TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädret

Maj 2023

#cybervädер

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 maj 2023

Dataintrång och dataläckor

- Antalet anmälningar om dataintrång i konton för sociala medier ökade med nästan 300 procent jämfört med genomsnittet i början av året.
- Även anmälningar om M365-dataintrång fortsatte att öka i början av månaden. I slutet av maj observerades dock en liten förbättring.

Bluff och nätfiske

- Enträgna bedragare skickar textmeddelanden och ringer efter.
- Allt flera telefonbedrägerier rings med falska telefonnummer. Traficoms föreskrift 28 förpliktar teleoperatörerna att förhindra förfalskning av uppringarens nummer från och med den 2 oktober.

Skadeprogram och sårbarheter

- En nolldagarssårbarhet observerades i filöverföringsprogrammet MoveIT. Man har observerat att sårbarheten ha utnyttjas i Finland och i andra länder.
- En nolldagarssårbarhet identifierades i Barracuda ESG-enheter.
- Sårbarheter i Zyxels brandväggar och VPN-produkter. Man har observerat att sårbarheten har utnyttjas i Finland och i andra länder.

Automation och IoT

- Vi publicerade en Informationssäkerhet Nu!-artikel med rubriken ”Dataintrång mot en systemleverantör inom industrin förutsätter snabba åtgärder även av dess kunder”.

Nätens funktion

- I maj förekom det fyra betydande störningar i allmänna kommunikationstjänster.
- Hamnoperatörer blev utsatta för överbelastningsangrepp.
- Speciellt angrepp på applikationsnivå har på sistone påverkat till exempel webbsidornas funktion.

Spionage

- Myndigheter i USA publicerade en rapport om det skadliga programmet Snake som hotaktören Turla använt.
- Rapporten ger anvisningar om hur man kan observera skadliga program i infekterade system.
- Dessutom tog myndigheterna bort det skadliga programmet i en del av de infekterade systemen.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Nya krav för stark autentisering som träder i kraft sommaren 2023 gör användningen av elektroniska tjänster allt tryggare. Syftet med de nya kraven är att användare enklare än tidigare kan kontrollera vilken tjänst de håller på att logga in.

Vi publicerade en artikel där vi påminner organisationer om att de även ska vara beredda för informationssäkerhetsincidenter mot leverantörer. Därför uppmanar vi speciellt att alla ägare av industriella miljöer bereder sig för den möjligheten att en leverantör som är kritisk för din egen produktion blir utsatt för ett dataintrång eller dataläckage.

En ny version av Cybermätaren samt nytt stödmaterial finns tillgängliga på våra webbsidor. Uppdateringarna i den nya versionen omfattar egenskaper som gör det enklare att använda verktyget, att rapportera observationer som stöd för beslutsfattandet samt att upprepa bedömningen. Anmäl dig till vårens och höstens presentations- och utbildningsevenemang!

Allmän översikt över cybersäkerheten i maj

- I maj ökade antalet anmälningar om dataintrång i konton för sociala medier avsevärt.
- Vid slutet av förra månaden observerades även dubbelbedrägerier där en person kontaktas flera gånger via textmeddelande eller telefon.
- Bedragarna försöker övertyga föremålet om att deras konto är utsatt för risk och uppmanar dem att överföra pengarna till ett säkerhetskonto.
- Anmälningar om M365-nätfiske ökade i maj men en liten förbättring observerades mot slutet av månaden.
  - Enligt Cybersäkerhetscentrets uppgifter har åtminstone ett M365-e-postkonto hackats i cirka 60 organisationer efter april.

Trenderna inom cybersäkerhet
de senaste 12 mån.