Därför är ”digitala brandövningar” nödvändiga i den nya digitala vården

Vården blir alltmer digital, mobil och uppkopplad – av många skäl: för att få flexiblare arbetssätt, höjd kvalitet och ökad effektivitet, men också för att minska sjukvårdskostnader och göra vårdyrket relevant för den yngre arbetskraften. Men i den här nya verkligheten lurar också faror.

Text: Kristian Borglund

Digitaliseringen inom vården har, liksom för samhället i stort, medfört att allt fler sjuksköterskor, läkare och chefer utför arbetsuppgifter via mobila enheter, egna jobbmobiler eller bärbara datorer.

En del använder sina enheter enbart på arbetsplatsen, medan andra tar med dem hem. Det behöver inte alls innebära problem, utan underlättar på många sätt. Att kunna se scheman, kommunicera, fatta beslut, förbereda arbetsdagen och så vidare på distans har blivit en självklar del av det nya arbetslivet.

Men säkerhetstänket behöver finns där, och säkerhetsrutinerna ska sitta. Många sjukhus och andra arbetsplatser inom regionerna behöver sätta strålkastarljus på sin säkerhetskultur, menar Malin Sölsnaes, chef för Atea Vård & Omsorg, och hennes kollega Carl-Johan, ansvarig för informationssäkerhet på Atea.

”HA ETT HELHETSPERSPEKTIV PÅ SÄKERHETEN”

– Det gäller att organisationen har ett helhetsperspektiv kring säkerheten – i alltifrån kravställning vid inköp, säkerhetsklassificering av data, behörighetshantering till att alla är medvetna om farorna, säger Malin.

Carl-Johan utvecklar:

– Säkerhetskulturen är avgörande. Enskilda medarbetare måste exempelvis få helt klart för sig hur deras bärbara datorer eller mobiltelefoner får hanteras. Som att inte koppla upp sig via wifi-nätverk på kaféer eller tåg med enheter som innehåller jobbappar. Då kan man råka ut för angrepp och få in skräp it-miljön. Detsamma gäller om man låter barnen ladda ner spel till enheten. Och de apparna som används i jobbet behöver förstås vara låsta och kräva separat inloggning, så att inte obehöriga kommer in där.

Malin Sölsnaes, chef för Atea Vård & Omsorg

INKÖP AV IT KRÄVER SAMARBETE FÖR ATT KRAVSTÄLLNINGAR SKA BLI RÄTT

När det gäller inköp av it-utrustning, it-system och it-applikationer behövs ett systematiskt samarbete mellan inköpsavdelningen, upphandling och it-avdelningen så att grundjobbet görs ordentligt ur ett säkerhetsperspektiv. Annars kan det lätt uppstå missförstånd och otydligheter.

Ta det här med säker inloggning. I kravställningen kanske ni ställer frågan, ”Finns det säker inloggning?” och får svaret, ”ja det finns det”. Men räcker det?

Carl-Johan Ekelund, ansvarig för informationssäkerhet på Atea

När en anställd slutar och tas bort från huvudsystemet, kommer den tidigare medarbetaren ändå finnas kvar som användare i applikationen med full tillgång till journaluppgifter?

– I den svenska Cybersäkerhetslagen som väntas börja gälla någon gång under nästa år, realiseras även NIS2. Där ställs krav på att säkerhetsbiten trycks in hårdare i upphandlingsförfarandet. Bland annat förväntas ni i fortsättningen ha ordentlig koll på era leverantörer och säkerställa att de har dygnet runt-förmåga att upptäcka och stoppa begynnande attacker, till exempel. Att skaffa sig möjligheten att granska sin leverantör säkerhetsmässigt blir en viktig punkt i kravställningen. I slutändan är det alltid er organisation som är ytterst ansvarig, säger Carl-Johan.

RÄTT NIVÅ PÅ KRAVSTÄLLNINGAR – OCH DIGITALA BRANDÖVNINGAR

Genom att ta hjälp av specialister får ni trygghet i era digitala arbetssätt.

– Många kämpar med att formulera rätt nivå av krav, eller saknar kompetensen att utvärdera om en leverantör faktiskt kan leva upp till kraven. Det är, och har alltid varit, en viktig del av det vi gör på Atea. Vi hjälper våra kunder att kravställa på rätt nivå, och säkerställa att leverantörerna har en tillräcklig grad av säkerhet. Vi ger också rådgivning om att få rätt rutiner på plats, säger Carl-Johan.

”Digitala brandövningar” saknas exempelvis ofta.

– Om det börjar brinna på en vårdavdelning, så finns det i allmänhet fungerande rutiner och checklistor för vad som ska hända då. Det är en naturlig del i verksamhetsplaneringen idag. Men motsvarande finns sällan vad gäller säkerheten, säger Malin.

För tips och fallgropar att undvika, besök: https://www.atea.se/valfardsteknik/digitala-brandovningar-varden/#faktaruta

ATEA