Studerende fandt sikkerhedshuller i Nettos app

Tre datalogistuderende ved Aarhus Universitet afslørede sikkerhedsproblemer i Nettos betalingsapp. Alligevel er de ikke nervøse for at bruge scan-selv-apps.

Henriette Stevnhøj, Aktuel Naturvidenskab.

Rasmus Vestergaard (t.v), Kasper Hebsgaard (midt) og Jonas Ahlers Nielsen studerer datalogi på Aarhus Universitet. Foto: MarjunDanielsen

Det kræver ikke et team af professionelle hackere at finde sikkerhedshuller i en af Danmarks mest brugte dagligvare-apps. Tre studerende fra Institut for Datalogi, Kasper Hebsgaard, Jonas Ahlers Nielsen og Rasmus Vestergaard Knudsen, brugte et kursus på at analysere Netto+-app og fandt fejl, der i princippet kunne lade kunder forlade butikken uden at betale.

»Det var ikke fordi, vi gjorde noget ekstraordinært. Vi har bare brugt den viden, vi fik på kurset,« fortæller Rasmus.

Sammen med sine medstuderende fulgte han kurset System Security på Institut for Datalogi, som handler om at analysere sikkerheden i digitale systemer. Som en del af forløbet vælger de studerende en app, som de skal undersøge for sikkerhedshuller. For de tre studerende faldt valget på Nettos betalingsapp, som kunder bruger til at scanne varer, se betalingsaviser og betale i Nettos butikker landet over.

»Faktisk sad vi i caféen i Storcenter Nord over for Netto, mens vi arbejdede,« fortæller Kasper.

En digital mellemmand

Netto+-appen er en såkaldt "white label"-løsning. Det er et færdigt produkt, som Salling Group har købt af en it-virksomhed og sat deres eget præg på. Samme system bruges også i Føtex og Bilka.

Det viste sig at være et godt valg, forklarer Jonas: »App'en har for os interessante komplekse funktioner; login, kamera, betaling, personlige data – der var noget af arbejde med.«

Metoden var teknisk set simpel. Gruppen satte en proxy op – en form for digital mellemmand – så al trafik fra telefonen kørte gennem deres computere. Dermed kunne de se præcis, hvad appen spurgte serveren om, og – vigtigere – hvad serveren svarede.

Og her fandt de en brist. Når man betaler i appen, genererer den en QR-kode, som man skal scanne for at komme ud af butikken. Appen spørger konstant serveren: "Har jeg betalt? Har jeg betalt?" indtil der kommer et bekræftende svar.

»Vi kunne bare gå ind og sige til appen: Ja, du har betalt, selvom vi slet ikke havde betalt noget,« forklarer Kasper. »Så troede telefonen, at betalingen var gennemført, og den genererede en QR-kode til udgangen. Vi havde 50 sekunder til at gå ud af butikken, og det så helt normalt ud for eventuelle medarbejdere.«

Selfies og rådne tomater

Lige så nemt kunne de omgå appens tilfældige kontrol, hvor kunder skal vise kurven frem for en medarbejder. Den besked kunne de blokere, før den nåede frem til telefonen.

»Det er jo tyveri, så vi gennemførte ikke handlingen,« pointerer Rasmus. »Men pointen er, at vi kunne få appen til at se ud, som om vi havde betalt, uden at vi havde.« De studerende havde også et mere spektakulært fund. Inde i app'en henter Netto billeder til tilbudsaviser og reklamer fra et såkaldt Content Delivery Network, som er en server, hvor billederne ligger klar til download.

De studerende fandt linket til serveren i app'ens kode. Da de kopierede linket ind i en almindelig browser og manipulerede med URL'en, kunne de pludselig browse rundt i hele filstrukturen, og her faldt de over noget, som de studsede over.

»Der lå over 100.000 billeder, og det undrede os,« fortæller Jonas. »Det viste sig, at kunder kan sende et billede af eksempelvis dårlige avokadoer, de har købt og så få pengene tilbage. Billederne ender på denne server, og ved en fejl lå de offentligt tilgængeligt.«

Blandt billederne var selfies og fotos af folk i deres hjem.
»Det er jo ikke meningen, at ens personlige fotos skal ligge frit tilgængeligt på nettet, bare fordi man har sendt en klage over rådne tomater til Netto,« siger Rasmus.

Ingen avanceret hacking

De studerende understreger, at det ikke krævede avanceret hacking at finde hullerne. De brugte open source-værktøjer, som enhver kan downloade på fem minutter.

»Det er basale sikkerhedsfejl – konfigurationsfejl på serveren og manglende validering af data, forklarer Kasper.«

De studerende opdagede også, at appen havde svage krav til adgangskoder, og at man kunne oprette profiler med andres e-mailadresser uden verifikation.

Kasper, Jonas og Rasmus håber, at deres fund kan være med til at sætte fokus på, at selv store virksomheder med white label-løsninger kan have huller, som kan misbruges. De er dog ikke selv bekymrede for at bruge betalingsapps – eller andre former for apps. Men de har en håndfuld råd at dele ud af:

»Brug din ret til at få udleveret dine data,« råder Rasmus. »Hvis en virksomhed ikke kan redegøre for, hvad de har liggende, er det et tegn på, at de ikke har tilstrækkeligt styr på det.«

»Og vær kritisk med, hvad du deler,« tilføjer Kasper.
»Hvis du sender et foto i en reklamation, sender du det til en server, og ikke kun til en medarbejder. Hvis en app spørger om unødvendige tilladelser – som adgang til dine kontakter – så overvej, om det giver mening,« slutter Jonas.

Salling Group: Værdifuld indsigt

Salling Group er glad for, at studerende fra Institut for Datalogi går koncernens apps efter i sømmene. Det siger Michael Venø Bækgaard, som er Chief Information Security Officer i Salling Group.

»Det er positivt, at de studerende bruger virkelighedsnære cases i undervisningen, og vi sætter pris på, at de studerende er nysgerrige på vores apps,« siger Michael Venø Bækgaard. Han fremhæver, at de eksterne perspektiver, også fra studerende, kan bidrage med værdifuld indsigt, koncernen ikke nødvendigvis selv ville få øje på.

»Det er absolut en fordel, at eventuelle sårbarheder opdages af studerende frem for af aktører med ondsindede hensigter,« siger Michael Venø Bækgaard.

De konkrete fund fra gruppen med Kasper, Jonas og Rasmus i forbindelse med analysen af Nettos Plus-appen blev udbedret kort efter modtagelsen hos Salling Group. Det oplyser Michael Venø Bækgaard. ■