Onderstaand artikel is voor u doorgestuurd.

Attack navigator vindt en verhelpt zwakke plekken

Auteur: Mariëlle Stoelinga en Wolter Pieters

26 april 2013 **De recente cyberaanval op ING en Ideal maakt het weer eens pijnlijk duidelijk: *security* is en blijft een urgent probleem. Onder leiding van de Universiteit Twente ontwikkelt het Europese Trespass-project een tool die zwakke plekken in de beveiliging opspoort. Kern hierbij is de samenwerking tussen de bèta- en gammawetenschappen: technisch kan een systeem tot in de puntjes beveiligd zijn, als mensen er niet goed mee omgaan, is het nog steeds kwetsbaar voor aanvallen.**

Iedere organisatie beschikt over informatie die beter niet in de buitenwereld terecht kan komen. Of het nu gaat om geheime ingrediënten, beursgevoelige gegevens of klantendatabases, er is altijd wel iets te beschermen. Bovendien is steeds meer kritieke infrastructuur, zoals de elektriciteitsvoorziening en transportnetwerken, gekoppeld aan het internet. Hierdoor kunnen cyberaanvallen ook leiden tot grote problemen in de fysieke wereld, waaronder stroomuitval of, zoals we begin april hebben gezien met de aanval op ING en Ideal, ontregeling van het betalingsverkeer.

Tegelijk zijn de mogelijkheden waarop kwaadwillenden aan vertrouwelijke informatie kunnen komen of diensten kunnen manipuleren eindeloos. Informatie wordt geoutsourcet naar een cloudprovider, door een medewerker mee naar huis genomen of met laptop en al gestolen. Belangrijke systemen zijn vanaf een Ipad te bedienen en soms kunnen zelfs certificaten van websites worden vervalst omdat de provider zijn zaakjes niet op orde heeft. Hoe complexer de informatie-infrastructuur, hoe moeilijker dit te doorgronden is.

Daar komt nog bij dat mensen een belangrijke rol spelen in de beveiliging. Laat je iemand binnen die eruitziet als een loodgieter en die zegt een afspraak te hebben? Geef je je wachtwoord als iemand belt die zegt systeembeheerder te zijn? Iemand die geïnteresseerd is in de gevoelige informatie heeft vele mogelijkheden om binnen te komen.

Penetratietests

Om te kijken voor welke aanvalsscenario's een organisatie kwetsbaar is, kunnen we *penetration tests* laten uitvoeren. Een gespecialiseerd bedrijf probeert dan binnen te dringen. In het simpelste scenario doet het dit op afstand via het internet. Er kan ook fysieke toegang aan te pas komen, en zelfs *social engineering*, het manipuleren van mensen. In het laatste geval moeten we goede procedures hebben om te zorgen dat mensen niet onnodig worden belast.

Bij de UT hebben we dit eerder laten zien in een experiment. Aan een aantal medewerkers hebben we een laptop ter beschikking gesteld om te evalueren. Zij kregen instructies om de computer te allen tijde in hun kantoor te bewaren, niet te gebruiken voor belangrijke data en met een slotje vast te maken. Vervolgens hebben we studenten gevraagd deze laptops terug te stelen. Ze stelden hiervoor scenario's op, en na goedkeuring mochten ze deze uitvoeren.

Uiteindelijk slaagde ongeveer de helft van de pogingen. Studenten deden zich voor als medewerkers van de ICT-helpdesk die een probleem wilden verhelpen, gebruikten daarbij valse e-mails of telefoonnummers als bewijs of vroegen collega's om de deur te openen als de medewerker er niet was. De vele geslaagde pogingen laten zien dat niet iedereen even goed oplet, maar veel pogingen mislukten ook juist doordat iemand wél ingreep. De mens kan dus zowel de zwakste als de sterkste schakel zijn.

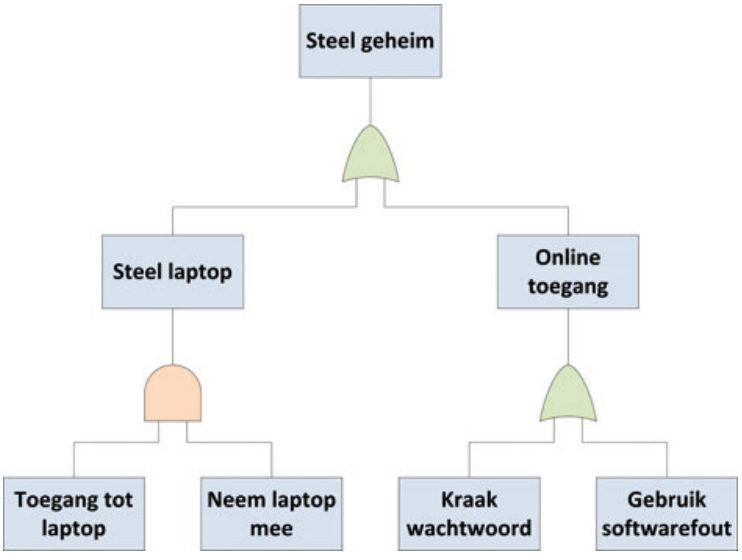
Met penetratietests kunnen we zo bepalen welke aanvalsscenario's in de praktijk slagen, en daarmee in aanmerking komen voor maatregelen. Maar hoe komen we aan de scenario's?

Grote pakkans

Vaak worden *attack trees* gebruikt om aan te geven op welke manieren een aanvaller een specifiek doel kan bereiken (zie Figuur 1). Voor het hoofddoel, het verkrijgen van toegang tot een stuk informatie, moet hij dan subdoelen halen. Zo kan hij bijvoorbeeld een laptop stelen waarop de informatie staat of een wachtwoord achterhalen en op afstand inloggen. Om een laptop te ontvreemden, moet hij de ruimte zien binnen te komen waar de computer staat en die onopgemerkt mee naar buiten krijgen. Zo wordt de boom van mogelijkheden steeds groter. Het blijft echter mensenwerk om de attack trees op te stellen. Daardoor worden vaak mogelijkheden over het hoofd gezien.

In het Visper-project (typo3/www.utwente.nl/ewi/visper) hebben we eerder *attack navigators* ontwikkeld die scenario's automatisch genereren uit een model van de organisatie. Hierbij worden ruimtes, mensen, computers en gegevens gerepresenteerd op een 'kaart' en bepalen regels welke acties er mogelijk zijn. Iemand die in de gang is en de sleutel heeft, kan bijvoorbeeld in de volgende stap toegang krijgen tot de kamer. En om aan de sleutel te komen, kan hij iemand vragen die de sleutel heeft. Op die manier kunnen we doorrekenen op welke manieren een aanvaller van buiten de organisatie (of van binnen uit) bij zijn doel kan komen en automatisch een attack tree opstellen van alle mogelijkheden. Het is wel zaak om een goede kaart van de organisatie te hebben.

In het Europese project Trespass (typo3/www.trespass-project.eu) (Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security) ontwikkelen we deze navigators verder, zodat we ook kwantitatieve eigenschappen kunnen meenemen. Hierbij werken we samen met zestien andere partners uit heel Europa. Het totale budget bedraagt maar liefst 13,5 miljoen euro.



De rode splitsing links in de attack tree geeft aan dat een aanvaller beide acties eronder moet uitvoeren. De groene splitsingen rechts duiden aan dat hij een van de beide acties eronder kan kiezen.

Met de in Trespass ontwikkelde methodes willen we niet alleen kunnen zeggen welke scenario's er mogelijk zijn maar ook welk risico daaraan verbonden is. We kunnen bijvoorbeeld bepalen wat de makkelijkste manier is om bij het geheime recept of de bediening van een sluis te komen. Een scenario dat de aanvaller heel veel moeite kost, of een grote pakkans heeft, zal minder risico met zich meebrengen dan een heel makkelijk uit te voeren scenario. Uiteindelijk kunnen organisaties met de ontwikkelde tools vaststellen waar de zwakke plekken zitten en hoe effectief beveiligingsmaatregelen zijn.

Zwakke plekken

Trespass kiest voor een modelgebaseerde aanpak van *security*. De kaart voor de te ontwikkelen attack navigator bestaat uit een beschrijving (door middel van grafen) van alle *assets* (waardevolle data, kritieke infrastructuur, bedrijfsgeheimen), fysieke objecten (al dan niet beveiligde ruimtes, USB-sticks) en actoren (gebruikers, rollen en mogelijkheden).

Binnen dit sociotechnische securitymodel voegen we kwantitatieve gegevens toe over de schade van een aanval, de kosten voor de aanvaller en de kans van slagen. Bij dit soort gegevens worden vaak vraagtekens geplaatst: hoe komen we aan realistische data? Uiteraard is dat lastig, maar security is inherent een kwantitatief probleem: moeten we investeren in een betere firewall of in training van personeel, zodat dat minder kwetsbaar is voor social engineering? Om dat te beslissen, hebben we kwantitatief inzicht nodig in onder meer de risico's en de profielen van aanvallers.

Door middel van graaftransities in het model beschrijven we de acties van de actoren, en daarmee mogelijke aanvalsscenario's en hun eigenschappen. Het doorrekenen van de routes op de kaart moet op een efficiënte manier gebeuren, omdat de kaarten al snel groot worden en er zeer veel aanvalsmogelijkheden kunnen zijn. Hiervoor zijn speciale technieken beschikbaar, die door slim te rekenen de verwerkingstijd binnen de perken houden.

De uitkomst van de analyse geeft aan waar de zwakke plekken zitten en waar het dus zinvol is om maatregelen toe te voegen. Ook kunnen de modellen bepalen in hoeverre een maatregel de risico's daadwerkelijk beperkt. Als er een ander scenario is dat de maatregel omzeilt, dan zal deze niet heel veel nut hebben. Zetten we bijvoorbeeld een slot op deur A, maar is de kamer ook toegankelijk via deur B, dan wordt het risico niet wezenlijk minder.

De kaarten voor de attack navigators hebben nog een ander voordeel. Vaak is het in kaart brengen van een organisatie al voldoende om de beveiliging te verbeteren. Dan blijken er toch mensen te zijn die hun wachtwoord op een briefje op hun scherm plakken of computers waarop niet automatisch de nieuwste virusscanners worden geïnstalleerd. Zo draagt het Trespass-project op verschillende manieren bij aan een betere cybersecurity.

Mariëlle Stoelinga en Wolter Pieters zijn vanuit de Universiteit Twente respectievelijk de UT en de TU Delft betrokken bij het Trespass-project.

Redactie Nieke Roos