TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädret

Februari 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 februari 2024

Dataintrång och dataläckor

- Inloggningsförsök i nätverksutrustning och dataintrång i M365-konton fortsatte. I flera M365-incidenter utnyttjades AiTM-nätfiske.
- Vid dataintrång i konton för sociala medier krävdes en lösensumma av kontoägarna för återställning av kontot.

Bluff och nätfiske

- Mer än 80 SMS-avsändaridentifikationer har skyddats mot bedrägerier. Varje skyddad avsändaridentifikation minskar brottslingars sätt att göra bedrägerier i myndigheters och företags namn.
- Man skickar dock en hel del SMS-bedrägerimeddelanden också utan någon trovärdig avsändaridentifikation i fråga om trafikförseelser och obetalda bilskatter.

Skadeprogram och sårbarheter

- Ivantis sårbarheter visar hur kritisk informationssäkerhet i kantdatorsystem är.
- Den amerikanska cybersäkerhetsmyndigheten CISA berättade om dataintrånget i sitt Ivanti-system.
- I början av mars publicerades ett sårbarhetsmeddelande om en kritisk sårbarhet i programvaran JetBrains TeamCity.

Automation och IoT

- En smart present kan vara en tråkig överraskning – bekanta dig med produktens informationssäkerhets-egenskaper före köpbeslutet.
- Utebliven funktion i automation som används på lantgårdar kan medföra allvarliga konsekvenser. Ett utpressningsprogram i en dator som styr utfordring av produktionsdjur på lantgård hotade djurens välfärd.

Nätens funktion

- I februari fanns det 2 störningar i funktionen av allmänna kommunikationstjänster.
- I början av februari riktade hacktivister överbelastningsangrepp mot ett rekordantal inhemska organisationer.

Spionage

- Amerikanska myndigheter störde ett angreppsnät som bildats av knäckta Ubiquiti EdgeRouter-anordningar.
- Enligt myndigheterna användes de bland annat för förmedling och insamling av inloggningsuppgifter som stulits i en APT28-aktörs kampanjer samt för routning av angreppstrafik.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Tillsammans mot textmeddelandebedrägerier – redan över 80 avsändaridentifikationer har skyddats.

Det blev nya skyldigheter för onlineplattformar på internet och för andra digitala tjänster när EU:s rättsakt om digitala tjänster (DSA) började tillämpas 17.2.2024. Avsikten med den nya regleringen är att minska olagligt innehåll och öka transparens för tjänsterna.

Allmän överskit över cybersäkerheten i februari

- Nätfiske efter Microsoft 365-konton ökade igen i februari. Meddelanden som maskerats som säker e-post ledde till en nätfiskesida där man fiskade efter användarnamn och lösenord.
  - Cybersäkerhetscentret uppmanar alla Microsoft 365-kunder att kommunicera internt om hoten om nätfiskemeddelanden.
  - På nätfiskesidorna har man använt avancerad adversary-in-the-middle-automatik (AitM) som i vissa fall även kan förbigå flerfaktorsautentisering.
    - Tvångsinförande av flerfaktorsautentisering är ett effektivt skydd samt en grund för andra skyddsmetoder mot nätfiskekampanjer.
- VD-bedrägerier och andra faktureringsbedrägerier har också förekommit i februari.
  - Organisationer ska ge sina medarbetare, utan att glömma sommarvikarier och praktikanter, klara anvisningar för organisationens faktureringspraxis och säkra kontrollpraxis, och man ska alltid hålla fast vid dem.
  - Om man tvivlar på huruvida ett meddelande är riktigt kan man alltid säkerställa detta genom att ringa upp avsändaren.

Trenderna inom cybersäkerhet
de senaste 12 mån.