

Så kan välfärdstekniksektorn förbättra sin IT-säkerhet!

apr 28, 2023

I takt med att vi förlitar oss mer på teknik för att stödja tillhandahållandet av hälso- och sjukvårdstjänster och sociala tjänster blir det allt viktigare att se till att IT-system och data är säkra och skyddade från potentiella hot.

Användningen av välfärdsteknik, såsom fjärrövervakningssystem för patienter, smarta sensorer och hälsoapplikationer, ger både möjligheter och utmaningar när det gäller IT-säkerhet. Välfärdsteknik kan bidra till att förbättra kvaliteten på och tillgängligheten till hälso- och sjukvård och sociala tjänster, men den medför också nya risker och sårbarheter som måste åtgärdas.

Cybersäkerhet är ett område i ständig utveckling som innebär en rad komplexa utmaningar och frågor. Några av de viktigaste frågorna som cybersäkerhetsbranschen står inför idag inkluderar hur man skyddar sig mot sofistikerade cyberattacker, hur man hanterar och säkrar stora mängder känsligdata, hur man säkerställer efterlevnad av allt strängare regler och hur man håller sig uppdaterad med de senaste cybersäkerhetshoten och trenderna.

Johan Lenander är VD för Tunstall AB och har över 15 års erfarenhet av att arbeta inom säkerhetsbranschen med en djup förståelse för de utmaningar och möjligheter som presenteras av det ständigt föränderliga landskapet för IT-säkerhet.

– Det finns ett växande behov av samarbete och informationsutbyte mellan organisationer, eftersom cyberattacker blir vanligare och mer sofistikerade. Eftersom vi fortsätter att förlita oss mer på teknik är det viktigt att vi förblir vaksamma och proaktiva i vår strategi för cybersäkerhet. Under de senaste åren har det förekommit flera högprofilerade cybersäkerhetsincidenter som har belyst de potentiella riskerna och sårbarheterna i samband med vårt ökande beroende av digital teknik, berättar Johan Lenander, VD på Tunstall i Sverige.

Välfärdstekniken har potential att revolutionera vård- och omsorgssektorn och tillhandahålla innovativa lösningar för att förbättra livskvaliteten för individer i behov av vård och omsorg. Men som med all teknik finns det också tillhörande risker och utmaningar, särskilt inom cybersäkerhet.

När tekniken fortsätter att utvecklas ökar också riskerna i samband med användningen. Detta gäller särskilt välfärdsteknik, där utsatta individer och känsliga personuppgifter ofta är inblandade.

– Tunstall som marknadsledande global aktör med 5 miljoner anslutna slutanvändare och 15 trygghetscentraler världen över arbetar aktivt och dedikerat med dessa frågor. Vi arbetar för att identifiera och mildra dessa hot genom ett omfattande tillvägagångssätt som inkluderar riskbedömningar, säkerhetsrevisioner och implementering av bästa praxis för IT-säkerhet. Vi är engagerade i att säkerställa säkerheten och integriteten för individer som använder välfärdsteknik, och vi kommer att sträva efter att utveckla effektiva och hållbara lösningar för att ta itu med dessa utmaningar, säger Johan.

Johan Lenander, VD Tunstall AB

Konkreta tips till företag inom välfärdstekniksektorn för att förbättra sin IT-säkerhet:

1. Utveckla och implementera ett informationssäkerhetshanteringssystem (ISMS) baserat på ISO 27001-standarden. Denna ram kan bidra till att säkerställa att säkerhetsrisker identifieras och hanteras och att det sker en kontinuerlig förbättringsprocess.
2. Genomföra regelbundna riskbedömningar för att identifiera sårbarheter och potentiella hot mot välfärdstekniska system och data. Detta kan hjälpa till att informera säkerhetsplanering och resursallokering.
3. Implementera starka åtkomstkontroller, till exempel tvåfaktoraутентisering och rollbaserad åtkomst, för att förhindra obehörig åtkomst till välfärdstekniksystem och data.
4. Se till att programvara och system hålls uppdaterade med de senaste säkerhetskorrigeringarna och försvaren för att minska mot kända sårbarheter.
5. Använd kryptering för att skydda känsliga personliga och hälsorelaterade data både när de lagras och när de överförs.
6. Utveckla och implementera säkerhetspolicys och rutiner för anställda och användare av välfärdsteknik och tillhandahålla regelbunden utbildning i säkerhetsmedvetenhet för att säkerställa att de är medvetna om sitt säkerhetsansvar.
7. Utför regelbundna penetrationstester för att identifiera sårbarheter som kan utnyttjas av angripare.
8. Säkerställ att fysiska säkerhetsåtgärder, såsom övervakningskameror och åtkomstkontroller för fysiska enheter, finns på plats för att förhindra obehörig åtkomst till välfärdstekniska system och enheter.

Genom att implementera dessa och andra praxis för IT-säkerhet kan företag inom välfärdstekniksektorn hjälpa till att skydda sina system och data från potentiella hot och ge sina kunder och intressenter större försäkran om att känslig information och hälsorelaterade data hanteras säkert.