DigSam-podkast om digital sikkerhet

Podkastvert: Janne Dugstad
Gjest: Henriette Henriksen

Janne Dugstad (heretter **JD**):
Velkommen til en podkast om digital sikkerhet og brudd på digital sikkerhet i helse- og sosialtjenester. Podkasten er en del av DigSam-prosjektet og dere kan finne oppgaver til denne podkasten på websiden til DigSam.

Jeg heter Janne Dugstad, og leder senter for helse og teknologi ved Universitetet i Sørøst-Norge. Jeg skal snakke med Henriette Henriksen som er informasjonssikkerhetsleder i Vestre Viken Helseforetak.

Hvordan blir man informasjonssikkerhetsansvarlig, og hva er din faglige bakgrunn?

Henriette Henriksen (heretter **HH**):
Det var et veldig godt spørsmål Janne. Min faglige bakgrunn er utgangspunkt i en gammel teknolog, det vil si at jeg har jobbet i mange år med veldig tung drift og bakenforliggende drift på infrastruktur. Også tok jeg videreutdanning for man har hatt en gryende interesse for dette med sikkerhet. Man må jo være over snittet interessert i både sikkerhetspolitikk og de trender som rører seg der ute og som kan påvirke de de digitale tjenestene som vi skal levere.

JD:
Nå nevnte du et ord som vi kommer til å snakke om mange ganger, og det er infrastruktur. Kan du forklare hva det er?

HH:
Infrastrukturen er veldig enkelt forklart når du logger deg på din PC så logger du deg på mot en infrastruktur. Du får tilgang til tjenester som du skal konsumere. Det kan være alt fra E-post, tilgang til internett og tilgang til pasientopplysninger i pasientjournalen. Det er altså hele det bakenforliggende som danner det nettverk og datasystemer.

JD:
Når du jobber som informasjonssikkerhetsansvarlig, hva er det du gjør da?

HH:
Vi har vi et veldig vidt spenn i utgangspunktet. Vi jobber alt i fra avvik, altså når ting har gått galt, da jobber vi veldig reaktivt, men vi foretrekker alltid å være proaktive, nettopp for å forebygge at hendelser skal skje. Så vi jobber med alt i fra ledelsessystem til informasjonssikkerhet. Det vil si de prosedyrene som sier hva vi kan og hva vi ikke kan gjøre. Altså hva vi skal huske på. Dette med ansattes adferd, hva kan de bruke og ikke bruke, til å bygge dette med sikkerhetskultur i egen virksomhet. Og det er dette med den gode sikkerhetskulturen, det er der vi ser vi har mest å vinne fordi vi kan dekke oss opp med veldig mye teknologi.

Men vi vil alltid ha et gap mellom teknologien og hvordan vi rigger sikkerheten rundt den, og de ondsinnede aktørene. Og det gapet må vi dekke med bevisste brukere hos oss. Så vi bruker veldig mye tid mot det.

JD:
Så dere jobber mot for eksempel de som er ansatt ute i tjenestene?

HH:
Ja, vi har nyansattdager, fagdager og kurs for alt fra sykepleiere til leger i spesialisering, og de som gjerne har andre tjenester hos oss som for eksempel både elektrikere og vaskepersonale. De er alle berørte av å ivareta en god sikkerhet i sykehusene.

JD:
Har du noe inntrykk av hva helsepersonell kan om dette fra før? Er dette noe man har mye kunnskap om, eller hvor viktig er det å ha mye fokus på det?

HH:
Det jeg tenker er at helsepersonell har veldig god kunnskap om taushetsplikten. Den sitter veldig godt i ryggmargsrefleksen deres. Men så tenker jeg og at dette med å forvalte taushetsplikten i en travel hverdag, det er der vi ser det gjerne kan falle litt på post. Og det handler rett og slett om at man gjerne ikke er bevisst på alle de områdene hvor taushetsplikten faktisk blir brutt eller kan bli brutt med tanke på egne handlinger, altså ikke overlagte handlinger, men rett og slett litt uoppmerksomhet i en veldig travel hverdag.

JD:
Så det er nyttig å bli gjort klar over situasjoner hvor man må være litt ekstra oppmerksom?

HH:
Det er sikkert og visst. Og det handler som oftest om de veldig små tinga for eksempel dette med å låse maskinen før du går på toalettet eller før du henter deg en kaffe.

JD:
Vi skal komme nærmere inn på hvilke feil ansatte i helse- og sosialtjenester gjør i sine travle arbeidsdager og som kan gjøre at sensitive personopplysninger kan komme på avveie eller at eksterne får tilgang inn i datasystemene og fagsystemene, eller at eksterne aktører på annen måte kan påvirke informasjonssikkerheten.

Og så skal vi diskutere hva man kan gjøre etter at en slik hendelse er blitt oppdaga, hva ledelsen gjør, hvordan pasienter eller andre berørte blir informert og hva vi som jobber i en organisasjon kan gjøre for å lære av feilene og for å komme videre.

Hvor ofte forekommer det brudd på digital sikkerhet?

HH:
Jeg vil påstå at det forekommer daglig, også tenker jeg at det her kan vi differensiere på to områder. Vi har alle forsøkene på inntrengning i den bakenforliggende infrastrukturen, altså det som de ansatte ikke ser eller merker noe til. Der har vi flere millioner hendelser i døgnet hvor majoriteten faktisk blir stoppet

av vår IKT-leverandør. Men det er klart noe kan og slippe gjennom der og, vi vet at alle har jo mottatt en e-post som vi kaller for "phishing" der man prøver seg, og som slipper gjennom de sikkerhetssystemene vi har.

Men så har vi og sikkerhetsbrudd som går igjen på dette med atferd. Vi var jo så vidt innom det. Dette som handler om å låse maskinen, bruk av mobiltelefoner. Og så vet vi at her har vi mørketall. Nå har vi nettopp kjørt en sikkerhetsundersøkelse i Vestre Viken for å prøve å avdekke disse forholdene. Vi ser at det er svært lite avviksmeldinger på det. Og det tror jeg ofte handler om at folk gjerne ikke er selv klar over at dette er et avvik i utgangspunktet, før noen gjør de oppmerksom på det. Så vi håper at vi på sikt kan få enda bedre tall på dette, for vi vet at det skjer daglig.

JD:
Hva er de vanligste feilene som ansatte i helsetjenesten gjør?

HH:
"Feil og feil", jeg liker ikke å si at det er feil heller altså, for det handler om at man har en veldig travel hverdag og man skal rekke over ganske mye, og det å være litt uoppmerksom, vil jeg gjerne kalle det. Det kan være å gå fra maskinen ulåst, så står gjerne da pasienters journalsystem oppe og tilgjengelig for ganske mange, både andre ansatte og besøkende.

Vi har dette med å sende sensitiv informasjon på e-post. Man bruker jo e-posten i alle andre sammenhenger, og til og med både bank og politi sender jo gjerne informasjon på e-post, hvorfor skal ikke vi i helsesektoren gjøre det, det er et veldig enkelt og brukervennlig system, men det innehar ikke den tilstrekkelige sikkerheten som blir krevet til å behandlesensitiv informasjon.

Og så ser vi og det siste elementet som er på fullt inntog inn, og det er dette med bruk av mobiltelefoner og bruk av kamera rett og slett. Man skal dokumentere en skade som har skjedd og så tenker man ikke at dette er sin egen private mobiltelefon også har man plutselig pasientsensitiv informasjon på sin private mobil, og så har vi hatt noen tilfeller der de har automatisk opplasting til en sky hvor de lagrer bildene sine. Da har vi tatt det til et nytt nivå igjen. Og det ser vi er noe som treffer oss mer og mer.

JD:

En annen ting som jeg har hørt om og som har vært diskutert i alle år også før vi fikk datasystemer er dette med å gå inn og sjekke opp noen journalopplysninger på noen du egentlig ikke har et faglig ansvar for der og da.

HH:
Ja det ser vi treffer også rett som det er. I utgangspunktet sier vi alltid det at å ta et oppslag på en pasientopplysning krever et hjemmelsgrunnlag. Hjemmelsgrunnlaget som oftest og det som vi kan si noe om nå er det at du skal yte helsehjelp. Det er et eget hjemmelsgrunnlag i seg selv, så har vi andre som forskning og kvalitetssikring. Men vi vet man gjerne tar oppslag på for eksempel egne barn og foreldre og det kan være de beste intensjoner det, men det er veldig sjelden man yter helsehjelp til nære relasjoner. Som regel ønsker ikke helsepersonell å gjøre det selv.

Men vi har og hatt noen tilfeller der man har tatt oppslag på for eksempel kollega. Igjen så var det de beste intensjoner, vil gi et lite eksempel på det og det er mange år siden:

Vi hadde en ansatt som var i lykkelige omstendigheter og ventet barn. Og kollegaene hadde jo veldig lyst til å gjøre stas på sin kollega og syntes dette var veldig hyggelig. Kollegaen ble sykmeldt kort tid før fødsel og de ansatte hadde jo tenkt at de skulle være hyggelig og ikke plage henne med masse spørsmål om hun hadde født og så videre. Så de tenkte de skulle gjøre noe klokt, og det var jo rett og slett å ta oppslag i fødesystemet for å se om de fant henne der. Og det gjorde de til slutt. Kollegaen hadde født og man så ut ifra fødselsnotatene at det hadde i grunn vært en litt dramatisk fødsel, og de ble veldig bekymret og dermed tok de oppslag i pasientjournalen for å høre hvordan det hadde gått. Det endte i hvert fall med at den fødende både fikk blomster, konfekt, gratulasjoner og de beste ønsker fra sine kollegaer som syntes dette var veldig artig og gøy når den lille hadde kommet.

Men den ansatte som hadde født den var ikke like begeistra, fordi fødselen hadde vært litt traumatisk og så hadde man heller ikke sagt noe om fødselen til annet enn den nærmeste familie nettopp for å skape litt ro rundt hele situasjonen. Og klart da ble man litt spørrende til hvordan disse opplysningene hadde dukket opp. Og da fikk vi beskjed at vi må gå inn og se i innsynsloggen i de ulike systemene for vi logger jo alt. Og da ser vi jo at det var oppslag både i fødesystemet, det var oppslag i pasientjournal og det gir jo vi ut til den ansatte som nå sånn sett var å regne som pasient hos oss.

Og klart det gjør noe med arbeidsmiljøet på den avdelingen og i tillegg til for det er klart hun var veldig skuffa og lei seg over at kollegaene hadde tatt oppslag om det, som igjen var med de beste intensjoner. Men jeg tror og de andre ansatte plutselig fikk en liten aha-opplevelse, at hvis vi kan ta oppslag på henne så hvem har tatt oppslag i min journal? Så dermed hadde vi en liten runde på det.

Men det som vi sier er gode intensjoner er ingen hjemmelsgrunnlag for oppslag i journal.

JD:
Når det gjelder det med oppslag i journal, Henriette, så sa du at det er en logg på det ikke sant. Og det vil si også at hvis en pasient har mistanke om at noen har fått opplysninger om en selv, så kan man kreve å få den loggen utlevert, det var sånn ikke sant?

HH:
Ja det er en pasientrettighet de har så dermed er vi lovpålagt å ha den innsynsloggen og der logger vi alltid fra hva folk har tatt oppslag i, hva de har skrevet i pasientjournalen. Har de skrevet ut noe, alt blir logga. Og mye av disse loggene er og tilgjengelig direkte for pasienten via HelseNorge-portalen.

Klart den loggen ikke er like utfyllende, men der ser de mye og så ender det som regel opp i at vi mottar en henvendelse fra pasienten der de ønsker den utfyllende. Og der blir de ansatte utlevert med fullt navn.

JD:
En annen situasjon som jeg tror mange kan kjenne seg igjen i er dette med notater. At det tas notater, og at det tas utskrifter og at det flyter litt med sånne personopplysninger, pasientdata egentlig litt rundt omkring.

HH:
Ja vi har jo vært i samme situasjon hos oss og der jeg tidligere har måttet ta daglige runder på sykehuset

jeg var der og da for å se hva ligger igjen på printeren. Og der kunne man finne ganske mye i utgangspunktet. Det kunne være alt i fra journalnotater til resepter. Heldigvis har vi kommet oss videre. Nå har jo mange bedrifter, inkludert oss i Vestre Viken det vi kaller for sikker print. Det vil si at vi sender til print, men vi får ikke henta ut før vi kommer fysisk til printeren og legger på kortet vårt. Dermed må vi stå der til den kommer ut. Så det ser vi har vært enormt forebyggende på alt det som vi fant tidligere.

JD:
Jeg jobber som forsker og jeg har vært ute i en del sykehjem og boliger og slikt i kommunehelsetjenesten. Og der ser jeg ofte at for eksempel passord og brukernavn, det er sånn som er teipet opp på veggen. Jeg vet ikke om du har noe erfaring med det, men jeg tror vi kan fastslå at det ikke er god praksis.

HH:
Det er neppe god praksis. Igjen vil jeg påstå at alle virksomheter har opplevd det, om det er teipet på veggen eller teipet under et tastatur. Vi har sett alle fasettene og mulighetsrommet hvor folk legger de brukernavnene og passordene. Det som er utfordringen med det er at man mister den totale sporbarhet i det og man gjør seg og sårbar for vi vet faktisk ikke hvem andre som da kan se de brukernavnene og passordene.

JD:
Så i et system så er det aller beste at hver enkelt bruker har sitt personlige passord og brukernavn, ikke sant?

HH:
Det er riktig og når det kommer til pasientjournalsystemer så er det og et krav om at det skal være personlig nettopp på grunn av dette med logginga som vi har, så må det være unikt for hver bruker.

JD:
Det kan være at de eksemplene jeg har sett - jeg forsker jo på velferdsteknologi - så det kan jo være at teknologien ikke er koblet opp mot fagsystemene på samme måte. Men det burde vært samme tilnærming likevel.

HH:
Det bør være samme tilnærming og det kan hende at det kan ha vært et brukernavn og passord for eksempel på innlogging på Windows bare for å si noe og den er ikke direkte mot fagsystemet, men allikevel vil det være en sårbarhet knyttet til det nettopp fordi at du har faktisk oppgitt brukernavn og passordet ditt inn til selve infrastrukturen. Vi hadde neppe gjort det hvis det var nettbanken.

JD:
Da tenker jeg at vi skal gå over til det neste hovedtemaet vårt som er når en sånn hendelse har skjedd at det har vært et brudd på personvern eller informasjonssikkerhet. Hva gjør man egentlig da?

HH:
Ja det er et veldig godt spørsmål for det er klart det kommer litt an på hva informasjonssikkerhetsbruddet består av. Men det er klart når vi har identifisert og klassifisert et stort

brudd for eksempel et hackerangrep på hele virksomheten, så har man gjerne både vært gjennom beredskapssituasjoner der vi har hatt både kriseledelse og krisestab. Og vi har gjerne også foretatt mitigerende tiltak og fått driften på kjøl igjen. Men så er spørsmålet hva vi gjør etterpå? For jeg er veldig opptatt av at vi skal både snakke om det for dette har veldig god læringseffekt, og som oftest så skal vi og melde det til diverse tilsynsmyndigheter.

Datatilsynet vil alltid være en instans å melde sikkerhetshendelser til av alvorlig karakter, eller hvor vi ser at det er brudd på personvernet til pasienter og brukere.

JD:
Nå brukte du et annet faguttrykk, og det var "mitigerende tiltak".

HH:
Det er i grunn et fælt ord i utgangspunktet, jeg skal innrømme. Det er risikoreduserende tiltak altså. Man blir litt fagpreget, her har vi som jobber med sikkerhet veldig mye å lære, at vi må huske å gjøre oss forståelige for brukerne slik at de skjønner hva budskapet vårt faktisk består av.

JD:
Helsepersonell bruker også veldig mye faguttrykk, så det er en ganske kjent situasjon når vi skal kommunisere med både brukere, pasienter og pårørende også.

Når det først oppstår en hendelse så må man gjøre tiltak for å stoppe hendelsen så godt man kan. Og det er det ledelsen som gjør da, altså de som jobber med sikkerhet som har det som ansvarsområde som gjør det. Også har man dette med skadetid også, for det det kan være sånne typer skader at for eksempel datasystemene går ned. Så da må man kanskje ha noen rutiner for hva som skjer da?

HH:
Altså jeg vil jo si det at hvis vi havner i en situasjon hvor datasystemene våre går ned, så er vi i utgangspunktet godt over i en beredskapssituasjon av et gitt nivå. Det vil si at det er viktig at virksomheten har gode beredskapsplaner slik at en er i stand til å yte den tjenesten som er primær-hovedmålet vårt. Hos oss vil det være å yte helsehjelp, det skal vi være i stand til uavhengig om systemene er oppe eller nede.

JD:
Det som skjer for de ansatte da, altså helsepersonellet eller hvis man er i en sosialtjeneste for den saks skyld, så vil jo det være at man faktisk da må kunne gjøre jobben sin selv om man ikke har disse systemene tilgjengelig.

HH:
Det stemmer, og dermed er det og veldig viktig at man trener på slike situasjoner slik at man ikke havner i en setting der når det først går ned så vet man ikke helt hva man skal gjøre. Så trening, trening, trening på disse områdene.

JD:
Og det er ledelsens ansvar at det skjer, men som ansatt så må man ta del i en sånn type trening og opplæring.

HH:
Det stemmer. Det vil alltid være et ledelsesansvar, men klart du har og et ansvar som ansatt å ta aktiv del i en slik trening som det.

JD:
Også er det sånn at de som er berørt av dette og ikke bare de som jobber der, men de som er pasienter eller pårørende eller brukere av en tjeneste, de får også beskjed på noe vis. Vi snakket litt om det i sted, at hvis det er et sånt oppslag i journalen hvor noen som ikke egentlig hadde tilgang, eller hadde noe rettferdiggjort grunn til å gå inn og lese en journal da kan man få beskjed om det.

Det jeg ikke spurte deg om i stad når det gjelder akkurat det med journaloppslag og at dere har disse loggene det er om dere har noe system for å følge med på det? Er det sånn at dere for eksempel oppdager hvis noen uvedkommende er inne?

HH:
Ja altså i dag så kjører vi manuell kontroll. I tillegg så kan det og hende at leder har mistanke om eller at andre har varslet, eller at både pasienter og pårørende selv har en indikasjon på at uvedkommende har vært inne i journaler. Da kjører vi kontroll. Nå skal vi igangsette et større prosjekt som skal automatisere dette for oss. Det vil si at vi har gitt noen visse kriterier og parametere som gir indikasjon på uberettiget oppslag slik at vi skal få en bedre kontinuitet og bredde på hva vi faktisk klarer å fange opp. Og alt dette handler om til syvende og sist å skape tillit ute til pasienter og brukere.

JD:
Også snakket vi i stad om at hvis en sånn hendelse skjer, om man oppdager det og pasienter er involvert så blir de varslet.

HH:
Pasientene blir alltid varslet når det har vært uvedkommende inne i journalen deres. I tillegg til så vil vi og ofte sende en melding til Datatilsynet om at vi har hatt brudd på personvernsikkerheten og hvilke tiltak vi har iverksatt, både for den forulempa, men ikke minst og de interne.

JD:
Men sånn internt da, altså i organisasjonen eller virksomheten eller på en avdeling. Du hadde dette eksempelet med den fødselen hvor noen sjekka noen opplysninger som de ikke burde ha gjort. Er det sånn at man går inn og tar tak i det på avdelingen, eller hvordan gjør man det?

HH:
Ja altså jeg henstiller jo alltid til å snakke om det. I det man snakker om avvik som har skjedd så får man og løftet bevisstheten opp på et helt annet nivå. Ikke for at vi har et behov for å "name and shame", det er ikke det som er intensjonen, men det er det som øker forståelsen. Hva kan man gjøre. Hva kan man ikke gjøre. Hva er eventuelle konsekvenser og ringvirkninger. Vi er veldig opptatt med dette at de må forstå dette her med pasientenes behov til tillit til helsesektoren.

Men det kan og være at vi skal se enda litt på hvorfor har i grunn situasjonen eller hendelsen oppstått overhodet? Kan vi gjøre noe med innretningen? Er det arbeidssituasjonen som er årsaken? Men til syvende og sist dette med å snakke om det, som jeg alltid sier.

JD:
Så det er en sånn type debrief da?

HH:
Det blir jo en debrief på det som har skjedd og det er rett og slett det å lære av hendelsen, og så kan man jo si at det vil være veldig reaktivt sett opp mot hendelsen i så måte, men allikevel så vil det være proaktivt for kommende hendelser.

JD:
Ja så vi deler kunnskap, erfaringer, lærer noe av det og så går vi videre.

HH:
Nettopp, og det er det som er en del av sikkerhetskultur.

JD:
Og idet man kan si at man går videre så er man inne i det daglige, eller månedlige, eller årlige, hvordan man gjør det, arbeidet med sikkerhetskultur?

HH:
Ja det stemmer. Klart vi henstiller jo alltid til å ha dette som en iallfall månedlig agenda. Det er rett og slett og fordi, det er ikke lovverket som endrer seg så veldig ofte. Det er tunge, store, langdryge prosesser, men teknologien og trusselbilde endrer seg ganske raskt, så der er stadig nye områder/momenter som vi må være på vakt på, men klart og vi har jo hele veien litt nytt helsepersonell inne og, og klart de skal og komme inn i dette tankesettet. For til syvende og sist så er det pasientopplysninger vi skal verne om.

JD:
Da har vi snakket om digital sikkerhet og hvilken adferd ansatte i helse og sosialsektoren bør ha for å bidra til å ivareta personvern og informasjonssikkerhet. Takk til informasjonssikkerhetsansvarlig Henriette Henriksen i Vestre Viken helseforetak og takk for at dere har hørt på podkasten.