Tito Phiri
Aalborg universitet
Studienr: 2020-0392
Cyberangreb: Forebyggelse, detektion og håndtering

Indhold

Abstract

Når man arbejder med IT systemer hvor IT sikkerhed er i høj fokus, så kan det være nødvendigt først at identificere de angribere der udgør den største trussel mod ens organisation og system. Det er umuligt at beskytte sig mod alle former for IT trusler der findes, og der findes ikke noget system som er 100% sikkert[1].

Scandiatransplant

Scandiatransplant (sctp) er en organisation som blev grundlagt til organudveksling mellem landende Danmark, Sverige, Finland, Norge, Estland og Island.
Hvis man kigger på disse lande som selvstændig ift. transplantation, så er populationen i hvert af disse lande for lille til at kunne have en optimal donor pool med organer til transplantation, optimal

1 Secure and Resilient Software Development

brug af organer, eller til at kunne have en optimal ”akut venteliste” til transplantation. Scandiatransplant er grundlagt I 1969, og ejes af hospitalerne som også er dem der foretager transplantationerne i disse nævnte lande. Scandiatransplants databaser indeholder historisk data omkring alle de transplantationer som er foretaget siden dens grundlæggelse.

YASWA

YASWA står for Yet Another Scandiatransplant Web Application, og er den platform som programmørene arbejder på hos sctp. Al information, indtastning, tilføjelse af nye donorer og recipienter osv., forgår via YASWA. Programmørene vedligholder og videreudvikler på YASWA.

Krav

Da sctp arbejder med personhenførbar data, så er de forpligtet til opfylde kravene der stilles om persondataloven, som eksempelvis at beskytte personoplysinger[2]. Da sctp skal sørge for at passe godt på hospitalernes data, og dermed også patientoplysningerne, så skal der være høj fokus på fortrolighed, hvilket bland andet kan afhjælpes ved bruge af autorisation når data skal tilgås. Men man vil også gerne være sikker på at der ikke er foretaget uønskede ændringer af dataen, og at man kan regne med at eksempelvis den blodtype, vævstype mm., som står oplyst om patienten er den rigtige. Derfor skal der også være høj fokus på integritet. Ligeledes er der behov for at man kan tilgå dataen på ethvert tidspunkt, da der eksempelvis kan komme et organ fra en afdød doner på et hvert øjeblik. Da er det nødvendigt at man kan tilgå YASWA og få sendt organtilbuddet rundt, og foretage de nødvendige operationer. Dette viser altså også et behov for høj tilgængelighed. Så altså er der lige stor behov for fortrolighed, integritet og tilgængelighed.

Overordnet struktur

Scandiatransplant holder til og har base på Aarhus universitetshospital (auh). Sctp's applikation YASWA kører på auh's servere, men bruger sin egen database. Sctp har opsat firewalls og diverse foranstaltninger for at forsøge at forhindre uautoriseret adgang, men derudover er YASWA også beskyttet af auh's firewalls. Dvs. at man for at få ssh adgang til YASWA, skal igennem både sctp's og auh's firewalls.

Hvad skal besyttes?

Det som skal beskyttes hos sctp er patientdata. Derudover skal medarbejdernes login naturligvis også beskyttes, da det er den mekanisme som forhindrer uatoriserede i at læse patientdataen.

Mulige angribere

Sctp's mulige angribere kunne være avancerede eller profesionelle cyber kriminelle som eksempelvis kunne være ude på at få fat på data fra patienterne, eller blot få indsigt i eller kryptere dataen, for så derefter at kunne kræve ransomware. For en virksomhed som sctp kunne man argumentere at et ransomware angreb er en meget oplagt og alvorlig trussel, da det kan koste menneskeliv hvis ikke sctp har adgang til patientdata som der opereres på konstant. Desuden er ransomware angreb ifølge *”ENISA Threat Landscape 2021”* blevet vurderet som den største cyber trussel i 2020-2021[3].

2 https://www.datatilsynet.dk/hvad-siger-reglerne/grundlaeggende-begreber-/
3 ENISA Threat Landscape 2021.pdf

Det behøver dog ikke nødvendigvis være avancerede cyber kriminelle der er mulige angribere af sctp's systemer, det kunne også være unge mennesker som lige har fundet ud af at det er sjovt og nemt f.eks at lave et DOS eller DDOS angreb, uden at tænke over hvad det kunne have af konsekvenser for offrene. DDOS angreb er et af de mest kritiske trusler mod IT systemer da de belaster og nedlægger systemet, hvilket gør det umuligt at udføre sit arbejde[4]. Slutteligt, og ikke at ignorere, så kunne en angriber også være en tidligere eller nuværende ansat.

Muligt scenarie på et ransomware angreb

Sctp og deres ansatte føler sig meget sikre på at et ransomware angreb mod dem er næsten så godt som umuligt. Hvordan skulle det dog kunne lade sig gøre for angriberne at komme ind i sctp's systemer når de har så mange beskyttelsesmekanismer sat op. For at man overhovedet kan ssh til sctp's servere, så skal man først igennem Region-midts firewalls, og skulle man være så heldig at komme igennem der, så skal man også lige forbi sctp's firewalls. Desuden, så lagrer Region-midt vores back-up som ligger et andet sted. Angriberne skal altså også lige have kendskab til hvor Region-midts back-up ligger. Vi kan simpelthen ikke se hvordan det skal kunne lade sig gøre.

Men hvad sctp dog ikke ved, er at der i noget tid har været planlagt et ransomware angreb mod dem, hvor angiberne er i gang med at indsamle information om deres systemer og drift. Angriberne er både danske og udenlandske, hvor danskeren som hedder Marne, er en tidligere ansat hos Region midt som blev afskediget pga. sctp, som han blandt andet supporterede da han var ansat hod Region-midt.
Og så er Marne i øvrigt også træt af altid at være i minus på kontoen i slutningen af hver måned, så med de penge han kunne få fra et velykket ransomware angreb, så behøver han ikke at røre en finger resten af sine dage. Han er dog ikke så skarp med IT, så han har slået sig sammen med nogle udenlanske hakkere som han kan arbejde sammen med. Han har en masse information om hvor de forskellige informationer kan hentes, og hvor de mulige svagheder kunne være hos Region-midt, da han har insider viden. De professionelle hakkere har prøvet det før, så de går i gang med at indhente nogle af de manglende oplysning ved brug af social engineering. Deres planlægning og arbejde kan ses ud fra nedenstående Framework.

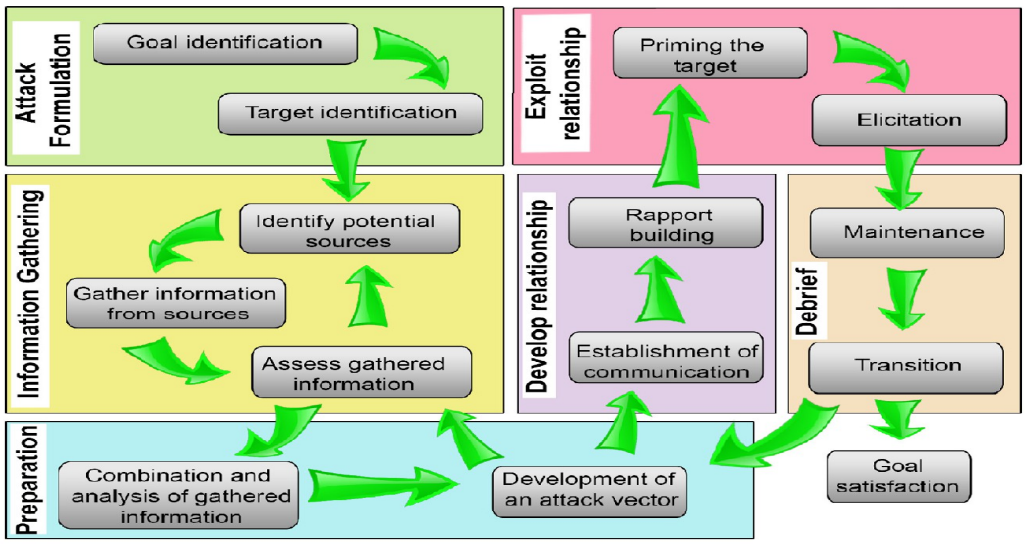

Fig. 2 – Social engineering attack framework.

4 ENISA Threat Landscape 2021.pdf

Attack formulation

Første skridt er identifikation af målet, som på billedet ses under Attack Formulation, og i dette tilfælde er målet sctp.

Information gathering

Næste skridt er information indsamling. Marne som tidligere er ansat hos Region-midt kender lidt til sctp's struktur, da han har supporteret dem. På det tidspunkt var det nødvendigt at han kunne komme ind på sctp's servere ved at ssh. Derfor var der en programmør der oprettede en gæstbruger konto, som skulle have sudo adgang. Marne fandt ud af at sctp ikke slettede den gæst bruger, efter som det altid var den han skulle bruge de gange han skulle ind på deres servere, og han kunne fint smutte ind så længe han sad på Region-midts netværk, og dette er inklusiv Region midts gæste netværk, som sctp havde whitelistet som en del af godkendte IP adresser der kunne få adgang.

Under information indsamling har angriberne også brug for at finde ud af om der er sket noget nyt ift. om der gemmes flere backups andre steder siden Marne blev afskediget.
Derfor ringer Marne ind til Region-midts interne IT support på nummeret han kender fra da han var ansat. Det var det nummer sctp og andre kunder ringede på internt. Da Marne ringer ind, udgiver han sig for at være en medarbejder fra sctp, og siger at sctp er ved at prøve at få overblik over nogle adskillige ting, og vil i den forbindelse gerne vide hvor mange backups der tages. Så han vil gerne vide om der er kommet flere lokationer end dem han kender til. Han får at vide af en IT support at der bliver taget backups som ligger 2 forskellige steder. Dette er de samme steder Marne allerede kender til fra da han var ansat. Han skaffer sig selv fysisk adgang til det sted ved at iklæde sig det Region midt tøj som man kan hente i depotet i kælderen. Man skal godt nok bruge et adgangskort for at komme ind af et par elektroniske døre, men han ved af erfaring at han bare kan få nogen til at bippe ham ind ved at sige at han har glemt sit kort på kontoret.

Denne process med at skaffe sig adgang til de backup som Region-midt tager formentlig tid og omhyggelig arbejde fra angriberne, men da jeg ikke har så meget kendskab til den del af Region midt, antager vi at Marne med sin mange års viden og erfaring fra sin tid hos Region-midt, får skaffet sig adgang til serverne. Sctp har ikke kontrol over den del med hvor backup bliver lagret, og hvordan det gøres.

Preparation

Nu da Marne har indsamlet den nødvendige viden, hvor han har adgang til backupen, og samtidig har ssh adgang til sctp's servere, så kan angriberne gå i gang med at analysere og lave en attack vector.

Attack vector

På nuværende tidspunk kan selve angrebet begynde at planlægges. Her vil man typisk udvikle en plan som indeholder det præcise tidspunkt på angrebet, hvilket tidspunkt man skal besøge eller kontakte de nødvendige interessanter som skal tildele den nødvendige adgang[5]. Men i Marnes tilfælde skal der ikke kontaktes nogen, da han ved at han kan komme ind på sctp's servere hvis han

5 Social engineering attack examples, templates and scenarios
(Francois Mouton, Louise Leenen, H.S. Venter)

er på Region-midts gæstenetværk.

Develop relationship and exploit relationship

Der er ikke behov for at Marne kontakter noget hos sctp, og prøver at udvikle et forhold med nogen da han allerede ved hvordan han skal komme ind på serverne. Det sidste skridt mangler her er selve angrebet, hvilket leder os til goal satisfication.

Goal satisfication

Da angriberne har formået at få adgang til Region-midts servere der indeholder backups, og samtidig har adgang til sctps servere, så er det eneste der mangler nu, at kryptere dataen på det aftalte tidspunkt, og ligge systemet ned. Herfra kan de komme med kravet om ransomware. Dette ville stille sctp i en meget svær situation, da det handler om liv eller død.

Kapabilitet og ressourcer

Det beskrevede angreb kræver ikke de store resourcer, da der ikke skulle bruges computer kræft, som f.eks ved et DDOS angreb. Det eneste der skal bruges i denne kontekst, er viden til at navigere sig igen styresystemet, og brug af ssh, samt at være i stand til at kryptere data så det er umuligt for sctp at dekryptere uden koden.

Organisatoriske foranstaltninger

En måde at gøre den ovenstående process sværer for angriberne, er først og fremmest at sørge for at have styr på hvem der har adgang til systemerne. Man skal have styr på hvilke brugere der har ssh adgang, og hvilke rettigheder de har. Hvis man af en eller anden grund ikke skal slette brugerne, så bør man sørge for kun at give dem de rettigheder de har brug for, og ikke flere.
En anden ting der kunne være behjælpelig i ovenstående situation, er at have logs og monitorering, så man har styr på hvem der tilgår systemet, og hvornår det sker.

I Region-midts tilfælde kunne man måske også argumentere for at personalet skal have strenge krav om ikke at lukke nogen ind som ikke har kort. Man kunne sørge for at have en kontaktperson eller vagt som personalet kunne ringe til, hvis der er en som har glemt sit kort. Vagten kunne så følge med vedkommende for at se om han rent faktisk hører til på stedet.

Recovery plan

En anden foranstaltning der er vigtig, er en recovery plan, som er med til at forbedre sikkerheden. Dette indebærer at lave regelmæssige backups som lagres forskellige lokationer, og som hurtigt kan hentes frem og tages i brug i tilfælde af en katastrofe[6]. En recovery plan laves ikke kun på grund af hackere, men også i tilfælde af hvis der f.eks skulle være et jordskælv, oversvømmelse, ildebrænd mm. Ydermere, så skal en recovery plan kigges igennem regelmæssigt, og opdateres om nødvendigt[7].

6 Kizza2020_Book_GuideToComputerNetworkSecurity
7 Kizza2020_Book_GuideToComputerNetworkSecurity

Andre trusler mod YASWA

Et eksempel på andre mulige angreb som sctp kunne stå over for, kan nævnes DDOS angreb som i Marnes tilfælde nok ville være emotionelt, finasielt og personligt motiveret. Her kunne der gøres brug af botnet, hvor der gøres brug af tusindvis af inficerede maskiner til at sende requests til sctp's server for at gøre det umuligt for de brugerne at tilgå systemet og udføre deres arbejde.

Et andet eksempel på mulige angreb, kunne være cross-site scripting, hvor angriberen injicerer ondsindet eksekverbar js kode i YASWA, hvis man ikke sørger for at filtrere på inputet, og fortælle systemet at det givet input skal behandles som data, og ikke kode. Her kan angriberen eksemplevis sørge for at videresende brugeren til en side/server som han har kontrol over.

Center for cybersikkerhed

CFCS anbefaler at have en beredskabsplanlægning og krisestyring. Den minder meget om den nævnte recovery plan. CFCS giver nogle råd som har resulteret i at vi har gennemgået, forbedret og opdateret vores beredskabsplaner. Et meget relevant punkt, er også at alle personer er bekendte med beredskabsplanen. Det kan for rigtig mange måske godt glippe eller forglemmes når man får nye ansatte, og der bliver ikke fulgt op på det.

Det anbefales også at man afprøver om man kan reetablere fra backuppen. Her kunne man måske også tænke at lade de nye programmører afprøve den del, så det ikke altid er den samme person.

I det brugte eksempel tidligere, kunne Marne komme ind via ssh adgang. CSCF nævner hvor vigtigt det er at logs gennemses jævntligt. I dette tilfælde kunne man formentlig også opdage hvis en oprettet bruger tilgår systemet på et tidspunkt som vedkommende ikke burde.

Ydermere ligger CFCS også vægt på awareness, hvor det anbefales at medarbejdere ved hvordan de skal rappotere om sikkerhedshændelser.

Konklusion

Nogle gange kan man have et meget sikkert system, som næsten er uigennemtrængeligt. Men det er ikke nok kun at gå efter at have de nyeste og mest sikre teknologier, hvis ikke man samtidig også uddanner og gører personalet opmærksom på relevansenomkring sikkerhed, og hvor lidt der egentlig skal til for at det går galt. Ud over det eksempel der er givet, hvor man måske ikke lige får slettet en bruger eller en tidligere ansat, så kan der også være sådan noget som at man måske ikke lige får låst sin computer/skærm når man lige skal på toilettet. Hackere bliver dygtigere, og finder på nye smuthuller og måder at bryde ind i systemerne på. Man kan godt synes at man har et godt og sikkert system, og også føle sig sikker fordi man er beskyttet af noget software fra en anderkendt udbyder, men det burde ikke få folk til at føle sig for sikre, og tage det let på nogle ting. Vi skal konstant arbejde på at forbedre os mht. sikkerheden. Angriberne skal bare bruge én mulighed/fejl fra brugerne af systemerne[8]. Derfor er det ikke nogen dårlig idé at benytte sig af de frameworks og råd der gives og benyttes af eksperterne som dagligt arbejder på at forbedre sikkerheden.

8 Brugbart og sigende citat fra en af seminarne

Referenceliste

[1] ENISA Threat Landscape 2021.pdf

[2] Social engineering attack examples, templates and scenarios
(Francois Mouton, Louise Leenen, H.S. Venter)

[3] Kizza2020_Book_GuideToComputerNetworkSecurity

[4] Center for cybersikkerhed https://www.cfcs.dk/da/

[5] https://www.datatilsynet.dk/

[6] Secure and Resilient Software Development

[7] Slides fra Grundlæggende teknisk IT-sikkerhed og
Cyberangreb: Forebyggelse, detektion og håndtering