TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

Mars 2020

#cyberväder berättar om betydande säkerhetsincidenter och -fenomen under månaden. Den här produkten är primärt avsedd för informationssäkerhetsansvariga. Läsaren får en snabb helhetsbild av vad som hänt på cybersäkerhetsfältet under perioden i fråga. Läget kan vara:

lugnt

oroande

allvarligt

Cybervädret mars 2020

Dataintrång och dataläckor

- Antalet anmälda Office 365–dataintrång minskade något.
- Kundsystemet Kanta blev utsatt för flera dataläckor, och även finländska personers uppgifter hamnade i fel händer.

Bedrägerier och nätfiske

- Bedrägerier under coronatemat har gällt försäljning av obefintliga skydd och tester.
- Bluffsamtal från tekniskt stöd upphörde helt 24.3.

Skadliga program och sårbarheter

- Se till att de åtgärder som möjliggör distansarbete inte äventyrar företagsnätets informationssäkerhet.
- COVID-19-temat används mycket för spridning av skadligt innehåll.

Automation

- Antalet automationsmiljöer som är öppna mot internet ökar. Fjärruppkoppling ska öppnas först efter en omsorgsfull analys.

Nätverkens funktion

- Kommunikationsnäten har fungerat bra trots ökat distansarbete och distansstudier.
- En del av överbelastningsangreppen hade indirekta verkningar även bl.a. för funktion av distansförbindelser.

Spionage

- Coronavirustemat utnyttjas också vid cyberspionage.
- Ouppdaterade system är ett attraktivt mål också för APT-grupperna.

Top 5 cyberhot - betydande långsiktiga fenomen

1

Utnyttjandet av sårbarheter blir snabbare, vilket kräver snabba uppdateringar. Apparater och tjänster vars datasäkerhet inte har beaktats lämnas öppna på nätet och skyddsåtgärderna samt underhållet är bristfälliga.

2

Nätfiske är väldigt vanligt och mottagaren kan ha svårt att upptäcka att det är fråga om ett bedrägeri. Detta utnyttjas också i riktade attacker och spionage.

3

Utpressningsangrepp med omfattande konsekvenser hotar affärsverksamhetens kontinuitet. Skadorna i enskilda fall har ökat till tiotals miljoner euro.

4

En otydlig ansvarsfördelning mellan tjänsteleverantören, underleverantörerna och beställaren försämrar hanteringen av datasäkerheten. Brister i kontrollen av loggar gör det svårare att upptäcka hot.

5

Organisationer kan inte hantera sina cyberrisker. Man kan inte förutse hur hoten påverkar verksamheten och därför underskattas riskerna. Det finns brister i återhämtningsplanerna.

Corona-extra

För mars månaden har Cybersäkerhetscentret också utarbetat ett särskilt cyberväder med de viktigaste coronatemana. Cybervädret om Corona publiceras som en del av cybervädret men är inte ett permanent avsnitt.

Cybervädret för corona mars 2020

Dataintrång och dataläckor

- Eventuella fördröjda uppdateringar kan medföra dataintrång och dataläckor.
- Social- och hälsovårdsbranschen är ett globalt mål för brottslingar, eftersom den är en kritisk aktör under coronavirusutbrottet.

Bedrägerier och nätfiske

- Cybersäkerhetscentret har hittills fått ganska få anmälningar om bedrägerier och nätfiske som utnyttjar corona.
- Olika spammeddelanden med corona som tema skickas till såväl privatpersoner som företag.

Skadliga program och sårbarheter

- Sjukhus och laboratorier runtom i världen har rapporterat om utpressningsprogram.
- Även andra samhällskritiska aktörer kan vara ett intressant mål för brottslingar.

Automation

- Fördröjda uppdateringar och ändringsarbeten kan bidra till dataintrång och spridning av skadliga program.
- Här ska man också se till att det finns tillgång på egen eller samarbets-parters personal till exempel för installationer eller uppdateringar.

Nätverkens funktion

- Trots ökat hemarbete räcker de finländska kommunikationsnätens kapacitet för elektronisk ärendehantering och distansarbete.

Spionage

- De som spionerar utnyttjar också coronatemat för sina angrepp.
- Världshälsoorganisationen WHO har varit utsatt för flera avancerade cyberkampanjer.

Top 5 coronarelaterade cyberhot - betydliga fenomen över en längre period

1

Sårbarheter kan inte uppdateras tillräckligt snabbt, om tjänsteleverantörers eller organisationers resurser minskar. Cybersäkerhetscentret har sedan länge observerat att brottslingar allt snabbare börjar utnyttja sårbarheter.

2

Nätfiske och bedrägerier som utnyttjar coronatemat kommer antagligen att öka och få nya former när epidemin sprider sig också i Finland. För att kunna avvärja hotet är det viktigt att ge anvisningar för personalen.

3

Omfattande utpressningsangrepp är ett stort hot, speciellt för kritiska aktörer. Brottslingarna upplever sannolikt att virusutbrottet ökar organisationernas vilja och förmåga att betala lösensumman.

4

Personalbrist är möjlig under de kommande veckorna när risken för smitta ökar. Senast nu ska man tänka på hur man kan trygga tillgången till kunnig personal – såväl på distans som på plats.

5

Överbelastningsangrepp. Internetsidor med många besök är enkla föremål för brottslingar. Om information inte finns tillgänglig via officiella källor kan en del av människorna söka information någon annanstans på internet eller i sociala medier, vilket ökar möjligheten att falla för bedrägerier och disinformation.

Vad kan du göra för att förbättra din cybersäkerhet?

1

Håll dina apparater uppdaterade. En dator eller en annan apparat påminner i allmänhet om tillgängliga uppdateringar genom att visa ett skrivbordsmeddelande. Skjut inte upp installation av de tillgängliga uppdateringarna.

2

Använd olika lösenfraser i olika system. Använd inte samma användarnamn och lösenord för arbetsplatsens system och användarkonton som du använder till exempel för näthandel eller inloggning på din fritids-e-post.

3

Kontrollera vilka tjänster och applikationer du använder. Om du inte använder en applikation kan du avlägsna den. Se också till att dina konton för sociala medier har korrekta integritetsinställningar.

4

Använd betrodda och skyddade nät. Om du arbetar på distans och använder ett trådlöst lokalnät, dvs. WLAN eller WiFi, se till att nätet är lösenordsskyddat. I stället för ett främmande nät ska du använda till exempel nätförbindelsen för din telefon. Använd gärna WLAN för distansarbete för att undvika belastningen i telefonnätet.

5

Ta säkerhetskopior. Ibland är det värt att flytta data från apparaten till en annan plats. Om apparaten drabbas av fel finns uppgifterna sparade och de kan återställas. Så kan du till exempel behålla dina foton, om telefonen går sönder.