TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädret

Januari 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 januari 2024

Dataintrång och dataläckor

- Dataintrång i M365-konton ökade i början av året. Intrången gjordes till exempel genom nätfiskemeddelanden med säker e-post som tema.
- Vi fick flera anmälningar om inloggningsförsök till VPN-tjänster, en del av försöken ledde till att datorn smittades av utpressningsprogrammet Akira.

Bluff och nätfiske

- Intrång i e-postkonton gick från en organisation till annan med hjälp av nätfiskemeddelanden med säker e-post som tema.
- I förfalskade textmeddelanden som verkade komma från polisen hotade man med böter för fortkörning.
- Bedrägerimeddelanden som skickats i MinSkatt-tjänstens namn fortsatte mycket rikligt även i januari.

Skadeprogram och sårbarheter

- Det fanns kritiska och utnyttjade sårbarheter i Ivantis produkter.
- Sårbarheten Cisco Anyconnect har utnyttjats som ett led för utpressningsprogrammet Akira att göra intrång.
- Under januari publicerades fem och i början av februari två meddelanden om kritiska sårbarheter.

Automation och IoT

- I seminariet Kyberala murroksessa (Cybersektorn i förändring) berättade man om nuläget för cyberregleringen.
- Skadliga program som smittar IoT-enheter är populära hos cyberbrottslingar från år till år. Brottslingar skapar nya botnät med nya egenskaper speciellt på basis av källkoden för Mirai.

Nätens funktion

- I januari förekom det 3 störningar i allmänna kommunikationstjänster.
- Överbelastningsangrepp som begåtts av hacktivister fortsätter.
- Organisationer förbereder sig, skyddar sig och avvärjer överbelastningsangrepp på bra rutin.

Spionage

- Microsoft berättade om ett angrepp som Midnight Blizzard gjort mot Microsofts molntjänster.
- Angreppet gjordes också mot Microsofts andra kundorganisationer.
- Angriparen hade som mål att söka information bland annat om beslutsfattarnas och cybersäkerhetsexperternas e-poster.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Seminariet Kyberala murroksessa (Cybersektorn i förändring) ordnades 23.1.2024. Inspelningen av evenemanget publiceras så snart som möjligt på Traficoms YouTube-kanal. Presentationsmaterial har publicerats på seminariets programsida.

Ansökan om stöd för finansiering av moderna cybersäkerhetslösningar och -innovationer i små och medelstora företag är öppen t.o.m. 1.3.2024. Det totala understödsbeloppet är 1,5 miljoner euro. Finansieringsstöd kan beviljas högst 600 000 euro per projekt.

Vi publicerade en Informationssäkerhet Nu! -artikel *Valet tryggas genom myndighetssamarbete*. Cybersäkerhetscentret är med och stöder justitieministeriet och andra valmyndigheter i förberedelserna och beredskapen för de nationella valen.

Informationssäkerhet i smarta enheter blir bättre genom reglering fr.o.m. 1.8.2024 när obligatoriska informationssäkerhetskrav för trådlösa apparater börjar tillämpas.

Allmän överskit över cybersäkerheten i januari

- Överbelastningsangreppen fortsätter också år 2024. Tiotals inhemska organisationer har listats som föremål för överbelastningsangrepp för rysksinnade hacktivistgrupper i början av 2024.
  - Helt nya föremål på listorna har under början av året funnits till exempel från kommun- och utbildningssektorer.
  - Förra året var speciellt finans-, logistik- och transportsektorn samt aktörerna inom statsförvaltningen populära föremål.
- I början av året har flera kritiska sårbarheter offentliggjorts.
  - Ett exempel är kritiska sårbarheter i Ivantis produkter, som även används i stor utsträckning i Finland.
- Organisationernas aktiva delning av information ökar andra organisationers förmåga att skydda sig mot digitala hot. Cyberhotet som en organisation möter kan följande dag drabba en annan organisation. Öppen och aktuell delning av information minimerar konsekvenser och kostnader av hoten. Att lära sig av andra är också kostnadseffektivt när man inte behöver återupptäcka samma sak som redan används på annat håll.

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

1.

Hotnivån mot Finlands cybermiljö har blivit förhöjd.

Antalet riktade angrepp har ökat. Betydelsen av organisationernas beredskap ökar på grund av den förhöjda hotnivån.

2.

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.

3.

Informationssäkerheten och kontinuiteten i leverans- och servicekedjor är allt mer kritiska.

Att förstå underleveranskedjor 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.

Cybersäkerheten är beroende av experter och cybersäkerhetskunskaper är viktiga för alla!

Ny reglering och det faktum att cybersäkerhet smälter samman med företagens dagliga funktioner ökar allt mer behovet av olika experter. Även med tanke på riskhanteringen och kontinuiteten är det viktigt för organisationerna att säkerställa tillräcklig kompetens under alla årstider.

Trenderna inom cybersäkerhet
de senaste 12 mån.