TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädret

November 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

Månadens nyckeltal

Nätfiske efter Microsoft 365-koder var speciellt aktivt i november. Nätfiske gällde speciellt bedrägerimeddelanden med Dropbox som tema.

Det tog under två veckor att reparera undervattenskabeln C-Lion1. På land kan avbrott konstateras och repareras till och med under några timmar.

Cybervädret i november 2024

Dataintrång och dataläckor

- M365-konton hackades aktivt med nätfiskemeddelanden med Dropbox som tema som ledde till AiTM-nätfiskesidor.
- Det gjordes några anmälningar om webbtjänster som avslöjade information som var tillgänglig för alla på ett obehövligt omfattande och öppet sätt.

Bluff och nätfiske

- S-banken, OP, MittKanta och Danske Bank har varit bedragarnas favoriter i november.
- En avsevärd andel av bedrägeritrafiken för nätfiske efter bankkoder skickas fortfarande per textmeddelande.

Skadeprogram och sårbarheter

- Tjänster och kontrollpaneler som kan ses på det offentliga nätet har anmälts till ägare av tjänster.
- Försök att utnyttja sårbarheter i Fortinets gamla FortiEMS-versioner samt FortiManager-sårbarheten.

Automation och IoT

- Black Friday påminde igen om hur viktig informationssäkerhet och kontinuerliga uppdateringar är när man köper. [1]
- Ny version och finsk översättning av cybersäkerhetsstandarden för automations- och kontrollsystem IEC 62443-2-1 är färdig. [2]
- SANS har publicerat rapporten OT/ICS om dagsläget i cybersäkerheten [3]

Nätens funktion

- I november observerades 6 funktionsstörningar i allmänna kommunikationsnät.
- De avbrutna telekommunikationskablarna reparerades snabbt. Näten fungerade trots avbrott.
- För överbelastningsangrepp har läget blivit lugnare mot slutet av året.

Spionage

- I cyberspionage används regelbundet nolldagarssårbarheter.
- I november rapporterades det runt om i världen om en sårbarhet i Fortinets VPN-program som en kinesisk aktör hade utnyttjat.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Dataintrång som använder AiTM-tekniken (adversary-in-the-middle) kan observeras och förhindras genom att införa autentisering utan lösenord samt genom att göra strängare villkorliga regler för M365-tjänster. [4, 5]

Vi publicerade tips för administratörer för nätbutiker om hur digital skimming kan upptäckas och förebyggas och vilka åtgärder som bör vidtas efter att skimming har observerats. Digital skimming är stöld av kreditkorts- eller betalkortsuppgifter då en kund använder dem i en webbutik. [6]

Natos cyberövning Cyber Coalition arrangerades vid månadsskiftet november-december. Övningen är en del av den kontinuerliga beredskapen för incidenter som gäller hela samhället och som görs med både nationella myndigheter och internationella parter. [7]

Guiden Beredskap för störnings- och krissituationer, som riktar sig till hela befolkningen, publicerades på webbplatsen Suomi.fi. Guiden omfattar ett avsnitt om hur man kan förbereda sig för cyberangrepp och -störningar. Inrikesministeriet genomförde guiden tillsammans med Myndigheten för digitalisering och befolkningsdata MDB och ett omfattande samarbetsnätverk. [8]

Allmän översikt över cybersäkerheten i november

- November visade hur viktigt beredskap är när det i Finland förekom två mycket olika incidenter i det digitala samhället. I början av vecka 47 rapporterades det om ett avbrott i undervattenskabeln C-Lion1 mellan Finland och Tyskland och senare under samma vecka kom det en kraftig Jyri-storm från söder till Finland. [9]
  - Tisdagen den 11 november arrangerade Traficom tillsammans med andra myndigheter och Cinia, som äger C-Lion1-kabeln, ett informationstillfälle om sjökabelavbrottet. Kabelavbrottet hade inte några synliga konsekvenser för Finlands telekommunikationsförbindelser till andra länder och samhällets försörjningsberedskap äventyrades inte. Centralkriminalpolisen undersöker kabelavbrottet.
  - Under stormen Jari i november var tiotusentals hushåll utan el i Finland. Långvariga elavbrott kan orsaka problem till exempel i mobilförbindelser.
  - Allt som allt är det finländska samhällets resiliens på god nivå. Trots detta kan störningar ha ganska kortvariga lokala konsekvenser för telekommunikationsförbindelser.
- November har beskrivits som årets gråaste månad och dessutom har den präglats av bedrägeri- och nätfiskekampanjer i olika bankers namn. En avsevärd andel av bedrägeritrafiken för nätfiske efter bankkoder skickas fortfarande per textmeddelande.
  - Även i de anmälningar som Cybersäkerhetscentret har fått om M365-nätfiske syntes Dropbox som tema och en del avdem har lett till dataintrång.
  - Vi har regelbundet tagit emot anmälningar om cybersäkerhetsincidenter gällande hotell- och resebokningstjänster som även lett till ekonomiska förluster. Till exempel i Finland pågår flera olika bedrägerisätt runt temat Booking.com. Vi publicerade en Informationssäkerhet nu!-artikel om ämnet vid början av november. [10]
- För överbelastningsangrepp har situationen blivit lugnare och jämfört med hösten har centret fått färre anmälningar om störningar som de medfört.

Trenderna inom cybersäkerhet
de gångna 12 mån.