CENTER FOR CYBERSIKKERHED

15. februar 2015
CN

Varsling om skærpet opmærksomhed vedrørende risiko for defacement af og DDoS mod hjemmesider m.v.

Der har været skudepisoder den 14. februar 2015 og natten til den 15. februar 2015 i København. Politiet efterforsker skudepisoderne som terrorhændelser.

Erfaringsmæssigt efterfølges sådanne hændelser af forskelige former for cyberangreb. Der er ofte tale om simple defacements af eller DDoS-angreb mod statslige og ikke-statslige hjemmesider, herunder mediehjemmesider. Der er med andre ord tale om simple angreb, der kan iværksættes uden nævneværdig forberedelse.

Defacements er en angrebstype, hvor hele eller dele af en hjemmeside erstattes med slagord til støtte for en sag. DDoS er en angrebstype, hvor en hjemmeside overvældes af forespørgsler, som derved forhindrer legitime brugeres adgang til hjemmesiden.

Opmærksomheden henledes på, at der som følge af hændelserne i København er risiko for, at danske hjemmesider og andre internetvendte tjenester kan blive forsøgt angrebet som led i en politisk tilkendegivelse. På samme vis kan der være risiko for, at myndighedens eller virksomhedens konti på sociale medier, så som Twitter og Youtube, forsøges overtaget ved at gætte kodeordet eller ved at forsøge at lokke kodeordet ud af myndighedens eller virksomhedens medieansvarlige. På Center for Cybersikkerheds hjemmeside er der en vejledning om imødegåelse af DDoS.

Center for Cybersikkerhed har på nuværende tidspunkt ikke konkret viden om, at cyberangreb er forestående.

Center for Cybersikkerhed anbefaler imidlertid, at ejere af hjemmesider og andre internetvendte tjenester udviser skærpet opmærksomhed og vurderer, om it-sikkerheden omkring de internetvendte tjenester er tilstrækkelig, herunder og organisationens kodeord til sociale medier har den rettet grad af kompleksitet, samt gennemgår egne beredskabsplaner for forretningskritiske tjenester, der kan angribes via internettet.

Indberetninger som cyberangreb på civil infrastruktur, der er relateret til denne hændelse, bedes ske til Center for Cybersikkerhed på e-mail contact@govert.dk eller i særligt hastende tilfælde på vagttelefon 6093 4827 (ingen pressehenvendelser – se nedenfor for kontaktinformation til Center for Cybersikkerheds pressevagt).

Indberetninger om cyberangreb på militær infrastruktur, der er relateret til denne hændelse, bedes ske til Center for Cybersikkerhed på FIIN til FE-KTP-MILCERT.

I forbindelse med evt. indberetning bedes oplysningerne nævnt i denne varslings bilag medsendt.

Evt. pressehenvendelser bedes rettet til chefen for Center for Cybersikkerhed, Thomas Lund-Sørensen, via pressevagten på telefon 2016 0593

Bilag: Hvad skal man gøre, når man er blevet hacket - eller har mistanke om, at man er hacket?

Hvis man har mistanke om, at et eller flere af ens systemer er blevet kompromitteret, bør man først og fremmest undersøge egne logs for tegn på IT-angreb. Typisk handler det om at spore kommunikation fra et internetdomæne gennem egen firewall, routere til den PC eller server, der har kommunikeret. Det bør ligeledes undersøges, hvilken kommunikation PC'en eller serveren ellers har foretaget og hvordan, om der er oprettet/ændret filer, om antivirus er opdateret og aktivt, og om system- eller applikationsloggen viser tegn på unormal aktivitet.

Det er vigtigt i denne situation at have de kritiske briller på og nøje vurdere, om det angreb, der undersøges, er det eneste eller primære IT-angreb på organisationen, eller om der er andre og flere angreb i gang samtidigt. Denne vurdering er afgørende, når angrebets omfang og skadevirkning efterfølgende skal fastslås.

Center for Cybersikkerhed kan bistå statslige myndigheder med rådgivning i den konkrete situation. Kontakt Center for Cybersikkerhed ved mistanke om hacking, og forsøg at have følgende oplysninger klar:

- Hvilke systemer er under angreb? (OS, IP-adresser, domæne)
- Hvilke konsekvenser vurderes angrebet at kunne have? (tyveri af følsomme oplysninger, nedetid, adgang til andre systemer)
- Hvordan blev angrebet opdaget?
- Er der særlige karakteristika ved angrebet?
- Hvilke foranstaltninger er blevet iværksat, og hvilke forventes at kunne have en effekt?
- Hvilken slags logs er tilgængelige, er der mulighed for at øge logning ved igangværende angreb?
- Er angrebet blevet politianmeldt?
- Kan relevante parter inddrages? (Må Center for Cybersikkerhed f.eks. tage kontakt til teleudbyder)
- Relevante kontaktpersoner og deres telefonnumre og e-mail-adresser