TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädret

Oktober 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 helhetsbild av vad som har hänt och vad som kommer att hända på cybersäkerhetsfältet.

Cybervädret kan vara:  lugnt  oroande  allvarligt

Månadens nyckeltal

Transport- och kommunikationsverket Traficom har delat ut 6 miljoner euro i stöd för utveckling av informationssäkerheten. Stöd delades ut till 313 företag som är vitala för samhället i Finland. De beviljade stödbeloppen varierar från 371 euro till 100 000 euro.

Vid slutet av oktober hade Cybersäkerhetscentret fått kännedom om 16 incidenter om utpressningsprogram i Finland i år. Antalet under motsvarande tidpunkt år 2023 var 25. I genomsnitt får Cybersäkerhetscentret årligen cirka 40 anmälningar om utpressningsprogram.

Cybervädret i oktober 2024

Dataintrång och dataläckor

- Sårbarheten i FortiManager ledde till dataintrång även i Finland.
- M365-konton hackades igen med ett nytt aktivt nätfisketema där offret fick ett meddelande om att lösenordet håller på att gå ut.
- I oktober rapporterades om intrångsförsök gällande low&slow som varade flera månader och där inloggningsförsök görs med liten volym över en lång tidsperiod.

Bluff och nätfiske

- En aggressiv SMS-nätfiskekampanj började vid slutet av oktober i olika aktörers namn. Som SMS-avsändarnamn fanns både korrekta och inkorrekta varianter av Terveystalo, Traficom, Fortum och Mehiläinen.
- Myndigheters och internettjänsteleverantörers samarbete har gjort det möjligt att radera bedrägliga nätfiskesidor från nätet då de fiskar efter bankkoder.

Skadeprogram och sårbarheter

- Fortinet har publicerat korrigeringar till en kritisk sårbarhet i FortiManger-produkten som varit utsatt för aktivt utnyttjande.
- Man ska se till att informationssäkerheten i utrustning i hemmen är i ordning. Sårbar nätverksutrustning kan användas till exempel för överbelastningsangrepp.

Automation och IoT

- På sistone har man observerat flera cybersäkerhets-angrepp och -problem där man har utnyttjat osäkra IoT-apparater för hemmet.
- NIST har publicerat en rapport om begränsningar för att ta i drift IoT-apparater.
- Den heltäckande rapporten motsvarar till stora delar också Cybersäkerhetscentrets observationer.

Nätens funktion

- I oktober observerades sju funktionsstörningar i allmänna kommunikationsnät, av vilka alla förutom en var lindriga.
- Överbelastningsangrepp anmäls fortfarande mer aktivt än i början av året men läget har blivit lugnare sedan september.

Spionage

- APT-grupper som associerats med Ryssland försöker spionera statsförvaltningens och försvarsbranschens objekt i Europa och USA samt i Ukraina.
- En kinesisk aktör gjorde ett intrång i teleoperatörers system i USA för att få information om valet. Intrånget riktades speciellt mot teleavlyssningssystem.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Cybersäkerhetscentret publicerade en artikel om sörja för domännamnens giltighet. Domännamn utgör en avsevärd immateriell egendom som kan äventyra informationssäkerheten om den hamnar i fel händer.

Traficom uppdaterade det nationella dokumentet om kryptografiska krav av konfidentiatlitet genom att foga kvantsäkra algoritmer i de nationella kriterierna. Nyckelgeneratoralgoritmen ML-KEM och signaturalgoritmerna ML-DSA och SLH-DSA som standardiserats av NIS godkänns för nationell användning. Traficom rekommenderar att organisationerna tar i bruk de kvantsäkra algoritmerna så snart som möjligt.

Statsrådets session godkände den reviderade nationella cybersäkerhetsstrategin. I strategin anges att cybersäkerheten är en bestående del av den övergripande säkerheten där vitala samhällsfunktioner sköts i samarbete med myndigheter, näringslivet, organisationer och medborgare.

Cybersäkerhetscentret rekommenderar att medborgarna tar flera metoder för stark autentisering i bruk. På så sätt är tillgången till tjänster som kräver elektronisk identifiering inte beroende av en enda aktör.

Allmän översikt över cybersäkerheten i oktober

- I oktober konstaterades att antalet cyberincidenter som anmälts till Cybersäkerhetscentret hade ökat efter en något lugnare början av hösten.
- I höstvädret har det förekommit tillfälliga regnmoln samt grådask mot finländska organisationer på grund av olika nätfiske- och bedrägerikampanjer som kommit via e-post och textmeddelanden. Speciellt M365-kampanjer har i en del av fallen lett till dataintrång.
  - Textmeddelandebedrägerier skickas under användarnamn som verkar vara både falska och genuina. Cybersäkerhetscentret rekommenderar att alla organisationer som skickar textmeddelanden skyddar sitt SMS Sender ID så snart som möjligt.
  - Vid början av oktober fick tiotusentals finländare ett varningsmeddelande av polisen. I meddelandet berättades att personen som mottagit meddelandet har en ökad risk att bli föremål för brottslingars intresse. Bakgrunden till varningsmeddelanden är en databas som polisen har tagit över av brottslingar. På listorna har funnits namn och telefonnummer för finländare samt födelsetid för vissa av dessa personer.
  - Cybersäkerhetscentret delar information om pågående bedrägerikampanjer till exempel i Veckoöversikten och i Informationssäkerhet Nu! -artiklar.
- Överbelastningsangreppen fortsatte aktivt på samma sätt som i föregående månad. Angreppen riktades fortfarande speciellt mot olika banker inom finanssektorn.

Top 5-cyberhot i den närmaste framtiden (6 månader– 2 år)

1.

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.

2.

Utpressningsprogram - Betydande hot mot organisationer

Under det senaste året har flera organisationer i Finland drabbats av ett utpressningsprogram, och antalet ökar kontinuerligt också globalt.

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.

Skyddet av kommunikationsinfrastruktur blir allt viktigare

Skyddet av kommunikations- och systeminfrastruktur är viktigt utomlands och i Finland, både på grund av de skador och naturfenomen som de blir utsatta för samt på grund av avsiktliga störningar orsakade av utomstående.

Trenderna inom cybersäkerhet
de gångna 12 mån.