Region Hovedstaden

Center for
It, Medico og Telefoni

Systemoptimering og
informationssikkerhed

BNOTAT

Direkte 51446980

Til: **It- og afbureaukratiseringsudvalget**

Dato: 2. august 2017

Bilag 1 – beslutningssag om handlingsplanen for informationssikkerhed

Regionens digitale trusselsbillede

Trusselsbilledet for Region Hovedstaden er et meget bredt og kompliceret billede, men ligner samtidig det billede, som andre større virksomheder, både offentlige og private, står overfor. Det er derfor delvist et velkendt billede, som regionen allerede har iværksat forskellige mitigerende tiltag overfor.

Samtidig er det dog også et billede som netop nu er under forandring – ikke så meget i typen af trusler – men i høj grad i styrken og dygtigheden, hvormed de udføres. Der har derfor været en række eksempler de seneste måneder, hvor store virksomheder, og også hospitaler mv. i sundhedsvæsenet, lammes. Regionen har dog ikke været ramt hårdt af disse angreb, bl.a. fordi regionen ikke var blandt de primære mål, men også fordi de traditionelle sikkerhedstiltag i regionen har virket tilfredsstillende.

Udviklingen i bredt funderede angreb bekræfter også, at det aldrig vil være muligt at gøre regionens netværk, systemer og data 100 pct. sikker fra truslerne. Der kan dog gøres meget for at minimere risiko for at et angreb lykkes, omfanget af et succesfuldt angreb, samt tiden det vil tage at komme tilbage til normal situation igen. Tab af arbejdstid og reduceret leveranceevne må forventes ved et succesfuldt angreb af de fleste angrebstyper.

De mest almindelige eksterne trusler og angreb som regionen udsættes for er:

- DDoS
  - DDoS står for distributed denial of service og er et angreb, hvor et meget stort antal maskiner sættes op til at spørge en hjemmeside eller et netværk om noget. Hjemmesiden eller netværket bliver dermed overbelastet af trafikken, og bliver enten meget langsom eller lukker ned. Det kan i regionens tilfælde betyde, at andre systemer, der er afhængige af berørte systemer eller netværk, bliver påvirket, og dermed reducerer driftssikkerheden. DDoS kan ligeledes anvendes til at redu-

cere sikkerheden og dermed potentielt give ekstern adgang til systemer og data.

- Malware
  - Malware er forskellige typer ondsindet kode med forskellige skadelige formål som fx ransomware. Ransomware krypterer filer og/eller områder på harddiske/servere, således at brugeren ikke kan tilgå dem uden en kode. Bagmændene kræver efterfølgende penge for at udlevere koden. Øget awareness hos alle regionens medarbejdere er den vigtigste foranstaltning imod malware. Det er normalt kun muligt at fjerne malwaren ved helt at slette PC/server og indlæse seneste backup.
- Phishing
  - Phishing-angreb er mails, der sendes ud i stort antal i et forsøg på at få folk til at oplyse informationer, der kan misbruges – det kan fx være oplysninger om brugernavn, password, kontonummer, kreditkortnummer eller andre værdifulde informationer. Som ved malware, er øget awareness hos alle medarbejdere et væsentligt element, hvorpå regionen kan reducere sandsynligheden for at et phishing-angreb lykkes.
- Hacking
  - Hacking er en betegnelse for en eller flere personers aktive angreb på programmer, systemer eller netværk. Sådanne angreb sker oftest gennem svagheder eller sårbarheder i systemerne. Hacking er en mere direkte og aktiv form for angreb end de ovenstående. Idet denne type ofte benytter sig af, for de fleste, ukendte tekniske sårbarheder, og er fagligt meget dygtige, er det både vanskeligt og omkostningskrævende at være på et internationalt højt sikkerhedsniveau overfor denne form for angreb.

Regionens sikkerhedstiltag

I forhold til de ovennævnte trusler så har administrationen implementeret en række tekniske sikkerhedsforanstaltninger, der skal gøre det så trygt som muligt for regionens medarbejdere at bruge digitale systemer og udstyr i udførelsen af deres arbejde; disse uddybes nedenfor.

Regionen abonnerer på en DDoS beskyttelse hos vores internetudbyder. Produktet er en service, der både detekterer og lukker for de fleste typer udefrakommende DDoS angreb. Denne beskyttelse skal sikre, at regionens netværk kan modstå de fleste DDoS angreb, så denne type angreb så vidt muligt ikke skaber forstyrrelser på de netværksafhængige systemer, der er kritiske for driften.

Idet regionen ikke kan tillade sig at ”lukke teknisk ned” i flere dage eller en uge, er ransomware endvidere en trussel, som regionen er nødt til at prioritere. Derfor har regionen en såkaldt sandboxing service, hvortil vores firewalls uploader mistænkelige filer, der så scannes for skadelig adfærd. Yderligere abonnerer regionen på ”Threat

Prevention", som ligger på vore firewalls og identificerer og klassificerer trafik med kendte trusler, som behandles i henhold til opsatte regler.

De af regionens Windowsbaserede maskiner, som er administreret af CIMT, har installeret sikkerhedspakker, der dels scanner PC'ere og dels forhindrer at brugere tilgår kendte skadelige websider, hvilket reducerer sandsynligheden for at malwareprogrammer kan hente yderligere skadelige programmer. Det bedste værn mod malware er dog awareness hos regionens ansatte således, at de ikke åbner filer eller klikker på links, der indeholder skadelig software. Derudover skal ansatte huske at gemme deres data på regionens fællesdrev, hvor der foretages jævnlige backup.

Phishing-angreb kan potentielt være meget problematiske for regionen, hvis eksterne skaffer sig adgang til de følsomme sundhedsdata, som regionen har. Phishing-mails har en del fællestræk med spam, og regionen identificerer centralt uønskede mails og stopper dem, ligesom der centralt er spærret for at tilgå områder på internettet, der er registreret som sikkerhedsproblematiske.

CEO-fraud, som er en meget specialiseret form for phishing, retter sig mere mod direkte økonomisk vinding og kræver, at regionen har gode kontroller i forhold til overførsel af penge for at mindske regionens sårbarhed. Det vigtigste middel mod phishing angreb er dog medarbejdernes adfærd. Regionen har allerede gode kontrolprocedurer til økonomistyring, det er dog stadig vigtigt, at regionens medarbejdere ved, hvordan de skal forholde sig til uventede mails.

Hacking er en meget bred disciplin og kræver en målrettet indsats af hackeren. Dygtige hackere bliver aldrig opdaget, og de er meget svære at beskytte sig imod. Denne type angreb er i sundhedsregi endnu ikke normen, idet hacking normalt er enten en specifikt bestilt opgave med et specifikt formål eller hvor hackeren vil hente data, der kan sælges til en høj værdi, hvilket vi endnu ikke har set i en dansk kontekst. Forholdsregler imod hacking er opbygning af et højt teknisk sikkerhedsniveau, hvilket vil gøre det svært for mindre dygtige hackere, men ikke forhindre de dygtige i at få adgang. På denne baggrund investerer særligt udsatte virksomheder i sikkerhedssystemer, der kan se at en hacker enten er inde eller har været inde, og hvilke systemer/data, der har haft hackerens interesse.