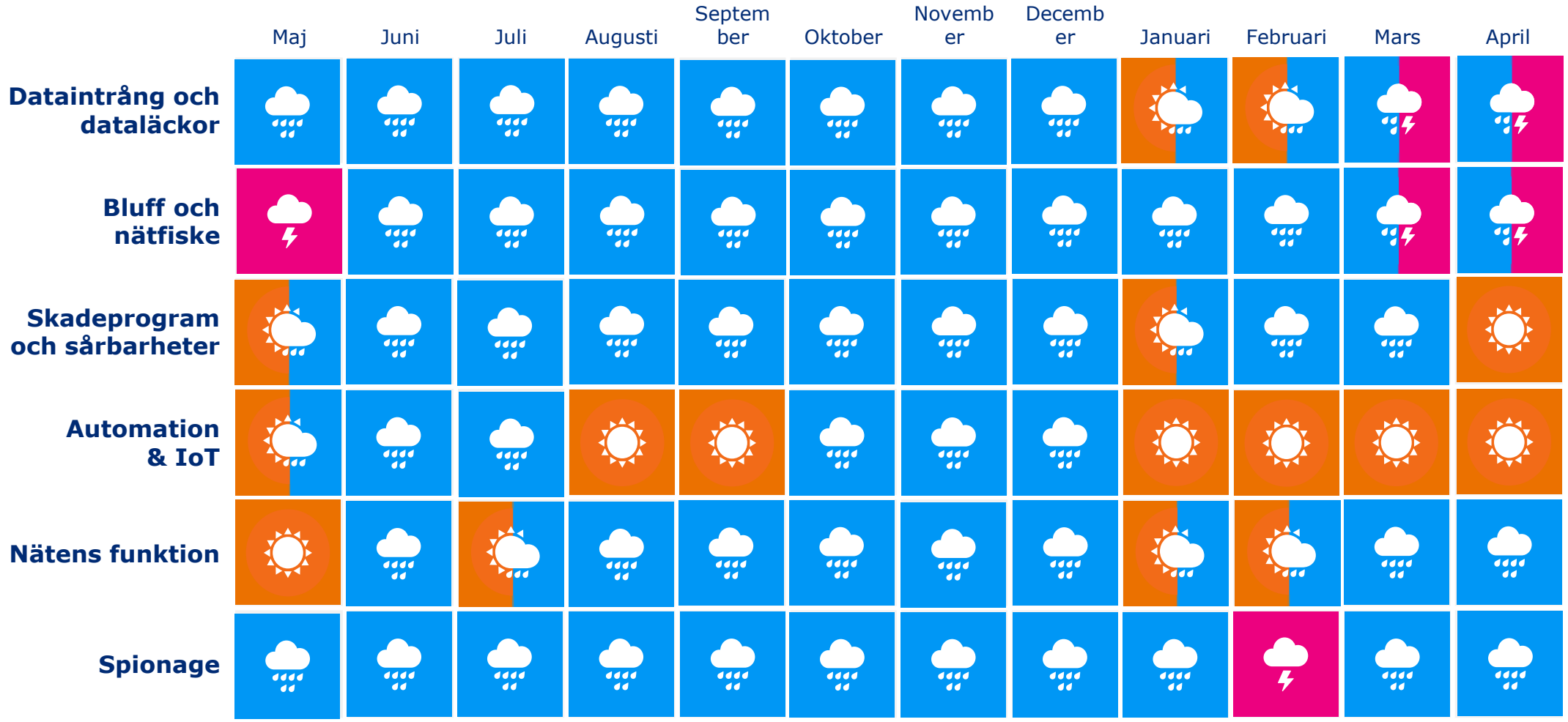
Cybersäkerhetscentret, Centralkriminalpolisen och Elisa höll en gemensam presentation om samarbetet mellan Traficom och finländska teleoperatörer för att förebygga förfalskning av telefonnummer i informationssäkerhetsevenemanget RSA Conference i USA i slutet av april.

Enligt ett examensarbete som gjordes för Cybersäkerhetscentret används en praxis som underlättar anmälan av sårbarheter ännu inte på ett omfattande sätt i Finland. Praxisen baserar sig på RFC 9116 som rekommenderar att organisationerna alltid publicerar sina kontaktuppgifter för sårbarheter på en och samma plats.

# Allmän översikt över cybersäkerheten i april

- Nätfiske mot företagens e-postkonton och dataintrång i konton verkar ha olika teman varje vecka. Under den senaste månaden har vi åtminstone observerat nätfiske mot säker e-post och meddelanden som verkar komma från Adobe och Microsoft OneDrive. I nästan alla fall som rapporterats till oss skulle flerfaktorsautentisering ha skyddat kontona.
- I april hade Traficom och Skyddspolisen en gemensam aktuell översikt över hotnivån mot cybersäkerheten som har förblivit förhöjd. Finländska organisationer är nu ständigt föremål för ett kontinuerligt ökande intresse. Speciellt antalet riktade angrepp har ökat.
- När sommaren och semesterperioden närmar sig blir även olika fakturabedrägerier vanligare. Cybersäkerhetscentret har under de senaste tiderna fått en hel del anmälningar om försök till fakturabedrägerier från företag från olika håll i Finland. Alla organisationer bör utbilda sin personal – även säsong- och sommararbetare – om organisationens faktureringsförfaranden för att förebygga VD- och faktureringsbedrägerier.

# Trenderna inom cybersäkerhet
de senaste 12 mån.



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

## 1.

**Hotnivån mot Finlands cybermiljö har blivit förhöjd.**

Antalet riktade angrepp har ökat. Betydelsen av organisationernas beredskap ökar på grund av den förhöjda hotnivån.

## 2.

**De ekonomiska och politiska fenomenen reflekteras även i cybersäkerheten.**

Fenomenen kan ses snabbt i den digitala miljön och de kan medföra svårförutsebara händelser i cybersäkerheten.

## 3.

**Organisationer bör vara förberedda för AI-relaterade utmaningar.**

Organisationer bör försöka identifiera de utmaningar som artificiell intelligens medför och vara förberedda för dem till exempel genom att utbilda sin personal.

**Ny**

**Uppdaterad**

**Symboler**

## 4.

**Informationssäkerheten och kontinuiteten i leverans- och servicekedjor är allt mer kritiska.**

Att förstå underleveranskedjor är centralt för organisationernas egen cybersäkerhet. Majoriteten av organisationerna är mer eller mindre beroende av utlagda digitala tjänster.

## 5.

**Cybersäkerheten är beroende av experter och cybersäkerhetskunskaper är viktiga för alla!**

Behovet av cybersäkerhetsexperter blir allt mer diversifierad.

Ny reglering och cybersäkerhetens sammansmältning med företagens dagliga verksamhet ökar behovet av experter ännu mer.