“In de toekomst wordt alles via internet bestuurd”

Ronald Prins (1969) is directeur van cyberbeveiligingsbedrijf Fox-IT. Hij studeerde Technische Wiskunde aan de TU Delft en heeft zich gespecialiseerd in de cryptografie, het versleutelen van informatie. Van 1994 tot 1999 werkte hij bij het Nederlands Forensisch Instituut waar hij voor de recherche vele cryptografische beveiligingen heeft gekraakt. In 1999 richtte hij samen met Menno van der Marel cyberbeveiligingsbedrijf Fox-IT op. Fox-IT heeft bijna tweehonderd werknemers en haalt een jaaromzet van zo’n vijfentwintig miljoen euro.

Veiligheid is meer dan crypto

“Technisch gezien is digitale veiligheid is grotendeels gebaseerd op cryptografie en voor cryptografie is wiskunde absoluut onmisbaar. Maar met cryptografie alleen wordt de digitale wereld niet veiliger. Als gebruikers onveilig omgaan met veilige spullen is goede cryptografie voor niets geweest.

In de politiek wordt nog teveel gedacht dat digitale veiligheid een ingenieursprobleem is en dat technici nieuwe dingen moeten uitvinden. De winst valt echter vooral op het organisatorische vlak te halen. Je moet preventie ook goed inbedden in een organisatie. Detectie en respons helpen daarbij en hiervoor is samenwerking tussen wiskunde en management, tussen IT- en veiligheidsdiensten, hard nodig. Nu gaat circa negentig procent van het geld naar preventie, zoals firewalls, bewustwordingsprogramma’s en versleuteling. Ik verwacht dat in de toekomst ongeveer driekwart van het geld naar detectie en respons zal gaan.

Naast preventie, detectie en respons wordt de wiskundige analyse van Big Data steeds belangrijker. Bij inlichtingendiensten zien we nu al een verandering van het James Bond-tijdperk van iemand fysiek volgen naar een tijdperk van informatieverzameling via het internet. De Amerikaanse NSA is de grootste werkgever van wiskundigen ter wereld. Daar werken zesduizend wiskundigen!

Tenslotte wordt het steeds belangrijker om digitale veiligheid in al zijn aspecten te meten. Ook daarbij kan de wiskunde helpen. Bedrijven willen via een benchmark weten hoe veilig hun systemen zijn. Daarvoor moet veiligheid meetbaar zijn, want dan kan een bedrijf erop sturen en investeringen gericht inzetten.”

Kwetsbaar internet

“Digitale veiligheid is complexer dan veel mensen denken. Een vliegtuig is ook complex, maar voor het overgrote deel is een vliegtuig een afgesloten systeem. Een simpele laptop is dat niet. Die staat via het internet in open verbinding met de rest van de digitale wereld. Daarnaast is er meestal allerlei software op gedownload waarvan we niet precies weten wat het allemaal doet. Verder is een laptop gebaseerd op chips waarin geheime diensten misschien achterdeurtjes hebben ingebouwd waardoor ze toegang kunnen krijgen.

Bij Fox-IT roepen we wel eens een afschrikwekkend beeld op: geef onze hackers een week de tijd en in heel Nederland kan niemand meer pinnen. Gelukkig is zoiets in de praktijk nog niet gebeurd, maar ik weet wel dat Nederland een paar keer goed is weggekomen. We moeten onszelf niet in slaap sussen omdat het nog niet is gebeurd. In de toekomst wordt alles via internet bestuurd: niet alleen auto’s, treinen en vliegtuigen, maar ook sluizen en vitale infrastructuur zoals het elektriciteitsnet. Dat is handig, maar het maakt een samenleving ook kwetsbaar.”

Cyberoorlog

“Op de ouderwetse manier van oorlogvoeren kon je nog wiskundige speltheorie toepassen. Maar het toepassen van speltheorie veronderstelt dat je een oorlog met een model kunt beschrijven. Helaas is bij een cyberoorlog zelden bekend wie de vijand is en wie met hem meevecht. Dit is een nachtmerrie voor politici. Politici denken nog in traditionele domeinen: land, lucht, water en de ruimte boven de aarde. Cyberspace is een vijfde domein. In cyberspace kan iedereen die dat wil meedoen aan een cyberoorlog. Nu nog heeft de traditionele krijgsmacht het voor het zeggen, maar straks zitten mensen met toetsenborden tegenover elkaar.”