# Jagten på sikkerhedshuller i dagligdagens apps

Når Diego F. Aranha underviser på Aarhus Universitet, lærer han sine studerende at tænke som hackere. Målet er at finde de sikkerhedsbrister i, som virksomhederne selv overser i deres apps.

Henriette Stevnhøj, Aktuel Naturvidenskab.

## DIEGO F. ARANHA

**Diego F. Aranha er lektor ved Institut for Datalogi på Aarhus Universitet, hvor han forsker i at gøre systemer, der anvender kryptografi, sikre og praktisk anvendelige i virkeligheden. Dette inkluderer omfattende sikkerhedsanalyser af eksisterende systemer inden for områder som banker, elektroniske afstemninger og digital identitet.**

**Han leder aktuelt arbejdspakken indenfor cybersikkerhed på Aarhus Universitets interdisciplinære tematiske center DIGIT og fungerer som Principal Investigator for forskningscenteret Concordium Blockchain Research Center Aarhus (COBRA). Han er blevet anerkendt med to Google Latin America Research Awards indenfor privatlivsbeskyttelse samt MIT Technology Reviews Innovators Under 35 Brazil Award for sit arbejde med sikkerhed ved elektronisk stemmeafgivelse.**

Tænk et øjeblik tilbage på, hvordan din dag begyndte.

Det første, du gjorde, var sandsynligvis at række ud efter din mobil. Du scrollede gennem nyhederne, scannede de sociale medier, godkendte måske en overførsel på Mobile Pay, læste på Rejseplanen og tjekkede ind på bussen med Rejsekortet?

For de fleste af os er apps en uundværlig del af hverdagen. Vi bruger apps til at betale med, navigere rundt i trafikken, kommunikere med lægen, tracke løbeture eller høre musik med. Apps sparer tid, forkorter vejen til underholdning og letter tilværelsen.

Men prisen er usikkerhed. Det siger lektor i datalogi ved Aarhus Universitet, Diego F. Aranha.

»Mange apps håndterer følsomme eller personlige data og er afhængige af komplekse tekniske systemer og tredjepartsintegrationer. De kan derfor have fejl eller sårbarheder, som i værste fald kan udnyttes eller føre til datalæk og misbrug,« siger han.

Han ved, hvad han taler om. Han er ekspert i kryptografi og cybersikkerhed med et særligt fokus på at analysere sikkerheden i digitale systemer.

### Et systemisk problem

Siden 2020 har han undervist kandidatstuderende i at dissekere apps for sikkerhedshuller, og han har endnu til gode at afvikle et kursus, hvor de studerende ikke er stødt på apps med sikkerhedsproblemer. Det gælder endda også for apps fra virksomheder, som er blevet analyseret af studerende fra året før.

Selvom fundene er konkrete, handler det for Diego F. Aranha ikke om at udskamme enkelte virksomheder. Problemet er systemisk, forklarer han.

»Mange virksomheder arbejder med komplekse systemer, hvor hastighed, funktionalitet og nye features ofte prioriteres højere end grundig sikkerhed. Samtidig bliver apps hele tiden opdateret og koblet op på nye tjenester, som øger risikoen for, at der opstår nye sårbarheder, som ikke altid bliver opdaget eller rettet i tide.«

### Inspiration fra brasilianske bankapps

Diego F. Aranha har en fortid som forsker i Brasilien, blandt andet ved University of Brasília og University of Campinas, hvor han også har taget sin ph.d.

Idéen til kurset opstod for mere end 10 år siden, da han i Brasilien vejledte et bachelorprojekt, hvor en studerende satte sig for at afprøve sikkerheden i otte bankapps. Resultatet var, at seks ud af syv apps havde alvorlige sikkerhedshuller.

»Som kryptograf ved jeg, at der findes sikkerhedsbrister overalt, men det var stadig alarmerende at se antallet og alvoren af fejlene i bankernes systemer,« fortæller Diego F. Aranha.

Da den bachelorstuderende efterfølgende fortalte bankerne om deres sikkerhedsproblemer, var de overraskende nok ikke særligt interesserede i resultaterne – eller de løsninger, som den studerende præsenterede. I al fald ikke før, den brasilianske presse kom på sagen.

Så kom der skred i tingene, som Diego F. Aranha formulerer det.

»Projektet gav mig idéen til et kursus, hvor de studerende analyserer apps fra deres hverdag for at undersøge, hvor udbredt pro-

Foto: MarjunDanielsen

blemet med sikkerhed egentlig er. Derudover skal de kunne give en løsning på de problematiske fund,« siger Diego F. Aranha.

**De gode hackere**

På kurset får de studerende praksisorienteret viden om at bygge it-systemer op fra bunden med sikkerhed som et centralt element. Så træner de metoder til at angribe og forsvare forskellige typer af computersystemer. Målet er at kunne identificere svagheder i software. Reelt er det etisk hacking, siger Diego F. Aranha.

»Mange forbinder "hacking" med noget negativt, men på dette kursus er vi de gode – vi hacker apps for bedre at beskytte brugernes persondata.«

På kurset skal de studerende selv vælger den app, de skal "hacke".

»Når de studerende vælger deres app efter personlig interesse, lægger det et ekstra lag af relevans på undervisningen.«

Analysen er tilrettelagt sådan, at de studerende undersøger apps, der kører deres egne data på deres egne enheder og lokale netværk, så der ikke sker nogen forstyrrelser af tjenester eller drift. Men virksomheden skal nikke til det, før analysen finder sted, understreger Diego F. Aranha.

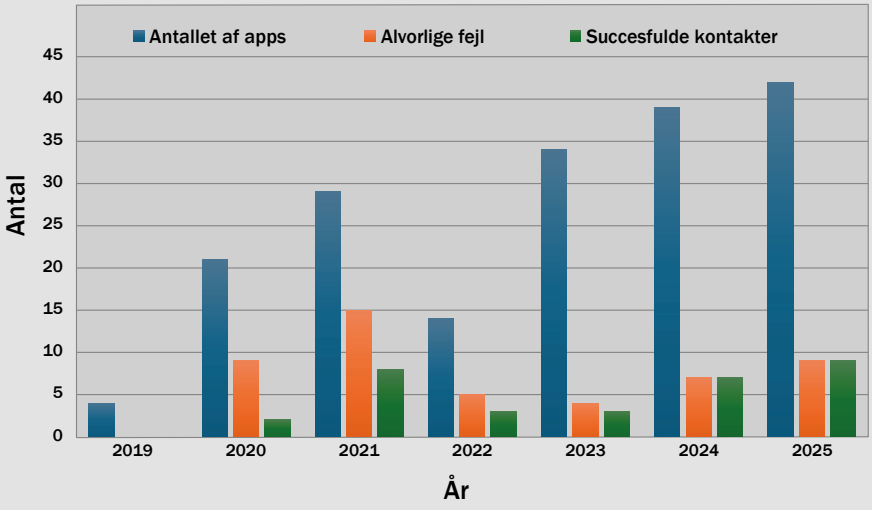
»Det er dansk lovgivning, som kræver forudgående tilladelse til sikkerhedsanalyser. De studerende risikerer reelt at overtræde loven, hvis de tilgår data, som ikke tilhører dem, selv ved et uheld. Her er der en forskel i lovgivningen mellem Danmark og Brasilien, hvor brasiliansk lov kræver "ond tro" for at gøre handlinger strafbare. Dansk lov skelner ikke mellem en etisk sikkerhedsanalyse og ondsindet hacking med profit for øje,« forklarer Diego F. Aranha.

**Blandet modtagelse af resultaterne**

Han kunne godt ønske sig klarere retningslinjer for at minimere risiko for, at de studerende begår lovbrud, når de tester appsene.

»Når vi skal bede om tilladelse på forhånd for at gennemføre sikkerhedsanalyser, bliver etisk sikkerhedsforskning begrænset. Men det er en betingelse, vi tilpasser efter,« siger Diego F. Aranha.

På fem år har mere end 100 studerende været gennem lektorens kursus, og de studerendes analyser spænder vidt; fra apps med minimale fejl til mere problematiske fund i populære forbruger-apps.




## RESULTATER FRA DIEGO F. ARANHAS KURSUS

**Søjlediagrammet viser en oversigt over resultater fra Diego F. Aranhas kursus, der har kørt siden 2020. For de enkelte år ses tre søjler:**

**Den blå søjle viser antallet af apps, der blev analyseret af de studerende det pågældende år.**

**Den orange søjle viser antallet af rapporter, der påviste så alvorlige fejl i de undersøgte apps, at de studerende fandt det relevant at melde tilbage til virksomheden/institutionen bag app'en.**

**Endelig viser den grønne søjle, hvor mange af de indmeldte fejl, der førte til en succesfuld kontakt med firmaet.**

**2022 skiller sig ud med et fald i antallet af undersøgte apps, fordi kurset dette år blev flyttet fra forårs- til efterårssemesteret.**

I ét tilfælde viste en gruppe, at de kunne manipulere sig til et større antal bonuspoint i en butiksapp og omveksle dem til gratis varer. En anden gruppe analyserede en fitness-app og opdagede, hvordan de kunne låse døren til træningscentret op, uden at være til stede på adressen.

Virksomhedernes modtagelse af analyserne og resultaterne fra de studerende har gennem årene været blandet. Nogle virksomheder er meget interesserede og åbne. Andre ignorerer eller afviser, at der er problemer.

Diego F. Aranha er ikke overrasket. »Jeg undrer mig ikke længere, men jeg kan godt blive lidt frustreret over, at det ikke har effekt, selv om en virksomhed gentagne gange får vist de samme sikkerhedsfejl.«

Diego F. Aranha understreger, at ingen har lidt overlast eller fået lækket personlige eller følsomme data. Men eksemplerne illustrerer, at sårbare apps har mærkbare konsekvenser i den virkelige verden.
For Diego F. Aranha ligger den største succes dog ikke nødvendigvis i de huller, der bliver lukket her og nu, men i de eksperter, han sender ud i erhvervslivet:

»Det allermest positive er, at de fleste studerende har fået personligt og kritisk perspektiv på sikkerheden i digitale tjenester, som vi alle sammen bruger. Det er viden, de tager med sig videre i deres professionelle liv og kan omsætte til gavn for alle.« ■