STYRKET INDSATS MOD ØKONOMISK IT- KRIMINALITET

Hovedpunkter i politiets strategi for indsatsen mod økonomisk it-kriminalitet frem mod 2020

POLITI

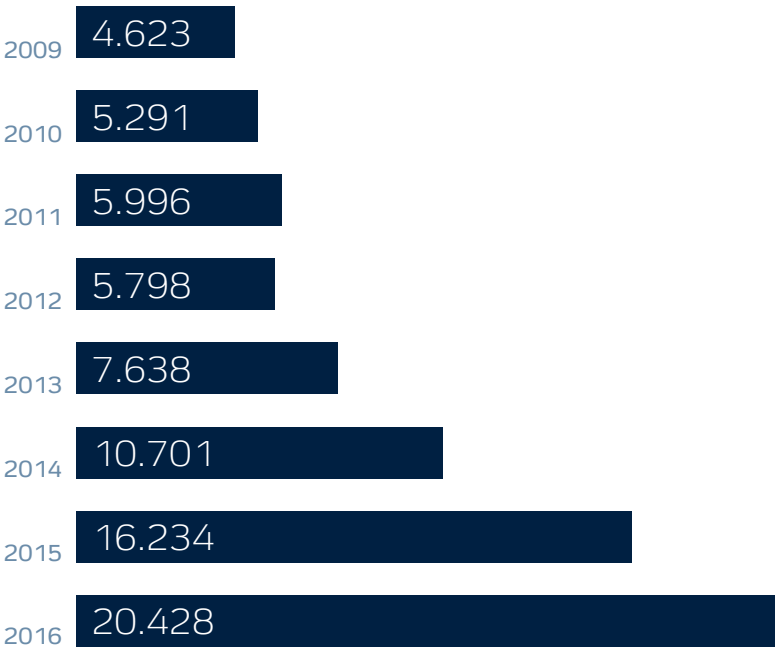
FLERE SAGER OG EN NY KOMPLEKSITET

Den økonomisk kriminalitet, som bliver begået ved brug af it og mod it-systemer, er stigende. Både antallet af sager, deres kompleksitet og de kriminelles tekniske muligheder for at skjule deres identitet udfordrer politiets muligheder for at forebygge og bekæmpe kriminaliteten.

Økonomisk it-kriminalitet er et strategisk prioriteret område i politiet. Frem mod 2020 vil vi arbejde mere analytisk og derved blive mere effektive i vores forebyggelses- og efterforskningsindsats.

Vi skal opklare flere sager om økonomisk it-kriminalitet, og risikoen for at blive offer for økonomisk it-kriminalitet skal reduceres. Vi vil gå efter dem, der skader flest, og i den forbindelse fokusere særligt på de gerningspersoner, der har begået mange forhold.

Figur 02 Databedrageri, bedrageri med stjålne dankort, øvrige kontokort samt tyveri fra pengeautomat

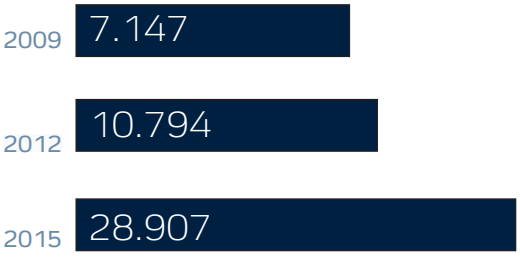


Kilde: Rigspolitiet

78%

– så mange føler sig utrygge over for risikoen for at få stjålet og misbrugt betalingsoplysninger og andre oplysninger på nettet ifølge Forbrugerrådet TÆNK

Figur 01 Antal anmeldelser af bedrageri (samlet)



Kilde: Rigspolitiet

Økonomisk it-kriminalitet bliver på nuværende tidspunkt ikke registreret selvstændigt, men registreres bl.a. som bedrageri og databedrageri. Derfor er det ikke muligt at sige noget om den præcise udvikling i antallet af anmeldelser på området. Men når man ser på alle anmeldelser om f.eks. bedrageri, er der en tydelig stigning i anmeldelser siden 2012. Økonomisk it-kriminalitet er formentlig en af hovedårsagerne til denne stigning.

Økonomisk it-kriminalitet kan antage mange forskellige former, f.eks. falske netbutikker, hacking eller overbelastningsangreb mod en hjemmeside (DDOS) med henblik på afpresning.

Økonomisk it-kriminalitet – og it-kriminalitet generelt – er kendetegnet ved, at kriminaliteten kan overskride by- og landegrænser. Den kan finde sted, uden at offer og gerningsmand har nogen kontakt – og uden et gerningssted i traditionel forstand.

I perioden 2009-2016 er antallet af anmeldelser om databedrageri, tyveri fra pengeautomat mv. steget med

350%

EFFEKTIV EFTERFORSKNING

Efterforskningen af økonomisk it-kriminalitet udfordres især af, af der er tale om et stort antal sager, og sager hvor gerningspersonerne kan være svære at identificere. Digitale spor og kriminalitet via digitale enheder skaber både muligheder og udfordringer, som kræver særlige kompetencer. Herudover kræver kriminalitetsformen et bredt samarbejde internt i politiet og med vores offentlige og private samarbejdspartnere – også internationalt.

Politiet skal i efterforskningen af økonomisk it-kriminalitet have særligt fokus på opklaringen af gentagen økonomisk it-kriminalitet, herunder serieforbrydelser, centrale bagmænd og organiserede forbrydelser. Derfor retter vi især opmærksomheden mod monitering, analyse og vidensdeling på tværs af hele Danmark.

STØRRE MODSTANDS-DYGTIGHED OVER FOR IT-ANGREB

Ofre for økonomisk kriminalitet er ikke altid klar over, at de er eller har været udsat for et it-angreb. Politiet skal derfor blive endnu bedre til at advare og informere både borgere og virksomheder om it-rettede angreb.

22%

– så mange undlader at handle på nettet af frygt for brud på deres sikkerhed ifølge Danmarks Statistik

Politiet skal i stigende grad forstyrre mulige eller igangværende it-angreb. Desuden skal vi påvirke borgernes og virksomhedernes adfærd, så de bliver mindre sårbare over for økonomisk it-kriminalitet.

Jo hurtigere politiet kan gribe ind og forstyrre og bremse disse 'angreb', desto færre ofre og potentielle skadevirkninger vil angrebene medføre. Vi skal derfor hurtigst muligt kunne iværksætte relevante tiltag og videregive nødvendige informationer, når nye trends og kriminalitetsbølger opdages.

MERE VIDEN OG BEDRE DATA

Alle anmeldelser tæller. Uden en anmeldelse kan politiet ikke efterforske den enkelte sag. Samtidig bidrager alle anmeldelser til at kunne afdække sammenhænge mellem gerningsmænd, trends og modus i de enkelte sager. For politiet er det derfor vigtigt at monitere og registrere alle forhold, og derfor har vi brug for, at borgere, der har været udsat for økonomisk it-kriminalitet, anmelder det til politiet.

53.000

– så mange sager om misbrug med dankort på internettet var der mindst i 2016 ifølge tal fra Nets

Det er vores forventning, at antallet af anmeldelser for økonomisk it-kriminalitet kommer til at stige markant i strategiperioden. Det er et strategisk mål i sig selv, at flere forurettede vil vælge at anmelde det til politiet, hvis de har været udsat for økonomisk it-kriminalitet, så vi i politiet kan analysere på et mere fyldestgørende billede af den samlede datamængde.

Vi vil retsforfølge flere gerningspersoner især serieforbrydere

OVERSIGT OVER STRATEGIENS MÅL OG INDSATSER

STRATEGISK MÅL

Politiet vil forebygge og bekæmpe kriminalitet, der udnytter den stigende digitalisering i samfundet til uberettiget økonomisk vinding

NATIONALE MÅLSÆTNINGER

At opklare flere sager om økonomisk it-kriminalitet

At reducere risikoen for at blive offer for økonomisk it-kriminalitet

NATIONALE OG LOKALE INDSATSER

Styrke den effektive efterforskning mod gerningspersoner – også på tværs af politikredse

Forebygge it-angreb og øge borgeres og virksomheders modstandsdygtighed over for it-angreb

Intensivere politiets muligheder for at forstyrre de kriminelle, begrænse skader og gøre det sværere at begå økonomisk it-kriminalitet

Opbygge mere viden og bedre datakvalitet – både ved hjælp af bedre grundregistrering og via eksterne samarbejder