Van cyberaanvallen tot identiteits-fraude

ELISA COSTANTE

Hoe maak je van het internet een veilige plek? Cyber-security en privacy specialist Elisa Costante zoekt het uit.

Tekst EDDA HEINSMAN
Foto JAN WILLEM STEENMEIJER

Costantes missie: zoveel mogelijk mensen en organisaties bewust maken van de risico's die ze lopen op internet. 'Ik wil mensen niet bang maken, maar de toenemende digitalisering brengt nu eenmaal risico's met zich mee. Je kunt het zo gek niet bedenken of er zit een geautomatiseerd systeem achter: banken, treinen, verkeerslichten, waterwerken. Je wil er niet aan denken wat er kan gebeuren als iemand kwaad in de zin heeft.'

En het kan goed misgaan. Als voorbeeld geeft Costante het schadelijke computerprogramma STUXNET dat in 2010 ontwikkeld werd door cybercriminelen om het Iraanse nucleaire programma te saboteren. Of meer recent de malware Carbanak waardoor dieven honderden miljoenen dollars bij banken konden ontvreemden.

INTERNETVEILIGHEID
Tijdens haar promotieonderzoek aan de Technische Universiteit Eindhoven bracht Costante in kaart wat er online gebeurt met je persoonlijke data, waar het allemaal terecht komt en waar het allemaal mis kan gaan. 'Het mooie van mijn promotieonderzoek is dat ik privacy binnen een volledige datacyclus heb onderzocht: gebruikers, sites, webservices en data repositories: een soort archief waar gebruikte data worden opgeslagen. Op elk van deze plekken kan het misgaan en ik zocht voor elk van deze partijen een manier om fraude tegen te gaan.'

VEILIGHEIDSLABEL
Costante ontwikkelde een soort veiligheidslabel voor websites. Het label brengt bijvoorbeeld in kaart hoeveel data de site van je bewaart en deelt met andere partijen. Als gebruiker heb je vaak niet door dat wanneer je een site gebruikt, je gegevens automatisch ook terecht komen op andere sites. Costantes tool scant automatisch de *terms and conditions* en *privacy policies* van websites en vertaalt en vat deze samen in een overzichtelijk label voor de site. Daarmee heb je in een oogopslag, zonder je door alle gebruikersvoorwaarden te worstelen, door hoe de site omgaat met je persoonlijke gegevens.

'Ik heb het systeem gebouwd en daarmee aangetoond dat het mogelijk is geautomatiseerd alle gebruiksvoorwaardes van de site en onderliggende sites in kaart te brengen. Maar voor nu is het bij een prototype gebleven. Ik had geen tijd om er ook een downloadbare app van te bouwen. Er is interesse van een Belgisch instituut voor databeveiliging en het onderzoek is openbaar, dus mogelijk komt het label er nog wel.'

DATALEK
Een ander deel van het onderzoek ging over het monitoren van data repositories. Als er heel veel partijen zijn die gebruik maken van de data, hoe ontdek je dan dat iemand ze uit een database haalt voor oneigenlijk gebruik? 'Ik ontwikkelde een tool om zo'n datalek snel op te sporen. Mijn tool brengt eerst in kaart wat normaal gedrag is, om vervolgens abnormaal gedrag direct te herkennen (anomaly detection) en onmiddellijk alarm te slaan. Dergelijke tools bestaan al, maar zijn veelal gebaseerd op regels. Maar het is moeilijk om van te voren alle regels op te stellen, want je weet niet wat er mis kan gaan – er zijn geen regels voor de echte wereld. Bovendien is mijn systeem sneller, en beter omdat het niet alleen maar zegt: er is iets aan de hand vanaf dit IP adres maar direct aangeeft wat er aan de hand is.'

> 'De toenemende digitalisering brengt nu eenmaal risico's met zich mee'

DAGELIJKSE REALITEIT
Al tijdens de laatste fase van haar promotieonderzoek ging Costante aan de slag bij het bedrijf SecurityMatters, spin-off van de TU Eindhoven. Haar werk gaat verder waar haar promotie-onderzoek ophield. Op het moment werkt ze aan vitale infrastructuursystemen als elektriciteitsnetwerken, banksystemen en waterwerken. 'Een van de vragen die ik had was: je observeert wat normaal gedrag is, maar wat als dat normale gedrag verandert? Hoe pas je dan je systeem aan en voorkom je dat je een vals alarm afgeeft? Hier ben ik nu een grote stap in aan het maken bij SecurityMatters.'

Costante heeft nog veel werk te verzetten. Voorzichtig lachend geeft ze toe dat zelfs bij haar thuis alles nog niet optimaal beveiligd is. 'Zelf let ik er goed op, maar mijn vriend niet! Hij laat bijvoorbeeld zijn emailadres op allerlei sites achter.' Heeft ze nog tips? 'Kies een veilig wachtwoord, gebruik niet overal hetzelfde. En gebruik geen gratis wifi! Dat is vaak slecht beveiligd.' ●

COMMIT/project THeCS
Partners: Technische Universiteit Eindhoven, SecurityMatters, Roessingh Research and Development, Roessingh Centrum voor Revalidatie