SAMARBEJDE MELLEM POLITIET OG VIRKSOMHEDERNE MOD CYBERKRIMINALITET

Indhold

DET PRIMÆRE SIGTE MED SKYT ER IKKE EFTERFORSKNING OG RETSFORFØLGNING AF IT-KRIMINELLE, MEN FOREBYGGELSE, HINDRING AF IT-KRIMINALITET OG SKADESBEGRÆNSNING FOR DERVED AT MINDSKE OMFANGET AF IT-ANGREB RETTET MOD VIRKSOMHEDERNE.

Om samarbejdet

For at Danmark som samfund kan være i stand til at dæmme op for IT-kriminalitet og nedbringe omfanget af IT-angreb, er der behov for et samarbejde mellem virksomheder og politiet.
Et samarbejde hvor virksomheder sammen med politiet indgår i dialog og erfaringsudveksling om forebyggelse og hindring af angreb mod virksomhedens IT-systemer, samt hvordan man lettest håndterer følgerne af IT-angreb.
Rigspolitiet, Nationalt Cyber Crime Center (NC3), har derfor taget initiativ til etablering af samarbejdet NC3SKYT, der etablerer rammerne for, at især små og mellemstore virksomheder i fortrolighed kan rette henvendelse til politiet om IT-angreb m.v. uden at oplysningerne derved nødvendigvis skal kunne læses i en døgnrapport, indgå i en efterforskning eller i en åben retssag.

Baggrund

- Der er en hastig stigning i IT-kriminalitet, og de IT-kriminelle udnytter stadig mere avancerede teknologier og sociale mekanismer.
- De fleste virksomheder har været tilbageholdende med at informere Politiet ved IT-angreb.
- Politiet har derfor i dag kun begrænset indsigt i omfanget af IT-angreb, disses konsekvenser for virksomhederne og dermed også kun i nogen grad kendskab til angrebsniveau og de metoder, der bliver brugt i forbindelse med angreb.

Den sårbare målgruppe

Det vurderes, at mindre og mellemstore virksomheder kan være særligt sårbare overfor IT-kriminalitet. Dette skyldes, at de IT-kriminelle ved, at;

- mindre og mellemstore virksomheder ofte vil være mere økonomisk sårbare end større virksomheder.
- mange af de mindre og mellemstore virksomheder har mindre fokus på IT-sikkerhed og IT-kriminalitet og er ikke altid tilstrækkeligt nok informeret om trusselsbilledet.
- små og mellemstore virksomheder ofte ikke har afsat tilstrækkeligt med menneskelige og økonomiske ressourcer til IT-sikkerhed.

SOM BETROET PARTNER I NC3 FÅR MAN BL.A. ADGANG TIL EARLY WARNINGS FRA NC3, FBI OG EUROPOL, ET FORTROLIGT FORUM OG REGIONALE OG NATIONALE KONFERENCER.

Gevinster ved samarbejdet

Med NC3SKYT tilsigtes at opnå bedre vidensdeling, der skal føre til højnelse af den generelle IT-sikkerheds-awareness i virksomhederne. Det er ønsket, at dette kan føre til, at virksomheder bliver bedre til at beskytte sig mod angreb og bedre rustet til at håndtere de negative effekter af eventuelle angreb på virksomhedens IT-systemer.

- Politiet, vil i kraft af henvendelserne fra virksomhederne, få et større indblik i omfanget af angreb på virksomheders IT-systemer og særligt et mere detaljeret indblik i, hvilken type af angreb der aktuelt er de mest fremherskende.
- På grundlag af indsamlet information fra samarbejdet, vil politiet kunne foretage en early warning af virksomhederne i NC3SKYT om nye typer angreb og eventuelt angive URL-adresser, der anbefales blokeret i virksomhedens firewall.

- Det internationale samarbejde mod malware styrkes. Prøver på malware fra virksomhedernes IT-systemer bliver delt med Europol med henblik på at indgå i fælleseuropæiske analyser af malware-typer, hvis resultater ligeledes kan deles med virksomhederne.

DE OPLYSNINGER, SOM NC3SKYT MODTAGER I DET FORTROLIGE NETVÆRK, VIL BLIVE ANVENDT I FORBINDELSE MED UDARBEJDELSE AF NATIONALE, REGIONALE OG BRANCHESPECIFIKKE TRUSSELSVURDERINGER.

Deltagere i NC3SKYT har adgang til følgende:

- Lokale møder bl.a. i regi af lokale erhvervsråd og Dansk Industri's regionalforeninger om aktuelle trusler og relevante modforanstaltninger.
- Fortroligt forum for erfaringsudveksling af oplysninger om IT-angreb, statistikker om IT-angreb med henblik på virksomhedens risikovurdering mv.
- Modtagelse af mails udsendt af NC3 om nationale og internationale trends, early warnings mv. som kan indeholde oplysninger om forskellige typer af malware, ransomware mv. udarbejdet af NC3, Europol og FBI. Mulighederne for etablering af et lukket site på internettet for deltagerne overvejes i NC3.
- Nationale og regionale konferencer om aktuelle emner

Indsigt

- De oplysninger, som NC3SKYT modtager, vil blive anvendt af NC3 i forbindelse med udarbejdelse af trusselsvurderinger etc.
- Deltagere får indsigt i FBI bulletiner, men FBI vil ikke få indsigt i deltagernes forhold, og der flyder således ingen data fra NC3SKYT til FBI om de deltagende virksomheder.
- NC3SKYT vil ikke få mere indsigt i virksomhederne eller deltageren end i det omfang, deltagerne vælger at dele oplysninger med NC3SKYT. Deltagerne vil ikke få tilgang til hinandens sager, men er velkomne til at diskutere dem indbyrdes.

Organisation og praktik

NC3 varetager i samråd med et Advisory Board den overordnede nationale og strategiske styring af NC3SKYT, men samarbejdet er imidlertid forankret og drevet lokalt i de enkelte politikredse. I den forbindelse spiller politikredsenes IT-ingeniører en central rolle i forhold til kommunikation med virksomhederne om IT-angreb mv.

POLITIKREDSENES IT-INGENIØRER SPILLER EN CENTRAL ROLLE I FORHOLD TIL KOMMUNIKATIONEN MED VIRKSOMHEDERNE OM IT-ANGREB MV.

Deltagelse

For at deltage som "betroet partner" i NC3SKYT, er det en betingelse at man udfylder en blanket om tavshedspålæg og samtykkeerklæring. Den udfyldte blanket giver politiet lov til at indhente relevante oplysninger i Kriminalregisteret samt i politiets øvrige registre. Derudover accepterer man ved sin underskrift et tavshedspålæg i forhold til kendskab til fortrolige oplysninger, eventuel adgang til materiale, som er klassificeret til "TIL TJENESTEBRUG", "For Trusted Partners" eller på anden måde er klassificeret, samt viden om hemmelige efterforskningsmetoder.

Blanketten kan man få udleveret ved at rette henvendelse til sin lokale IT-ingeniør (se kontaktinformation sidst i dokumentet). Den udfyldte blanket sendes til Rigspolitiet, NC3, som varetager screening af deltagerne i samarbejdet samt beslutning om optagelse på listen over betroede partnere.

Du kan sende en krypteret e-mail til NC3 ved at installere certifikatet tilhørende pol-nc3@politi.dk i dit e-mailprogram og benytte digital signatur i forbindelse med afsendelsen af mailen. Certifikatet kan fremsøges og downloades på NemID's hjemmeside: https://service.nemid.nu/dk-da/support/soeg_certifikat/ (skriv "pol-nc3@politi.dk" i søgefeltet) og klik herefter på "Hent certifikat", vælg "Åbn" og derefter "Installer certifikat".

Når du har installeret certifikatet, skal du vælge at kryptere din e-mail, inden du sender den.

Det bemærkes, at for at politiet skal kunne svare dig per e-mail, skal du også signere e-mailen med din egen digitale signatur. Læs mere om digital signatur på NemID's hjemmeside: https://www.nemid.nu/dk-da/digital_signatur/

Screening af deltagere

Alle kan i princippet deltage, men under hensyntagen til karakteren af det samarbejde, der lægges op til, vil der ske en screening af deltagerne. Det er således en forudsætning for deltagelse i samarbejdet, at Rigspolitiet forinden kan vurdere, at de pågældende repræsentanter for virksomhederne kan betragtes som "betroet partner". Dette skyldes bl.a. at deltagerne efterfølgende vil få adgang til FBI bulletiner, der er klassificeret "For Trusted Partners". Det er virksomheden som sådan, der er med i samarbejdet, men kontaktpunktet er den person, som virksomheden vælger at få screenet.

ET STÆRKT SAMARBEJDE MELLEM POLITIETS NC3 OG ERHVERVSLIVET VIL HJÆLPE TIL AT DÆMME OP FOR IT-KRIMINALITET - TIL GAVN FOR ALLE

Advisory Board

Advisory Board'et i NC3SKYT varetager den overordnede nationale og strategiske styring af NC3SKYT. Har man spørgsmål til deltagelse, kan man kontakte enten en af boardets medlemmer eller kontaktpersonen i den politikreds, man tilhører.

Advisory Boardet:

- Sikkerhedskonsulent Thomas Bach – M Networks A/S
  E-mail: tb@mnetworks.dk
- CEO Jacob Isaksen – Avian Digital Forensics
  E-mail: jis@avian.dk
- CEO Lennart Meineche, Brancheforeningen for IT-hostingvirksomheder i Danmark
  E-mail: lm@bfih.dk
- CEO Mette Nikander – C-Cure
  E-mail: mn@c-cure.dk
- Chefkonsulent Henning Mortensen – DI
  E-mail: hem@di.dk
- Centerchef Kim Aarenstrup – NC3
  E-mail: kaa006@politi.dk

Politikredsenes kontaktpersoner

Nordjyllands Politi:
It-ingeniør Johnny Vestergaard
Telefon: +45 22697793
E-mail: jve004@politi.dk

Midt- og Vestjyllands Politi:
IT-ingeniør Nicolai Frydenlund Larsen
Telefon: +45 22697792
E-Mail: nla013@politi.dk

Østjyllands Politi:
IT-ingeniør Simon Sørensen
Telefon: +45 41731493
E-mail: sso024@politi.dk

Sydøstjyllands Politi:
IT-ingeniør Jesper Frank Mørup
Telefon: +45 22697789
E-mail: jmo046@politi.dk

Syd- og Sønderjyllands Politi:
IT- ingeniør Michael Nielsen
Telefon: +45 22697791
E-mail: mni063@politi.dk

Fyns Politi:
IT-ingeniør Mathias Grund Sørensen
Telefon: +45 22697794
E-mail: mso058@politi.dk

Nordsjællands Politi:
IT-ingeniør Kim Havnemark Rasmussen
Telefon: +45 22697790
E-mail: kra035@politi.dk

Midt- og Vestsjællands Politi:
IT-ingeniør Anders Sabinsky Tøgern
Telefon: +45 41731497
E-mail: ato008@politi.dk

Sydsjællands og Lolland-Falsters Politi:
IT-ingeniør Peter Alexander Rasmussen
Telefon: +45 41910468
E-mail: pra026@politi.dk

Københavns Vestegns Politi:
IT-ingeniør Thomas Karnøe Sørensen
Telefon: +45 41731496
E-mail: tso023@politi.dk

Københavns Politi:
IT-ingeniør Claus Urbanek Hansen
Telefon: +45 41731498
E-mail: cha030@politi.dk