TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädret

April 2024

#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 2024

Dataintrång och dataläckor

- En kritisk sårbarhet i Palo Alto (CVE-2024-3400) ledde till flera dataintrång och försök till dataintrång. Vi fick cirka 15 anmälningar på basis av vilka allvarliga skador kunde dock undvikas.
- I april hackades M365-användarkonton med nätfiskemeddelanden med DropBox som tema. AiTM-tekniken användes i en del av intrången.

Automation och IoT

- Det har funnits avsevärda cyber-säkerhetsproblem i konsument-produkter. För en del av dem har kommunikationen väckt missnöje hos konsumenter. Dålig kris-kommunikation är en betydande risk för företagets anseende och affärsverksamhet.
- Planering och övning av kriskommunikation är kärnan i kontinuitetshanteringen.

Bluff och nätfiske

- Bedrägerimeddelanden används för att sprida skadliga program till Android-telefoner i ett inkassobolags namn. Textmeddelanden och telefonsamtal som verkar komma från Kredinor styr mottagarna att installera ett ”antivirusprogram” i telefonen, men i verkligheten är det ett skadligt program som stjäl bankuppgifter.
- Webbplatser har också förfalskats för webbadresser som slutar på .fi bland annat i PRS:s namn.

Nätens funktion

- I april förekom det 9 störningar i allmänna kommunikationstjänster.
- Hacktivisters överbelastningsangrepp riktade sig inte mot Finland i april.
- Andra överbelastningsangrepp har inte rapporterats ha några betydande konsekvenser.

Skadeprogram och sårbarheter

- Varning 1/2024: I produkten Palo Alto Global Protect som används brett i organisationer fanns en sårbarhet (CVE-2024-3400) som utnyttjades aktivt.
- Efter det att anmälningarna till Cybersäkerhetscentret minskade beslöt vi att ta bort varningen 7.5.2024.

Spionage

- Observationer som associerats med Sandworm kom upp i flera publikationer.
- Det skadliga programmet som aktören använde som bakdörr observerades bland annat i Ukraina och Estland.
- I Ukraina rapporterades att en aktör hade berett angrepp mot den lokala energi-, vatten- och värmeproduktionen.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Vid M365-dataintrång används allt oftare nätfisketekniken AiTM. Vi publicerade en anvisning i vilken vi berättar om förloppet vid nätfiske där AiTM-tekniken utnyttjas, att identifiera den samt om hur du känner igen sådant nätfiske och skyddar dig mot det.

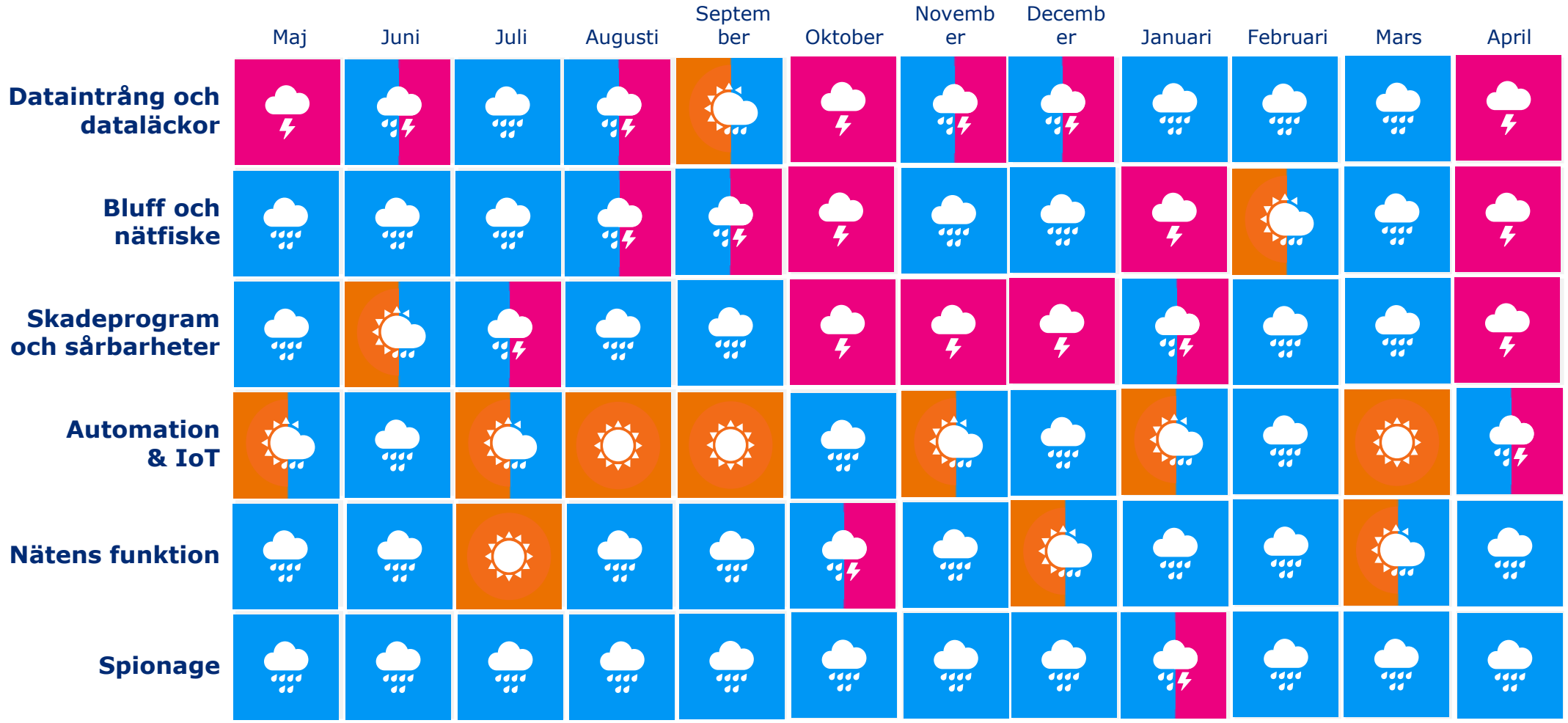
Brottslingarna har krävt en lösensumma för att återställa de hackade användarkontona. Du ska aldrig betala någon lösensumma för den stöder fortsatt brottslighet och utpressning.

Läs i vår nya blogg tips hur vi tillsammans kan bekämpa för att bli av med verksamhetsförutsättningarna för Mirai och flera andra skadliga program.

Allmän överskit över cybersäkerheten i april

- Vi publicerade 18.4.2024 Varningen 1/2024 om dataintrång i Palo Alto GlobalProtect-produkter.
  - Palo Alto GlobalProtect Gateway och GlobalProtect Portal som används för hatering av den är produkter som organisationer använder till exempel för att upprätta en säker distansuppkoppling med VPN.
  - Läget var slutligen lugnare än förväntat, och varningen togs bort 7.5.2024.
- Fitsec har publicerat ett sätt att dekryptera filer som drabbats av det skadliga programmet Akira och tillhandahåller sin hjälp till Akiras offer på sina sidor.

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 underleverantörskedjan är centralt för organisationernas egen cybersäkerhet. De flesta organisationer är mer eller mindre beroende av utlagda digitala tjänster.

Ny

Uppdaterad

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.