KOGELVRIJ VEST VOOR JE SOFTWARE

Herbert Bos is een wetenschapper met een missie: tegen cybercriminelen. Hij sloeg een nieuwe weg in bij het veiliger maken van softwareprogramma's. Hard nodig. 'Het aantal incidenten neemt de komende vijf jaar toe.'

"Ik liep van Station Zuid naar de VU en dacht na over het probleem van een collega. Opeens zag ik heel duidelijk dat ik het van een heel andere kant kon benaderen." Een totaal nieuwe manier van cybercrime-beveiliging van computerprogramma's was geboren. Een einde aan de toenemende stroom van hacks zoals die bij KPN, LinkedIn, banken en overheden kwam een stukje dichterbij. Hoogleraar Systems and Network Security Herbert Bos, probeert software te beschermen tegen cyberdieven en -inbrekers. Dat dit

> 'Daar heb je weer zo'n zeurpiet', zag je ze denken'

urgent is, begint eindelijk door te dringen. "Als ik vroeger langsging bij politiek en beleidsmakers om te praten over beveiliging van datasystemen, dan waren ze geïrriteerd. 'Daar heb je weer zo'n zeurpiet', zag je ze denken. Geïrriteerd zijn ze nog steeds, maar nu omdat het niet snel genoeg gaat."

WERELDTOP

Na zijn promotie bij de University of Cambridge kwam Bos in 2004 naar de groep Computersystemen van de VU. Hier kon hij zijn ei kwijt. "Met het bouwen van veilige computersystemen zitten we in de wereldtop. In Amerika zijn universiteiten die, in de breedte, beter zijn dan wij, maar wij zitten bij de handvol topuniversiteiten op dit gebied in Europa."
Bos kreeg na zijn ingeving tussen Station Zuid en de VU meteen 1,3 miljoen van de EU om het idee verder te onderzoeken: een prestigieuze ERC Starting Grant. Daarmee zette hij een groot onderzoek naar reverse engineering op. Om softwareprogramma's veiliger te kunnen maken, moet je weten hoe ze werken. Dat staat in de broncode. Uit concurrentieoverwegingen houden de softwareontwikkelaars die broncode geheim. Hij kan ook verloren zijn gegaan. Programma's worden soms wel dertig jaar gebruikt. Dan is de kans dat de producent nog over de broncode beschikt of zelfs dat het bedrijf nog bestaat niet zo groot.

HEILIGE GRAAL

Om programma's te beveiligen tegen dergelijke trucs, moet je de broncode aanpassen. Maar die was dus niet of niet meer bekend. "Dat probleem, daar werken onderzoekers al decennialang aan. Voor ons is dat een soort heilige graal," zegt Bos. "Onderzoekers probeerden de binaire brei van eentjes en nulletjes die een programma produceert, terug te vertalen naar de broncode die het programma stuurt door er patronen in te herkennen."
De truc van Bos is dat hij het over een heel andere boeg gooit. Hij kijkt niet meer naar de eentjes en nulletjes, maar naar de manier waarop het programma gebruik maakt van informatie. Weet je meer over de informatie, dan weet je meer over hoe het programma, dus de broncode, werkt. Bos: "Stel je hebt een werknemersbestand. Dat bestaat uit velden met bijvoorbeeld leeftijd, salaris, adres. Alle velden worden apart benaderd door het programma. Het ene veld ziet er bijvoorbeeld uit als een woord, misschien de naam van de werknemer. In een ander veld staat een getal. Het salaris misschien, waarbij dingen worden opgeteld of afgetrokken. Een woord is een andere soort data dan een getal. Zo kun je semantische informatie uit het programma peuteren." Die moet de onderzoekers stukje bij beetje leiden naar de broncode.
Toch heeft Bos niet de illusie dat je compleet veilige computersystemen kunt creëren, al zou je bij nul beginnen. "Daarvoor zijn de systemen gewoonweg te complex geworden. En bij nul beginnen kan niet eens. Er is nog heel veel oude software in gebruik, in stoplichten, liftsystemen, treininstallaties. Je beveiliging is zo sterk als je zwakste schakel. Daarom willen we oude software veiliger maken. We willen als het ware een kogelvrij vest over die kwetsbare software heentrekken."

GEFOCUST OP VERKOPEN

Je zou denken dat softwareproducenten als Microsoft en Apple hun eigen programma's beveiligen, maar zij zijn meer gefocust op verkopen dan op investeren in dure beveiliging. "Bedrijven gedragen zich veelal ontzettend laks", vindt Bos. "Aan de andere kant is het

> 'De enorme complexiteit van de huidige computersystemen garandeert dat ze onveilig zijn'

ook heel moeilijk om je computersystemen goed te beveiligen. De enorme complexiteit van de huidige computersystemen garandeert dat ze onveilig zijn. Het is simpelweg niet meer te overzien."
Zelf softwareprogramma's aanvallen is soms de meest haalbare manier om de zwakke plekken te ontdekken, vindt Bos. Hij en zijn onderzoeksteam zijn daarom zelf gaan 'hacken'. Zo krijgen zij ook meer inzicht in hoe criminele hackers te werk gaan. Weet je waar de fout zit, dan kun je er iets tegen ondernemen.
Bos heeft iets met hacken. "Die grenzen opzoeken van wat mogelijk is, dat is gewoon erg leuk. Hackers zijn vaak hele slimme en creatieve mensen. Op de middelbare school kraakten wij computerspelletjes om ze te kunnen spelen zonder ze te kopen, schandalig!", lacht hij. Nu leert hij ook zijn studenten hacken. "Ze treden in de voetsporen van superhacker Kevin Mitnick, die als eerste het San Diego Super Computer Center heeft gehackt. We hebben dat systeem nagebouwd en studenten mogen Kevin Mitnick zijn." Hij stimuleert zijn studenten ook om mee te doen aan internationale hackingkampioenschappen, er is een vast team geformeerd.

> 'We gaan een gigántisch tekort aan informatici krijgen'

WAARSCHUWEN

Bos vindt het behalve leuk ook heel belangrijk om mensen goed op te leiden, niet in het minst omdat de samenleving veel behoefte heeft aan mensen met verstand van computerbeveiliging. "Het aantal incidenten gaat de komende vijf jaar niet afnemen, het neemt eerder toe. We gaan een gigántisch tekort aan informatici krijgen."
Bedrijven bellen Bos dan ook voortdurend op zoek naar stagiaires of sollicitanten.
Er is veel belangstelling voor zijn onderwijs. Onder invloed van bijvoorbeeld de activiteiten van Anonymous is het nerd-imago van de studie informatica ook flink veranderd, merkt hij. Zelf koos hij bewust niet voor het bedrijfsleven maar voor de wetenschap. "Ik vind het belangrijk om iets voor de maatschappij te doen. Ik zie het als onze verantwoordelijkheid om te waarschuwen als dingen niet goed beveiligd zijn. Het zijn uiteindelijk burgers die er last van hebben als hun privégegevens op straat komen te liggen, of als hackers vervuild water over een gebied laten lopen, zoals in Australië."
Die maatschappelijke component is belangrijk voor Bos. Zo is hij lid van het Innovatieplatform Veilig Verbonden en medeopsteller van de Nationale Cyber Security Research Agenda. Met de kennis die hij opdoet, kunnen anderen vervolgstappen maken. "Dit doet er toe in de maatschappij. Als je weet hoe een virus een cel binnendringt kan een farmaceut daar een medicijn tegen ontwikkelen. Als wij weten

> 'Ik slaap heel weinig... En ik heb geen tv, dat scheelt heel veel tijd'

hoe een virus software binnendringt, dan kan iemand anders daar weer iets mee."
Zelf houdt Bos zich graag bij de wetenschap, zijn grote hartstocht. "Ik ben gefascineerd door wetenschap. In mijn onderwijs en onderzoek kan ik die fascinatie overbrengen. Goed nadenken past bij me. Ik zit wel vrijwel elke avond te werken, maar niet meer tot vier uur 's nachts, zoals vroeger." Toch vindt hij tijd voor andere dingen, zoals zeilen, tekenen en hardlopen. "Hoe dat kan? Ik slaap heel weinig... En ik heb geen tv, dat scheelt heel veel tijd."

ALS DE DOOD

Behalve een indrukwekkend aantal publicaties in toptijdschriften, leverde Bos ook al een aantal zeer succesvolle promovendi af. "Het is fantastisch hoe ze hun promotietraject hebben doorlopen. Daar draag ik ook aan bij, ja." Als hoogleraar mist hij het 'werk waarbij je je handen vuil maakt' wel een beetje. "Het liefst zit ik samen met een aio aan een interessant probleem te werken. We hebben een aantal ontzettend slimme jongens en meisjes in de groep. Daarmee samenwerken is fantastisch. Ze bedenken soms dingen dat je denkt: dit is geniaal, dat had ik nooit kunnen bedenken. Geweldig. Soms denk ik ook: die kan veel verder komen dan ik, die heeft een enorme potentie. Als hoogleraar besteed je veel tijd aan vergaderen, coördineren en begeleiden. Als je niet oppast voer je zelf nauwelijks nog onderzoek uit. Dat lijkt me verschrikkelijk. Weet je waar ik als de dood voor ben? Dat je met een aio spreekt en niet meer weet waar hij het over heeft. Zo ver is het gelukkig nog niet gekomen!"

Anita Mussche

OP TIJD CRASHEN

Internet is het breekijzer van de cyberinbreker. Computers overnemen kan bijvoorbeeld door ze via internet te overstelpen met grote hoeveelheden informatie en zo een buffer overflow te veroorzaken. Je webbrowser reserveert voor het laden van een webpagina een stukje programmageheugen. Als de browser niet van tevoren controleert of er genoeg plek is voor de binnenkomende informatie, dan kunnen andere delen van het geheugen worden overschreven. Bijvoorbeeld die waarin staat wie er toegang heeft tot bepaalde informatie. Daarmee ligt de computer open voor een overname.
Bos en zijn team ontwikkelden een geheel nieuwe techniek, Body Armor, die ervoor zorgt dat een programma crasht voor het wordt overgenomen. Eerst lokaliseren ze alle buffers in de browser en alle instructies die iets met deze buffers doen. Ze omzeilen daarbij de problematische broncode door te focussen op iets anders: de machinecode. Die bestaat uit hele basale instructies waarmee de processor van een computer wordt aangestuurd. Ook deze code is niet bekend, maar van een paar machine-instructies weet Bos dus precies dat ze dienen om iets in de buffer van de browser te schrijven. De onderzoekers passen die instructies zo aan dat alle pogingen om een buffer overflow te veroorzaken worden opgemerkt en de het programma zichzelf bij gevaar afsluit.