TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädret

November 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 november 2023

Dataintrång och dataläckor

- Angrepp med utpressningsprogram på grund av dataintrång riktades speciellt mot industrisektorn i november. I de flesta fall var de cyberkriminella grupperna Akira och LockBit bakom incidenterna.

Bluff och nätfiske

- I början av november försökte man genom en omfattande textmeddelandekampanj lura hyrespengar till fel konto.
- Innehavare av Facebook-sidor skrämdes med hotet om avstängning av sidorna på grund av olika orsaker. Bedragaren försökte kapa sidorna till sig själv.
- Aggressivt nätfiske efter bankkoder skrämde människor med okända betalningar och kontoavstängningar.

Skadeprogram och sårbarheter

- Vi har fått flera anmälningar om observationer av utpressningsprogram.
- Det fanns flera kritiska sårbarheter i Ciscos utrustning, vilket krävde omedelbar uppdatering.
- Vi kartlade sårbarheten Citrix Bleed (CVE-2023-4966) och kontaktade flera organisationer.

Automation och IoT

- En politisk överenskommelse nåddes om EU:s cyberresiliensakt (CRA).
- Unitronics programmerbara kontrollenheter för logik (PLC) blev föremål för dataintrång även i Finland. Kontrollenheterna används från vattenreningsverk till små kraftverk. Angreppen har lyckats bland annat på grund av svaga standardlösenord.

Nätens funktion

- I november förekom det 7 betydande störningar i allmänna kommunikationstjänster.
- Hacktivister riktade överbelastningsangrepp mot Finland även i november.
- Organisationer har inte rapporterat om några betydande konsekvenser för tjänster med anledning av överbelastningsangrepp.

Spionage

- Skyddspolisen varnade igen i november om att nätutrustning avsedd för konsumentbruk används för cyberspionage.
- Dåligt skyddade och sårbara internetanslutna apparater hackas för att utgöra en del av angreppsinfrastrukturen och de utnyttjas för att göra det svårare att observera ett cyberangrepp.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Från och med sommaren har man kunnat se hur cyberbrottslingar allt snabbbare kan utnyttja publicerade sårbarheter. Man ska ta hand om uppdateringar året om, också under julhelgerna.

Minnesregeln för säkerhetskopiering 3 – 2 – 1. Ta minst 3 säkerhetskopior, förvara dem på minst 2 olika format och ställen samt ha minst 1 säkerhetskopia som inte är kopplad till nätet.

Vi publicerade en ny anvisning Tietoturva on koko organisaation asia - vinkkejä henkilöstön tietoturvakoulutuksen suunnitteluun (Informationssäkerhet är en fråga för hela organisationen - tips för planering av informationssäkerhetsutbildning för personalen).

Stöd för utveckling av informationssäkerheten till 24 företag - stödbeloppen på högst 100 000 euro delades ut i sin helhet.

Allmän överskit över cybersäkerheten i november

- Trenderna i november omfattade utnyttjande av kända sårbarheter för dataintrång och för angrepp med utpressningsprogram.
  - I november offentliggjordes ett flertal kritiska sårbarheter som förutsatte omedelbara uppdaterings- eller begränsningsåtgärder av administratörer.
  - Det har observerats att utpressningsprogrammet Akira utnyttjar Ciscos nätutrustningssårbarhet (CVE-2023-20269) även i Finland.
- Aktörer som sprider utpressningsprogram försöker ofta också kryptera eller störa säkerhetskopiorna. På det här sättet blir det mycket svårare för företag att organiskt återhämta sig. Förvara alltså minst 1 säkerhetskopia så att den inte är kopplad till nätet.
- E-postkonton är brottslingars favoritmål. Skicka gärna känsliga uppgifter via säker e-post och förvara dem på något annat ställe än i e-brevlåda.

Trenderna inom cybersäkerhet
de senaste 12 mån.