

ITSikkerhedsGruppen´s

BIOMETRISK DATA

PAS PÅ DEM

Marts, 2020

Biometriske data - nemt & smart...eller?

Biometriske data som f.eks. fingeraftryk, iris og ansigtstræk anvendes i større og større grad til login. Hvorfor? Fordi det er nemt, hurtigt og det automatiserer login. Vi behøver ikke længere huske -endnu- en indviklet adgangskode. Vi skal bare kigge på skærmen, så er vi logget ind. De fleste af os kender det fra vores laptops eller telefoner, som har én eller anden form for biometrisk adgangsmulighed.

Tidligere var opfattelsen at ens fingeraftryk kunne stå alene, og derfor kunne anvendes som bevis. Men man blev klogere, og fandt ud af, at et fingeraftryk helst ikke skulle stå alene som bevismateriale. Godt nok er sandsynligheden meget lav for at 2 fingeraftryk opfattes ens, men den er der!

Hvad så hvis man kombinerer biometrisk data? F.eks. ved at anvende både ansigtstræk og fingeraftryk. Jo, det øger selvfølgelig sikkerheden for, at der er tale om én bestemt person. Sikkerheden øges og alt synes fint.....eller?

Biometrisk data anvendes i stigende grad som adgangskontrol til tjenester og enheder (f.eks. computere/servere), og anbefales af mange p.g.a. det er nemt. De skal ikke huskes eller udskiftes som en adgangskode. Faktisk kan de ikke udskiftes (det kræver i hvert fald mere end almindelig kendt viden og metoder) Og vi ser da også at flere og flere af "de store spillere" på tech-markedet udvikler deres adgangskontrol til at anvende biometrisk data.

Når det nu er så smart og nemt, og vi ser at udviklingen går den vej, hvorfor er det så, at ITSikkerhedsGruppen løfter "bekymringsflaget"?

Fordi, I skal tænke jer om! Man behøver ikke anvende biometrisk login i den grad som udviklingen tillader!

Kombinationen af vores biometriske data er helt unik. Den gør os til dem vi er. Forestil dig konsekvensen, hvis alle dine biometriske data blev kopieret og anvendt imod dig. Hvad vil du gøre?

"Men det sker jo heller ikke", tænker du måske. Men jo, det gør det desværre. En undersøgelse fra sikkerhedsfirmaet Kaspersky viser, at 37% af de enheder der opbevarer biometrisk data for os (og som beskyttes af deres løsninger), alene i efteråret 2019 har været forsøgt inficeret med malware. Det er voldsomt og meget bekymrende! Hvis det ikke allerede er lykkedes for cyber-kriminelle, så er det kun et spørgsmål om tid, før det lykkes for dem. Og så er h..... løs, og vi vil opleve en uset stigning i identitetstyveri. Så kære kunder (eller kommende kunder): Tænk jer godt om inden I benytter løsninger som gør alting nemmere og hurtigere.

Understøttet af flere større undersøgelser er det vores opfattelse, at mindst 50% af alle virksomheder har været udsat for cyberangreb indenfor det sidste år.

Vi finder det yderst alarmerende, at vores biometriske data i stigende grad anvendes og deles så voldsomt. Tag f.eks. vores børn og deres anvendelse af ansigtsgenkendelse og fingeraftryk, når de anvender Apps. Deres data er gemt *et-eller-andet-sted-verden* og er mere værdifulde for kriminelle og cyberkriminelle end f.eks. et kreditkortnummer.

Alligevel er vi mere opmærksomme på at skjule kreditkortnumre end biometrisk data.

Tankevækkende ik´?

Balancen mellem at have en smidig it-hverdag og samtidig være en smule it-sikkerheds-paranoid er ofte hårfin. Men at gå alt for meget på kompromis, er ikke løsningen. I bund og grund anvender de fleste biometrisk data til *et-eller-andet*, og det er også fint nok.

Men vores bekymring går på, at vi ikke får tænkt os ordentligt om. For på vejen hen mod en smartere hverdag, hvor enhver form for forsinkelse/besværlighed bliver betragtet som en unødvendig forhindring, risikerer man at tænke brugervenlighed fremfor bruger-/kunde-/virksomheds-sikkerhed.

Lidt at tænke over:

- De fleste nyere telefoner har biometrisk adgangskontrol
- De fleste har installeret Apps, der har tilladelse til at anvende telefonens kamera, mikrofon, data, kontaktpersoner o.s.v.
- En nyere undersøgelse viser, at over 2/3 af vores telefoner er inficeret af malware
- De fleste anvender deres telefon på arbejdspladsen
- Kunder, samarbejdspartnere og tilkaldt servicepersonale har også telefoner på sig

Kan du se udfordringen?

Nu skal vi ikke gå hen og blive alt for mistroiske og paranoide. Men at lukke øjnene og håbe på det bedste, er ikke vejen frem.

Bliv taget mere seriøs og vis, at dit firma *gør noget*. Gør noget for at beskytte jeres kunder, jeres medarbejdere og data.

Fortrolige information og persondata skal beskyttes forsvarligt!

