TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

# Cybervädret

Oktober 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 oktober 2023

## Dataintrång och dataläckor

- I oktober publicerade vi en gul varning om ett mycket aktivt och omfattande M365-nätfiske och dataintrång.
- I oktober fick vi några anmälningar om att man hade skickat ett skadligt program som ZIP-fil i samband med en inbjudan till ett Teams-möte.

## Bluff och nätfiske

- Med skatteåterbäring som tema försökte man lura bankkoder.
- Nätfiske efter bankkoder maskerat som säker e-post ökade så mycket att vi publicerade en gul varning om det.
- Vid slutet av oktober försökte man genom en omfattande textmeddelandekampanj lura hyrespengar avsedda för hyror i november.

## Skadeprogram och sårbarheter

- I oktober publicerades flera kritiska sårbarheter, av vilka flera även hade utnyttjats.
- Ett modem eller en router är en port till vårt hemnät. Därför är det särskilt viktigt att trygga dem när brottslingar letar efter sårbarheter i nätet manuellt eller automatiserat.

## Automation och IoT

- Varken informationssäkerhet eller tillgång till uppdateringar verkar spela en väsentlig roll i Black Friday-erbjudanden.
- Amerikanska myndigheter publicerade anvisningar om användningen av öppen källkod i OT-miljöer.
- APT-gruppen har utvecklat sin förmåga att påverka automationssystemen i kritisk infrastruktur.

## Nätens funktion

- I oktober förekom det 16 betydande störningar i allmänna kommunikationstjänster.
- Hacktivistgruppen NoName057(16) har riktat överbelastningsangrepp mot tiotals organisationer i Finland under hösten.
- Överbelastningsangrepp på applikationsnivå har påverkat en del organisationer.

## Spionage

- Olika sårbarheter utnyttjas aktivt inom cyberspionage.
- I oktober rapporterade man till exempel om utnyttjandet av sårbarheter i komprimeringsverktyget WinRAR, Atlassian Confluence, Roundcube-postservrar och Jetbrains TeamCity för spionage.

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

Seminariet Informationssäkerhet 2023 ordnades torsdagen den 12 oktober 2023. Inspelningen av webbinariet samt presentationsmaterialet finns på våra webbsidor.

Traficoms och Försörjningsberedskapscentralens färska utredning kartlade nuläget och utvecklingsbehoven inom programvaruutveckling.

Vi publicerade en ny anvisning om hur man kan skydda hemnätet och routern.

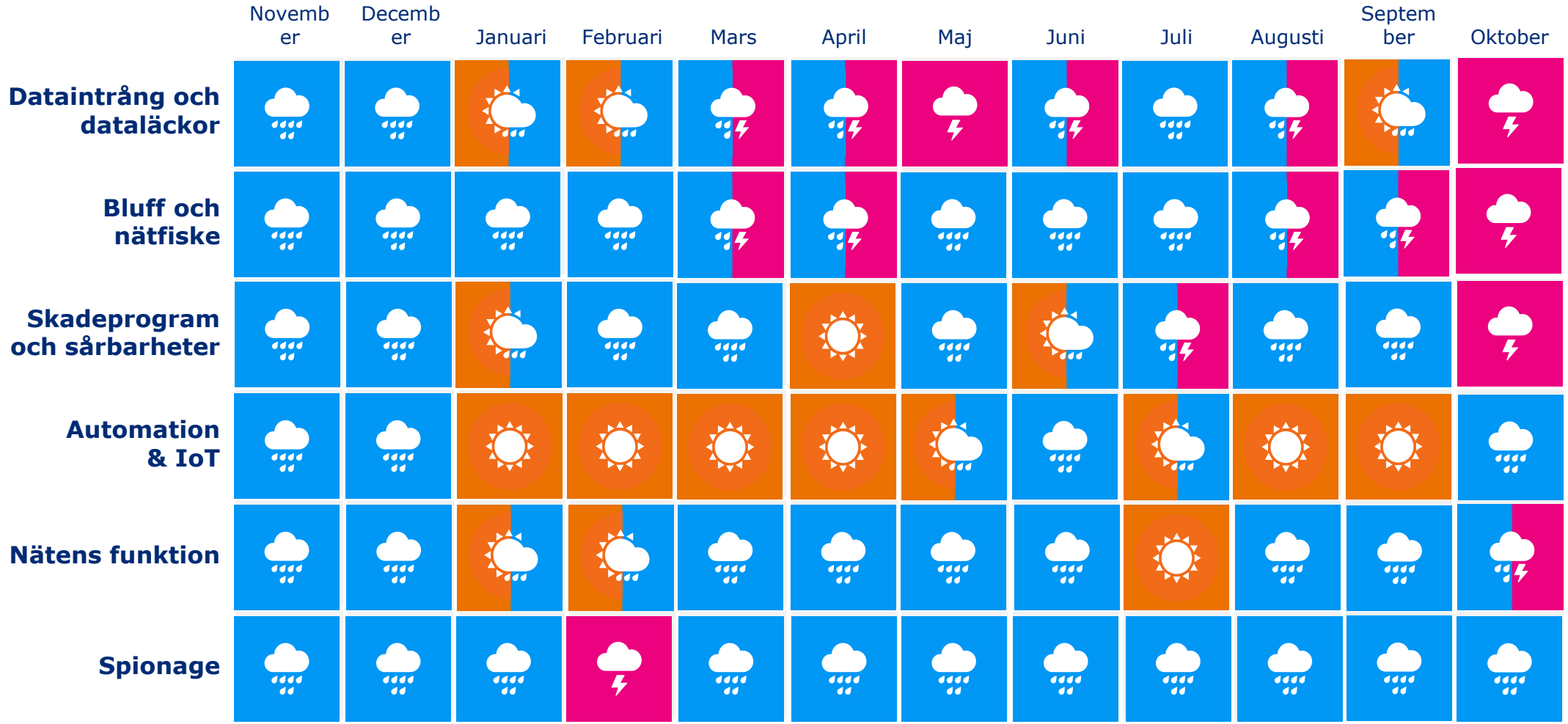
Inspelningen av webbinariet om resultatöversikten för kampanjen Ketjutonttu (Kedjetomten) den 5 oktober 2023 samt kampanjens slutrapport finns på vår webbplats.

Vi publicerade en ny anvisning om att säkerställa informationssäkerheten i fristående arbetsstationer.

# Allmän överskit över cybersäkerheten i oktober

- Flera kritiska sårbarheter publicerades i oktober.
  - Det är alltid bra att uppdatera systemen och utrustningen så snart som möjligt!
- Den 20 oktober 2023 publicerade vi en allvarlig varning om en dataintrångsvåg i Microsoft 365-konton där man fiskat efter lösenord till Microsoft 365-miljön genom förfalskade e-postmeddelanden. Nätfiskemeddelandena använde sig av säker e-post som tema vilket ökade de förfalskade meddelandenas trovärdighet. Kampanjen hade ett exceptionellt stort antal offer.
  - Varningen togs bort som inaktiv den 8 november 2023.
- I början av oktober trädde i kraft Traficoms föreskrift som ålägger teleoperatörerna att förhindra samtal som kommer från utlandet med falska finländska nummer även för mobilnumrens del. Till följd av detta har antalet anmälningar om bedrägerisamtal från förfalskade nummer minskat i oktober.

# 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.

**Allvarliga sårbarheter utnyttjas allt snabbare**

Förutom att installera en korrigerande uppdatering är det ofta nödvändigt att undersöka om sårbarheten redan utnyttjats innan man installerar uppdateringen.

## 3.

**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.

**Nytt**

**Uppdaterat**

**Symboler**

## 4.

**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.

## 5.

**Cybersäkerheten är beroende av experter och cybersäkerhetskunskaper är viktiga för 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.