Identity papers and certificates [Cory Doctorow - CC BY-SA 2.0]

Den digitale Wall of Fame

Baggrund og status for antiphishing mekanismer

I flere hundrede år har håndværksvirksomheder haft signerede næringsbreve, samt certifikater og æresbevisninger fra kendte tredjeparter hængende fremme for at betrygge deres kunder. Virksomheder har også qua deres bygninger og indretning kunnet overbevise besøgende om at den handlende har investeret store resurser i etablering og drift af virksomheden. Så det har været en dårlig forretning for svindlere at opføre og bemande f.eks. en falsk Bilka butik.

Sådan er det – både heldigvis og desværre – ikke på internettet:

- ***"Heldigvis"*** fordi det er lettere og billigere at starte en ny virksomhed, der kan betjene kunder i store dele af verden frem for blot lokalt
- ***"Desværre"*** fordi det også er blevet ekstremt let og billigt at lave ny svindel-virksomheder, herunder at udgive sig for andre "normale" virksomheder

Siden Peter Steiner i World Wide Webs barndom i 1993 fangede dette problem med frasen: *"On the internet, nobydy knows you're a dog"* er der ikke gjort meget for at hjælpe internet brugere med at vurdere udgivere af websites og afsendere af mails.

Den gang var alle de normale registre for personer og virksomheder langt fra klare til at blive anvendt i forbindelse med aktiviteter på internettet. Derfor måtte de ny internetaktører ty til diverse nødløsninger for sikkerhed, som desværre er blevet hængende. Nu hvor mange basale registre er blevet digitale og åbne, virker nødløsningerne i stedet som undskyldning for ikke at gennemføre mere generiske sikkerhedsløsninger baseret på "linked data".

Det er derfor at sikkerheden mod f.eks. phishing på internettet endnu i dag hovedsageligt er baseret på varemærke-loven samt brugernes evne til at vurdere autenticiteten af websites og emails på basis af stavefejl og andre sproglige finurligheder. ***"Den digitale wall of fame"*** vil sikre brugerne validerede relevante oplysninger til deres vurdering.

I de seneste 10 år har Google, Apple, Microsoft og Mozilla sammen med en række "Certificate Authorities" uden held forsøgt at udbrede en lignende løsning, hvor sidstnævnte skulle indhente oplysninger fra virksomhedsregistre, banker m.m. Herefter kunne basale identitetsoplysninger som navn, by og registreringsnummer indsættes i de certifikater, som benyttes til kryptering af forbindelsen mellem to parter for at sikre integritet og konfidentialitet.

Sådan kunne virksomheder med EV certifikat indtil for nylig få vist deres navn i gængse browsere, som Chrome, Safari og Firefox

Men Google, Apple og Mozilla har nu opgivet at komme videre med understøttelsen af disse EV certifikater. Det skyldes en række problemer med hele konceptet og dermed udbredelsen. Under 0,7% af de virksomheder, der har valgt kryptering af deres trafik har valgt at benytte disse særlige EV certifikater.

Mange undersøgelser omkring sikkerheds-advarsler viser at de blot er til irritation, hvis de kommer for ofte. De viser også at advarsler helst skal være meget tydelige, når de dukker op. Derfor er det væsentligt at ny løsninger tager højde for de problemer, der har begrænset udbredelsen af EV certifikater, herunder:

- Meget få store og velkendte virksomheder køber EV certifikater. Disse certifikater understøtter heller ikke koncernstrukturer, hvor selskaber i forskellige lande deler samme domæne. Mindre virksomheder forstår omvendt ikke hvorfor det er vigtigt for dem at identificere sig over for kunder, når de store ikke gør det.
- Anskaffelse af EV certifikater er relativt dyrt og kompliceret for små og mellemstore virksomheder
- CA'ernes forretningsmodel har vist sig at føre til sjusk og svindel med udstedelse af certifikater, så browser-udbydere har måttet udvikle omfattende sikkerhedsmekanismer for at holde styr på dem.
- EV Certifikater kan ikke uden store omkostninger anvendes i kombination med prisbillige DDOS beskyttelses og Web Application Firewall tjenester som f.eks. Cloudflare
- EV Certifikater kan kun verificere firmanavne og sikrer dermed ikke mod at andre kan oprette firmaer med lignende navn, med samme navn i andre jurisdiktioner (phishing), eller opfinde navne, der i sig selv antyder pålidelighed (falsk anprisning).
- En virksomheds brug af EV certifikat har ikke kunnet benyttes til at gøre virksomheden mere søgbar og køb af et EV-certifikat har derfor haft meget lav markedsmæssig værdi for virksomheden selv.

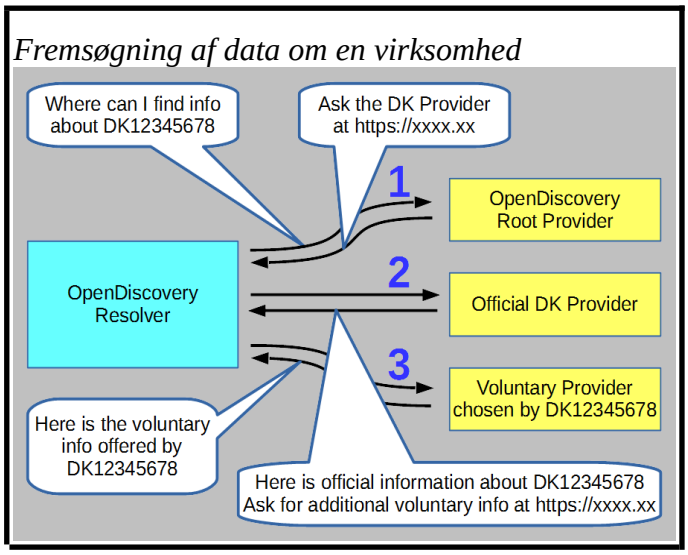
Danmark, Norden og Europa i front med det troværdige internet

Den digitale udvikling er gået forbi de fleste myndigheder og traditionelle virksomheder i USA, mens de ny techgiganter har mere interesse i at konsolidere deres respektive økosystemer og dermed gøre disse mere attraktive og sikre end det åbne internet. Derfor skal vi ikke forvente ny sikkerheds- og tillidsmekanismer fra den kant.

Derimod er vi i Europa og specielt i Norge, Finland og Danmark kommet meget længere med digitalisering af kritiske samfundstjenester og med at tilgængeliggøre offentlige data, der kan hjælpe med at dokumentere identitet, danne basis for tillid og dermed reducere mulighederne for phishing.

Formålet med ***"Den digitale wall of fame"*** er at udnytte alle disse oplysninger til win-win for virksomheden og dens besøgende ved at kunne bruge og præsentere relevante oplysninger på forståelig form til rette bruger på det rigtige tidspunkt. Altså helt svarende til den indledningsvist beskrevne traditionelle "Wall of Fame". Det kan hjælpe både forbrugere og medarbejdere i virksomheder til at spotte forsøg på phishing. Da den umiddelbart lader sig implementere i et PC-browser miljø (sværere på mobil) er virksomhedsbrugere dog den oplagt første målgruppe.

Grafikken nedenfor skitserer hvordan en rekursiv proces ("OpenDiscovery") ud fra det internationale virksomheds-nummer kan finde først det relevante virksomhedsregister (f.eks. CVR i Danmark), hente relevante oplysninger i registret og ud fra web-adressen i virksomhedsregistret finde supplerende information placeret på en af virksomheden valgt lokation. Det vil typisk være tredjepartsoplysninger i form af signerede beviser eller links til bekræftelse af sådanne. Det kan dog også være virksomhedens egne påstande om ejerskab af andre internetdomæner og online resurser.



Den eneste, men grundlæggende forudsætning for at disse oplysninger bliver autoritative og dermed phishingsikre er at:

- Virksomhedsregistret indeholder et domænenavn ("website adresse")
- Websitet indeholder virksomhedsnummeret på en bestemt standardiseret placering

så begge altså peger specifikt på hinanden.

Denne automatiserbare gensidige pegning erstatter fuldt ud den identitetsverifikation, som på kompliceret indirekte vis bliver foretaget manuelt af en Certificate Authority i forbindelse med udstedelsen af EV certifikater. I det simple tilfælde hvor en dansk virksomhed har et enkelt website, skal virksomheden altså blot hhv indtaste webadressen på VIRK (som over 78.000 allerede har gjort) og på websitet indlægge en fil med deres virksomhedsnummer. Ligesom store hosting-udbydere i dag tilbyder kryptering af forbindelser gratis via automatisk genererede PKI certifikater, vil de dog også som standard kunne indlægge den nævnte fil, så website ejeren slipper helt for denne del.

Princippet bag ***"Den digitale Wall of Fame"*** tillader endvidere at tjenesteudbydere, der driver resolveren kan whiteliste alle de mest kendte virksomheder og domæner (f.eks. Top1000). Herved vil man langt hurtigere kunne begynde at vise negative indikatorer for virksomheder/websites, der ikke kan identificeres. Ved benyttelse i virksomheder, vil den enkelte virksomhed herudover også kunne whiteliste sine kunder og samarbejdspartnere.

"Den digitale Wall of Fame" vil fra starten principielt kunne tilbyde gratis identitets verifikation af virksomheder i Norge, Finland, Danmark, Grækenland, Belgien og New Zealand som alle har indført support for webadresse i deres virksomhedsregistre. Andre kan have gjort det (uopdaget af mig) og flere lande formodes at være på vej.

Samtidigt kan løsningen gøres bagud kompatibel med bestående EV certifikater via "Certificate Transparency", som browserleverandørerne har påtvunget alle Certificate Authorities. Via dataopsamling fra transparency logs kan man give virksomheder i alle øvrige lande de samme ekstra fordele, som virksomhederne i de ovennævnte lande, herunder websitets mulighed for brug af eksterne tjenester til DDOS beskyttelse og Web Application Firewall.

Visning af data om en virksomhed (fra PoC)

De data, der som minimum vises til en bruger ved besøg på et websted vil være data fra landets virksomhedsregister, hvilket kan variere fra land til land. I et rent dansk Proof of Concept har vi valgt at medtage bl.a. stiftelsesår, branche og medarbejder-antal, så det f.eks. for Danske Bank vil fremgå: "Stiftet før 1900", "Banker, sparekasser og andelskasser" og "1000+ medarbejdere", altså data som ikke lader sig manipulere af svindlere på samme måde som virksomhedsnavn.

Information herudover kræver generelt at virksomheden selv indlægger relevante verificerbare påstande via et "Business Publisher" modul, hvilket ofte vil være branchespecifikt. F.eks. kan en fødevare-virksomhed ønske at få indsat sin officielle "smileystatus". Almene informationer som medlemskab af e-mærket, Erhvervsstyrelsens kommende mærke for IT-sikkerhed, trustpilot-score, link til Proff, og advarsel om mulig mailsvindel (manglende DMARC reject policy) kan dog automatisk medtages, når de foreligger hos kilden.

Status og næste trin

Der foreligger et basalt fungerende, demonstrerbart Proof of Concept. Vi håber at kunne benytte denne challenge som afsæt til en fuld implementering i samarbejde med brugervirksomheder og hostingudbydere. Det vil omfatte whitelisting facilitet, flere virksomhedsregister integrationer, bagud kompatibilitet til EV certifikater, "Business Publisher", samt arbejde med browserudvidelsen og et tilsvarende visningsplugin til én eller flere mailklienter (som kræver kombination med DMARC). Vi håber at kunne gennemføre dette med funding fra et EU småprojekt-program med dette fokus, i samarbejde med relevante danske virksomheder og eventuelt med relevante fonde.

På sigt kan brugen af Opendiscovery integreres i smarte søgefunktioner, så brugeren ved søgninger på forhånd kan navigere udenom falske og usikre websteder. Det vil herved samtidigt gøre udstilling af identitet og kvalifikationer yderligere attraktivt for virksomheder og facilitere et reelt decentralt forretningsmæssigt alternativ til platforme.

Referencer

Proof of Concept med link til browserudvidelse, OpenSource kode m.m.: https://www.opendiscovery.biz/
Uddybende whitepaper: https://www.bedreid.dk/identity-and-trust-beyond-ev-certificates