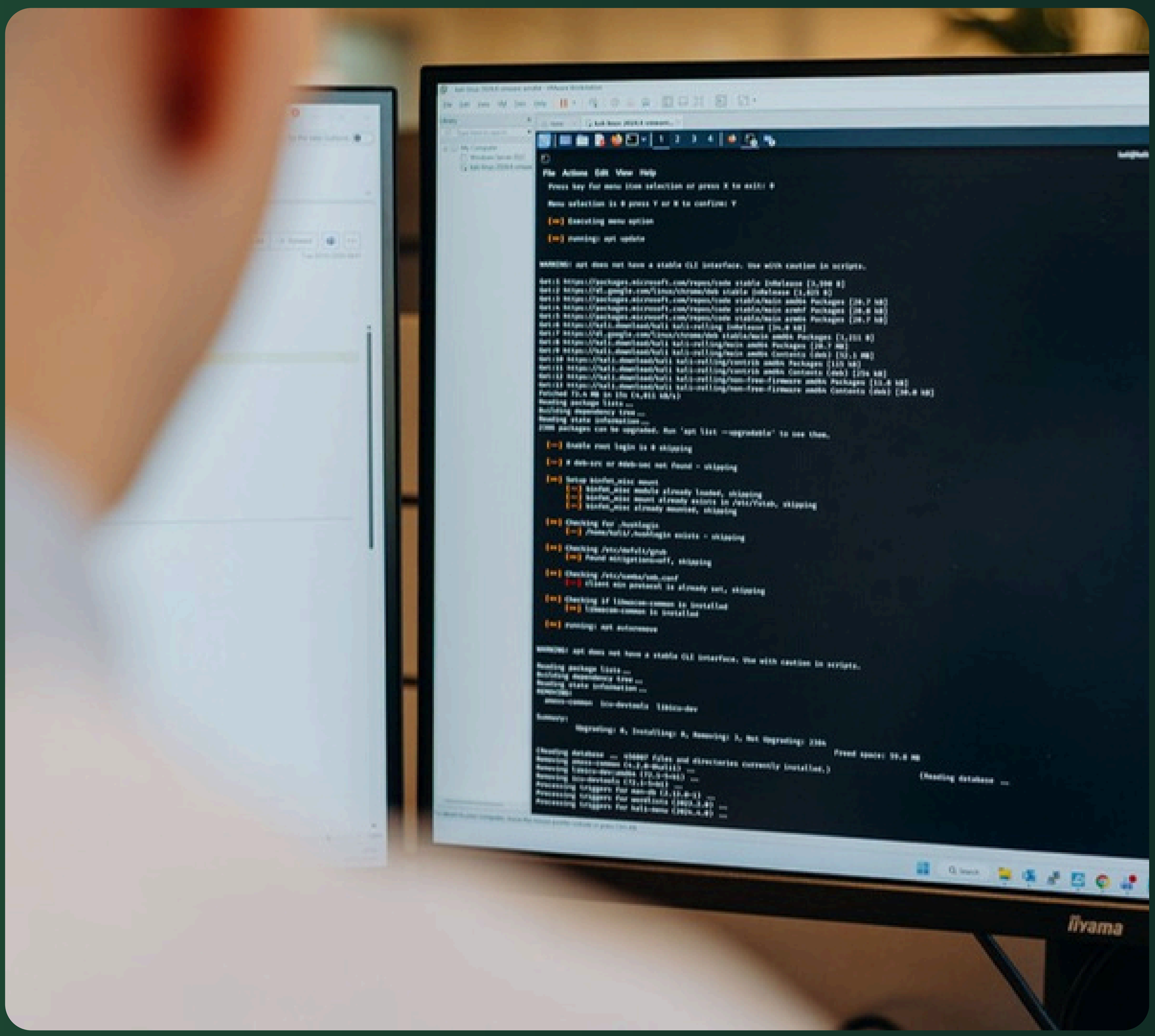
Hoe wij toegang kregen tot medische software



Wat als één gewone login voldoende is om patiëntendossiers in te kijken én medicatie aan te passen? Het klinkt als een slecht filmscenario, maar voor één medisch centrum was het realiteit. In deze case study lees je hoe een ogenschijnlijk kleine IT-keuze kon uitgroeien tot een groot juridisch en menselijk risico, en wat ondernemers en IT managers hieruit kunnen leren.

Een goedbedoelde modernisering

Het verhaal begint onschuldig. Een medisch centrum contacteert Serso voor een algemene IT evaluatie en modernisering. Geen incident, geen hack, gewoon de wens om de IT omgeving toekomstbestendig te maken.
Zoals bij veel zorgorganisaties was hun IT landschap historisch gegroeid. Verschillende softwarepakketten voor patiëntendossiers, medicatiebeheer en administratie, geleverd door meerdere leveranciers. Alles werkte, dus was er weinig reden geweest om fundamentele keuzes in vraag te stellen.
Net daar schuilt vaak het gevaar.

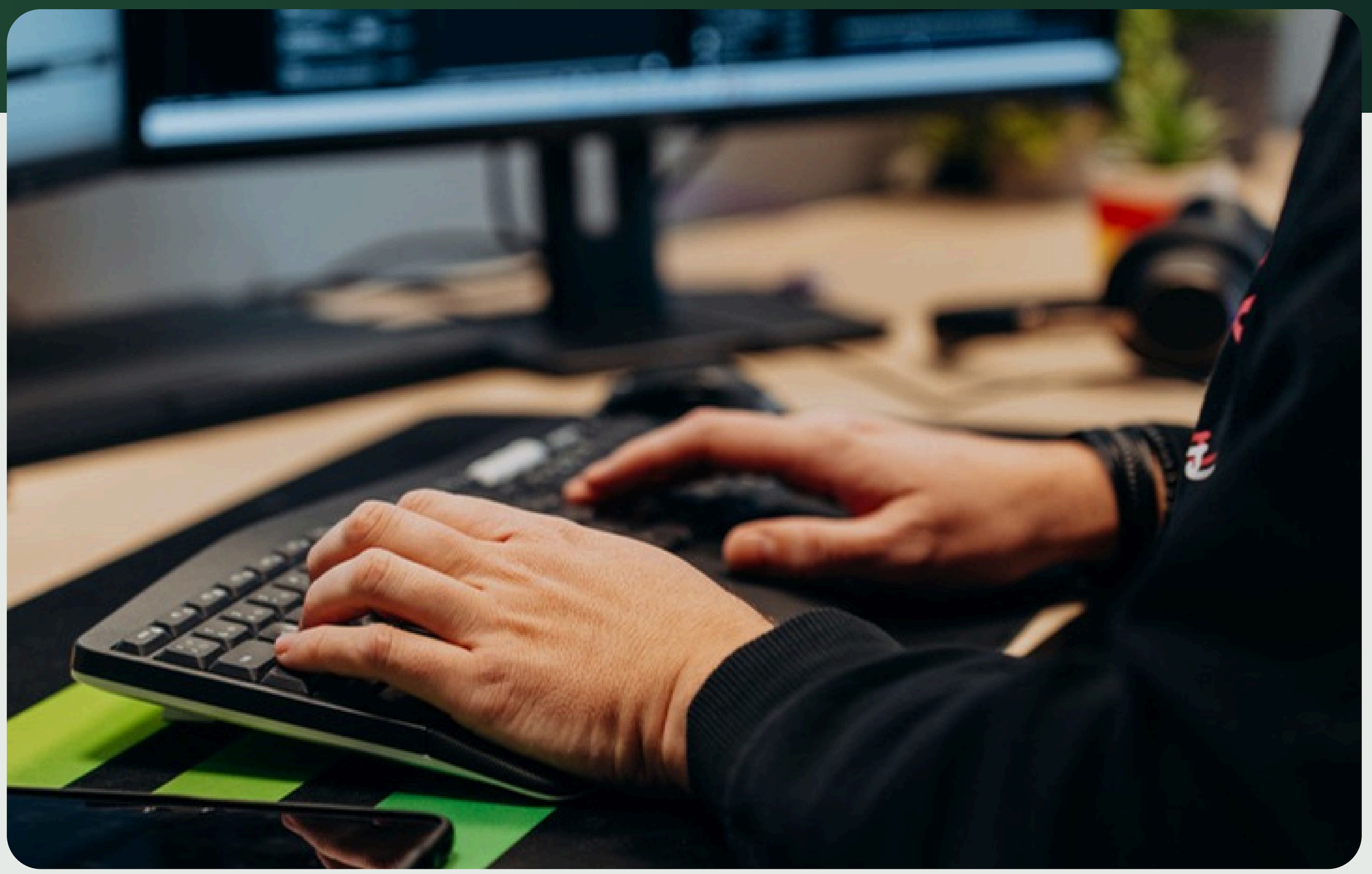
Wat bleek bij nader onderzoek

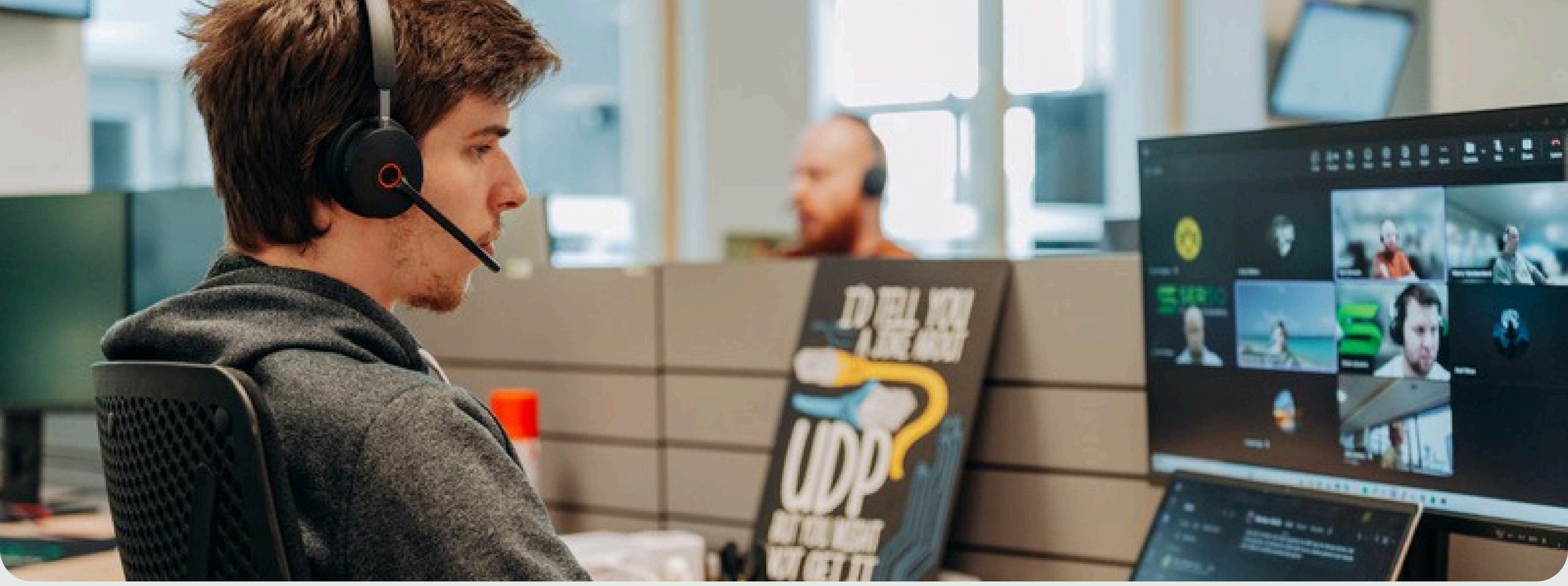
Tijdens de analyse van de toegangsrechten viel iets op. Gebruikers hadden veel meer rechten dan nodig was voor hun dagelijkse taken. Met één standaard gebruikersaccount kon men zowel in patiëntendossiers als in applicaties voor medicatiebeheer.

Even wat duiding. Toegangsrechten bepalen wie wat mag zien of doen in een systeem. Het principe dat Serso hanteert heet least privilege. Dat betekent dat elke gebruiker enkel toegang krijgt tot wat strikt noodzakelijk is voor zijn of haar functie.

In dit geval was dat principe volledig losgelaten. Er was geen duidelijke rolverdeling, geen periodieke controle van rechten en geen logging. Logging is het bijhouden van wie wanneer wat doet in een systeem, cruciaal om afwijkend gedrag te detecteren.

Met andere woorden, als iemand iets fout deed, bewust of onbewust, zou niemand het merken.





Waarom blijft dit zo vaak onder de radar

In zorgomgevingen ligt de focus terecht op continuïteit en gebruiksgemak. Artsen en verpleegkundigen moeten snel kunnen werken, systemen mogen niet in de weg zitten. Toegangen worden daarom vaak ruim toegekend, tijdelijk bedoeld, maar nooit meer herbekeken.
Daarbovenop leeft het idee dat gespecialiseerde medische software standaard veilig is. Men vertrouwt op de leverancier, terwijl beveiliging in de praktijk vaak afhangt van hoe die software geconfigureerd en beheerd wordt.
Zonder duidelijke governance, afspraken en opvolging sluipen risico's er langzaam in.

De mogelijke impact, en die is niet theoretisch

De gevolgen van deze situatie waren potentieel enorm. Ongeoorloofde inzage in patiëntgegevens betekent een zware GDPR inbreuk, met juridische sancties en reputatieschade tot gevolg.
Maar het ging verder dan dat. Toegang tot medicatiegegevens betekent ook de mogelijkheid om doseringen aan te passen. In het slechtste geval kan dat rechtstreeks een risico vormen voor de gezondheid van patiënten.
Dit is het moment waarop IT geen abstract gegeven meer is, maar een directe impact heeft op mensenlevens.

De kijk van Serso als cybersecuritypartner

Voor Serso is toegangsbeheer één van de fundamenten van cybersecurity, zeker in sectoren zoals zorg en welzijn. Begrippen als least privilege, periodieke reviews, logging en monitoring zijn geen luxe, maar basisvoorwaarden.
Monitoring betekent dat systemen continu opgevolgd worden om verdachte activiteiten snel te detecteren. Niet om gebruikers te wantrouwen, wel om fouten of misbruik tijdig te stoppen.
Veiligheid en gebruiksgemak hoeven geen tegenpolen te zijn. Met de juiste inrichting kunnen ze elkaar net versterken. Dat is waar de expertise van Serso het verschil maakt: pragmatisch, onderbouwd en afgestemd op de realiteit van de organisatie.

De belangrijkste les voor ondernemers en IT managers

Als je werkt met gevoelige data, volstaat vertrouwen niet. Niet in software, niet in leveranciers en zelfs niet in goedbedoelende medewerkers.
Zonder structureel toegangsbeheer en opvolging is het geen kwestie van of het misloopt, maar wanneer.

Tot slot

Deze case staat niet op zichzelf. Ze komt vaker voor bij organisaties met een lange IT geschiedenis en meerdere applicaties. De goede boodschap is dat veel risico’s perfect beheersbaar zijn, als je ze tenminste zichtbaar maakt.
Wil je weten hoe jouw organisatie er vandaag voor staat, of welke blinde vlekken er mogelijk zijn in jouw IT omgeving, dan is een onafhankelijke security audit vaak de eerste, nuchtere stap. Soms confronterend, maar altijd verhelderend.

Zou u vandaag met zekerheid kunnen aantonen wie toegang heeft tot welke gevoelige gegevens?
Serso helpt u om uw IT-omgeving kritisch te toetsen en risico’s beheersbaar te maken, zonder uw werking te verstoren.

Neem een kijkje op onze website